Ukraine Ministry of Transport and Communications

State Department of Communications
A.S. Popov Odessa National Academy of Telecommunications

Vorobienko P.P., Veretennikova V.P., Kuznetsova G.P.

Data and Network Security

COURSE
to improve language skills and competence
in professional communication

TEXTBOOK

Odessa 2009

УДК 004.7+004.56.57+621.39(075)

В 7.5

Воробиенко П.П. Data and Network Security : Учебник / Воробиенко П.П., Веретенникова В.П., Кузнецова Г.П. – Одесса: ОНАС им. А.С. Попова, 2009. – 164 с.

ISBN 978-966-7598-35-8

Под редакцией доц., к.т.н. Онацкого А.В.
Рецензенты: к.ф.н., доц. ОНУ им. И.И. Мечникова Кравченко Н.А.,
к.п.н., доц. ПДПУ им. К.Д. Ушинского Мельник И.С.

Курс Data and Networks Security состоит из 8 частей. Учебник построен на современных английских и американских текстах по специальности.

Курс Data and Networks Security может быть использован:

- *студентами, которые изучают курс по специальности «Телекоммуникации», «Информационная безопасность» с целью повышения и развития языковых навыков по специальности;*
- *преподавателями, которые стремятся читать лекции студентам на английском языке;*
- *студентами других специальностей, которые желают улучшить свой языковый коммуникативный уровень с целью дальнейшего использования иностранного языка для усовершенствования профессиональных знаний.*

Учебник содержит много текстов для чтения и дискуссий по специальности с написанными упражнениями для повышения навыков понимания, обмена информацией, говорения и усовершенствования знаний грамматики и профессиональной лексики. Также существует много возможностей для обсуждения интересных вопросов и проблем с целью сделать языковую коммуникацию эффективной. Студенты и те, кто усовершенствуют владение иностранным языком, имеют возможность использовать свои профессиональные знания, чтобы улучшить навыки коммуникации. Этот курс может быть полезен студентам, которые только планируют свою дальнейшую карьеру и тем, кто уже достиг определенных профессиональных успехов.

Гриф предоставлен Министерством транспорта и связи Украины.
Письмо № 6778/23/14-08 от 22.09.2008 р.

ISBN 978-966-7598-35-8

CONTENTS

Unit I. Telecommunications

Text 1. Why Telecommunications is Importaın ……………………………………………..5
Text 2. Trends in Telecommunications…………………………………………………8
Text 3. A Telecommunications Network Model……………………………………12
Text 4. Communications Networks……………………………………………………16
Text 5. Client Server Computing……………………………………………………...23

Unit II. Systems Software

Text 1. The Operating System………………………………………………………...29
Text 2. Three types of User Interfaces………………………………………………...34
Text 3.Managing Tasks……………………………………………………………….39
Text 4. Microcomputer operating systems & operating environments……………….44
Text 5. Windows for DOS (Windows 3.X)……………………………………………48
Text 6. Windows 95 & later…………………………………………………………...50
Text 7. External Utility Programs……………………………………………………..52

Unit III. Managing Information Technology

Text 1. Security and Control Issues in Information Systems………………………….57
Text 2. Information System Controls…………………………………………………60
Text 3. Facility Controls………………………………………………………………67

Unit IV. Information Theory

Text 1. Information Theory…………………………………………………….......73
Text 2. Coding Theory……………………………………………………………......76
Text 3. Applications of Information Theory…………………………………………..79

Unit V. Algebraic algorithms & structures

Text 1. Computer Software in Science and Mathematics……………………………..82
Text 2. Data Structures and Algorithms……………………………………………….85
Text 3. Structure and Decoding of block codes……………………………………….90

Unit VI. Cryptography

Text 1. Cryptography……………………………………………………………........96
Text 2. History of cryptography and cryptanalysis……………………………………99
Text 3. Modern Cryptography………………………………………………………..101
Text 4. Cryptanalysis…………………………………………………………….......109
Text 5. Cryptographic primitives…………………………………………………….113

Unit VII. Network and System Security

Text 1. Security……………………………………………………………………….118
Text 2. How different is network security from computer security?..............................122
Text 3. Data Loss Prevention……………………………………………………......124
Text 4. Security and Performance Management……………………………………..127
Text 5. Network Security and Backup Systems……………………………………...130
Text 6. Three forms of Data Security and Security Problems……………………….134

Unit VIII. Data Security Technologies

Text 1. Network Security Technologies and Protocols:
AAA, VPN and Firewall……………………………………………………138
Text 2. Schemes for Intrusion Detection……………………………………………..143
Text 3. Mixing features………………………………………………………………147
Text 4. Security cameras……………………………………………………………..150
Text 5. Using covert surveillance…………………………………………………….154
Text 6. Scanner Systems……………………………………………………………..158
Text 7. Retinography……………………………………………………………......161

REFERENCE LITERATURE

1. *James A. O'Brien.* Management Information Systems. The MC-Graw-Hill Companies, Inc., 1996.

2. Williams Saywer Hutchinson. Using Information Technology. The Mc Graw-Hill Companies, Inc., 1997.

3. *Глушко М.М., Выгонская Л.Н., Перекальская Т.К.:* учеб. английского языка [для студентов-математиков старших курсов] – М.: Изд. Московского университета, 1992.

4. *English-Ukrainian* Dictionary of Telecommunications. – Львів: СП «БаК», 1996.

5. *IEEE Spectrum*, December, 2000.

6. *Alexander L.G.* Longman English Grammar Practice for Intermediate Students. Longman Group UK Limited, 1990.

7. *Большой* англо-русский словарь. – М.: Русский язык, 1979.

8. *Новый большой* англо-русский словарь. В 3-х т. – М.: Русский язык, 1998.

9. *Oxford English* for Information Technology. Oxford University Press, 1999.

10. *Clark G.C.*, Jr. and Cain, J.B. Error Correction Coding for Digital Communications. Plenum Press, New York, 1981.

11. *LAN* Magazine / Network Magazine. – № 44, March, 1992.

12. *Stephen Kent*. IEEE Spectrum, December, 2000.

Electronic recourses

1. en.wikipedia.org/wiki/

2. iNFUSED BYTES On Line http://www.enlight.ru/ib

3. @MSIT Store:C:\Documents

4. From www.rsasecurity.com

5. http://www.iso

6. http://www.its

7. www.stephenwolfram.com/publications/articles/general/

8. Niklaus Wirth , Algorithms & Data Structures , Prentice-Hall (1986), 288 pp. akps.ssau.ru/forth/pattern/pat4th-h.html

9. Richard Pavelle, Michael Rothstein and John Fitch.Computer Algebra./ en.wikipedia.org/wiki

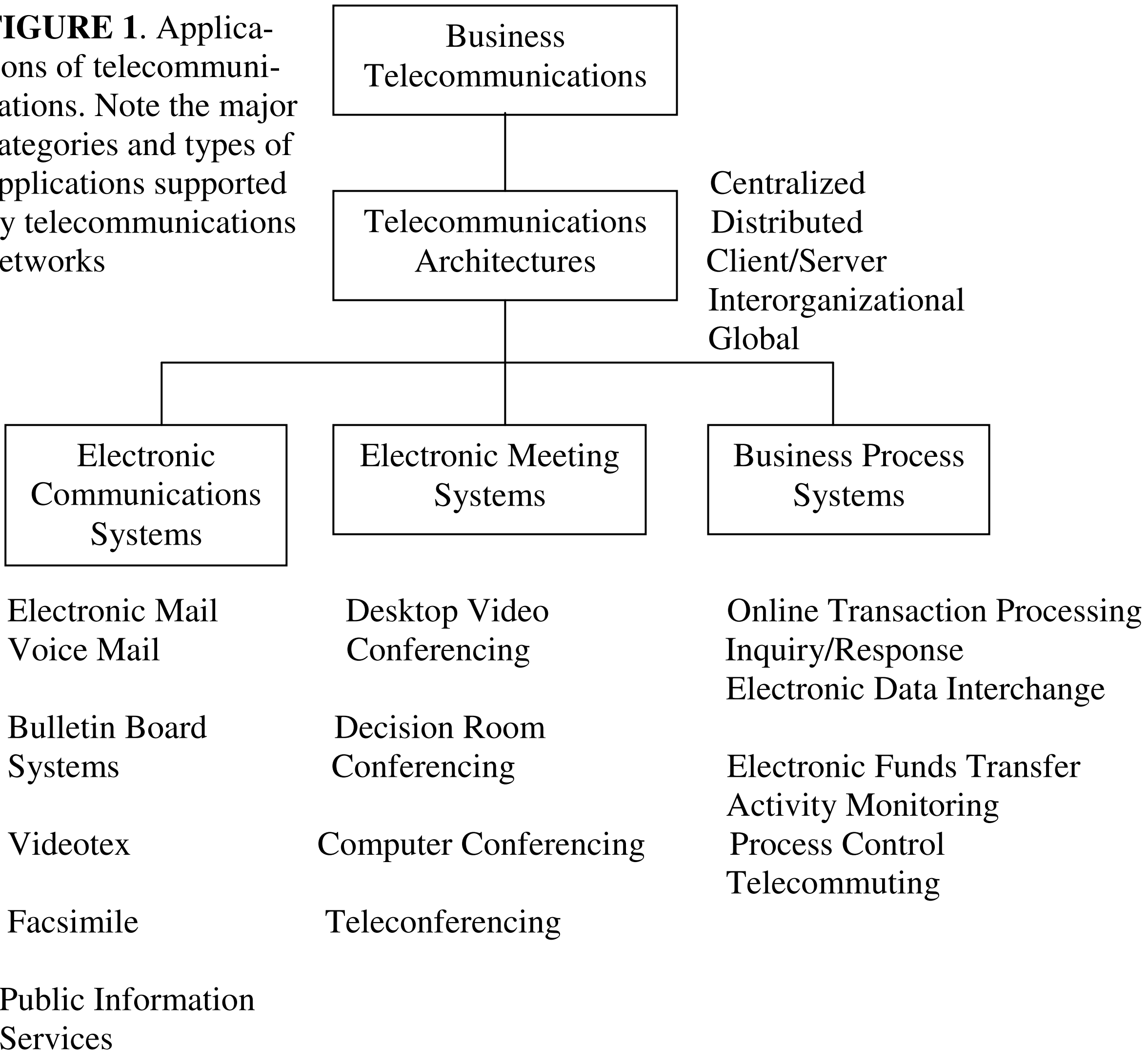
Unit I. TELECOMMUNICATIONS

Text 1. WHY TELECOMMUNICATIONS IS IMPORTANT

Nowadays, many organizations can not survive without interconnected *networks* of computers to service the information processing and communications needs of their end users.

End users need to communicate electronically to succeed in today's global information society. Managers, end users, and their organizations need to electronically exchange data and information with other end users, customers, suppliers, and other organizations. Only through the use of telecommunications they can perform their work activities, manage organizational resources, and compete successfully in to-days fast-changing global economy. As a managerial end user, you will thus be expected to make or participate in decisions regarding a great variety of telecommunications options.

FIGURE 1. Applications of telecommunications. Note the major categories and types of applications supported by telecommunications networks


Business Telecommunications
Telecommunications Architectures
Centralized
Distributed
Client/Server
Interorganizational
Global
Electronic Communications Systems
Electronic Meeting Systems
Business Process Systems
Electronic Mail
Voice Mail
Bulletin Board Systems
Videotex
Facsimile
Public Information Services
Desktop Video Conferencing
Decision Room Conferencing
Computer Conferencing
Teleconferencing
Online Transaction Processing
Inquiry/Response
Electronic Data Interchange
Electronic Funds Transfer
Activity Monitoring
Process Control
Telecommuting

Telecommunications is the sending of information in any form (e.g., voice, data, text, and images) from one place to another using electronic or light-emitting media. *Data communications* is a more specific term that describes the transmitting and receiving of data over communication links between one or more computer systems and a variety of input/output terminals. The terms *teleprocessing, telematics,* and *telephony* may also be used since they reflect the integration of computer-based information processing with telecommunications and telephone technologies. However, all forms of telecommunications now rely heavily on computers and computerized devices. For this reason, the broader term *telecommunications* can be used as a synonym for data communications activities.

Telecommunications networks provide invaluable capabilities to an organization and its end users. For example, some networks enable work groups to communicate electronically and share hardware, software, and data resources. Other networks let a company process sales transactions immediately from many remote locations, exchange business documents electronically with its customers and suppliers, or remotely monitor and control production processes. Telecommunications networks can also interconnect the computer systems of a business so their computing power can be shared by end users throughout an enterprise. And, of course, telecommunications networks enhance collaboration and communication among individuals both inside and outside an organization.

Figure 1 emphasizes the many possible applications of telecommunications. It groups a large number of telecommunications applications into the major categories of electronic communications systems, electronic meeting systems, and business process systems. These applications can be supported by several major types of telecommunications architectures.

(From James A.O'Brien.Management Information Systems)

List of words and expressions

end user – конечный пользователь
to succeed – преуспевать
to survive – выжить
interconnected networks – объединенные сети
light-emitting media – свето-излучаемые средства
teleprocessing – дистанционная обработка данных, телеобработка
telematics – интегрированные средства обработки и передачи информации
to monitor – наблюдать, контролировать
to be shared – совместно используются
enterprise - предприятие
to enhance – повышать

Exercises

Comprehension Check

Exercise 1. Answer the following questions.

1. Why do end users need to communicate electronically? 2. How can they perform their work activities and compete successfully in today's global economy? 3. What could not many organizations survive without? 4. What is telecommunications? 5. What does the term *data communications* describe? 6. What reflects the integration of computer-based information processing with telecommunications and telephone technologies? 7. Do telecommunications networks provide invaluable capabilities to an organization and its end users? Give examples. 8. What do telecommunications networks enhance? 9. What can you say about the many possible applications of telecommunications? 10. What can these applications be supported by?

Exercise 2. Read the text and translate the following equivalents. Use them in your own sentences:

data, light-emitting media, the transmitting and receiving of data over communication links, a variety of input/output terminals, teleprocessing, telematics, telephony, terms, computer-based information processing, integration, to rely heavily on, computerized devices, to provide, invaluable capabilities, data communications activities, to enable work groups to communicate electronically, remote locations, an enterprise, to enhance, business process systems, telecommunications architectures.

Exercise 3. True or False? Read the statements and say whether they are true or false:

1. Managers, end users, and their organizations do need to electronically exchange data and information with other end users, customers, suppliers, and other organizations.

2. Telecommunications is the sending of information in any form (e.g., voice, data, text, and images) from one place to another using electronic or light-emitting medium.

3. The terms *teleprocessing, telematics,* and *telephony* may also be used as the synonym to telecommunications.

4. The broader term *telecommunications* can be used as a synonym for data communications activities.

5. Telecommunications networks provide some minor capabilities to an organization and its end users.

6. All networks enable work groups to communicate electronically and share hardware, software, and data resources.

7. Telecommunications networks can also interconnect the computer systems of a business.

8. Telecommunications networks enhance collaboration and communication among individuals.

9. These computer applications can be supported by several major types of telecommunications architectures.

Language Work

Exercise 1. Read these sentences. Underline the adverbs/adverbial phrases and circle the adjectives

Example: He read the book quickly because it was so interesting.

1. An organization can operate more efficiently and more creatively.
2. A network allows people to make decisions based on the most current information.
3. This leads to higher productivity.
4. We need to study managerial implications of telecommunications.
5. We will use these terms interchangeably.
6. Telecommunications networks are a vital part of today's businesses.
7. All forms of telecommunications now rely heavily on computers and computerized devices.
8. Some networks enable work groups to communicate electronically.

Exercise 2. Put the words in the right order to make questions:

1. perform can their work activities how they?

2. to participate be expected you will in decisions?

3. in any form to another telecommunications the sending is of information from one place?

4. describe what this specific term does?

5. be shared where their computing power by end users can?

Class activity

Exercise 1. Share into groups with your classmates. Discuss these questions.

1. Why can the broader term telecommunications be used as a synonym for data communications activities?

2. What major categories and types of applications are supported by telecommunications networks?

Text 2. TRENDS IN TELECOMMUNICATIONS

Major trends occurring in the field of telecommunications have a significant impact on management decisions in this area. Informed managerial end users should thus be aware of major trends in telecommunications industries, technologies, and applications that significantly increase the decision alternatives confronting their organizations. See Figure 2.

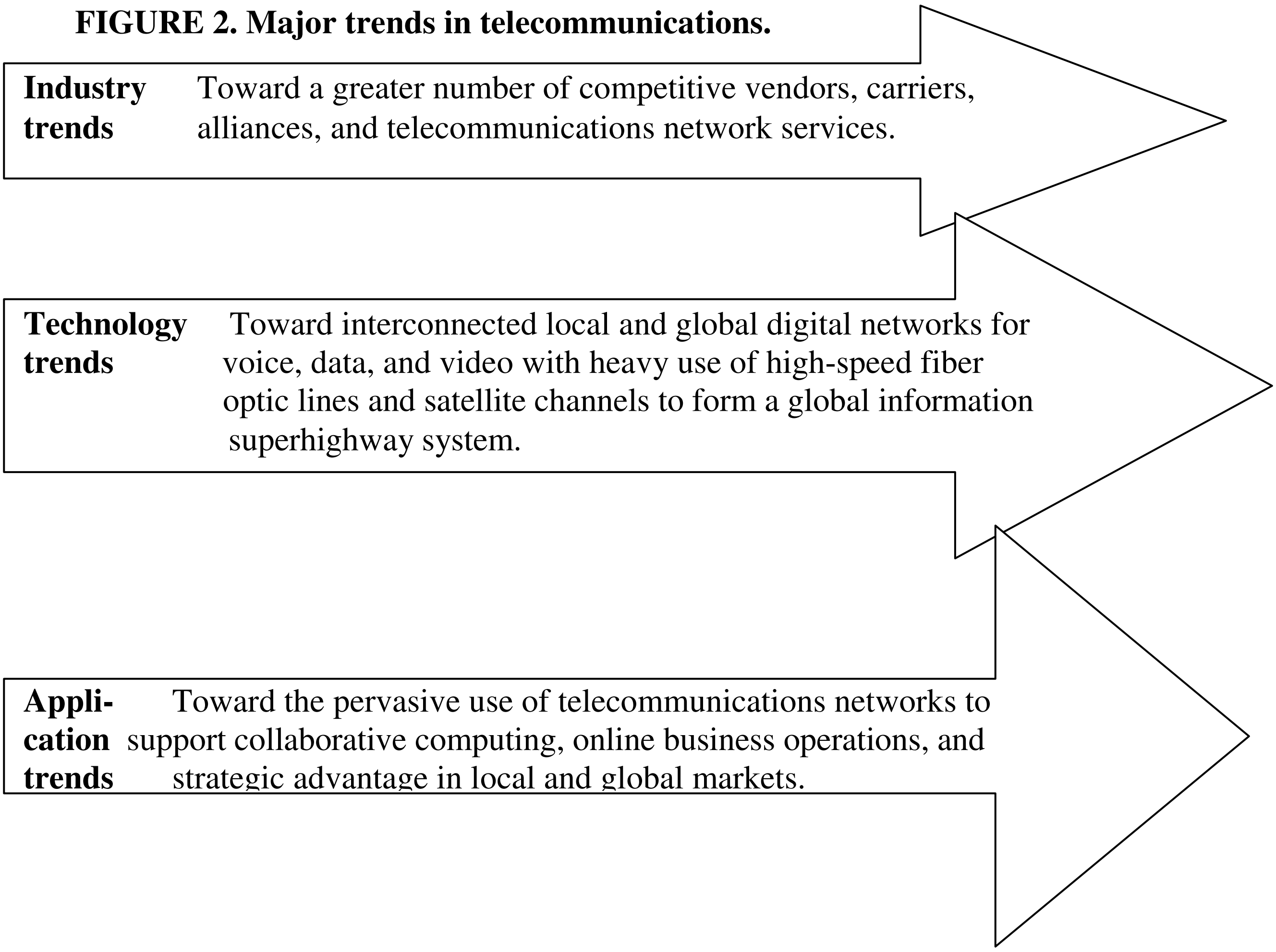
The competitive arena for telecommunications service has changed dramatically from a few government-regulated monopolies to many fiercely competitive suppliers of telecommunications services. With the breakup of AT&T and the Bell System in 1984, local and global telecommunications networks and services became available from a variety of large and small telecommunications companies. Hundreds of companies now offer businesses and end users a choice of everything from long-distance telephone services and access to communications satellite channels, to mobile radio and cellular phone services. Public information network services such as electronic mail, bulletin board systems, and commercial data banks are other examples. Thus, the services and vendor options available to meet company's telecommunications needs have increased significantly.

Digital technology will make the phones we use today seem like two cans joined by a string. Within some years, we will see cellular service that costs almost as little to use as the corner phone booth, handheld communicators that will let us scribble notes with an electronic stylus and zap them wirelessly anywhere on earth, and networks that will automatically deliver our calls to the people we want to reach, wherever they happen to be. Travelers will commune with the office network as fully and easily as if they were sitting at their desks; workers with computers will commingle video, voice, data, and images on a single line as they seamlessly collaborate with faraway colleagues.

Telecommunications is being revolutionized by a change from analog to digital network technologies. Telecommunications has always depended on voice-oriented analog transmission systems designed to transmit the variable electrical frequencies generated by the sound waves of the human voice. However, local and global telecommunications networks are rapidly converting to digital transmission technologies, which transmit information in the form of discrete pulses, as computers do. This provides (1) significantly higher transmission speeds, (2) the movement of larger amounts of information, (3) greater economy, and (4) much lower error rates than analog systems. In addition, digital technologies, including ISDN (Integrated Services Digital Network), will allow telecommunications networks to carry multiple types of communications (data, voice, video) on the same circuits.

Another major trend in telecommunications technology is a change in communications media. Many telecommunications networks are switching from copper wire-based media (such as coaxial cable) and land-based microwave relay systems to fiber optic lines and communications satellite transmissions. Fiber optic transmission, which uses pulses of laser-generated light, offers significant advantages in terms of reduced size and installation effort, vastly greater communication capacity, much faster transmission speeds, and freedom from electrical interference. Satellite transmission offers significant advantages in speed and capacity for organizations that need to transmit massive quantities of data over global networks. These trends in technology give organizations more alternatives in overcoming the limitations of their present telecommunications systems.

FIGURE 2. Major trends in telecommunications.



Industry trends Toward a greater number of competitive vendors, carriers, alliances, and telecommunications network services.

Technology trends Toward interconnected local and global digital networks for voice, data, and video with heavy use of high-speed fiber optic lines and satellite channels to form a global information superhighway system.

Application trends Toward the pervasive use of telecommunications networks to support collaborative computing, online business operations, and strategic advantage in local and global markets.

Another major telecommunications trend is toward easier access by end users to the computing resource of interconnected networks. This trend is based on both industry and technical moves toward building networks based on an *open systems* architecture. Open systems are information systems that use common standards for hardware, software, applications, and networking. Open systems create a computing environment that is open to easy access by end users and their networked computer systems. Open systems provide greater *connectivity,* that is, the ability of networked computers and other devices to easily access and communicate with each other and share information. An open system architecture also provides a high degree of network *interoperability.* That is, open systems enable the many different applications of end users to be accomplished using the different varieties of computer systems, software packages, and databases provided by a variety of interconnected networks. Sometimes, software known as *middleware* may be used to help diverse systems work together. Network architectures like the Open Systems Interconnection (OSI) model of the International Standards Organization promote open, flexible, and efficient standards for the development of open telecommunications networks.

The trend toward more vendors, services, advanced technologies, and open systems dramatically increases the number of feasible applications. Thus, telecommunications is playing a more important role in support of the operations, management, and strategic objectives of both large and small companies. An organization's telecommunications function is no longer relegated to office telephone systems, long-distance calling arrangements, and a limited amount of data communications with corporate mainframes. Instead, it has become an integral part of local and global networks of computers which are used to cut costs, improve the collaboration of work groups, develop online operational processes, share resources, lock in customers and suppliers, and develop new products and services. This makes telecommunications a more complex and important decision area for businesses which must increasingly compete in both domestic and global markets.

(From James A.O'Brien. Management Information Systems)

List of words ad expressions

to be aware of – быть осведомленным о …

breakup – неисправность; разрыв

long-distance telephone service – услуга междугородней телефонной связи

bulletin board system – система электронных объявлений

data bank – банк данных

corner phone booth – телефонная будка (кабина) на углу

to scribble – небрежно писать

to commune ['komju:n] – общаться

to commingle – смешивать, соединять

seamlessly –легко, цельно

information highway – информационная магистраль

pervasive – распространяющийся

sound wave – звуковая волна (20 Гц – 20 кГц)

error rate – частота появления ошибок

transmission medium (pl. media) – среда (канал) передачи (информации)

relay systems – системы передачи (сигнала)

capacity – пропускная способность

open systems architecture – архитектура открытых систем

connectivity – соединяемость

interoperability – совместимость; способность к взаимодействию

middleware – программное обеспечение средней сложности

feasible – выполнимый; возможный

mainframe – главный компьютер; универсальная ЭВМ

to share – совместно использовать

to lock in – блокировать; синхронизировать

Exercises

Comprehension Check

Exercise 1. Read the following equivalents. Translate and memorize them. Use the equivalents in your own sentences:

major trends, a significant impact on, to be aware of major trends in telecommunications industries, applications, the competitive arena for telecommunications service, to change dramatically, with the breakup of, local and global telecommunications networks and services, to become available, to offer a choice, long-distance telephone services, to have an access to communications satellite channels, public information network services, bulletin board systems, commercial data banks, vendor options, to meet company's telecommunications needs, digital technology, cellular service, the corner phone booth, handheld communicators, to scribble notes with an electronic stylus, to zap, to deliver calls, to commune with the office network, to commingle video, voice, data, and images, to depend on voice-oriented analog transmission systems, to transmit the variable electrical frequencies, to convert to digital transmission technologies, discrete pulses, much lower error rates, Integrated Services Digital Network, to carry multiple types of communications, communications media, to switch from copper wire-based media, a coaxial cable, laser-generated light, installation effort, vastly greater communication capacity, much faster transmission speeds, freedom from electrical interference, to give organizations more alternatives in, an open systems architecture; common standards for hardware, software, applications, and networking; to provide greater connectivity, interoperability, to accomplish, middleware, the Open Systems Interconnection, corporate mainframes.

Exercise 2. Discuss the following questions:

1. What can you say about industry trends?
2. Is telecommunications being revolutionized? Why do you think so?

Language work

Exercise 1. Match each group of words to the correct adjective suffix. The suffix must fit all three words in the group. What spelling changes do you have to make when you add the suffix?

1. Manager, commerce, resident	a) –ive
2. Compete, mass, effect	b) –al
3. Avail, vary, rely	c) –ial
4. Electron, strategy, cycle	d) –less
5. Globe, digit, region	e) –ent
6. Differ, depend, insist	f) –ic
7. Cord, wire, error	g) –able

Exercise 2. Work with a partner and think of the opposite of each adjective. Use your dictionary if necessary:

competitive, significant, small, digital, present, efficient, feasible, important, global, major.

Exercise 3. Write out from the text the sentences containing Present Participle and define its functions

Discussion

Exercise 1. Speak about modern trends in telecommunications

Text 3. A TELECOMMUNICATIONS NETWORK MODEL

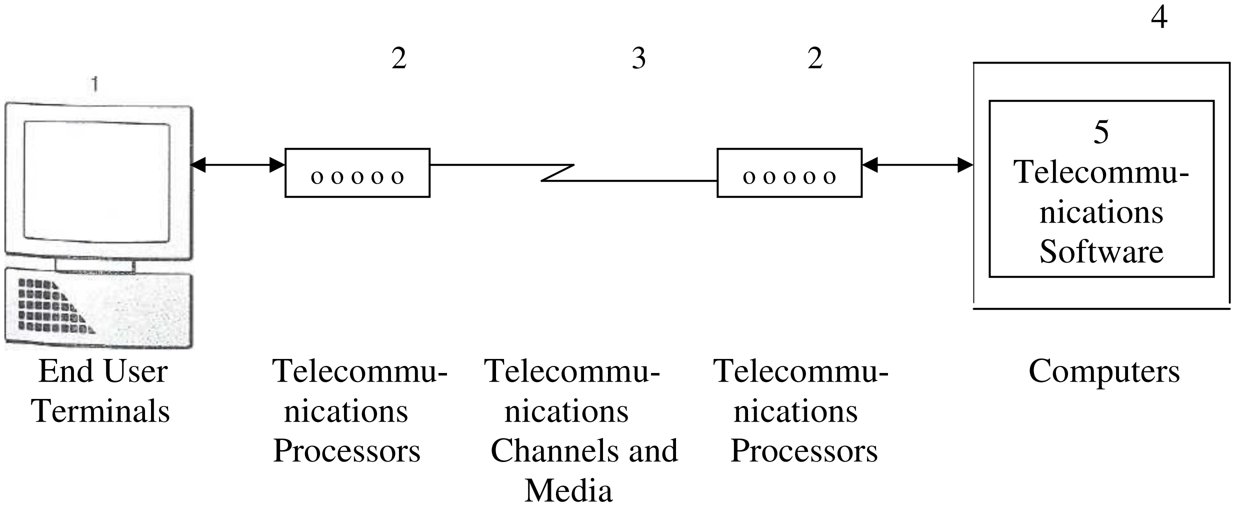
Before we discuss the use and management of telecommunications, we should understand the basic components of a *telecommunications* network. Generally, a *communications network* is any arrangement where a *sender* transmits a message to a *receiver* over a *channel* consisting of some type of *medium.* Figure 3 illustrates a simple conceptual model of a **telecommunications network,** which shows that it consists of five basic categories of components:

– **Terminals,** such as networked microcomputer workstations or video terminals. Of course, any input/output device that uses telecommunications networks to transmit or receive data is a terminal, including telephones, office equipment, and the *transaction terminals*.

– **Telecommunications processors**, which support data transmission and reception between terminals and computers. These devices, such as *modems* and *front-end processors,* perform a variety of control and support functions in a telecommunications network. For example, they convert data from digital to analog and back, code and decode data, and control the accuracy and efficiency of the communications flow between computers and terminals in a telecommunications network.

– **Telecommunications channels and media** over which data are transmitted and received. Telecommunications *channels* use combinations of *media,* such as copper wires, coaxial cables, fiber optic cables, microwave systems, and communications satellites, to interconnect the other components of a telecommunications network.

FIGURE 3. The five basic components in a telecommunications network: (1) terminals, (2) telecommunications processors, (3) telecommunications channels and media, (4) computers and (5) telecommunications software


4
2
3
2
1
ooooo
ooooo
5
Telecommu-nications Software
End User Terminals
Telecommu-nications Processors
Telecommu-nications Channels and Media
Telecommu-nications Processors
Computers

– Computers of all sizes and types are interconnected by telecommunications networks so that they can carry out their information processing assignments. For example, a mainframe computer may serve as a host *computer* for a large network, assisted by a minicomputer serving as *a front-end processor,* while a microcomputer may act as a *network server* for a small network of microcomputer workstations.

– Telecommunications control software consists of programs that control telecommunications activities and manage the functions of telecommunications networks. Examples include *telecommunications monitors* for mainframe host computers, *network operating systems* for microcomputer network servers, and *communications packages* for microcomputers.

No matter how large and complex real-world telecommunications networks may appear to be, these five basic categories of components must be at work to support organization's telecommunications activities. This framework can thus be used to help you understand the various types of telecommunications networks in use today.

There are many different types of telecommunications networks. However, from an end user's point of view, there are two basic types: *wide area* and *local area* networks.

Telecommunications networks covering a large geographic area are called *remote networks, long-distance networks,* or, more popularly, wide area networks (WANs). Networks that cover a large city or metropolitan area *(metropolitan area networks)* can also be included in this category. Such large networks have become a necessity for carrying out the day-to-day activities of many business and government organizations and their end users. Thus, WANs are used by manufacturing firms, banks, retailers, distributors, transportation companies, and government agencies to transmit and receive information among their employees, customers, suppliers, and other organizations across cities, regions, countries, or the world.

Local area networks (LANs) connect computers and other information processing devices within a limited physical area, such as an office, a building, manufacturing plant, or other work site. LANs have become commonplace in many organizations for providing telecommunications network capabilities that link end users in offices, departments, and other work groups.

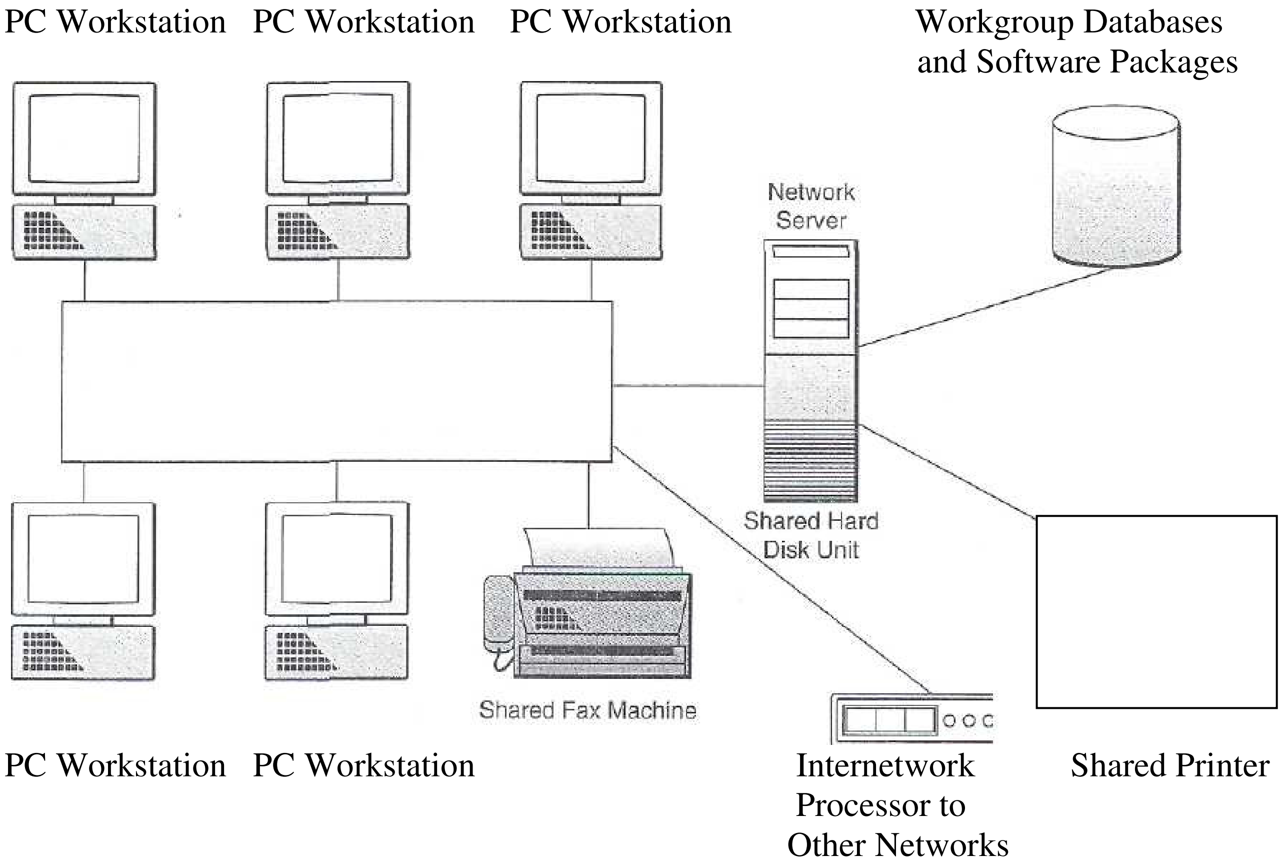
LANs use a variety of telecommunications media, such as ordinary telephone wiring, coaxial cable, or even wireless radio systems to interconnect microcomputer workstations and computer peripherals. To communicate over the network, each PC must have a circuit board installed called a *network interface card.* Most LANs use a powerful microcomputer having a large hard disk capacity, called *a file server* or network server, that contains a network operating system program that controls telecommunications and the use of network resources. For example, it distributes copies of common data files and software packages to the other microcomputers in the network and controls access to laser printers and other network peripherals. *See Figure 4.*

LANs allow end users in a work group to communicate electronically; share hardware, software, and data resources; and pool their efforts when working on group projects. For example, a project team of end users whose microcomputer workstations are interconnected by a LAN can send each other *electronic mail* messages and share the use of laser printers and hard magnetic disk units, copies of electronic spreadsheets or word processing documents, and project databases. LANs have thus become a more popular alternative for end user and work group computing than the use of terminals connected to larger computers.

Most local area networks are eventually connected to other LANs or wide area networks to create internetworks. That's because end users need to communicate with the workstations of colleagues on other LANs, or to access the computing resources and databases at other company locations or at other organizations. This frequently takes the form of *client/server* networks, where end user microcomputer workstations (clients) are connected to LAN servers and interconnected to other LANs and their servers, or to WANs and their mainframe *superservers.* Local area networks rely on internetwork processors, such as *bridges, routers, hubs,* or *gateways,* to make *internetworking* connections to other LANs and wide area networks.

The goal of such internetwork architectures is to create a seamless "network of networks" within each organization and between organizations that have business relationships. Such networks are designed to be open systems, whose connectivity provides easy access and interoperability among its interconnected workstations, computers, computer-based devices, databases, and other networks.

FIGURE 4. A local area network (LAN). Note how this LAN allows users to share hardware, software, and data resources



(From James A.O’Brien.Management Information Systems)

List of words and expressions

communication network – сеть связи
medium – носитель (данных); способ
transaction – обработка запроса, транзакция

hub – концентратор, расширитель, хаб
front-end processor – коммуникационный процессор, интерфейсный процессор, процессор ввода-вывода
host computer – ведущий компьютер, компьютер со множественным доступом; хост компьютер
network operating system – операционная система сети
long-distance network – межрегиональная сеть
wide-area network – сеть связи между удаленными пунктами
metropolitan area network – городская сеть для скоростной передачи данных
file server – файловый процессор (сервер)
software packages – пакеты программного обеспечения
spreadsheet – электронная таблица
router – маршрутизатор (устройство, обеспечивающее маршрутизацию пакетов между интерфейсами по заданным правилам)
gateway – межсетевой интерфейс, шлюз
internetworking – межсетевое взаимодействие

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What is a communications network? 2. How many basic categories and components does a telecommunications network consist of? 3. What is a terminal? 4. What supports data transmission and reception between terminals and computers? 5. What do telecommunications channels use? 6. When can computers of all sizes and types carry out their information processing assignments? 7. What does telecommunications control software consist of? 8. What types of telecommunications networks do you know? 9. What can you say about wide area networks? 10. Where are WANs used? 11. What do local area networks deal with? 12. What do LANs use? 13. Why have LANs become a more popular alternative for end user and work group computing? 14. What purpose are most local area networks connected to other LANs or wide area networks for? 15. Which form does this frequently take? 16. What do local area networks rely on? 17. What is the goal of such internetwork architectures? 18. What do open systems provide?

Exercise 2. Disagree with the following statements. Begin your sentences with:

Sorry, but I can’t agree with you; I don’t think so; it seems to me you are wrong:

1. It isn’t necessary to understand the basic components of a telecommunications network before discussing the use and management of telecommunications. 2. Video terminals perform a variety of control and support functions in a telecommunications network.3. Telecommunications channels use combinations of media, such as copper wires, coaxial cables, fiber optic cables, microwave systems, and communication satellites, to convert data from digital to analog and back. 4. A mainframe computer may not serve as a host computer for a large network. 5. These four basic categories of components must be at work to support organization’s telecommunications activities. 6. Large networks haven’t become a necessity for carrying out the day-to-day activities of many business and government organizations and their end users. 7. Local area networks connect computers and other information processing devices only within a large geographic area. 8. A project

team whose microcomputer workstations are interconnected by a LAN cannot send each other electronic mail messages and share the use of laser printers.

Language Work

Exercise 1. Complete the statements using the words from the box:

trend *the functions* *a message* *computing* *reception* *card*

1. A sender transmits …… to a receiver over a channel.
2. Telecommunications processors support data transmission and …… between terminals and computers.
3. The …… toward open, high-speed, digital networks with fiber optic and satellite links has made the concept of an information superhighway technically possible.
4. Telecommunications control software consists of programs that manage …… of telecommunications networks.
5. To communicate over the network, each PC must have a circuit board installed called a network interface …… .
6. End users need to access the …… resources and databases at other company locations.

Discussion

1. Do you think a simple conceptual model of a telecommunications network is important for its use and management? Why? Why not?

2. Why have LANs become commonplace in many organizations for providing telecommunications network capabilities? Do you think it has been a good reason?

Text 4. Communications Networks

Communications channels and hardware may have different layouts or networks, varying in size from large to small: wide area networks (WANs), metropolitan area networks (MANs), and local networks.

Features of networks are hosts, nodes, downloading, and uploading.

Networks allow users to share peripheral devices, programs, and data; to have better communications; to have more secure information; and to have access to databases.

A network, or communications network, is a system of interconnected computers, telephones, or other communications devices that can communicate with one another and share applications and data. Here let us consider the following:

- Types of networks-wide area, metropolitan area, and local
- Some network features
- Advantages of networks

Types of Networks: Wide Area, Metropolitan Area, & Local

Networks are categorized principally in the following three sizes:

– Wide area networks: A wide area network (WAN) is a communications network that covers a wide geographical area, such as a state or a country. The international pathway Internet links together hundreds of computer WANs. Most telephone systems—long-distance and local—are WANs.

– Metropolitan area network: A metropolitan area network (MAN) is a communications network covering a geographic area the size of a city or suburb. The purpose of a MAN is often to bypass local telephone companies when accessing long-distance services. Cellular phone systems are often MANs.

– Local network: A local network is a privately owned communications network that serves users within a confined geographical area. The range is usually within a mile—perhaps one office, one building, or a group of buildings close together, as a college campus. Local networks are of two types: private branch exchanges (PBXs) and local area networks (LANs), as we discuss shortly.

All of these networks may consist of various combinations of computers, storage devices, and communications devices.

Some Features: Hosts & Nodes, Downloading & Uploading

Many computer networks, particularly large ones, are served by a host computer. A host computer, or simply a host, is the main computer—the central computer that controls the network. On a local area network, some or all of the functions of the host may be performed by a computer called a server. A server is a computer shared by several users in a network.

A node is simply a device that is attached to a network. A node may be a microcomputer, terminal, or some peripheral device (a peripheral device is any piece of hardware that is connected to a computer).

As a network user you can download and upload files. Download means that you retrieve files from another computer and store them in your computer. Upload means that you send files from your computer to another computer.

Local Networks

Local networks may be private branch exchanges (PBXs) or local area networks (LANs).

LANs may be client/server or peer-to-peer and include components such as cabling, network interface cards, an operating system, other shared devices, and bridges and gateways.

The topology, or shape, of a network may take four forms: star, ring, bus and hybrid.

Although large networks are useful, many organizations need to have a local network—an in-house network—to tie together their own equipment. Here let's consider the following aspects of local networks:

- Types of local networks—PBXs and LANs
- Types of LANs—client/server and peer-to-peer
- Components of a LAN
- Topology of LANs—star, ring, bus, hybrid.
- Impact of LANs

Types of Local Networks: PBXs & LANs

The most common types of local networks are PBXs and LANs.

– Private branch exchange (PBX). A private branch exchange (PBX) is a private or leased telephone switching system that connects telephone extensions in-house. It also connects them to the outside phone system.

A public telephone system consists of "public branch exchanges"— thousands of switching stations that direct calls to different "branches" of the network. A private branch exchange is essentially the old-fashioned company switchboard. You call in from the outside, the switchboard operator says "How may I direct your call?" and you are connected to the extension of the person you wish to talk to.

Newer PBXs can handle not only analog telephones but also digital equipment, including computers. However, because older PBXs use existing telephone lines, they may not be able to handle the volume of electronic messages found in some of today's organizations. These companies may be better served by LANs.

– Local area network PBXs may share existing phone lines with the telephone system. Local area networks usually require installation of their own communication channels, whether wired or wireless. Local area networks (LANs) are local networks consisting of a communications link, network operating system, microcomputers or workstations, servers, and other shared hardware. Such shared hardware might include printers, scanners, and storage devices. Unlike larger networks, LANs do not use a host computer.

Many LANs mix elements from client/server and peer-to-peer models.

The word peer denotes one who is equal in standing with another. A peer-to-peer LAN is one in which all microcomputers on the network communicate directly with one another without relying on a server. Peer-to-peer networks are less expensive than client/server networks and work effectively for up to 25 computers. Beyond that they slow down under heavy use. They are thus appropriate for networking in small groups, as for workgroup computing

Components of a LAN

Local area networks are made up of several standard components:

– Connecting or cabling system: LANs do not use the telephone network.

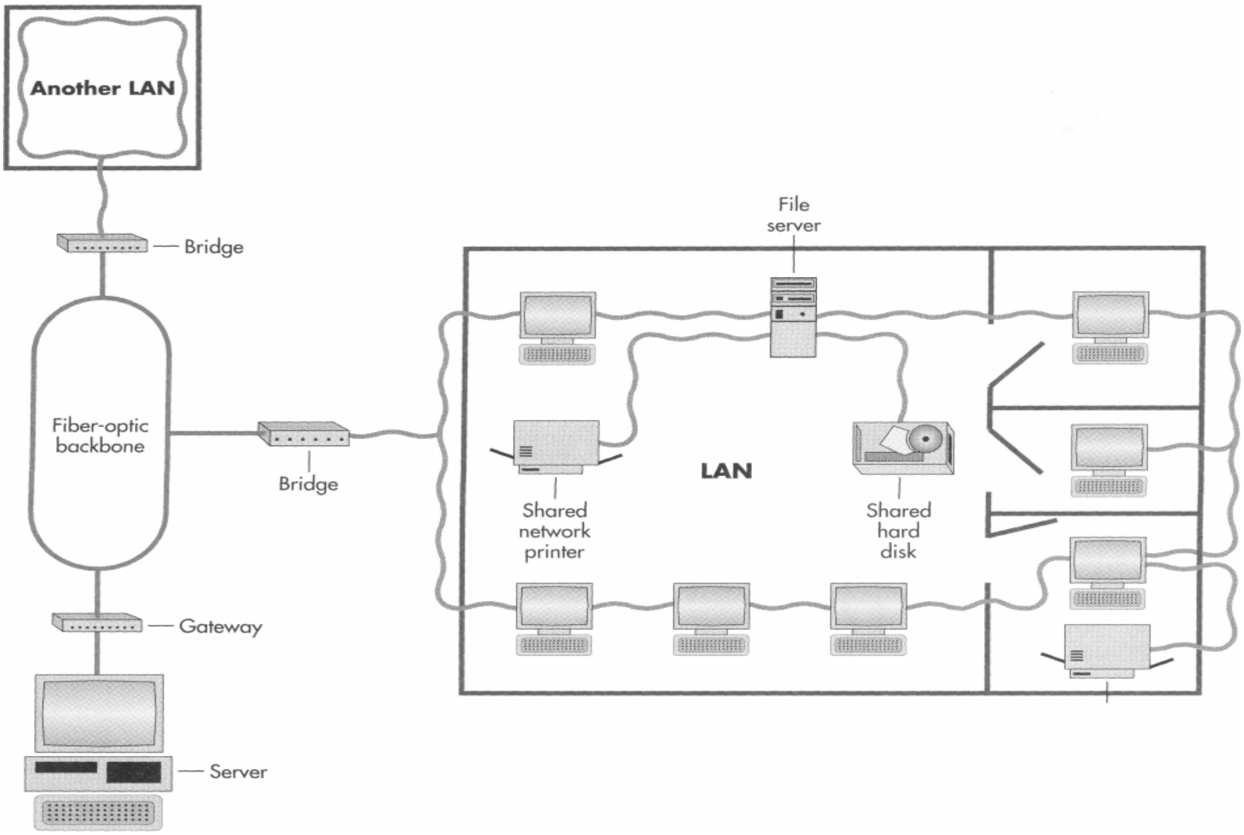
Instead, they use some other cabling or connection system, either wired or wireless. Wired connections may be twisted-pair wiring, coaxial cable, or fiber-optic cable. Wireless connections may be infrared or radio-wave transmission. Wireless networks are especially useful if computers are portable and are moved often. However, they are subject to interference.

– Microcomputers with interface cards: Two or more microcomputers are required, along with network interface cards. A network interface card, which is inserted into an expansion slot in a microcomputer, enables the computer to send and receive messages on the LAN.

– Network operating systems: The network operating system software manages the activity of the network. Depending on the type of network, the operating system software may be stored on the file server or on each microcomputer on the network.

– Other shared devices: Printers, fax machines, scanners, storage devices, and other peripherals may be added to the network as necessary and shared by all users.

– Bridges and Gateways: A LAN may stand alone, but it may also connect to other networks, either similar or different in technology. Hardware and software devices are used as interfaces to make these connections. A bridge is an interface that enables similar networks to communicate. A gateway is an interface that enables dissimilar networks to communicate, such as a LAN with a WAN.



Topology of LANs

Networks can be laid out in different ways. The logical layout, or shape, of a network is called a topology. The five basic topologies are star, ring, bus, hybrid.

A star network is one in which all microcomputers and other communications devices are connected to a central server. Electronic messages are routed through the central hub to their destinations. The central hub monitors the flow of traffic. A PBX system is an example of a star network.

The advantage of a star network is that the hub prevents collisions between messages. Moreover, if a connection is broken between any communications device and the hub, the rest of the devices on the network will continue operating. However, if the hub goes down, the entire network will stop.

A ring network is one in which all microcomputers and other communications devices are connected in a continuous loop. Electronic messages are passed around the ring until they reach the right destination. There is no central server. An example of a ring network is IBM’s Token Ring Network, in which a bit pattern (called a "token") determines which user on the network can send information.

The advantage of a ring network is that messages flow in only one direction. Thus, there is no danger of collisions. The disadvantage is that if a connection is broken, the entire network may stop working.

Three LAN topologies: star, ring, bus

In a star network, all the network's devices are connected to a central server, through which all communications must pass. In a ring network, the network's devices are connected in a closed loop. If one component fails, the whole system may fail. In a bus network, a single channel connects all communications devices:

–Bus network: In a bus network, all communications devices are connected to a common channel. There is no central server. Each communications device transmits electronic messages to other devices. If some of those messages collide, the device waits and tries to retransmit again. An example of a bus network is Xerox's Ethernet.

One advantage of a bus network is that it may be organized as a client/server or peer-to-peer network. The disadvantage is that extra circuitry and software are needed to avoid collisions between data. Also, if a connection is broken, the entire network may stop working.

– Hybrid networks are combinations of star, ring, and bus networks. For example, a small college campus might use a bus network to connect buildings and star and ring networks within certain buildings.

– FDDI network technology. A newer and higher-speed network is the FDDI, short for Fiber Distributed Data Interface. Capable of transmitting 100 megabits per second, an FDDI network uses fiber-optic cable with an adaptation of ring topology. The FDDI network is being used for such high-tech purposes as electronic imaging, high-resolution graphics, and digital video.

The Impact of LANs

Sales of mainframes and minicomputers have been falling for some time. This is largely because companies have discovered that LANs can take their place for many functions, and at considerably less expense. This trend is known as downsizing. Still, a LAN, like a mainframe, requires a skilled support staff. Moreover, LANs have neither the great storage capacity nor the security that mainframes have, which makes them inappropriate for some applications.

(From William Saywer Hutchinson. Using Information Technology)

List of words and expressions

Hardware – аппаратное обеспечение
different layouts – различное расположение
host – сервер, главный компьютер, хост
node – узел (связи)
downloading – загрузка (информации), скачивание
uploading – пересылка, выгрузка
to share applications and data – совместно использовать программные приложения и информацию (данные)
to consider – считать, полагать
pathway – путь, тракт (коммуникационный)
confined – ограниченный
to be attached to – быть соединенным с …
private branch exchange – внутренняя телефонная станция с внешними линиями связи

peer-to-peer communication – связь между одинаковыми по состоянию устройствами

bridge – мост; соединять

gateway –шлюз, межсетевой интерфейс

bus – шина

FDDI (Fiber Distributed Data Interface) – интерфейс для передачи данных по волоконно-оптическим каналам

under heavy use – при интенсивном использовании

the flow of traffic – поток трафика

to prevent collision between messages – предотвращать столкновения конфликтов между сообщениями

high resolution graphics – графика с высокой разрешающей способностью

Exercises

Comprehension Check

Exercise 1. Answer the following questions

1. What may communication channels and hardware have? 2. Speak about features of networks. 3.What do networks allow users to do? 4. What is a network? 5. What types of networks do you know? 5. How does WAN function? 6. What is a purpose of a network? 7. Who do local networks serve? 8. What are computer networks served by? 9. Give a definition of a server. 10. What is a node? 11. What types can local networks be divided into? 12. What topology may LAN take? 13. A private branch exchange is the old-fashioned company switchboard, isn’t it? 14. What does the word “peer” denote? 15. Are peer-to peer networks more expensive than client/server networks? 15. What are standard networks made up of? 16. Speak about LAN topologies. 17. What is the impact of LANs?

Exercise 2. Match the terms in Table A with its definitions in Table B

Table A
1. A network
2. A host
3. Hybrid networks
4. A server
5. A bridge
6. A gateway
7. A node
8. PBX
9. A peer-to-peer LAN
10. Wireless networks

Table B
a) is a private or leased telephone switching system that connects telephone extensions in-house
b) is an interface that enables similar networks to communicate
c) is an interface that enables dissimilar networks to communicate, such as a LAN with a WAN
d) is a computer shared by several users in a network
e) are combinations of star, ring, and bus networks

f) are subject to interference
g) is the central computer that controls the network
h) is one in which all microcomputers on the network communicate directly with one another without relying on a server
i) is a system of interconnected computers, or communications network, telephones, or other communications devices that can communicate with one another and share applications and data
j) is a device that is attached to a network

Exercise 3. Find the corresponding ending for the following statements

1. Download means	**A** client/server or peer-to-peer and include components such as cabling, network interface cards, an operating system, other shared devices, and bridges and gateways.
2. A private branch exchange	**D** is the old-fashioned company switchboard.
3. LANs may be	**C** require installation of their own communication channels, whether wired or wireless.
4. LANs	**D** include printers, scanners, and storage device.
5. Wireless networks	**E** that you send files from your computer to another computer.
6. A network interface card	**F** enables the computer to send and receive messages on the LAN.
7. Shared hardware	**G** are subject to interference.
8. Local area networks	**H** direct calls to different branches of the network.
9. Public branch exchanges	**I** that you retrieve files from another computer and store them in your computer.
10. Upload means	**J** do not use the telephone network. They use some other cabling or connection system

Language work

Exercise 1. Complete the following sentences with the verbs in the corresponding form:

To manage, to monitor, to prevent, to be connected, to be linked to, to transmit, to use:

1. In a bus network each communications device ……… electronic messages to other devices.
2. The hub ……… collisions between messages.
3. The network operating system software ………the activity of the network.
4. In a star network, all the network's devices………… to a central server.
5. In a ring network all microcomputers and other communications devices ……… in a continuous loop.
6. The central hub ……… the flow of traffic.
7. FDDI network ……… fiber-optic cable with an adaptation of ring topology.

The function of an item

We can describe the function of an item differently. Study the following examples.

With the help of the Present Simple.

1. Cache controller *looks* after cache coherency.

Used to-infinitive, Used for+ing form

2. Cache controller is used to look after cache coherency.

3.Cache controller is used for looking after cache coherency.

Emphasizing the function

4.The function of a cache controller is to look after cache coherency.

(From William Saywer Hutchinson. Using Information Technology)

Exercise 2.Describe the functions of these items in two ways

1. A mouse
2. Slot cards
3. CPU
4. Monitor
5. CD-ROM drive
6. Clock
7. PDA
8. Barcodes
9. Scanner
10. ATM

Discuss the following problems

Exercise 1.Share into groups. List the advantages and disadvantages of a network Compare your answers.

Advantages of a network	Disadvantages of a network

Exercise 2. Write the instruction for assembling a LAN

Text 5. CLIENT / SERVER COMPUTING

Client/server computing has become the model for a new *information architecture* that will take enterprisewide computing into the 21st century. Computing power has rapidly become distributed and interconnected throughout many organizations through networks of all types of computers. More and more, networked computer systems are taking the form of client/server networks. In a client/server network, end user microcomputer workstations are the clients. They are interconnected by local area networks and share application processing with LAN servers, which also manage the networks. These local area networks may also be interconnected to other LANs and wide area networks of client workstations and servers. See Figure 5.

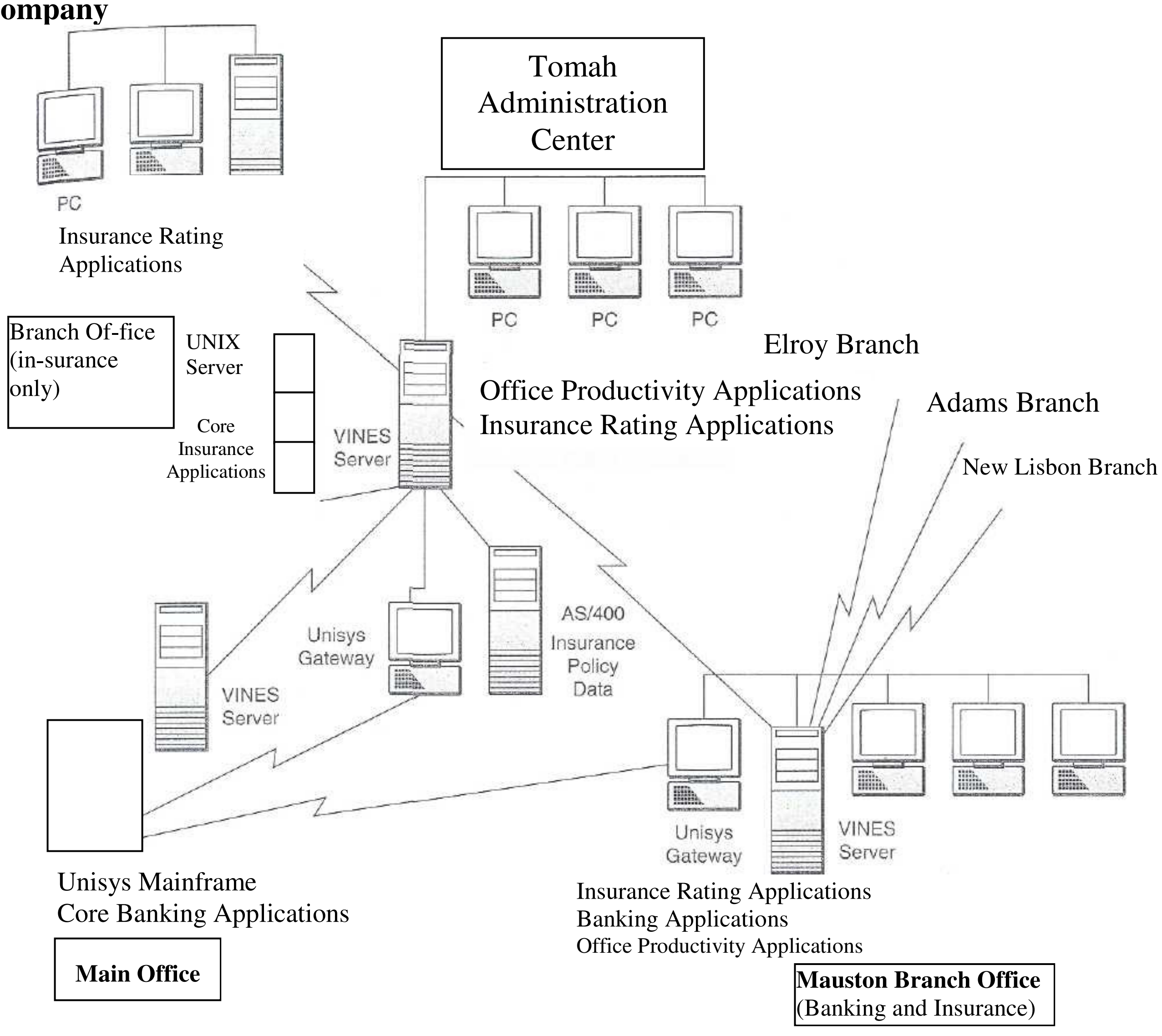
With client/server computing, end users at client LAN workstations can handle a broad range of information processing tasks. They can thus perform some or most of the processing of their business applications. This includes data entry and other user interface activities, inquiry response, transaction processing, updating databases, generating reports, and providing decision support. LAN severs can share application processing, manage work group collaboration, and control common hardware, software, and databases. Thus, data can be completely processed locally, where most input and output (and errors and problems) must be handled anyway, while still providing access to the workstations and servers in other networks. This provides computer processing more tailored to the needs of end users and increases information processing efficiency and effectiveness as users become more responsible for their own applications systems.

Client/server computing also lets large central-site computers handle those jobs they can do best, such as high-volume transaction processing, communications, network security and control, and maintenance and control of large corporate databases. User clients at local sites can access these *superservers* to receive corporatewide management information or transmit summary transaction data reflecting local site activities.

Client/server computing is the latest form of distributed processing. In *distributed processing,* information processing activities in an organization are accomplished by using a network of computers interconnected by telecommunications links instead of relying on one large *centralized* computer facility or on the *decentralized* operation of several independent computers. For example, a distributed processing network may consist of mainframes, minicomputers, and microcomputers, dispersed over *a* wide geographic area and interconnected by wide area networks. Or it may take the form of a client/server network of end user workstations and network servers distributed within user departments in interconnected local area networks.

Client/server computing may also involve cooperative processing. Cooperative processing allows the various types of computers in a distributed processing network to share the processing of parts of an end user's application. Application software packages are available which have common user interfaces and functions so they can operate consistently on networks of micro, mini, and mainframe computer systems. For example, an end user could use a spreadsheet package provided to his or her microcomputer workstations by a local area network server to perform financial analysis on databases managed by a corporate mainframe.

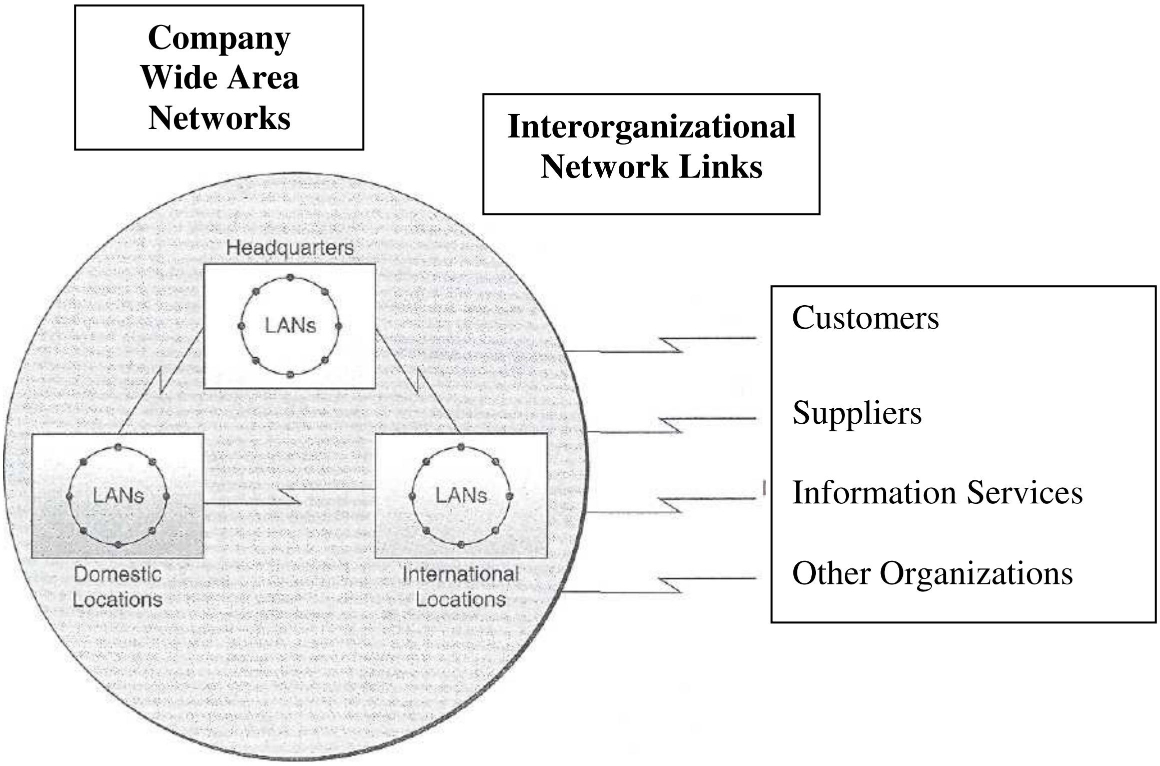
FIGURE 5. A client/server model for distributed and cooperative processing. Note the functions performed by different types of computers acting as clients, servers, and superservers for the Westland Group; a Wisconsin banking and insurance company



Tomah Administration Center
PC
Insurance Rating Applications
PC
PC
PC
Elroy Branch
Branch Of-fice (in-surance only)
UNIX Server
Core Insurance Applications
VINES Server
Office Productivity Applications
Insurance Rating Applications
Adams Branch
New Lisbon Branch
Unisys Gateway
AS/400 Insurance Policy Data
VINES Server
Unisys Gateway
VINES Server
Unisys Mainframe
Core Banking Applications
Main Office
Insurance Rating Applications
Banking Applications
Office Productivity Applications
Mauston Branch Office
(Banking and Insurance)

Many of the applications of telecommunications we have just mentioned can be classified as inter-organizational networks. As Figure 6 illustrates, such networks link company's wide area and local area networks to the networks of its customers, suppliers, information service providers, and other organizations. For example, you can think of a computerized account inquiry system for access by customers as an example of an interorganizational network. So is the use of electronic document interchange, which links the computers of a company with its suppliers and customers. Accessing information services such as Dow-Jones News Retrieval or the data banks of government agencies for information about market and economic conditions is another example. Electronic funds transfer applications also depend on interorganizational networks established among banks, businesses, employees, customers, and suppliers.

FIGURE 6. Interorganizational systems rely on network links between an organization and its customers, suppliers, and other organizations



Thus, the business use of telecommunications has moved beyond the boundaries of work groups and the organization. Now many business firms have extended their telecommunications networks to their customers and suppliers, both domestically and internationally. Such *interorganizational systems* build new strategic business relationships and alliances with those *stakeholders* in an attempt to increase and lock in their business, while locking out competitors. Also, transaction processing costs are frequently reduced, and the quality of service increases. In addition, the availability of external information about industry, market, economic, and political developments provides better information for managerial decision making. Because of these benefits, the trend toward increased connectivity between the networks of an organization and its external stakeholders is expected to continue.

(From James A. O’Brien. Management Information Systems)

List of words and expressions

client/server computing – обработка информации между клиентом и сервером, компьютер клиент-сервер

data entry – ввод данных

inquiry response – ответ на запрос

transaction processing – обработка запроса

to update – обновлять, модернизировать

tailored – приспособленный

summary transaction data – итоговые данные транзакции

cooperative processing – объединенная обработка (информации)

distributed processing network – сеть распределенной обработки

retrieval – поиск, выборка

stakeholder - посредник

Exercises

Comprehension Check

Exercise 1. Put down problem questions to the text.

Exercise 2. Find the English equivalents in the text for the following:

стать моделью для новой информационной архитектуры, вычислительная мощь, сетевые компьютерные системы, конечный пользователь, рабочие станции, совместно использовать прикладные программы, управлять компьютерной сетью, справляться с широким перечнем информационных задач, коммерческие приложения, ввод данных, обновление баз данных, обеспечивать доступ к рабочим станциям и серверам других сетей, выполняться при помощи, иметься в наличии, использовать таблицы, электронный обмен документами, служащие, поставщики, выйти за пределы рабочих групп и организаций, создавать стратегические деловые отношения, улучшать качество услуг, доступность внешней информации, ввиду данных преимуществ, связуемость.

Exercise 3. Speak about client/server technology. Make a short oral summary. Present it to the class.

Language work

Passives

1. Police *have installed* VCRs on many roads.
2. Barcode just *has been converted* into electronic pulses.

In Sentence 1 the verb is active and in 2 it is passive, the Present Perfect Passive. Why? Is there any difference? In the first sentence the agent is responsible for the action (the police). In the 2 the agent is not mentioned? But you can guess that it is a scanner. The Passive is used to describe a situation where the action is more important than the agent.

(From James A. O'Brien. Management Information Systems)

Exercise 1. Choose the correct alternative in each of these sentences:

1. Many of the applications of telecommunications *have just mentioned / have just been mentioned.*
2. The trend toward high-speed, digital networks *has captured / has been captured* the interest of both business and government.
3. Computing power *has become / has been become* distributed and interconnected through networks of all types of computers.
4. These local area networks *have interconnected / have been interconnected* to other LANs and wide area networks lately.
5. Virtual work groups *have already formed / have already been formed* to work on joint projects.

Exercise 2. Look at the first sentence in each pair and highlight the passive verb forms. Then complete the second sentence, which is active:

1. a) A broad range of information processing tasks can be handled by end users at client LAN workstations.

b) End users at client LAN workstations …… a broad range of information processing tasks.

2. a) We were given the information we needed.

b) He …… us the information we needed.

3. a) Most of the processing of their business applications are performed.

b) They …… most of the processing of their business applications.

4. a) Information processing activities in an organization have been accomplished by using a network of computers.

b) We …… information processing activities in an organization by using a network of computers.

5. a) She was proud to have been promoted.

b) She was proud that they had …… her.

6. a) A spreadsheet package is being provided to his or her microcomputer workstations by a local area network server.

b) A local area network server …… a spreadsheet package to his or her microcomputer workstations.

Exercise 3. Rewrite the following sentences into Passive:

1. We use computer systems in a variety of work situations where earlier it was necessary to employ people.
2. Hospitals can increasingly use computers.
3. In airports highly trained experts use computers.
4. Police use speed traps to catch drivers breaking speed limits.
5. Large supermarkets have used computers for decades already.
6. Scanner devices called barcode readers convert barcodes into prices.
7. The till prints the item and the price on the paper receipt.
8. We refer to one character of data as a byte.
9. Asynchronous transmission sends the data one byte or character at a time.
10. In a client/server network, the main server computer provides the services (sharing of printers, programs or data, etc).
11. Terminals require the server to do most or all of the processing.

12. The hub connects all electronic devices.

13. A simple computer comprises a processor and memory, display, keyboard, mouse and a hard disk drive.

14. A backbone, i.e. a network transmission path, handles major data traffic.

15. A special computer, called a router, directs messages when we link several networks.

Discuss the following problems

Exercise 1. What can be done to minimize the disadvantages of LANs using. Divide into groups, discuss and put down your notes. Share your points with your classmates.

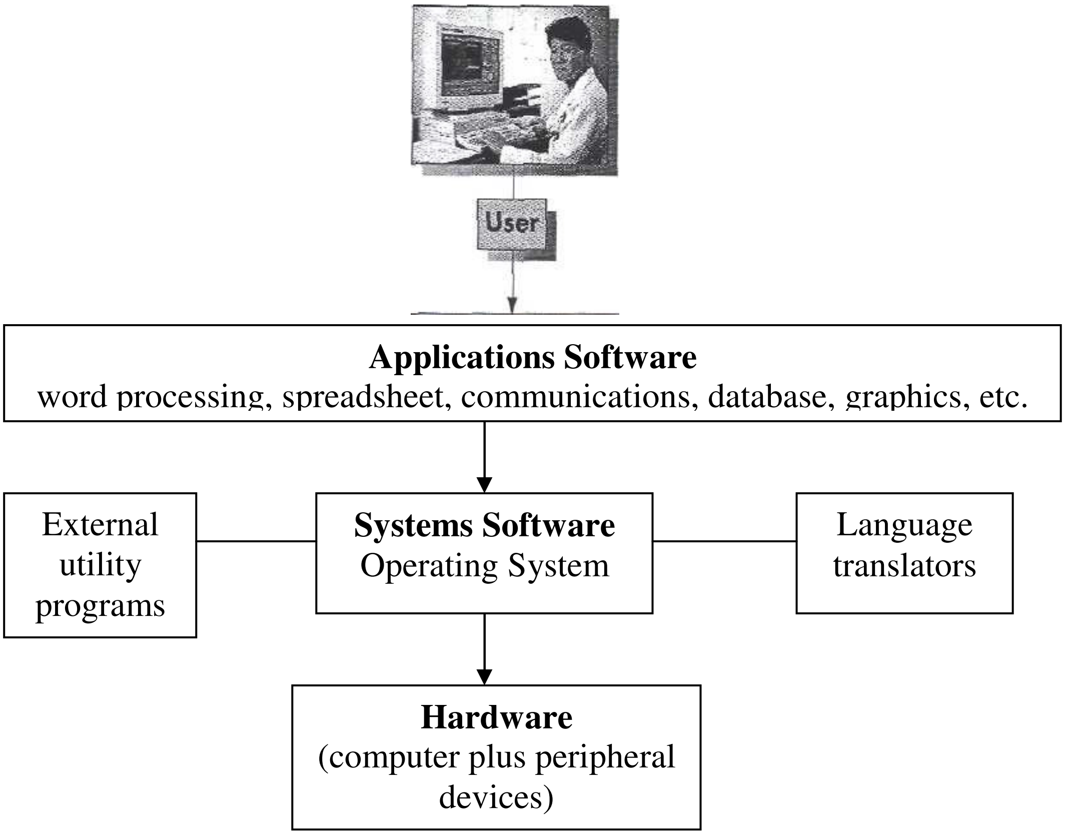
Unit II. SYSTEMS SOFTWARE

Text 1. The Operating System

An operating system is required for applications software to run on your computer. The user usually works with the applications software but can bypass if to work directly with the systems software for certain tasks.

The operating system (OS) consists of the master system of programs that manage the basic operations of the computer**.** These programs provide resource management services of many kinds, handling such matters as the control and use of hardware resources, including disk space, memory, Central Processor Unit (CPU) time allocation, and peripheral devices. The operating system allows you to concentrate on your own tasks or applications rather than on the complexities of managing the computer.

FIGURE 7. The three types of systems software


User
Applications Software
word processing, spreadsheet, communications, database, graphics, etc.
External utility programs
Systems Software
Operating System
Language translators
Hardware
(computer plus peripheral devices)

Different sizes and makes of computers have their own operating systems. For example, Cray supercomputers use UNICOS and COS, IBM mainframes use MVS and VM, Data General minicomputers use AOS and DG, and DEC minicomputers use VAX/VMS. Pen-based computers have their own operating systems—PenRight, PenPoint, Pen DOS, and Windows for Pen Computing—that enable users to write scribbles and notes on the screen. *These operating systems are not compatible with one another.* That is, in general, an operating system written for one kind of hardware will not be able to run on another kind of machine.

Microcomputer users may readily experience the aggravation of such incompatibility when they buy a new microcomputer. Should they get an Apple Macintosh with Macintosh

Systems Software, which won't run IBM-compatible programs? Or should they get an IBM or IBM-compatible (such as Compaq, Dell, or Zenith), which won't run Macintosh programs? And, if the latter, should they buy one with DOS with Windows, Windows 95, OS/2, Windows NT, or Unix? Should they also be concerned with an operating system such as NetWare that will link several computers on a local area network? Should they wait for a new operating system to be introduced that may resolve some of these differences?

Before we try to sort out these perplexities, we should see what operating systems do that deserves our attention. We consider:

- Booting
- Housekeeping tasks
- User interface
- Managing computer resources
- Managing files
- Managing tasks

The operating system begins to operate as soon as you turn on, or "boot," the computer. The term ***booting*** **refers to the** process **of loading an operating system into a computer's main memory from diskette or hard disk.** This loading is accomplished by a program (called the *bootstrap loader* or *boot routine)* that is stored permanently in the computer's electronic circuitry. When you turn on the machine, the program obtains the operating system from your diskette or hard disk and loads it into memory. Other programs called *diagnostic routines* also start up and test the main memory, the central processing unit, and other parts of the system to make sure they are running properly. As these programs are running, the display screen may show the message "Testing RAM" (main memory). Finally, other programs (indicated on your screen as "BIOS," for basic input-output system) will be stored in main memory to help the computer interpret keyboard characters or transmit characters to the display screen or to a diskette.

All these activities may create a jumble of words and numbers on your screen for a few seconds before they finally stop. Then a guide may appear, such as "A:\>" or "C:\>." This is the system prompt. **The** *system* ***prompt*** **indicates the operating system has been loaded into main memory and asks ("prompts") you to enter a command.** You may now enter a command. The operating system remains in main memory until you turn the computer off. With newer operating systems, the booting process puts you into a graphically designed starting screen, from which you choose the applications programs you want to run.

If you have not entered a command to start an applications program, what else can you do with the operating system? One important function is to perform common repetitious "housekeeping tasks."

One example of such a housekeeping task is formatting blank diskettes. Before you can use a new diskette that you've bought at a store, you may have to format it. ***Formatting,*** **or** ***initializing,*** **electronically prepares a diskette so it can store data or programs.**

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

master system – базовая (главная) система

resource management service – услуга управления ресурсами

disk space – место на диске

CPU time allocation – распределение времени центрального универсального процессора

spreadsheet – электронная таблица
pen-based computer – пен-компьютер
scribble – каракуля, неразборчивое письмо
aggravation – ухудшение, осложнение
incompatibility – несовместимость
to run a program – выполнять программу
perplexity – затруднение; запутанность
booting – загрузка
housekeeping task – задача обслуживания
bootstrap – программа загрузки компьютера; (программа самозагрузки)
boot routine – программа загрузки
diagnostic routine – диагностическая программа
jumble – смешивание, перемешивание
system prompt – напоминание системы
to enter a command – вводить команду
repetitious – без конца повторяющийся
initializing – инициализация; установка в исходное состояние; начальная загрузка
make – модель, конструкция

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What does the operating system consist of? 2. How do these programs provide resource management services? 3. Why does a computer need systems software? 4. What allows us to concentrate on our own tasks or applications? 5. Do different sizes and makes of computers have their own operating systems? Give your reasons. 6. Are these operating systems compatible with one another? 7. Will an operating system written for one kind of hardware be able to run on another kind of machine? 8. When may microcomputer users experience the aggravation of incompatibility? 9. Can an operating system designed for a mainframe run on a microcomputer? 10. What does the term booting mean? 11. What is loading accomplished by? 12. Where does the program obtain the operating system from when you turn on the machine? 13. What do diagnostic routines test? 14. What does the system prompt deal with? 15. How long does the operating system remain in main memory? 16. Why do microcomputer users have to format their diskettes before using them?

Exercise 2. Translate the following equivalents

An operating system, to be required for, applications software, to run on your computer, to bypass, to work directly, systems software, certain tasks, the master system of programs, to manage the basic operations of the computer, to provide resource management services, disk space, CPU time allocation, the complexities of managing the computer, different sizes and makes of computers, to write scribbles and notes on the screen, to be compatible with each other, to experience the aggravation of such incompatibility, to wait for a new operating system to be introduced, to resolve differences, to sort out these perplexities, to deserve our attention, to "boot" the computer, the process of loading an operating system, to be accomplished by a program, to be stored permanently in the computer's electronic circuitry, to turn on the machine, to obtain, diagnostic routines, to start up and test the main memory, the central processing unit, to make sure, to run properly, to transmit characters to the display screen, to create a jumble of words and numbers, the system prompt, to choose the applications programs you want to run, to perform common repetitious "housekeeping tasks," to format blank diskettes.

Exercise 3. Match the terms in Table A with the statements in Table B

Table A
1. The operating system (OS)
2. It
3. Pen-based computers
4. booting
5. The system prompt
6. The booting process
7. To perform common repetitious "housekeeping tasks"

Table B
A Is one important function.
B refers to the process of loading an operating system into a computer's main memory from diskette or hard disk.
C puts you into a graphically designed starting screen, from which you choose the applications programs you want to run.
D indicates the operating system has been loaded into main memory and asks ("prompts") you to enter a command.
E have their own operating systems.
F consists of the master system of programs that manage the basic operations of the computer.
G allows you to concentrate on your own tasks or applications rather than on the complexities of managing the computer.

Exercise 4. This is the description of Unix. Read it carefully. Use the following table to make a description of the Linux

Unix is a command-driven operating system used on all sizes of computers, but mostly large multi-user, multi-tasking mainframe computers. It is available in such version as Linux, Minix, Xenix, HP-UX, Ultrix, Venix, A/UX,AIX, Solaris and Power Open.

Type	Unix-based
Computer	A wide range of
Features	Wide variety of distribution kits is available
Graphics engine	XFree86
User Interface type	Command line, GUI
User Interface	KDE, Gnome
Source code availability	Freely available

(Oxford English for information Technology, p.41)

Language Work.

Exercise 1. Put the nouns below into three groups:

a) countable b) uncountable c) countable or uncountable

system, time, operation, incompatibility, circuitry, processing, housekeeping, graphics, software, communications, multiprogramming, interface, menu.

Exercise 2. Complete the statements using words from the box:

based operations display manages program written electronically through

1. The operating system …… the basic operations of the computer.
2. These …… include booting and housekeeping tasks.
3. A language translator is software that translates a program …… by a programmer.
4. The operating system also manages tasks …… multitasking, multiprogramming, time-sharing, or multiprocessing.
5. The …… screen may show the message "Testing RAM", as these programs are running.
6. Pen-…… computers have their own operating systems.
7. The …… obtains the operating system from your diskette or hard disk.
8. Formatting …… prepares a diskette so it can store data or programs.

Exercise 3. Rewrite each of these sentences like this:

One example of a housekeeping task is to format blank diskettes.

Formatting blank diskettes is one example of a housekeeping task.

1. Another function of the operating system is to execute and provide services for applications software.
2. One important function is to perform common repetitious "housekeeping tasks".
3. The role of the operating system is to communicate directly with the hardware.
4. Part of the work of mainframe operating systems is to support multiple programs and users.
5. The goal of this program is to accomplish loading an operating system into a computer's main memory from a diskette or a hard disk.
6. An important function of the operating system is to manage the computer's resources.
7. The main reason for installing these programs is to act as an interface between the user and the computer.

Exercise 4. Translate the following sentences into English:

1. Операционная система необходима для запуска приложений в твоем компьютере. 2. При выполнении определенных задач пользователь может напрямую работать с системным программным обеспечением. 3. Эти программы обеспечивают управление различными ресурсами, решая такие вопросы как контроль и использование аппаратного обеспечения, место на диске, память, распределение времени ЦПУ и работа периферийных устройств. 4. Различные операционные системы используются для различных марок и типов компьютеров. 5. Такие операционные системы как UNICOS and COS, MVS и VM, AOS и DG, VAX/VMS, PenRight, PenPoint, Pen DOS, и Windows for Pen Computing являются не совместимыми друг с другом. 6. Термин «загрузка» относится к процессу загрузки операционной системы в оперативную память компьютера с дискеты либо жесткого диска. 7. Другие программы, называемые диагностическими, запускают и тестируют оперативную память, центральный процессор и другие части системы для надежной работы. 8. Напоминание системы говорит о том, что операционная система загружена

в оперативную память и запрашивает «подсказку» для ввода команды. 9. Операционная система находится в оперативной памяти до выключения компьютера. 10. Форматирование или инициализация подготавливает дискету для сохранения данных либо программ в электронной форме.

Discussion

Exercise 1. Discuss the following questions:

1. What is the principal piece of systems software in any computer system?
2. How do these programs act as an interface between the user and the computer?

Text 2. THREE TYPES OF USER INTERFACES

Many operating-system functions are never apparent on the computer's display screen. What you do see is the user interface. **The *user interface* is the part or the operating system that allows you to communicate, or interact, with it.**

There are three types of user interfaces, for both operating systems and applications software—*command-driven, menu-driven,* and *graphical.* The latter two types of user interface are often called a *shell.*

Command-driven: A *command-driven interface* requires you to enter a command by typing in codes or words. An example of such a command might be DIR (for "directory"). This command instructs the computer to display a directory list of all file names on a disk.

You type a command at the point on the display screen where the cursor follows the prompt (such as following "C:\>"). Then you press the Enter key to execute the command. You'll recall that a *cursor* is a symbol (such as a blinking rectangle of light) that cues where you may type data or enter a command.

The command-driven interface is seen on IBM and IBM-compatible computers with the MS-DOS operating system.

Menu-driven: A *menu-driven interface* allows **you to choose a command** from **a** menu. Like a restaurant menu, **a** software ***menu*** offers **you options** to **choose from—in** this case, **commands** available **for** manipulating data, such as Print or Edit.

Menus are easier to use than command-driven interfaces, especially for beginners. Their disadvantage, however, is that they are slower to use. Thus, some software programs offer both features—menus for novice users and keyboard codes for experienced users.

Graphical: The easiest interface to use, the ***graphical*** *user interface (GUI),* uses **images** to represent options. Some of these images take the form of icons. ***Icons*** are small pictorial figures that represent tasks, functions, or programs—for example, a trash can for **a** delete-file function.

Another feature of the GUI (pronounced "gooey") is the use of windows. ***Windows*** **divide** the display screen **into** sections. Each window may show a different display, such as a word processing document in one and a spreadsheet in another.

Finally, the GUI permits liberal use of the mouse. The mouse is used as a pointing device to move the cursor to a particular place on the display screen or to point to an icon or button. The function represented by the icon can be activated by pressing ("clicking") buttons on the mouse. Or, using the mouse, you can move ("drag") an image from one side of the screen to the other or change its size.

Microcomputer users first became aware of the graphical user interface in Apple Macintosh computers (although Apple got the idea from Xerox). Later Microsoft made a graphical user interface available for IBM and IBM-compatible computers through its Windows program. Now most operating systems on microcomputers feature a GUI.

Behind the user interface, the operating system acts like a police officer directing traffic. This activity is performed by the *supervisor,* or *kernel,* the central component of the operating system. The supervisor, which manages the CPU, resides in main memory while the computer is on and directs other programs to perform tasks to support applications programs. Thus, if you enter a command to print your document, the operating system will select a printer (if there is more than one). It will then notify the computer to begin executing instructions from the appropriate program (known as a *printer driver,* because it controls, or "drives," the printer). Meanwhile, many operating systems allow you to continue writing. Were it not for this supervisor program, you would have to stop writing and wait for your document to print out before you could resume.

The operating system also manages memory – it keeps track of the locations within main memory where the programs and data are stored. It can swap portions of data and programs between main memory and secondary storage, such as your computer’s hard disk. This capability allows a computer to hold only the most immediately needed data and programs within main memory. Yet it has ready access to programs and data on the hard disk, thereby greatly expanding memory capacity.

There are several ways operating systems can manage memory. Some use *partitioning* – that is, they divide memory into separate areas called *partitions*, each of which can hold a program or data. Large computer systems often divide memory into *foreground* and *background* areas. High-priority programs are executed in foreground memory, and low-priority programs are executed in background memory. For example, if a user is interacting with a program, that program will be in foreground memory. While the user is entering data, the CPU will be unused. Thus, during that time, the CPU can be made available to process something in background memory, such as printing a spreadsheet. Programs wait on disk in *queues* for their turn to be executed.

Files of data and programs are located in many places on your hard disk and other secondary-storage devices. The operating system allows you to find them. If you move, rename, or delete a file, the operating system manages such changes and helps you locate and gain access to it. For example, you can *copy*, or duplicate, files and programs from one disk to another, You can *back up*, or make a duplicate copy of, the contents of a disk. You can *erase*, or remove, from a disk any files or programs that are no longer useful. You can *rename*, or give new filenames, to the files on a disk.

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

apparent – видимый, явный
driven – управляемый; приводимый в действие
shell – (программная) оболочка; среда
directory list – справочный список
cursor – стрелка, указатель
prompt – напоминание, подсказка
to recall – повторно вызывать
blinking rectangle – мигающий (мерцающий) прямоугольник
to cue – подавать сигнал; напоминать; указывать
novice user [‘novɪs] – начинающий пользователь

icon – пиктограмма, иконка (в терминологии Microsoft – «значок»)
pictorial – графический
small pictorial figures – маленькое графическое изображение
trash can – «корзина» пиктограмма, выбираемая при удалении файлов или объектов
to drag – медленно тянуть
supervisor – супервизор
kernel – ядро (внутренняя резидентная часть операционной системы)
to reside in – быть присущим, свойственным
printer driver – драйвер принтера
to swap – менять, обменивать
secondary storage – вспомогательное запоминающее устройство
partitioning – разделение; разбиение
foreground area – зона высокого приоритета
background area – зона низкого приоритета
to delete a file – удалять файл
to duplicate – дублировать
to back up – дублировать, создавать резервную копию
to erase – стирать (запись)

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. Are many operating-system functions apparent on the computer's display screen? 2. What does the user interface allow? 3. How many types of user interfaces are there? 4. What does a command-driven interface require? 5. Which command instructs the computer to display a directory list of all file names on a disk? 6. Why do you have to press the Enter key? 7. What operating system is the command-driven interface seen with on IBM and IBM-compatible computers? 8. What does a menu-driven interface allow? 9. What is the disadvantage of menus? 10. What do software programs offer? 11. What can you say about the graphical user interface? 12. Do windows divide the display screen into sections? 13. What is the mouse used for? 14. How can the icon be activated? 15. What is the central component of the operating system? 16. Where does the supervisor reside in? 17. What will happen if you enter a command to print your document? 18. How does the operating system manage memory? 19. What allows a computer to hold only the most immediately needed data and programs within main memory? 20. What areas do large computers divide memory into? 21. Where are high-priority programs executed? 22. Where are low-priority programs executed? 23. How can you move, rename or delete a file?

Exercise 2. Study the table. Find the corresponding ending of each sentence

1. The user interface	**A** allows you to choose a command from a menu.
2. A command-driven interface	**B** is seen on IBM and IBM-compatible computers with the MS-DOS operating system.
3. Menu-driven, and graphical interfaces	**C** are often called a shell.
4. The command-driven interface	**D** is the part or the operating system that allows you to communicate, or interact, with it.

5. A menu-driven interface	**E** wait on disk in queues for their turn to be executed.
6. The graphical user interface (GUI),	**F** manages the CPU, resides in main memory, directs other programs to perform tasks to support applications programs.
7. Icons	**G** divide the display screen into sections.
8. Windows	**H** permits liberal use of the mouse.
9. The GUI	**I** requires you to enter a command by typing in codes or words.
10. The supervisor	**J** represent tasks, functions, or programs.
11. The operating system	**K** keeps track of the locations within main memory.
12. Programs	**L** uses images to represent options.

Exercise 3. Study the following definitions. Work in pairs. Ask each other questions regarding the information in Table A and in Table B

Table A	**Table B**
command-driven interface Type of user interface that requires users to enter a command by typing in codes or words	**disk operating system (DOS)** Microcomputer operating system that runs primarily on IBM and IBM-compatible microcomputers. DOS is sold under the names MS-DOS by Microsoft Corporation, PC-DOS by IBM, and, until recently, DOS 7 by Novell
graphical user interface (GUI) User interface that uses images to represent options. Some of these images take the form of icons, small pictorial figures that represent tasks, functions, or programs	**external utility programs** Special programs that provide specific useful services not provided or performed less well by other system software programs
Macintosh Operating System (Mac OS) Operating system used on Apple Macintosh computers	**menu-driven interface** User interface that allows users to choose a command from a menu
NetWare Most popular operating system, from Novell, for orchestrating microcomputer-based local area networks (LANs) throughout a company or campus	**operating environment** Also known as a ***windowing environment or shell;*** adds a graphical user interface as an outer layer to an operating system. Common features of these operating environments are use of an electronic mouse, pull-down menus, icons and other graphic displays, the ability to run more than one application (such as word processing and spreadsheets) at the same time, and the ability to exchange data between these applications

operating system (OS)
Principal piece of systems software in any computer system; consists of the master set of programs that manage the basic operations of computer. The operating system remains in main memory until the computer is turned off

OS/2 (Operating System/2) & OS/2 Warp
Microcomputer operating system designed to run on many recent IBM and compatible microcomputers

time-sharing
Operating system software feature whereby a single computer processes the tasks of several users at different stations in round-robin fashion. Timesharing and multitasking differ slightly. With time-sharing, the computer spends a fixed amount of time with each program before going on to the next one. With multitasking the computer works on each program until it encounters a logical stopping point, as in waiting for more data to be input

Unix
Operating system for multiple users, with built-in networking capability, the ability to run multiple tasks at one time, and versions that can run on all kinds of computers

Windows
Operating environment made by Microsoft that places a graphical user interface shell around the MS-DOS and PC-DOS operating systems

Windows NT (New Technology)
Operating system intended to support large networks of computers, such as those involved in airline reservations systems

(From Williams Sawyer Hutchinson. Using Information Technology)

Language Work

Exercise 1. Make nouns from the adjectives in brackets to complete the sentences:

1. He made the correct (decisive).
2. A menu-driven interface contains menus offering displayed lists of (optional).
3. Using the mouse you can change the size of an (imaginative).
4. Windows divide the display screen into (sectional).
5. We outlined some of the risks of end user application (developable).
6. For a good signature-detection IDS, operational (real) leaves much to be desired.
7. These common standards are the key to the free flow of messages among the widely different computers and networks in the (systematic).

Exercise 2. Translate the following sentences.

1. Операционная среда Windows сделала DOS более легким в использовании, поскольку больше прикладных программ было написано для Windows, чем для DOS.

2. В отличие от традиционной операционной среды Windows, Windows NT является настоящей операционной системой, исключая необходимость в DOS и напрямую взаимодействуя с аппаратным обеспечением. Изначально, Windows NT была создана для работы на рабочих станциях и других более мощных компьютерах.

3. Командные интерфейсы используются на IBM и IBM-совместимых компьютерах с DOS.

4. DOS – наиболее распространенная микрокомпьютерная операционная система.

5. Графический пользовательский интерфейс легче в использовании, чем командный, поскольку позволяет свободно пользоваться мышью для передвижения курсора к определенному изображению на экране. Функция, представленная в виде пиктограммы, активируется путем нажатия кнопки мыши.

6. NetWare позволяет ПК обмениваться данными файлов, совместно использовать принтеры и файловые серверы.

7. Unix является портативной операционной системой. Основные пользователи Unix – это большие корпорации и банки, использующие программное обеспечение для решения всевозможных задач.

8. Внешние программы–утилиты доступны на отдельных дисках и используются, например, для восстановления поврежденных файлов.

9. Операционная система или среда может показывать несколько окон с различными приложениями на экране компьютера, такими как текстовый редактор, таблицы и графика.

10. Приложение не могут запускаться без системного программного обеспечения.

Discussion

Exercise 1. Speak about three types of user interfaces. Use the combinations given below: operating-system functions; the user interface; a command-driven interface; to display a directory list; to execute the command; a menu-driven interface; to choose a command; the graphical user interface; to take the form of icons; a pointing device; to become aware of.

Text 3. MANAGING TASKS

A computer is required to perform many different tasks at once. In word processing, for example, it accepts input data, stores the data on a disk, and prints out a document – seemingly simultaneously. Some computers' operating systems can also handle more than one program at the same time – word processing, spreadsheet, database searcher – displaying them in separate windows on the screen. Others can accommodate the needs of several different users at the same time. All these examples illustrate *task management* – a 'task' being an operation such as storing, printing, or calculating.

Among the ways operating systems manage tasks in order to run more efficiently are *multitasking, multiprogramming, time-sharing,* and *multiprocessing*. Not all operating systems can do all these things.

– **Multitasking** – executing more than *one program* concurrently: *Multitasking* is the execution of two or more programs by one user concurrently – not simultaneously – on the same computer with one central processor. You may be writing a report on your computer with one program while another program searches an online database for research material. How does the computer handle both programs at once?

The answer is that the operating system directs the processor (CPU) to spend a predetermined amount of time executing the instructions for each program, one at a time. In essence, a small amount of each program is processed, and then the processor moves to the remaining programs, one at a time, processing small parts of each. This cycle is repeated until processing is complete. The processor speed is usually so fast that it may seem as if all the programs are being executed at the same time. However, the processor is still executing only one instruction at a time, no matter how it may appear to the user.

– **Multiprogramming –** concurrent execution *of* different users' programs**:** *Multiprogramming* is the execution of two or more programs on a *multiuser* operating system. As with multitasking, the CPU spends a certain amount of time executing each user's program, but it works so quickly, it seems as though all the programs are being run at the same time.

– **Time-sharing –** round-robin processing *of* programs for several users: *Time-sharing* is a single computer's processing of the tasks of several users at different stations in round-robin fashion**.** Time-sharing is used when several users are linked by a communications network to a single computer. The computer will first work on one user's task for a fraction of a second, then go on to the next user's task, and so on.

How is this done? The answer is through *time slicing.* Computers operate so quickly that it is possible for them to alternately apportion slices of time (fractions of a second) to various tasks. Thus, the computer's operating system may rapidly switch back and forth among different tasks, just as a hairdresser or dentist works with several clients or patients concurrently. The users are generally unaware of the switching process.

Multitasking and time-sharing differ slightly. With multitasking, the processor directs the programs to take turns accomplishing small tasks or events within the programs. These events may be making a calculation, searching for a record, printing out part of a document, and so on. Each event may take a different amount of time to accomplish. With time-sharing, the computer spends a *fixed amount* of time with each program before going on to the next one.

– **Multiprocessing–simultaneous processing** of two or more programs by multiple computers: *Multiprocessing* is processing done by two or more computers or processors linked together to perform work simultaneously—that is, at precisely the same time. This can entail processing instructions from different programs or different instructions from the same program.

Multiprocessing goes beyond multitasking, which works with only one microprocessor. In both cases, the processing should be so fast that, by spending a little bit of time working on each of several programs in turn, a number of programs can be run at the same time. With both multitasking and multiprocessing, the operating system keeps track of the status of each program so that it knows where it left off and where to continue processing. But the multiprocessing operating system is much more sophisticated than multitasking.

Multiprocessing can be done in several ways. One way is *coprocessing,* whereby the controlling CPU works together with specialized microprocessors called *coprocessors,* each of which handles a particular task, such as display-screen graphics or high-speed mathematical calculations. Many sophisticated microcomputer systems have coprocessing capabilities.

Another way to perform multiprocessing is by *parallel processing,* whereby several full-fledged CPUs work together on the same tasks, sharing memory. Parallel processing is often used in large computer systems designed to keep running if one of the CPUs fails. These systems are called *fault-tolerant* systems; they have several CPUs and redundant components, such as memory and input, output, and storage devices. Fault-tolerant systems are used, for example, in airline reservation systems.

Operating system functions are summarized below (Figure 8).

FIGURE 8. Some operating system functions

Booting	Housekeeping Tasks	User Interface	Managing Computer Resources	Managing Files	Managing Tasks
Loads operating system into computer's main memory Uses diagnostic routines to test system for equipment failure Stores BIOS programs in main memory	Formats diskettes Displays information about operating system version Displays disk space available	Provides a way for user to interact with the operating system – can be command-driven, menu-driven, or graphical	Via the supervisor, manages the CPU and directs other programs to perform tasks to support applications programs Keeps track of locations in main memory where programs and data are stored (memory management) Moves data and programs back and forth between main memory and secondary storage (swapping)	Copies files / programs from one disk to another Backs up files / programs Erases (deletes) files / programs Renames files	May be able to perform multitasking, multiprogramming, time-sharing, or multiprocessing

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

managing tasks	управление заданиями
seemingly	по-видимому
at a time	сразу, одновременно
database searcher	лицо, занимающееся поиском базы данных
to accommodate	приспосабливать
task management	управление заданием
multitasking	многозадачность
multiprogramming	мультипрограммирование
time-sharing	распределение времени

multiprocessing – многопроцессорная обработка
concurrently – параллельно
round-robin processing – обработка задач в определенной очередности
time slicing – разделение времени
alternately – переменно
to apportion – распределять
to switch back / forth – переключать назад / вперед
to entail – влечь за собой
to go beyond – превышать что-либо
coprocessor – сопроцессор (отдельная микросхема, дополняющая главный процессор при выполнении каких-либо функций)
fault-tolerant system – система, устойчивая к повреждениям; отказоустойчивая система
redundant components – избыточные компоненты
diagnostic routine – диагностическая программа; программа диагностики
to track – определять; отслеживать
full-fledged – законченный; окончательно готовый; полный

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What is required to perform many different tasks at once? 2. Can some computers' operating systems handle more than one program at the same time? 3. What is task management? 4. What does multitasking deal with? 5. How many times is the cycle of program processing repeated? 6. What is multiprogramming? 7. What can you say about time-sharing? 8. What is time slicing? 9. What is the difference between multitasking and time-sharing? 10. What does multiprocessing deal with? 11. How can multiprocessing be done? 12. Which is faster: multiprocessing, multitasking, or time-sharing?

Exercise 2. Read the equivalents. Translate them:

to be required to do smth., to perform, to accept, to print out a document, simultaneously, to handle, to illustrate, concurrently, an online database, a research material, a predetermined amount of time, to execute the instructions, round-robin processing of programs, a fraction of a second, to switch back and forth, to be unaware of the switching process, to take turns, to make a calculation, to search for a record, a fixed amount of time, sophisticated, coprocessing capabilities, to keep track of, fault-tolerant systems, airline reservation systems.

Exercise 3. The following definitions of key terms have been mixed up. Find the corresponding ending for each definition

1. Multitasking	**A** are those that have several CPUs and redundant components, such as memory and input, output, and storage devices.
2. Multiprogramming	**B** occurs when several full-fledged CPUs work together on the same tasks, sharing memory. It is often used in large computer systems designed to keep running if one of the CPUs fails.

3. Multiprocessing	**C** is a single computer's processing of the tasks of several users at different stations in round-robin fashion.
4. Time-sharing	**D** is processing done by two or more computers or processors linked together to perform work simultaneously.
5. Parallel processing	**E** the execution of two or more programs by one user concurrently – not simultaneously – on the same computer with one central processor.
6. Fault-tolerant systems	**F** is the execution of two or more programs on a multiuser operating system when the CPU spends a certain amount of time executing each user's program, but it works so quickly, it seems as though all the programs are being run at the same time.

Language Work

Exercise 1. Insert the prepositions:

1. …… the ways operating systems manage tasks in order to run more efficiently are multitasking, multiprogramming, time-sharing and multiprocessing.
2. Using the mouse, you can move an image …… one side of the screen to the other.
3. Documentation is also invaluable …… the maintenance of a system as needed improvements are made.
4. All managers must accept the responsibility …… managing the information system resources of their work groups and departments.
5. You can make, online searches for information in a variety …… ways.
6. Businesses are connecting …… the Internet because it represents the wave of the future in business telecommunications.
7. Early attempts …… some direct mail companies met with almost unanimous resistance.
8. …… both multitasking and multiprocessing, the operating system keeps track of the status of each program.

Keys: in, with, from, by, among, to, for, of.

Exercise 2. Choose the correct conjunction in each of the following sentences:

1. The cycle is repeated *unless/until* processing is complete.
2. He won't get promotion *provided that/unless* he works hard.
3. Time-sharing is used *if/when* several users are linked by a communication network to a single computer.
4. *In case/if* the received sequence contains errors, it may no longer depict a valid path through the trellis.
5. For an uncoded system, MPSK is selected *if/when* the channel is bandwidth limited.
6. An error-correction coding scheme may be needed *on condition that/if* none of the allowable modulation schemes can meet the requirements.

Exercise 3. Translate the following into English:

1. Операцио́нная систе́ма – базовый комплекс компьютерных программ, обеспечивающий управление аппаратными средствами компьютера, работу с файлами, ввод и вывод данных, а также выполнение прикладных программ и утилит.

2. При включении компьютера операционная система загружается в память раньше остальных программ и затем служит платформой и средой для их работы.

3. ОС может осуществлять и другие сервисы, например, предоставление пользовательского интерфейса, сетевое взаимодействие и т. п.

4. С 1990-х наиболее распространёнными операционными системами для персональных компьютеров и серверов являются ОС семейства Microsoft Windows, Mac OS, системы класса UNIX (особенно GNU/Linux).

Современные ОС характеризуются следующими функциями:

– параллельное или псевдопараллельное выполнение задач (многозадачность);

– взаимодействие между процессами;

– межмашинное взаимодействие (компьютерная сеть);

– защита самой системы, а также пользовательских данных и программ от злонамеренных действий пользователей или приложений;

– разграничение прав доступа и многопользовательский режим работы (аутентификация, авторизация).

(From Wikipedia)

Discussion

Exercise 1. Outline the main ideas of the text and write a summary.

Exercise 2. Prepare a report on one of the most popular operating systems. Present your report to the class.

Text 4. MICROCOMPUTER OPERATING SYSTEMS & OPERATING ENVIRONMENTS

The principal microcomputer operating systems and operating environments are DOS, Macintosh Operating System, Windows 3.X (for DOS), OS/2 Warp, Windows 95, Windows NT, Unix, and NetWare.

An *operating environment*—also known as a *windowing environment* or *shell*—adds a graphical user interface or a menu-driven interface as an outer layer to an operating system. The most well-known operating environment is the Windows 3.X program sold by Microsoft, which adds a graphical user interface to DOS. Another is IBM's Workplace Shell, which provides a GUI for OS/2. Similar operating environments are available for Unix.

Common features of these operating environments are use of an electronic mouse, pull-down menus, and icons and other graphic displays. They also have the ability to run more than one application (such as word processing and spreadsheets) at the same time and the ability to exchange data between these applications.

There are reportedly over 100 million users of DOS. This makes it the most popular software of any sort ever adopted, and certainly the most popular systems software. *DOS*—for Disk Operating System—runs primarily on IBM and IBM-compatible microcomputers, such as Compaq, Zenith, AST, Dell, Tandy, and Gateway.

There are now two main operating systems calling themselves DOS.

– Microsoft's MS-DOS: DOS is sold under the name MS-DOS by software maker Microsoft. The "MS" stands for Microsoft. Microsoft launched its original version, MS-DOS 1.0, in 1981, and there have been several upgrades since then.

– IBM's PC-DOS: Microsoft licenses a version to IBM called PC-DOS. The "PC" stands for "Personal Computer." The most recent version is PC-DOS 7, released March 1995.

What do the numbers in the names mean? The number before the period refers to a *version.* The number after the period refers to a *release,* which has fewer refinements than a version. The most recent versions are all backward compatible. For operating systems, *backward compatible* means that users can run the same applications on the later versions of the operating system that they could run on earlier versions.

Recent versions of DOS have expanded the range of the operating system. For example, Version 4.0 of MS-DOS offered the options of a command-driven interface and a menu-driven interface. Version 5.0 added a graphics-based interface. Version 6.0 added features that took advantage of a computer's main memory. Version 6.22 added a data-compression feature to double the amount of information that could be stored on a hard-disk drive.

No doubt DOS will be around for years. After all, there are a great many old but still useful microcomputers running it and a great many application programs written for it. And many IBM mainframe systems use DOS-VSE. Nevertheless, as a command-driven, single-user program, DOS is probably a fading product. Although satisfactory for many uses, it will unquestionably be succeeded by other, more versatile operating systems.

The Apple Macintosh has always had one outstanding feature: it is easy to use. To be sure, it can't do as much as some other operating systems. Still, the easy-to-use interface has generated a strong legion of fans.

In the past, however, Apple kept Macintosh prices high, a deciding factor for many people in picking a personal computer.

Unfortunately, IBM-style and Macintosh microcomputers were designed around different microprocessors, so it was impossible to combine the best of both. IBM and IBM-compatible computers used microprocessors built by Intel. These were the Intel 80286 [called the '286 *chip),* 80386 *['386 chip),* 80486 *['486 chip),* the Pentium (the successor to the '586 chip), and most recently the Pentium Pro. Macintoshes were built around microprocessors made by Motorola—the 68000, 68020, 68030, 68040, and PowerPC chips. Intel chips could not run Macintosh programs and Motorola chips could not run DOS programs.

Still, the Mac, introduced in 1984, set the standard for icon-oriented graphical user interfaces. Indeed, the Macintosh Operating System (Mac **OS)** is easy to use because Apple designed its hardware and software together, from the start.

The Macintosh System 7.5 operating system has an important program, a file manager called the *Finder,* which manages the desktop screen and its icons. System 7.5 also enables users to read MS-DOS and Windows files, even if they don't have the software to create such files. In addition, System 7.5 has a feature called Apple Guide, which offers "active assistance." Active assistance helps users accomplish different tasks on the computer—for example, explaining how to share files with other users.

Although the Macintosh is easy to use, not as many programs have been written for it as for DOS/Windows-based systems. Only about 6900 commercial applications packages have been written for Macs, according to BIS, a Norwell, Massachusetts, market research firm. By contrast, some *29,400* applications packages are available for DOS computers. However, its graphics capabilities make the Macintosh a popular choice for people working in commercial art, desktop publishing, multimedia, and engineering design.

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

windowing environment – оконная операционная среда

shell – оболочка

graphical user interface – графический интерфейс пользователя

pull – down menus – спадающее меню

icon –иконка; изображение

spreadsheet – электронная таблица

release – выпуск; версия; вариант

refinement – повышение качества; улучшение

backward compatible – обратно-совместимый

a fading product – исчезающий продукт

versatile – технологичный; универсальный

in picking – собирая

desktop screen –экран рабочего стола (компьютера)

multimedia – мультимедийный

Exercises

Comprehension Check

Exercise 1. Ask problem questions to the text.

Exercise 2.Read and translate the following equivalents:

the principle operating systems, a windowing environment, an outer layer, similar, to run several applications at once, primarily, IBM compatible, a period, to refer to, a release, a refinement, to expand the range, a graphics based interface, to add features, to double the amount of information, a fading product, unquestionably, versatile.

Exercise 3. In the text find the definitions for the following key terms. Write them out and memorize them:

a shell, a release, a version, backward compatible, a Finder.

Exercise 4. Read the text again and choose the answer (A B or C) which you think fits best according to the text:

1. When you buy a PC, it comes
   A with IBM equipment.
   B with an operating system.
   C with an application program.
2. The number before the period refers to
   A a version.
   B a command – driven interface.
   C an operating environment.
3. A file manager manages
   A elaborate on –screen images.
   B typed commands.
   C the desktop screen and its icons.

4. Active assistance helps users

A store the amount of information on a hard-disk drive.

B accomplish different tasks on the computer.

C type commands .

Language Work

Exercise 1. Complete the sentences with the correct preposition:

1. Similar operating environments are available …… Unix .

2. This minimizes their detrimental effects …… the accuracy and integrity of ongoing computer operations .

3. The function represented …… the icon can be activated by pressing buttons on the mouse.

4. Windows divide the display screen …… sections.

5. File names can be up to 256 characters instead …… the 8 characters of DOS and Windows 3.X.

6. The choice of logarithmic base …… the following formulae determines the unit of information entropy used.

7. Common features of these operating environments have the ability to run more than one application …… the same time.

Exercise 2. Translate the following text. Use a dictionary. Translate the idea, not word by word

Working in the UNIX Environment

Before you can start using UNIX, your system administrator has to set up a UNIX account for you. Think of this account as your office – it's your place in the UNIX environment. Other users may also be at work on the same system. At many sites, there will be a whole network of UNIX computers. So in addition to knowing your account name, you may also need to know the hostname (name) of the computer that has your account.

Each user communicates with the computer from a terminal or a window. To get into the UNIX environment, you first connect to the UNIX computer. (You may have a terminal that's already connected to the computer.) Next, you start a session by logging in to your UNIX account. Logging in does two things: it identifies which user is in a session, and it tells the computer that you're ready to start working. When you've finished working, you log out – and, if necessary, disconnect from the UNIX computer.

Connecting to the UNIX Computer

If you turn on your terminal and see a message from the UNIX computer that looks something like this:

```
login:
```

Connecting from another operating system

If you're using a personal computer to connect to the UNIX system, you'll probably need to start a terminal emulation program. Some common programs are **procomm, qmodem, kermit, minicom, and telnet**. (There are lots of others.)

If you start the program and get a UNIX "login:" prompt, you're ready to log in. But if your screen stays blank or you get another message that you don't understand, check with another user or your system administrator for help.

Discussion

Exercise 1. Discuss these questions:

1. What can you say about an operating environment? What do its common features deal with?

2. Which options did recent versions of DOS offer? Give examples.

3. Study the following table. Use your knowledge and create the same table for Windows Vista.

System requirements for Windows XP Home and Professional editions as follows:

	Minimum	Recommended
Processor	233 MHz	300 MHz or higher
Memory	64 MB RAM (may limit performance and some features)	128 MB RAM or higher
Video adapter and monitor	Super VGA (800 x 600)	Super VGA (800 x 600) or higher resolution
Hard drive disk free space	1.5 GB	1.5 GB or higher
Drives	CD-ROM	CD-ROM or better
Devices	Keyboard and mouse	Keyboard and mouse
Others	Sound card, speakers, and headphones	Sound card, speakers, and headphones

Text 5. WINDOWS FOR DOS (WINDOWS 3.X.)

A *window* (lowercase "w") is a portion of the video display area dedicated to some specified purpose. An operating system (or operating environment) can display several windows on a computer screen, each showing a different applications program, such as word processing and spreadsheets. However, *Windows* (capital "W") is something else. ***Windows* is an operating environment made by Microsoft that lays a graphical user interface shell around the MS-DOS or PC-DOS operating system.** Like Mac OS, Windows contains windows, which can display multiple applications.

It's important to realize that Windows 3.X ("3.X" represents versions 3.0, 3.1, and 3.11) is different from *Windows 95*, which is not just an operating environment but a true operating system.

Microsoft's Windows 3.X is designed to run on IBM-style microcomputers with Intel microprocessors—the '386 and '486 chips. Earlier versions of Windows could not make full use of '386 and '486 chips, but later versions can. To effectively use Windows 3.X, one should have a reasonably powerful microcomputer system. This would include a '386 microprocessor or better, much more main memory than is required for DOS (a minimum of 4 megabytes), and a hard-disk drive.

Microsoft released Windows 3.0 (the first really useful version) in May 1990 and promoted it as a way for frustrated DOS users not to have to switch to more user-friendly operating systems, such as Macintosh. Indeed, Windows has about 80% of the Macintosh features. Although Windows is far easier to use than DOS, its earlier versions have not been as easy to use as the Mac operating system. This is because Windows sat atop the 11-year-old command-driven DOS operating system, which required certain compromises on ease of use. Indeed, the system had something of a split personality. In handling files, for example, after passing through the Macintosh-style display of icons the user had to deal with the DOS file structures beneath. In addition, many users complained that installing peripherals, such as a hard-disk drive, was somewhat difficult with DOS and Windows.

Yet, even if the various Windows 3.X versions were a bit creaky, they were certainly usable by most people. And when Windows 95 was rolled out, most of the objections vanished.

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

window – окно
dedicated to – посвященный чему-либо
hard-disk drive – жесткий диск; винчестер; дисковод жесткого диска
frustrated – несостоявшийся, разрушенный
atop – наверху, сверху
split personality – раздвоение личности
beneath - внизу
creaky – *зд.* ненадежные
to roll out – продвигаться, двигаться вперед
to vanish – исчезать

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What is a window? 2. Where can an operating system display several windows? 3. Is Windows an operating system? 4. Which versions does Windows 3.X represent? 5. What is Microsoft's Windows 3.X designed for? 6. What chips does it have? 7. What should one have to effectively use Windows 3.X? 8. When did Microsoft release Windows 3.0? 9. Does Windows have 80% of the Macintosh features? 10. Why is Windows far easier to use than DOS? 11. What did a user have to deal with in handling files?

Exercise 2. Find the English equivalents for the following:

буква нижнего регистра, быть предназначенным для, операционная среда, текстовый редактор, таблицы, оболочка, оперативная память, дисковод, технические характеристики, жаловаться, изображения, исчезать.

Language Work

Exercise 1. Complete the gaps in this summary of the text on Windows using these linking words and phrases.

because such as since in addition however although but

Several windows on a computers screen show different applications programs ….. word processing and spreadsheets. ….. , Windows is an operating environment made by Microsoft. ….. Windows contains windows they can display multiple applications. Earlier versions of Windows could not make full use of '386 and '486 chips, ….. later versions can. ….. Windows is far easier to use than DOS, its earlier versions have not been as easy to use as the Mac operating system. This is ….. Windows sat atop the 11-year-old command-driven DOS operating system. ….. , many users complained that a hard-disk drive was somewhat difficult with DOS and Windows.

Discussion
Exercise 1. Speak about advantages and disadvantages of Windows 3.X

Text 6. WINDOWS 95 & LATER

Windows 95, **the successor to Windows** 3.1 **for DOS,** is **a true operating** system **for** IBM-style **personal computers rather than just an operating environment.**

Following are just some of the features of Windows 95:

– Clean "Start": Instead of encountering a confusing array of similar program groups (as with Windows 3.X), you'll first see a clean "desktop" with a "Taskbar" of important icons at the bottom of the screen and one button labeled START.

– Better menus: Windows 3.1's quirky Program Manager and File Managers have been replaced by more accessible features called THE EXPLORER and MY COMPUTER, which let you quickly see what's stored on your disk drives and make tracking and moving files easier.

– Long file names: File names can now be up to 256 characters instead of the 8 characters (plus 3-character extension) of DOS and Windows 3.X. This means you can now have a file name for your resume, for example, of "Resume—January 15, 1997, version" instead of "RES11597." (Macintosh OS and OS/2 have always permitted long file names.)

– The "Recycle Bin": This feature allows you to delete complete files and then get them back if you change your mind.

– 32-bit instead of 16-bit: The new software is a 32-bit program, whereas most Windows 3.1 software is 16-bit. *Bit numbers* refer to how many bits of data a computer chip, and software written for it, can process at one time. Such numbers are important because they refer to the amount of information the hardware and software can use at any one time. This doesn't mean that 32-bit software will necessarily be twice as fast as 16-bit software, but it does promise that new 32-bit applications software will offer better speed and features once software developers take advantage of the design.

– Plug and play: It has always been easy to add new hardware components to Macintoshes. It used to be extremely difficult with IBM-compatible PCs. *Plug and play* refers to the ability to add a new hardware component to a computer system and have it work without needing to perform complicated technical procedures.

More particularly, *Plug and Play* (abbreviated *PnP)* is a standard developed for IBM-style PCs by Microsoft and chip maker Intel and incorporated into Windows 95 to eliminate user frustration when one is adding new components. Now when you add a new printer or modem, your PC will recognize the model and set it up.

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

successor – последователь
confusing array – беспорядочный массив
encountering – сталкивание
quirky [‘kwə:kɪ] – изворотливый

character extension – расширение символов (знаков)

recycle bin – «корзина» (экранная пиктограмма, обозначающая место промежуточного хранения удаленных файлов)

plug and play – «включай и работай»; самонастраиваемое устройство

frustration – крушение, провал

Exercises

Comprehension Check

Exercise 1. Answer the following questions

1. What is Windows 95? 2. What is clean “Start”? 3. Which features have Windows 3.1’s quirky Program Manager and File Managers been replaced by? 4. How long can file names be? 5. What does the “Recycle Bin” feature allow? 6. What can you say about the new software? 7. Which ability does *Plug and Play* refer to?

Exercise 2. Read and translate the following equivalents:

successor, a true operating system, a confusing array of similar programs, labeled, quirky, to make tracking files easier, characters, instead of, extension, to permit long file names, to delete complete files, plug and play, to take the advantage of a design, to perform complicated technical procedures, to recognize the model, to the set up a model.

Language Work

Exercise 1. Complete the statements using the words from the box:

provides invented several therefore successful type networks built-in databases

1. The operating system was modified and resold by …… companies.
2. NetWare has become the most popular operating system for coordinating microcomputer-based local area …… .
3. NetWare …… a shell around your own operating system.
4. Microsoft has not been an innovative organization in technology so much as a hugely …… marketing organization.
5. In workgroups, individuals work in groups sharing electronic files and …… over communications lines.
6. To use DOS, you must …… in an idiosyncratic string of words or letters or choose a written command from an on-screen menu.
7. Unix is an operating system for multiple users and has …… networking capability.
8. Unix was …… more than two decades ago by American Telephone & Telegraph.
9. ……, operating systems establish a user interface and execute and provide services for applications software.

Discussion

Exercise 1. Speak about the features of Windows 95.

Text 7. EXTERNAL UTILITY PROGRAMS

External utility programs are special programs that provide specific useful services not performed or performed less well by other systems software programs. Examples of such services are backup of your files for storage, recovery of damaged files, virus protection, data compression, and memory management. Some of these features are essential to preventing or rescuing you from disaster.

Some of the principal services offered by utilities are the following:

– Screen saver: A *screen saver* is a utility that supposedly prevents a monitor's display screen from being etched by an unchanging image ("burn-in"). Some people believe that if a computer is left turned on without keyboard or mouse activity, whatever static image is displayed may burn into the screen. Screen savers automatically put some moving patterns on the screen, supposedly to prevent burn-in. Actually, burn-in doesn't happen on today's monitors. Nevertheless, people continue to buy screen savers, often just to have a kind of "visual wallpaper." Some of these can be quite entertaining, such as flying toasters.

– Data recovery: One day in the 1970s, Peter Norton was doing a programming job when he accidentally deleted an important file. This was, and is, a common enough error. However, instead of re-entering all the information, Norton decided to write a computer program to recover the lost data. He called the program *The Norton Utilities.* Ultimately it and other utilities made him very rich.

A *data recovery utility* is used to *undelete* a file or information that has been accidentally deleted. *Undelete* means to undo the last delete operation that has taken place. The data or program you are trying to recover may be on a hard disk or a diskette.

– Backup: Suddenly your hard-disk drive fails, and you have no more programs or files. Fortunately, you have used a utility to make a backup, or duplicate copy, of the information on your hard disk. DOS has commands to help you make backups on diskettes, but they are not easy to use. Other utilities are more convenient. Moreover, they also condense (compress) the data, so that fewer diskettes are required.

– Examples of backup utilities are Norton Backup from Symantec, Backup Exec from Arcada Software, Colorado Backup, and Fastback Plus from Fifth Generation Systems.

– Virus **protection:** Few things can make your heart sink faster than the sudden failure of your hard disk. The exception may be the realization that your computer system has been invaded by a virus. **A *virus* consists of hidden programming instructions that are buried within an applications or systems program.** They copy themselves to other programs, causing havoc**.** Sometimes the virus is merely a simple prank that pops up a message. Sometimes, however, it can destroy programs and data. Viruses are spread when people exchange diskettes or download (make copies of) information from computer networks or the Internet.

Fortunately, antivirus software is available. ***Antivirus software* is a utility program that scans hard disks, diskettes, and the microcomputer's memory to detect viruses.** Some utilities destroy the virus on the spot. Others notify you of possible viral behavior, in case the virus originated after the antivirus software was released.

Examples of antivirus software are Anti-Virus from Central Point Software, Norton AntiVirus from Symantec, McAfee virus protection software, and ViruCide from Parsons Technology.

– File **defragmentation:** Over time, as you delete old files from your hard disk and add new ones, something happens: the files become *fragmented.* ***Fragmentation* is the**

scattering of portions of files about the disk in non-adjacent areas, thus greatly slowing access to the files.

When a hard disk is new, the operating system puts files on the disk contiguously (next to one another). However, as you update a file over time, new data for that file is distributed to unused spaces. These spaces may not be contiguous to the older data in that file. It takes the operating system longer to read these fragmented files. By using a utility program, you can "defragment" the file and speed up the drive's operation.

An example of a program for unscrambling fragmented files is Norton SpeedDisk utility.

– Data **compression:** As you continue to store files on your hard disk, it will eventually fill up. You then have three choices: You can delete old files to make room for the new. You can buy a new hard disk with more capacity and transfer the old files and programs to it. Or you can buy a data compression utility.

Data compression **removes redundant elements, gaps, and unnecessary data from a computer's storage space so less space is required to store or transmit data.** With a data compression utility, files can be made more compact for storage on your hard-disk drive. The files are then "stretched out" again when you need them.

Examples of data compression programs are Stacker from Stac Electronics, Double Disk from Verisoft Systems, and SuperStor Pro from AddStor.

– Memory management: Different microcomputers have different types of memory, and different applications programs have different memory requirements. *Memory-management* utilities are programs that determine how to efficiently control and allocate memory resources.

Memory-management programs may be activated by software *drivers.* **A *driver* is a series of program instructions that standardizes the format of data transmitted between a computer and a peripheral device,** such as a mouse or printer. Electrical and mechanical requirements differ among peripheral devices. Thus, software drivers are needed so that the computer's operating system will know how to handle them. Many basic drivers come with the operating system. If you buy a new peripheral device, however, you need to install the appropriate software driver so the computer can operate it.

Other examples of utilities are file conversion, file transfer, and security. A *file conversion utility* converts files between any two applications or systems formats—such as between WordPerfect and Word for Windows or between Windows and Mac OS. A *file transfer utility* allows files from a portable computer to be transferred to a desktop computer or a mainframe computer and vice versa. A *security utility* protects unauthorized people from gaining access to your computer without using a password, or correct code. Other utilities also exist.

(From Williams Sawyer Hutchinson. Using Information Technology)

List of words and expressions

external utility – внешняя сервисная программа; внешняя утилита; внешние средства

backup – дублирование, резервное копирование

recovery – восстановление

virus protection – противовирусная защита

data compression – сжатие данных; компрессия данных; уплотнение данных

memory management – управление памятью

screen saver – заставка
being etched – запоминаясь
burn-in – запоминание
visual wallpaper – фотообои (фон экрана компьютера)
to undelete – не стирать, не удалять
to condense – сокращать (напр., программу)
to invade – вторгаться
havoc [‘hævək] – разрушение
to pop up – неожиданно возникнуть
to download – «скачивать», загружать
to scan – сканировать
to notify – уведомлять
defragmentation – дефрагментация
non-adjacent – несмежный, непримыкающий
contiguous – соприкасающийся
security utility –утилита безопасности; средства безопасности (защиты)
prank - шутка

Exercises

Comprehension Check

Exercise 1. Answer the following questions

1. What are external utility programs? 2. What principal services offered by utilities do you know? 3. What does a screen saver deal with? 4. Why did Norton decide to write a computer program? 5. What is a data recovery utility used for? 6. What is a computer virus? 7. What does antivirus software do? 8. Which case do utilities notify you of possible viral behavior in? 9. What examples of antivirus software do you know? 10. What is file defragmentation? 11. What is fragmentation? 12. When can you speed up the drive’s operation? 13. What removes redundant elements, gaps, and unnecessary data from a computer’s storage space? 14. Why have data compression utilities become necessary for some users? 15. What are memory-management utilities? 16. What may memory-management programs be activated by? 17. Is a driver a series of program instructions? 18. What do many basic drivers come with?

Exercise 2. Read and translate the following equivalents. Use them in your own sentences

External utility program, to provide specific useful services, to back up files for storages, the recovery of damaged files, virus protection, data compression, memory management, to be essential to, to prevent, to rescue, screen saver, supposedly, to etch, visual wallpaper, entertaining, accidentally, to undelete a file, to undo, to condense data, to be invaded by a virus, hidden programming instructions, to cause havoc, a simple prank, to pop up a message, antivirus software, to detect viruses, on the spot, defragmentation, non-adjacent areas, a file conversion.

Exercise 3. Multiple-Choice Questions

1. Which of the following best describes the process of loading an operating system into a computer’s memory?

a) system prompt
b) formatting

c) backing up
d) booting
e) none of the above

2. Which of the following is the central component of an operating system?
a) supervisor
b) system prompt
c) operating environment
d) icons
e) all of the above

3. Which of the following do you need to transmit data between a computer and a peripheral device?
a) file conversion utility
b) peripheral utility
c) memory-management software
d) driver
e) all of the above.

Language Work

Exercise 1. Complete the following statements using words from the box:

intended receive utility operating data server processing

1. External …… programs provide services not performed by other systems software.
2. Information technology is concerned with the use of technology in managing and …… information.
3. The measure of …… is usually expressed by the average number of bits needed for storage or communication.
4. Widows NT, for New Technology, is an operating system …… to support large networks of computers.
5. These …… systems were principally designed to be used with stand-alone desktop machines.
6. A client / …… network is a type of local area network.
7. OS/2 can …… a fax and run a video while at the same time recalculating a spread-sheet.

Exercise 2. Complete the following sentences using a relative pronoun (which, who, that).

1. Peter Norton …… was doing a programming job accidentally deleted an important file.
2. Antivirus software is a utility program …… scans hard disks, diskettes, and the microcomputer’s memory to detect viruses.
3. Memory-management utilities are programs …… determine how to efficiently control memory resources.
4. OS/2 has a graphical user interface …… uses icons resembling documents, folders, printers, and the like.
5. The supervisor, …… manages the CPU, resides in main memory.
6. The power of Windows NT benefits engineers and others …… use workstations.

Exercise 3. Complete the gaps in this summary of the text on Macintosh Operating System using these linking words and phrases:

by contrast *because* *however* *although*

The Macintosh Operating System (Mac OS) is easy to use …… Apple designed its hardware and software together, from the start.

…… the Macintosh is easy to use, not as many programs have been written for it as for DOS / Windows – based systems. Only about 6900 commercial applications packages have been written for Macs. ……, some 29,400 applications packages are available for DOS computers. ……, its graphical capabilities make the Mackintosh a popular choice for people working in desktop publishing, multimedia, and engineering design.

Discussion

Exercise 1. Work in groups. What operating systems would you choose for the following areas and why?

– Supermarkets – Hospitals – Airports – Student's campus

Unit III. MANAGING INFORMATION TECHNOLOGY

Text 1. SECURITY AND CONTROL ISSUES IN INFORMATION SYSTEMS

As a manager, you will be responsible for the control of the quality and performance of information systems in your business unit. Like any other vital business asset, the resources of information systems hardware, software, and data need to be protected by built-in controls to ensure their quality and security. That's why controls are needed. Computers have proven that they can process huge volumes of data and perform complex calculations more accurately than manual or mechanical information systems. However, we know that (1) errors do occur in computer-based systems, (2) computers have been used for fraudulent purposes, and (3) computer systems and their software and data resources have been accidentally or maliciously destroyed.

There is no question that computers have had some detrimental effect on the detection of errors and fraud. Manual and mechanical information processing systems use paper documents and other media that can be visually checked by information processing personnel. Several persons are usually involved in such systems and, therefore, cross-checking procedures are easily performed. These characteristics of manual and mechanical information processing systems facilitate the detection of errors and fraud.

Computer-based information systems, on the other hand, use machine-sensible media such as magnetic disks and tape. They accomplish processing manipulations within the electronic circuitry of a computer system. The ability to check visually the progress of information processing activities and the contents of databases is significantly reduced. In addition, a relatively small number of personnel may effectively control processing activities that are critical to the survival of the organization. Therefore, the ability to detect errors and fraud can be reduced by computerization. This makes the development of various control methods a vital consideration in the design of new or improved information systems.

Effective controls are needed to ensure information system security, that is, the accuracy, integrity, and safety of information system activities and resources. Controls can minimize errors, fraud, and destruction in an information services organization. Effective controls provide quality assurance for information systems. That is, they can make a computer-based information system more free of errors and fraud and able to provide information products of higher quality than manual types of information processing. This can help reduce the potential negative impact (and increase the positive impact) that information technology can have on business survival and success and the quality of life in society.

Three major types of controls must be developed to ensure the quality and security of information systems. These control categories, illustrated in Figure 9 are:

- Information system controls
- Procedural controls
- Physical facility controls

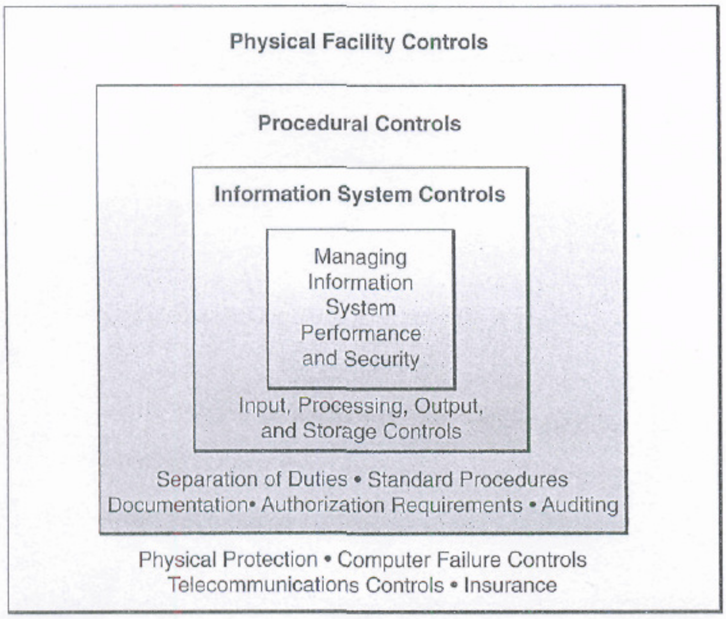

Physical Facility Controls
Procedural Controls
Information System Controls
Managing Information System Performance and Security
Input, Processing, Output, and Storage Controls
Separation of Duties • Standard Procedures
Documentation• Authorization Requirements • Auditing
Physical Protection • Computer Failure Controls
Telecommunications Controls • Insurance

FIGURE 9. The controls needed for information system security. Specific types of controls can be grouped into three major categories: information system, procedural, and physical facility controls

(From James A. O'Brien. Management Information Systems)

List of words and expressions

built-in control – встроенное управление (встроенный контроль)
computer-based system – система с использованием компьютеров
fraud – мошенничество
fraudulent – мошеннический, обманный
maliciously – с преступным намерением, умышленно
detrimental – вредный
personnel – персонал
cross-checking procedure – процедура перекрестной проверки наличия
electronic circuitry – электронные схемы
integrity - целостность
destruction – разрушение, уничтожение
quality assurance – гарантия качества

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What will you as a manager be responsible for? 2. Why do the resources of information systems hardware, software, and data need to be protected by built-in controls? 3. What have computers proven? 4. Can computer systems and their software and data resources be maliciously destroyed? 5. Can paper documents be visually checked by information processing personnel? 6. Why are cross-checking procedures easily performed? 7. What facilitates the detection of errors and fraud? 8. When is the ability to check visually the progress of information processing activities and the contents of databases significantly reduced? 9. Why are effective controls needed? 10. How many types of controls must be developed to ensure the quality and security of information systems? Name these control categories.

Exercise 2. Read and translate the following equivalents from English into Russian. Use the expressions to make up your own sentences:

to be responsible for, the performance of information systems, vital business asset, to be protected by, built-in controls, to ensure quality and security, to process huge volumes of data and perform complex calculations, fraudulent, to be accidentally or maliciously destroyed, to have some detrimental effect on the detection of errors and fraud, cross-checking procedures, to facilitate, to use machine-sensible media such as magnetic disks and tape, the contents of databases, a vital consideration, accuracy, integrity, and safety of information system activities and resources, to reduce the potential negative impact.

Exercise 3. Disagree with the following statements avoiding the simple negation:

1. You won’t be responsible for the control and quality and performance of information systems.
2. Computers haven’t been used for fraudulent purposes.
3. Nobody is involved in information processing systems.
4. Computer-based information systems accomplish processing manipulations within the electric circuitry of a computer system.
5. Effective controls don’t provide quality assurance for information systems.
6. Processing activities usually play insignificant role in the survival of the organization.

Language Work

Exercise 1. Complete the following sentences:

1. Computers can process huge volumes of …… .
2. Computers have had some detrimental effect on …… .
3. These characteristics of manual and mechanical information processing systems facilitate …… .
4. A relatively small number of personnel may …… .
5. The ability to detect errors and fraud can be reduced …… .
6. Three major types of controls must be developed to …… .

Exercise 2. Unjumble the sentences:

1. Systems of quality in and for you responsible of control the unit will be the business performance information your.
2. Process perform complex can that and huge have volumes computers they of calculations proven data.
3. Information controls are ensure security needed to system effective.
4. Information the developed types must major of to and of controls be three ensure quality security systems.

5. Do errors in based systems computer occur.

Exercise 3.Find the corresponding ending of each sentence:

1.	The resources of information systems hardware, software, and data need to be protected	– to ensure the quality and security of information systems.
2.	Computers have proven that they can process huge volumes of data and perform complex calculations	– have been accidentally or maliciously destroyed.

3.	Computer systems and their software and data resources	– more accurately than manual or mechanical information systems.
4.	Effective controls are needed	– by built-in controls to ensure their quality and security.
5.	Three major types of controls must be developed	– to ensure information system security.

Text 2. INFORMATION SYSTEM CONTROLS

Information system controls are methods and devices that attempt to ensure the accuracy, validity, and propriety of information system activities. Controls must be developed to ensure proper data entry, processing techniques, storage methods, and information output. Thus, information system controls are designed to monitor and maintain the quality and security of the input, processing, output, and storage activities of any information system. See Figure 10.

Have you heard the phrase "garbage in, garbage out" (GIGO)? Figure 11 shows why controls are needed for the proper entry of data into an information system. Examples include passwords and other security codes, formatted data entry screens, audible error signals, templates over the keys of key-driven input devices, and prerecorded and prenumbered forms. Input of source documents can also be controlled by registering them in a logbook when they are received by data entry personnel. Realtime systems that use direct access files frequently record all entries into the system on magnetic tape *control logs* that preserve evidence of all system inputs.

Computer software can include instructions to identify incorrect, invalid, or improper input data as it enters the computer system. For example, a data entry program can check for invalid codes, data fields, and transactions. Also, the computer can be programmed to conduct "reasonableness checks" to determine if input data exceeds certain specified limits or is out of sequence. This includes the calculation and monitoring of selected **control totals**.

Data entry and other systems activities are frequently monitored by the use of control totals. For example, a record count is a control total that consists of counting the total number of source documents or other input records and comparing this total to the number of records counted at other stages of input preparation. If the totals do not match, a mistake has been made. Batch totals and hash totals are other forms of control totals. A *batch total* is the sum of a specific item of data within a batch of transactions, such as the sales amounts in a batch of sales transactions. Hash totals are the sum of data fields that are added together for control comparisons only. For example, employee social security numbers could be added to produce a control total in the input preparation of payroll documents.

Once data is entered correctly into a computer system, it must be processed properly. Processing controls are developed to identify errors in arithmetic calculations and logical operations. They are also used to ensure that data are not lost or do not go unprocessed. Processing controls can include hardware controls and software controls.

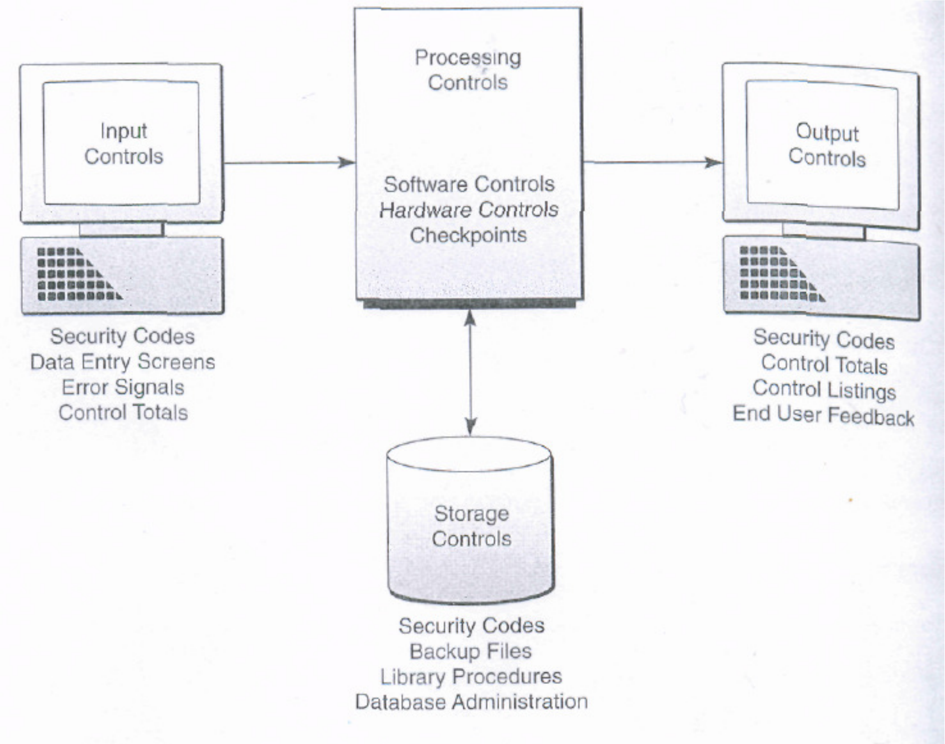


FIGURE 10. Examples of information system controls. Note that they are designed to monitor and maintain the quality and security of the input, processing, output, and storage activities of an information system

Hardware controls are special checks built into the hardware to verify the accuracy of computer processing. Examples of hardware checks include:

– **Malfunction detection circuitry** within a computer or telecommunications processor that can monitor their operations. For example, *parity checks* are made to check for the loss of the correct number of bits in every byte of data processed or transmitted on a network. Another example is *echo checks,* which require that a signal be returned from a device or circuit to verify that it was properly activated. Other examples are redundant circuitry checks, arithmetic sign checks, and CPU timing and voltage checks.

– **Redundant components.** For example, multiple read-write heads on magnetic tape and disk devices check and promote the accuracy of reading and recording activities.

– **Special-purpose microprocessors and associated circuitry** that may be used to support *remote diagnostics* and maintenance. These allow off-site technicians to diagnose and correct some problems via a telecommunications link to the computer.

Some software controls are designed to ensure that the right data is being processed. For example, the operating system or other software checks the internal file labels at the beginning and end of magnetic tape and disk files. These labels contain information identifying the file as well as provide control totals for the data in the file. These internal file labels allow the computer to ensure that the proper storage file is being used and that the proper data in the file have been processed.

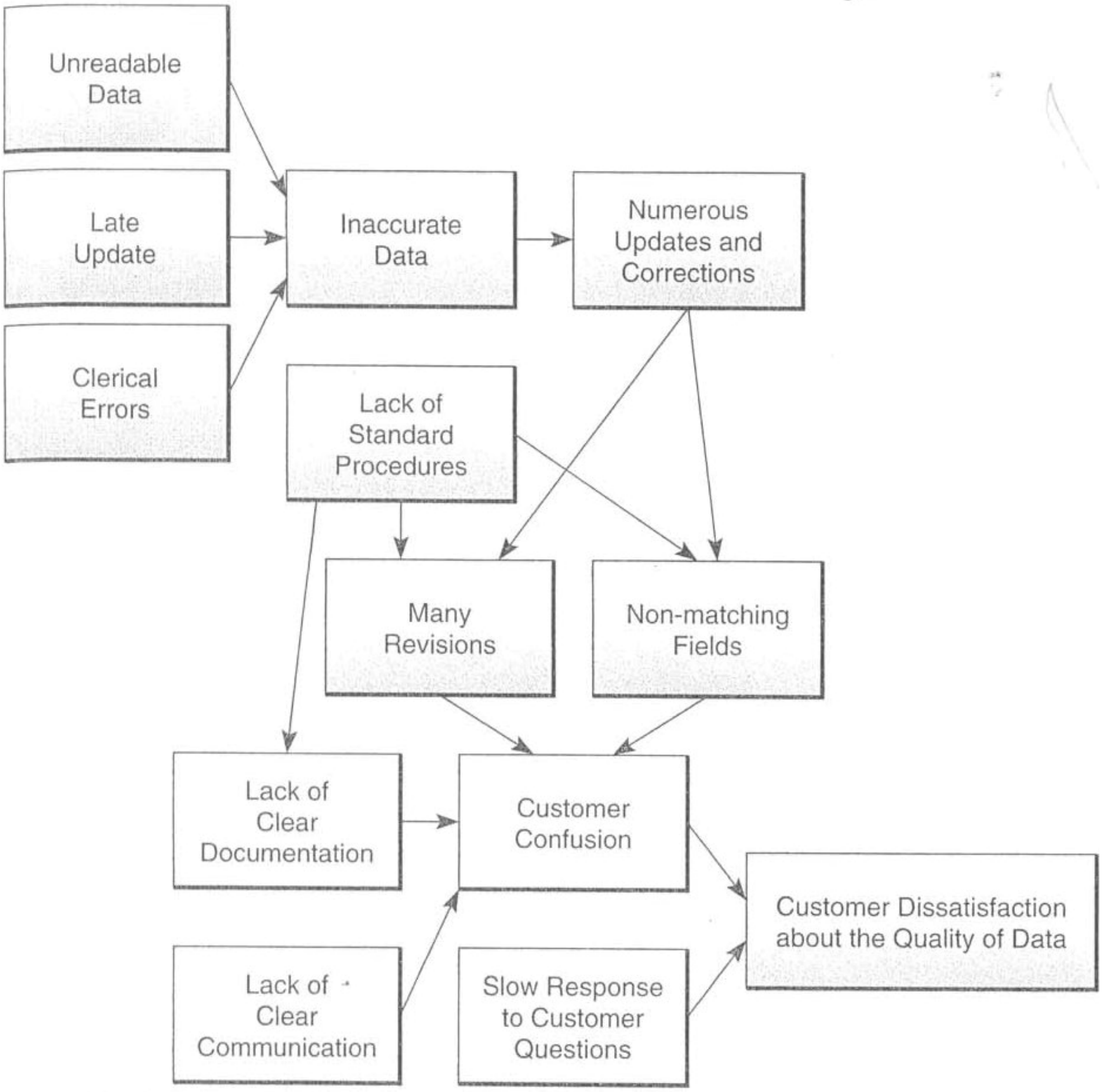

Unreadable Data
Late Update
Clerical Errors
Inaccurate Data
Numerous Updates and Corrections
Lack of Standard Procedures
Many Revisions
Non-matching Fields
Lack of Clear Documentation
Customer Confusion
Customer Dissatisfaction about the Quality of Data
Lack of Clear Communication
Slow Response to Customer Questions

FIGURE 11. Garbage in, garbage out. Input controls are needed for the proper entry of data into a computer system

Another major software control is the establishment of checkpoints during the processing of a program. *Checkpoints* are intermediate points within a program being processed where intermediate totals, listings, or "dumps" of data are written on magnetic tape or disk or listed on a printer. Checkpoints minimize the effect of processing errors or failures, since processing can be restarted from the last checkpoint (called a *rollback),* rather than from the beginning of the program. They also help build an **audit trail**, which allows transactions being processed to be traced through all of the steps of their processing.

Many input, processing, output, and storage controls may be provided by specialized system software packages known as **system security monitors**. System security monitors are programs that monitor the use of a computer system and protect its resources from unauthorized use, fraud, and destruction. Such programs provide the computer security needed to allow only authorized users to access the system. For example, identification codes and passwords are frequently used for this purpose. Security monitors also control the use of the hardware, software, and data resources of a computer system. For example, even authorized users may be restricted to the use of certain devices, programs, and data files. Finally, such programs monitor the use of the computer and collect statistics on any attempts at improper use. They produce reports to assist in maintaining the security of the system.

Output controls are developed to ensure that information products are correct and complete and are transmitted to authorized users in a timely manner. Several types of output controls are similar to input control methods. For example, output documents and reports are frequently logged, identified with route slips, and visually verified by input/output control personnel. Control totals on output are usually compared with control totals generated during the input and processing stages. Control listings can be produced that provide hard copy evidence of all output produced.

Prenumbered output forms can be used to control the loss of important output documents such as stock certificates or payroll check forms. Distribution lists help input-output control personnel ensure that only authorized users receive output. Access to the output of realtime processing systems is controlled, typically, by security codes that identify which users can receive output and the type of output they are authorized to receive. Finally, end users who receive output should be contacted for feedback on the quality of the output. This is an important function of systems maintenance and quality assurance activities.

How can we protect our data resources? First, control responsibilities for files of computer programs and organizational databases may be assigned to a librarian or database administrator. These employees are responsible for maintaining and controlling access to the libraries and databases of the organization. Second, many databases and files are protected from unauthorized or accidental use by security programs that require proper identification before they can be used. Typically, the operating system or security monitor protects the databases of realtime processing systems from unauthorized use or processing accidents. Account codes, passwords, and other security codes are frequently used to allow access to authorized users only. A catalog of authorized users enables the computer system to identify eligible users and determine which types of information they are authorized to receive.

Typically, a three-level password system is used. First, an end user logs on to the computer system by entering his or her unique identification code or user ID. The end user is then asked to enter a password in order to gain access into the system. Finally, to access an individual file, a unique *file name* must be entered. In some systems, the password to read the contents of a file is different from that required to write to a file (change its contents). This feature adds another level of protection to stored data resources. However, for even stricter security, passwords can be scrambled, or *encrypted,* to avoid their theft or improper use.

Many firms also use *backup files,* which are duplicate files of data or programs. Such files may be stored off-premises, that is, in a location away from the computer center, sometimes in special storage vaults in remote locations. Many realtime processing systems use duplicate files that are updated by telecommunication links. Files are also protected by *file retention* measures, which involve storing copies of master files and transaction files from previous periods. If current files are destroyed, the files from previous periods are used to reconstruct new current files. Usually, several *generations* of files are kept for control purposes.

(From James A.O’Brien. Management Information Systems)

List of words and expressions

validity – обоснованность, истинность; достоверность
formatted data entry – внесение (ввод) форматированных данных
template – шаблон; образец
key-driven – приводимый в действие при помощи ключа
prerecorded – предварительно записанный
prenumbered – предварительно пронумерованный
logbook – журнал; регистрационная книга
control log – журнал контроля
improper – неисправный, негодный
transaction – обработка запроса
to be out of sequence – быть вне последовательности (процедуры)
control total – контрольная сумма
a record count – отсчет записей (единиц количества информации)
batch total – контрольная сумма пакета
hash total – контрольная сумма (всего массива данных)
malfunction – неправильное (ложное) срабатывание; сбой; неисправность
parity check – контроль четности; контроль по четности
update – обновление, усовершенствование
echo check – эхо-контроль; проверка обратной пересылкой
CPU timing – синхронизация центрального универсального процессора
off-site technician – специалист, находящийся на расстоянии
checkpoint – контрольная точка
listing – распечатка (программ)
“dump” – “разгрузка” (памяти); дамп (вывод содержимого памяти на печать или экран)
rollback – возврат (для повторного пуска); откат
audit trail – след контроля (аудит); контрольная запись
system security monitor – управляющая программа системной безопасности
timely – своевременный; вовремя
to log – регистрировать, записывать
route slip – маршрутная регистрационная карточка
payroll check – контроль платежной ведомости
stock certificate – акционерный сертификат
to be scrambled – быть скремблированным (о передаче)
backup file – дублирующий файл
vault – хранилище
file retention – сохранение файла
master file – файл с основными данными; главный архив
eligible [‘elıdʒəbl] – приемлемый, подходящий

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What are information system controls? 2. Why must controls be developed? 3. How can input of source documents be controlled? 4. What do control totals deal with? 5. How can a mistake be determined? 6. What does a batch total mean? 7. What are hash totals? 8.

What are processing controls developed for? 9. Can processing controls include hardware controls and software controls? 10. What can you say about hardware checks? 11. What do echo checks require? 12. What checks and promotes the accuracy of reading and recording activities? 13. How can off-site technicians diagnose and correct some problems? 14. What are software controls designed for? 15. What do labels contain? 16. Are checkpoints intermediate points? 17. What minimizes the effect of processing errors and failures? 18. What allows transactions being processed to be traced through all the steps of their processing? 19. Which packages are known as system security monitors? 20. What do system security monitors provide? 21. How can we control the quality of the information products produced by an information system? 22. What is access to the output of realtime processing systems controlled by? 23. What protects the databases of realtime processing systems from unauthorized use? 24. What kind of a system is used? 25. What do backup files mean? 26. How are files protected by file retention measures?

Exercise 2. Read and translate the following equivalents. Use them in your own sentences:

Information system controls, to ensure the accuracy, validity, and propriety of information system activities, processing techniques, storage methods, to include passwords and other security codes, formatted data entry screens, audible error signals, templates over the keys of key-driven input devices, prerecorded and prenumbered forms, a logbook, invalid codes, data fields, and transactions, a batch total, hash totals, preparation of payroll documents, to identify errors in arithmetic calculations and logical operations, malfunction detection circuitry, parity checks, echo checks, to verify, redundant circuitry checks, CPU timing, voltage checks, redundant components, promote the accuracy of reading and recording activities, maintenance, to diagnose and correct some problems via a telecommunications link to the computer, the internal file labels, the proper data, system security monitors, to be restricted to, identification codes and passwords, prenumbered output forms, quality assurance activities, to identify eligible users, a three-level password system, unique identification code, to be scrambled, to be encrypted, to use backup files, to duplicate files of data or programs, realtime processing systems, by file retention measures, for control purposes.

Exercise 3. Agree or disagree with the following statements:

1. Information system controls are methods that attempt to ensure the accuracy and validity.
2. Input of source documents can not be controlled by registering them in a logbook.
3. The computer can be programmed to conduct “reasonableness checks” to determine if input data doesn’t exceed certain specified limits.
4. Data entry and other systems activities are frequently monitored by the use of control totals.
5. Hash totals are the sum of a specific item of data.
6. Processing controls are developed to identify errors in malfunction detection circuitry.
7. These internal file labels allow the computer to ensure that the proper storage file is being used.
8. Security monitors don’t control the use of the hardware, software, and data resources of a computer system.
9. Several types of output controls are similar to the source-coding theorem.

10. A catalog of authorized users enables the computer system to determine which types of information they are authorized to receive.

Language Work

Exercise 1. Insert the prepositions:

1. Controls are needed for the proper entry of data …… an information system. 2. A data entry program can check …… invalid codes, data fields, and transactions. 3. Data entry and other systems activities are frequently monitored …… the use of control totals. 4. A batch total is the sum of a specific item of data …… a batch of transactions. 5. Employee social security numbers could be added to produce a control total …… the input preparation of payroll documents. 6. Hardware controls are special checks built into the hardware to verify the accuracy …… computer processing. 7. Multiple read-write heads …… magnetic tape and disk devices check the accuracy of reading and recording activities. 8. Even authorized users may be restricted …… the use of certain devices, programs, and data files.

Keys: in, into, on, within, of, by, to, for.

Exercise 2. Form adverbs / adverbial phrases from adjectives in brackets and underline them:

1. Data entry is (frequent) monitored by the use of control totals.
2. Once data is entered (correct) into a computer system, it must be processed (proper).
3. Information products are transmitted to authorized users in a (timely) manner.
4. Output documents are (visual) verified by input/output control personnel.
5. Control totals on output are (usual) compared with control totals generated during the input and processing stages.
6. Access to the output of realtime processing systems is controlled, (typical), by security codes.
7. (Final), end users should be contacted for feedback on the quality of the output.

Exercise 3. Make questions for which the following words in bold type would be reasonable answers:

1. **Information system** controls are methods and devices that attempt to ensure **the accuracy, validity, and propriety of information system activities.**

2. **Information system controls are designed to** monitor and maintain the quality and security of the input, processing, output.

3. Input of source documents **can also be controlled by** registering them **in a logbook** when they are received by data entry personnel.

4. **Computer software** can include instructions to identify **incorrect, invalid, or improper input data** as **it enters the computer system**.

5. Data entry and other systems activities are **frequently** monitored **by the use of control totals.**

6. **Batch totals and hash totals** are other forms of control totals.

7. Processing controls are developed **to identify** errors in arithmetic calculations and **logical operations.**

8. Parity checks **are made to check** for the loss of the correct number of bits in every byte of data processed or transmitted **on a network**.

9. **The operating system** or other software checks the internal file labels **at the beginning and end** of disk files.

10. System security monitors are programs that **monitor the use of a computer system** and protect its resources from **unauthorized use, fraud, and destruction**.

11. **Account codes, passwords, and other security codes** are frequently used to allow access to authorized users only.

Exercise 4. Translate the following into English:

электро́нная цифрова́я по́дпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Схема электронной подписи обычно включает в себя:

- алгоритм генерации ключевых пар пользователя;
- функцию вычисления подписи;
- функцию проверки подписи.

Следует различать электронную цифровую подпись и код аутентичности сообщения, несмотря на схожесть решаемых задач (обеспечение целостности документа и неотказуемости авторства). Алгоритмы ЭЦП относятся к классу асимметричных алгоритмов, в то время как коды аутентичности вычисляются по симметричным схемам.

Class Activity

Exercise 1. Make up a short oral summary of Information System Controls and Security Issues.

Text 3. FACILITY CONTROLS

Physical facility controls are methods that protect physical facilities and their contents from loss or destruction. Computer centers are subject to such hazards as accidents, natural disasters, sabotage, vandalism, unauthorized use, industrial espionage, destruction, and theft of resources. Therefore, physical safeguards and various control procedures are necessary to protect the hardware, software, and vital data resources of computer-using organizations.

Encryption of data and the use of fire wall computers have become important ways to protect computer network resources. Passwords, messages, files, and other data can be transmitted in scrambled form and unscrambled by computer systems for authorized users only. This process is called encryption. Typically, it involves using a special mathematical algorithm, or key, to transform digital data into a scrambled code before it is transmitted, and to decode the data when it is received. Special microprocessors and software packages can be used for the encryption process. There are several competing encryption standards, including DES (Data Encryption Standard), RSA (by RSA Data Security), and the Skipjack algorithm of the U.S. government's proposed Clipper encryption microprocessor chip. See Figure12.

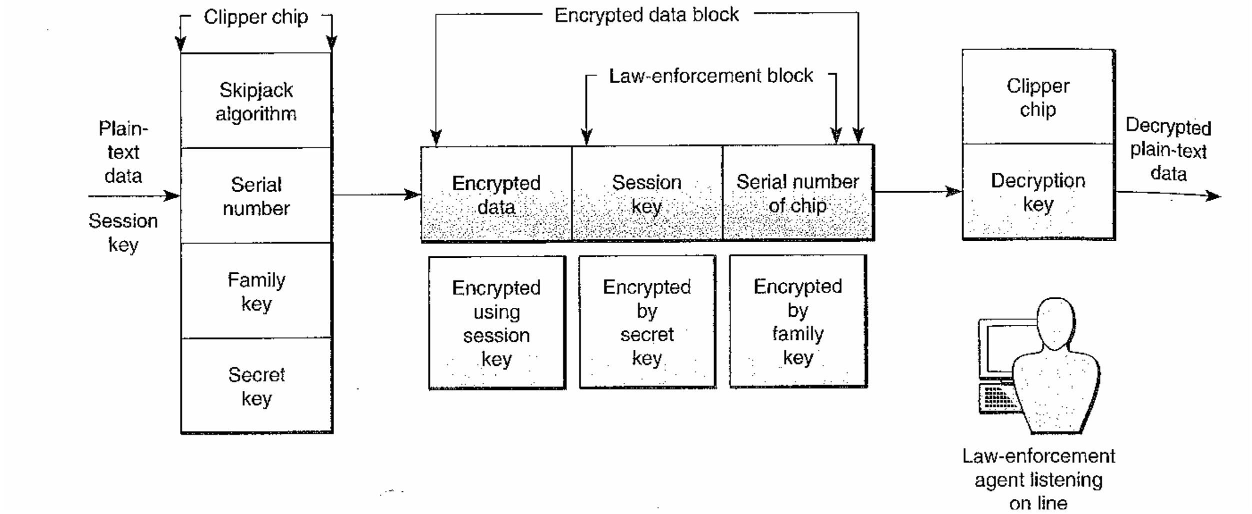


FIGURE 12. The encryption process of the controversial Clipper chip proposed by U.S. government. The Clipper microprocessor would allow law enforcement surveillance of encrypted data transmissions and files.

Another important method for control and security of telecommunications networks are **fire wall** computers. A network fire wall is a computer that protects computer networks from intrusion by serving as a safe transfer point for access to and from other networks. It screens all network traffic, and only allows authorized transmissions in and out of the network. Fire walls have become an essential component of organizations connecting to the Internet, because of its vulnerability and lack of security. Figure 13 illustrates the Internet fire wall system of AT&T.

Fire walls can deter, but not completely prevent, unauthorized access (hacking) into computer networks. In some cases, a fire wall may allow access only from trusted locations on the internet to particular computers inside the fire wall. Or it may allow only "safe" information to pass. For example, a fire wall may permit users to read E-mail from remote locations but not to run certain programs. In other cases, it is impossible to distinguish safe use of a particular network service from unsafe use and so all requests must be blocked. The fire wall may then provide substitutes for some network services (such as E-mail or file transfer) that perform most of the same functions but are not as vulnerable to penetration.

Providing maximum security and disaster protection for a computer installation requires many types of controls. Only authorized personnel are allowed access to the computer center through such techniques as **identification badges** for information services personnel, electronic door locks, burglar alarms, security police, closed-circuit TV, and other detection systems. The computer center should be protected from disaster by such safeguards as fire detection and extinguishing systems; fireproof storage vaults for the protection of files; emergency power systems; electromagnetic shielding; and temperature, humidity, and dust control.

Biometric controls are a fast-growing area of computer security. These are security measures provided by computer devices which measure physical traits that make each individual unique. This includes voice verification, fingerprints, hand geometry, signature dynamics, keystroke analysis, retina scanning, face recognition, and genetic pattern analysis. Biometric control devices use special-purpose sensors to measure and digitize a *biometric profile* of an individual's fingerprints, voice, or other physical trait. The digitized signal is processed and compared to a previously processed profile of the individual stored on magnetic disk. If the profiles match, the individual is allowed entry into a computer facility or given access to information system resources.

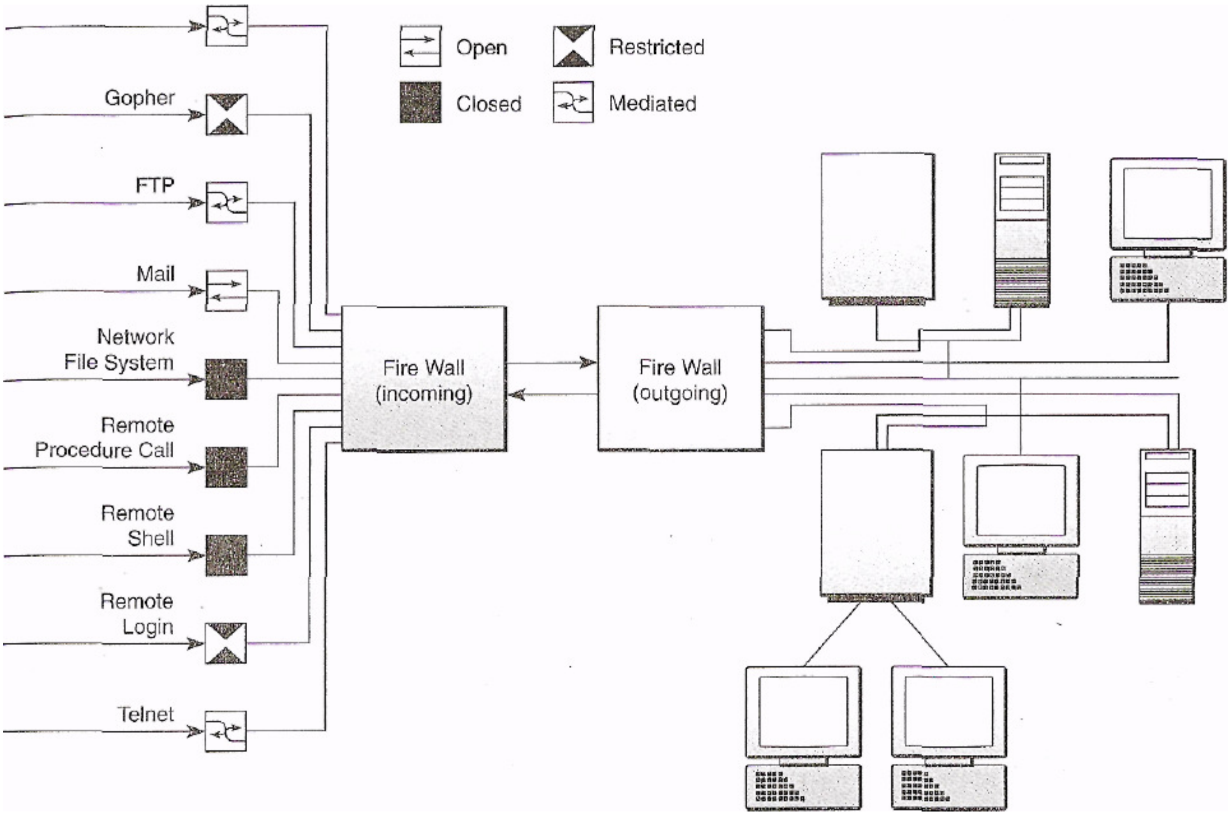


FIGURE 13. AT&T's Internet fire wall system

Layer	Threats	Fault Tolerant Methods
Applications	Environment, hardware and software faults	Application-specific redundancy and rollback to previous checkpoint
Systems	Outages	System isolation, data security, system integrity
Databases	Data errors	Separation of transactions and safe updates, complete transaction histories, backup files
Networks	Transmission errors	Reliable controllers; safe asynchrony and handshaking; alternative routing; error-detecting and error-correcting codes
Processes	Hardware and software faults	Alternative computations, rollback to checkpoints
Files	Media errors	Replication of critical data on different media and sites; archiving, backup, retrieval
Processors	Hardware faults	Instruction retry; error-correcting codes in memory and processing; replication; multiple processors and memories

FIGURE 14.Methods of fault tolerance in computer-based information systems

A variety of controls are needed to prevent a computer failure or minimize its effects. Computers fail for several reasons—power failure, electronic circuitry malfunctions, mechanical malfunctions of peripheral equipment, hidden programming errors, and computer operator errors. The information services department, typically, takes steps to prevent equipment failure and to minimize its detrimental effects. For example, computers with automatic and remote maintenance capabilities may be acquired. A program of preventive maintenance of hardware may be established. Adequate electrical supply, air conditioning, humidity control, and fire prevention standards must also be set. A backup computer system capability may be arranged with other computer-using organizations. Major hardware or software changes should be carefully scheduled and implemented to avoid problems. Finally, computer operators should have adequate training and supervision.

Many firms also use **fault tolerant** computer systems to ensure against computer failure. These systems have multiple central processors, peripherals, and system software. This may provide a *fail-safe* capability where the computer system continues to operate at the same level even if there is a major hardware or software failure. However, many fault tolerant computer systems offer *a fail-soft* capability where the computer system can continue to operate at a reduced but acceptable level in the event of a major system failure. Figure 14 outlines some of the fault tolerant capabilities used in many computer systems and networks.

(From James A.O'Brien. Management Information Systems)

List of words and expressions

hazard – риск, опасность
disaster – катастрофа
physical safeguards – физические меры безопасности
controversial – спорный
surveillance – надзор, наблюдение
Clipper chip – чип Клипера (название чипа для криптографической защиты информации)
session key – сеансовый (криптографический) ключ (действующий только в одном сеансе передачи сообщений)
enforcement – осуществление
fire wall – брандмауэр
scrambled code – скремблированный код
intrusion – проникновение, внедрение
transfer point – пункт передачи (данных)
to screen – показывать на экране
vulnerability – уязвимость
to deter – удерживать, помешать
hacking – взлом (хакерство)
substitute – замена
identification badge – идентификационный (опознавательный) знак (значок)
vault – хранилище
electromagnetic shielding – электромагнитное экранирование
physical trait – физическая особенность
fingerprint – отпечаток пальца
keystroke analysis – анализ нажатия кнопки
retina scanning – сканирование сетчатки (глаза)
biometric profile – биометрическое очертание

detrimental effect – вредное воздействие
backup computer system – дублирующая (резервная) компьютерная система
fault tolerant – устойчивый к повреждениям (ошибкам)
fail-safe capability – способность обеспечения надежности системы при отказе отдельных элементов

Exercises

Comprehension Check

Exercise 1. Ask your own questions to the text

Exercise 2. Read and translate the following equivalents:

physical facility controls, to protect contents from loss or destruction, to be subject to, hazards, natural disasters, sabotage, vandalism, unauthorized use, industrial espionage, destruction, theft of resources, encryption of data, the use of a fire wall, to protect computer network resources, to be transmitted in scrambled form, special mathematical algorithm, to transform digital data into a scrambled code, several competing encryption standards, a safe transfer point for access to and from other networks, to screen all network traffic, to protect computer networks from intrusion, because of its vulnerability, to deter, to distinguish safe use of a particular network service from unsafe use, penetration, electronic door locks, identification badges, fire detection and extinguishing systems, closed-circuit TV, fireproof storage vaults for the protection of files, electromagnetic shielding and temperature, humidity, dust control, biometric controls, voice verification, retina scanning; digitize a biometric profile of an individual's fingerprints, voice, or other physical trait; power failure, electronic circuitry malfunctions, mechanical malfunctions of peripheral equipment, hidden programming errors, a backup computer system capability, fault tolerant computer systems, to have multiple central processors, to provide a fail-safe capability.

Exercise 3. Read the text. Try to remember the main points. Retell it

Firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized zone (DMZ).

A firewall's function within a network is similar to firewalls with fire doors in building construction. In the former case, it is used to prevent network intrusion to the private network. In the latter case, it is intended to contain and delay structural fire from spreading to adjacent structures.

Without proper configuration, a firewall can often become worthless. Standard security practices dictate a "default-deny" firewall rule set, in which the only network connections which are allowed are the ones that have been explicitly allowed. Unfortunately, such a configuration requires detailed understanding of the network applications and endpoints required for the organization's day-to-day operation. Many businesses lack such understanding, and therefore implement a "default-allow" rule set, in which all traffic is allowed unless it has been specifically blocked. This configuration makes inadvertent network connections and system compromise much more likely.

Language Work

Exercise 1. Translate the following sentences paying attention to linking expressions:

1. Therefore, physical safeguards are necessary to protect the hardware, software, and vital data resources of computer-using organizations.
2. In addition, periodic audits by external auditors from professional accounting firms are a good business practice.
3. Finally, a production control section may monitor the progress of information processing jobs, data entry activities, and the quality of input/output data.
4. However, many fault tolerant computer systems offer a fail-soft capability.
5. In addition, the responsibility for maintaining a library of data files and program files is assigned to a librarian or database administrator.
6. For example, a fire wall may permit users to read E-mail from remote locations.

Exercise 2. Which of the underlined linking expressions in Exercise 1:

a) introduces a contrasting idea?

b) introduces a conclusion?

Exercise 3. Choose the best alternatives in the following sentences:

1. All managers must / can't accept the responsibility for managing the information system resources.
2. Passwords, messages and files can / must be transmitted in scrambled form and unscrambled by computer systems.
3. Special microprocessors and software packages couldn't / can be used for encryption process.
4. Procedures should / might tell employees what to do differently when their computers are not working.
5. The computer centre mustn't / should be protected from disaster by safeguards.
6. Computer operators should / can't have adequate training and supervision.
7. Humidity control and fire prevention standards can't / must also be set.
8. Many firms could / must survive only a few days without computing facilities.

Class Activity

Exercise 1. Discuss the advantages of methods of physical facility controls

Unit IV. INFORMATION THEORY

Text 1. INFORMATION THEORY

Information theory is a discipline in applied mathematics involving the quantification of data with the goal of enabling as much data as possible to be reliably stored on a medium and/or communicated over a channel. The measure of data, known as information entropy, is usually expressed by the average number of bits needed for storage or communication. For example, if a daily weather description has 3 bits of entropy, then, over enough days, we can describe daily weather with an *average* of approximately 3 bits per day (each bit being a 0 or a 1).

Applications of fundamental topics of information theory include ZIP files (lossless data compression), MP3s (lossy data compression), and DSL (channel coding). The field is at the crossroads of mathematics, statistics, computer science, physics and electrical engineering, and its impact has been crucial to success of the Voyager missions to deep space, the invention of the CD, the feasibility of mobile phones, the development of the Internet, the study of linguistics and of human perception, the understanding of black holes, and numerous other fields.

The main concepts of information theory can be grasped by considering the most widespread means of human communication: language. Two important aspects of a good language are as follows: First, the most common words (e.g., "a," "the," "I") should be shorter than less common words (e.g., "benefit," "generation," "mediocre"), so that sentences will not be too long. Such a tradeoff in word length is analogous to data compression and is the essential aspect of source coding. Second, if part of a sentence is unheard or misheard due to noise — e.g., a passing car — the listener should still be able to glean the meaning of the underlying message. Such robustness is as essential for an electronic communication system as it is for a language; properly building such robustness into communications is done by channel coding. Source coding and channel coding are the fundamental concerns of information theory.

Note that these concerns have nothing to do with the *importance* of messages. Information theory, however, does not involve message importance or meaning, as these are matters of the quality of data rather than the quantity of data, the latter of which is determined solely by probabilities.

Information theory is generally considered to have been founded in 1948 by Claude Shannon in his seminal work, "A Mathematical Theory of Communication." The central paradigm of classic information theory is the engineering problem of the transmission of information over a noisy channel. The most fundamental results of this theory are Shannon's source coding theorem, which establishes that, on average, the number of *bits* needed to represent the result of an uncertain event is given by its entropy; and Shannon's noisy-channel coding theorem, which states that *reliable* communication is possible over *noisy* channels provided that the rate of communication is below a certain threshold called the channel capacity. The channel capacity can be approached by using appropriate encoding and decoding systems.

Information theory is closely associated with a collection of pure and applied disciplines that have been investigated and reduced to engineering practice under a variety of rubrics throughout the world over the past half century or more: adaptive systems, anticipatory systems, artificial intelligence, complex systems, complexity science, cybernetics, informatics, machine learning, along with systems sciences of many descriptions. Information theory is a broad and deep mathematical theory, with equally broad and deep applications, amongst which is the vital field of coding theory.

Coding theory is concerned with finding explicit methods, called *codes*, of increasing the efficiency and reducing the net error rate of data communication over a noisy channel to near the limit that Shannon proved is the maximum possible for that channel. These codes can be roughly subdivided into data compression (source coding) and error-correction (channel coding) techniques. In the latter case, it took many years to find the methods Shannon's work proved were possible. A third class of information theory codes are cryptographic algorithms (both codes and ciphers). Concepts, methods and results from coding theory and information theory are widely used in cryptography and cryptanalysis.

(From http://en.wikipedia)

<u>List of words and expressions</u>

quantification – определение количества

information entropy – информационная энтропия

ZIP (Zone Improvement Plan) – стандарт сжатия файлов и формат архивов (разработчик – Фил Катц (Phil Katz)

data compression – уплотнение данных; сжатие данных

lossy – с потерями

DSL (Digital Subscriber Line) – абонентская цифровая линия

to be crucial – быть решающим

perception – понимание; восприятие

to grasp – понять; схватывать

tradeoff – замена

to be unheard – быть не услышанным

to glean – тщательно подбирать

robustness – трудность

seminal work – основополагающая работа

threshold – порог

channel capacity – пропускная способность канала связи

rubric – заголовок, рубрика

adaptive systems – приспосабливаемые системы

anticipatory systems – предупреждающие системы

complexity science – наука о комплексности

explicit – ясный, точный, определенный

net error rate – частота появления ошибок в сети

cipher – шифр

feasibility – выполняемость

to near – приближаться к …

МР- *сокр., комп.* Mandatory Protection; Memory Pointer; Minimal Protection

сеть. multiprocessing; system multiprocessor system; мультипроцессорная обработка

матем. наиболее мощный (критерий); математическое программирование (mathematical programming); мультипликативное свойство (multiplication property); проблема минимизации (minimization problem)

Comprehension Check

Exercise 1. Ask your own problem questions to the text

Exercise 2. What's the English for the following expressions:

информационная теория, прикладная математика, цель, передавать данные по каналу связи, энтропия, в среднем, приблизительно, применение фундаментальных аспектов информационной теории, сжатие данных, на пересечении математики и физики, развитие Интернета, изучение человеческого восприятия, обычные слова, понять значение основного сообщения, кодирование канала, только, определяться, надежная связь, пропускная способность канала связи, может быть получена, соответствующие системы кодирования и декодирования, искусственный интеллект, жизненно важная область изучения, криптографические алгоритмы, криптоанализ.

Exercise 3. Complete the statements using words from the box:

average coding bit probability channels maximized fundamental

1. The mathematical theory of information is based on …… theory and statistics.

2. The measure of data is usually expressed by the …… number of bits needed for storage or communication.

3. The most …… results of this theory are Shannon's source coding theorem.

4. Reliable communication is possible over noisy …… .

5. …… theory is concerned with finding explicit methods.

6. An important property of entropy is that it is …… when all the messages in the message space are equiprobable.

7. The most common unit of information currently in use is the …… .

Language Work

Exercise 1. Put the nouns below into three groups:

a) countable b) uncountable c) countable or uncountable

theory, entropy, compression, information, bit, mathematics, file, statistics, intelligence, importance, communication.

Exercise 2. Translate the following sentences into English:

1. Теория информации связана с информационной энтропией, коммуникационными системами, передачей данных и теорией скорости искажения, криптографией, сжатием данных, коррекцией ошибок и другими смежными областями.

2. Клод Элвуд Шеннон (англ. Claude Elwood Shannon) – американский математик и электротехник, один из создателей математической теории информации.

3. Шеннон предопределил своими результатами развитие общей теории дискретных автоматов, которые являются важными составляющими кибернетики.

4. Алгоритм Шеннона-Фано – один из первых алгоритмов сжатия, который впервые сформулировали американские учёные Шеннон и Фано.

5. Данный метод сжатия имеет большое сходство с алгоритмом Хоффмана, которое появилось на несколько лет позже.

6. Алгоритм использует коды переменной длины: часто встречающийся символ кодируется кодом меньшей длины, редко встречающийся — кодом большей длины.

7. Коды Шеннона-Фано префиксные, то есть, никакое кодовое слово не является префиксом любого другого.

8. Данное свойство позволяет однозначно декодировать любую последовательность кодовых слов.

(From Wikipedia)

Exercise 3. Match the words with their meaning. Make up your own sentences:

Applied	**A** An optical disk approximately 4 ¾ in(12 cm) in diameter, on which a program, data, music, etc. is digitally encoded for a laser beam to scan, decode, and transmit to a playback system, computer monitor or television set.
Goal	**B** A measure of the loss of information in a transmitted signal or message.
entropy	**C** The art or science of making practical application of the knowledge of pure sciences as physics or chemistry.
compression	**D** The act of apprehending by means of the senses or mind.
perception	**E** The act of compressing.
CD	**F** Very many; being or existing in greater quantity.
engineering	**G** The result of achievement toward which effort is directed, aim, end.
numerous	**H** To realize beforehand, foretaste or foresee, to expect, to look forward.
Seminal	**I** Having a practical purpose or use; derived from or involved with actual phenomena.
Anticipate	**J** Highly original and influencing the development of future events.

Class Activity

Exercise 1. Discuss these questions:

1. Why can the main concepts of information theory be grasped by considering the most widespread means of human communication: language?
2. What do you know about source coding and channel coding?

Text 2. CODING THEORY

Coding theory is the most important and direct application of information theory. It can be subdivided into data compression theory and error correction theory. Using a statistical description for data, information theory quantifies the number of bits needed to describe the data. There are two formulations for the compression problem – in lossless data compression the data must be reconstructed exactly, whereas lossy data compression examines how many bits are needed to reconstruct the data to within a specified fidelity level. This fidelity level is measured by a function called a distortion function. In information theory this is called rate distortion theory. Both lossless and lossy source codes produce bits at the output which can be used as the inputs to the channel codes mentioned above.

The idea is to first compress the data, i.e. remove as much of its redundancy as possible, and then add just the right kind of redundancy (i.e. error correction) needed to transmit the data efficiently and faithfully across a noisy channel.

This division of coding theory into compression and transmission is justified by the information transmission theorems, or source-channel separation theorems that justify the use of bits as the universal currency for information in many contexts. However, these theorems only hold in the situation where one transmitting user wishes to communicate to one receiving user. In scenarios with more than one transmitter (the multiple-access channel), more than one receiver (the broadcast channel) or intermediary "helpers" (the relay channel), or more general networks, compression followed by transmission may no longer be optimal. Network information theory refers to these multi-agent communication models.

(From http://en.wikipedia)

List of words and expressions

to subdivide into – подразделять на …
error correction – исправление ошибок
to quantify – определять количество
lossless data compression – уплотнение данных без потерь
lossy data compression – уплотнение данных с потерями
fidelity level – уровень точности воспроизведения
distortion function – функция искажения
rate distortion – частотное искажение
redundancy – избыточность
faithfully – верно, точно
to justify – подтверждать
source-channel separation – классификация канала источника
multiple-access channel – канал группового доступа
broadcast channel – радиовещательный канал
relay channel – радиорелейный канал
multi-agent communication – связь между мультисредами

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What theory is the most important and direct application of information theory? 2. What can coding theory be divided into? 3. How does information theory quantify the number of bits needed to describe the data? 4. How many formulations are there for the compression problem? 5. What does lossy data compression examine? 6. What is the fidelity level measured by? 7. Where do both lossless and lossy source codes produce bits? 8. What theorems is the division of coding theory into compression and transmission justified by? 9. Which situation do these theorems hold in? 10. What models does network information theory refer to?

Exercise 2. Translate the following equivalents from the text. Find the sentences with them. Translate the idea, not word by word:

Coding theory, direct application, to be subdivided into, error correction, to quantify, lossless data compression, to reconstruct, a specified fidelity level, a distortion, redundancy, efficiently and faithfully, a noisy channel, compression and transmission, to justify, theorems, multiple access channel, multi agent communications models.

Language Work

Exercise 1. Complete the sentences with the correct preposition:

1. …… information theory this is called rate distortion theory.

2. Coding theory can be subdivided …… data compression theory and error correction theory.

3. …… these constraints, we would like to maximize the amount of information.

4. This capacity has the following property related to communicating …… information rate R.

5. The mathematical theory of information is based …… probability theory and statistics.

6. The erasure represents complete loss …… information about an input bit.

7. The rate of a source of information is related …… its redundancy and how well it can be compressed.

Exercise 2. Find the corresponding ending of each sentence:

1. Coding theory	**A** refers to these multi-agent communication models.
2. This fidelity level	**B** only hold in the situation where one transmitting user wishes to communicate to one receiving user.
3. Both lossless and lossy source codes	**C** is to first compress the data.
4. The idea	**D** is the most important and direct application of information theory.
5. This division of coding theory into compression and transmission	**E** is justified by the information transmission theorems, or source-channel separation theorems.
6. These theorems	**F** produce bits at the output which can be used as the inputs to the channel codes mentioned above.
7. Network information theory	**G** is measured by a function called a distortion function.

Exercise 3. Translate the following into English:

– Теорема отсчётов Уиттакера-Найквиста-Котельникова-Шеннона (*теоре́ма Коте́льникова*) гласит, что, если непрерывный сигнал $x(t)$ имеет спектр, ограниченный частотой F_{max}, то он может быть однозначно и без потерь восстановлен по своим дискретным отсчётам, взятым с частотой:

$$f_{\text{дискр}} < 2 \cdot F_{\max},$$

где $F_{\max}$ – верхняя частота в спектре, или, по-другому, по отсчётам, взятым с периодом:

$$T_{\text{дискр}} < 1/(2 \cdot F_{\max}).$$

Теорема была сформулирована В. А. Котельниковым в 1933 году в его работе «О пропускной способности эфира и проволоки в электросвязи» и является одной из основополагающих теорем в теории и технике цифровой связи.

– Элементарный цифровой канал телефонной сети – 64000 бит/с. Диапазон частот, в который помещается голос человека, составляет 300-3400 Гц. Для дискретизации по теореме Котельникова необходимо удвоить частоту 3400 Гц, получаем 6800 Гц. Далее 1200 Гц выделяется под служебное использование. 11 шагов квантования необходимо сделать, чтобы не потерять качество речи, но благодаря особенностям человеческого слуха это число сократили до 8 с помощью операции компандирования. В итоге получается 8000 × 8 = 64000 бит/с.

(From Wikipedia)

Discussion
Exercise 1. Speak on the compression problem

Text 3. APPLICATIONS OF INFORMATION THEORY

Information theoretic concepts are widely used in making and breaking cryptographic systems. Shannon himself defined an important concept now called the unicity distance. Based on the redundancy of the plaintext, it attempts to give a minimum amount of ciphertext necessary to ensure unique decipherability.

Shannon's theory of information is extremely important in intelligence work, much more so than its use in cryptography would indicate. The theory is applied by intelligence agencies to keep classified information secret, and to discover as much information as possible about an adversary. The fundamental theorem leads us to believe it is much more difficult to keep secrets than it might first appear. In general it is not possible to stop the leakage of classified information, only to slow it. Furthermore, the more people who have access to the information, and the more those people have to work with and review that information, the greater the redundancy that information acquires. It is extremely hard to contain the flow of information that has high redundancy. This inevitable leakage of classified information is due to the psychological fact that what people know does somewhat influence their behavior, however subtle that influence might be.

A good example of the application of information theory to covert signaling is the design of the Global Positioning System signal encoding. The system uses a pseudorandom encoding that places the radio signal below the noise floor. Thus, an unsuspecting radio listener would not *even be aware that there was a signal present*, as it would be drowned out by assorted noise sources (eg, atmospheric and antenna noise). However, if one integrates the signal over long periods of time, using the "secret" (but known to the listener) pseudorandom sequence, one can eventually detect a signal, and then discern modulations of that signal. In the GPS system, the C/A signal has been publicly disclosed to be a 1023-bit sequence, but the pseudorandom sequence used in the P(Y) signal remains a secret. The same technique can be used to transmit and receive covert intelligence from short-range, extremely low power systems, without an Enemy even being aware of the existence of a radio signal. This is analogous to steganography.

(From http://en.wikipedia)

List of words and expressions

unicity distance [ju:’nɪsɪtɪ] – единичное расстояние
plaintext – открытый текст, незашифрованный текст
ciphertext – зашифрованный текст, шифротекст
unique decipherability – однозначная расшифруемость
to indicate – обозначать, показать

adversary – нарушитель

inevitable leakage [ɪn’evɪtəbl] – неизбежная утечка

subtle – едва различимый

global positioning system – глобальная (спутниковая) система местоопределения; система глобального позиционирования

pseudorandom encoding – псевдослучайное кодирование

noise floor – минимальный уровень шума

to be drowned out – пересиливаться, заглушаться

to disclose – обнаруживать

pseudorandom sequence – последовательность псевдослучайных чисел; псевдослучайная последовательность

steganography – стеганография

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What is widely used in cryptographic systems? 2. What did Shannon define? 3. What is unicity distance concept based on? 4. Shannon's theory of information is extremely important in intelligence work, isn’t it? 5. How is the theory applied? 6. What does the fundamental theorem lead us to believe? 7. Is it possible to stop the leakage of classified information? Why? 8. What is a good example of the application of information theory? 9. What does the system use? 10. What technique can be used to transmit and receive covert intelligence from short-range, extremely low power systems? 11. Is this analogous to steganography?

Exercise 2. Outline the main ideas of the text and write a summary

Language Work

Exercise 1. Complete the following sentences using a relative pronoun (who, which, that):

1. The more people …… have access to the information, the greater the redundancy that information acquires.
2. The choice of logarithmic base in the following formulae determines the unit of information entropy …… is used.
3. It is extremely hard to contain the flow of information …… has high redundancy.
4. The system uses a pseudorandom encoding …… places the radio signal below the noise floor.
5. The mutual information of X is relative to Y …… represents conceptually the average amount of information about X.
6. A memoryless source is one in …… each message is an independent identically-distributed random variable.
7. Shannon …… founded information theory in his seminal work stated noisy-channel coding theorem.

Exercise 2. Complete the following sentences using the proper verb form from the box:

is based can be considered are used can be used have been disclosed deals

1. Information theoretic concepts …… in making and breaking cryptographic systems.

2. Bit …… on the binary logarithm.

3. In the GPS system, the C/A signal …… to be a 1023-bit sequence.

4. Any process that generates successive messages …… a source of information.

5. Information technology …… with the use of electronic computer and computer software to convert, store, protect, process, transmit and retrieve information.

6. The same technique …… to transmit and receive covert intelligence from short-range, low power stations.

Exercise 3. Translate the following into English

1. Компьютеры представляют сейчас или будут представлять в ближайшем будущем опасную угрозу тайне частной жизни.

2. Многие компьютеры содержат персональные данные и доступны через удаленные терминалы, они являются непревзойденным средством накопления больших массивов информации об отдельных людях и группах людей.

3. Компьютерные системы могут быть приспособлены к защите хранящейся на них информации от всех людей, за исключением, тех, кому разрешен доступ к ним, путем зашифрования данных в формы, весьма устойчивые к попыткам взлома.

4. Криптографическое зашифрование может быть достигнуто двумя совершенно различными путями: с помощью шифров и с помощью кодов.

5. Шифр всегда определяет символы подстановки для некоторого заданного набора букв алфавита.

6. С помощью кода можно выразить только то, что было обдумано заранее и предусмотрено для передачи в виде секретного списка, такого, например, как кодовая книга.

7. В наше время слово "код" имеет широкий смысл – говорят о кодах обнаружения и исправления ошибок, кодах сжатия данных, телекоммуникационных кодах, коммерческих кодах и кодах, включающих все виды замысловатых электрических сигналов и волновых форм.

8. Вся криптография сводится к подстановкам. В своей простейшей форме подстановка может быть задана с помощью таблицы.

9. Двоичная система счисления, содержащая ровно две цифры, 0 и 1, идеально подходит для криптографического преобразования данных компьютерами.

10. Перевод в двоичную систему – необходимая в компьютерной криптографии операция. Например, двоичный шифр подстановки состоит из, первое, перевода каждой буквы алфавита в пятицифровое двоичное число, и, второе, из зашифрования двоичного эквивалента.

Class Activity

Exercise 1. Collect all the material about information theory and discuss the problems of its present-day applications

Unit V. ALGEBRAIC ALGORITHMS & STRUCTURES

Text 1. COMPUTER SOFTWARE IN SCIENCE AND MATHEMATICS

> Computation offers a new means of describing and investigating scientific and mathematical systems. Simulation by computer may be the only way to predict how certain complicated systems evolve.
>
> Stephen Wolfram

Scientific laws give algorithms, or procedures for determining how systems behave. The computer program is a medium in which the algorithms can be expressed and applied. Physical objects and mathematical structures can be represented as numbers and symbols in a computer, and a program can be written to manipulate them according to the algorithms. When the computer program is executed, it causes the numbers and symbols to be modified in the way specified by the scientific laws. It thereby allows the consequences of the laws to be deduced.

Executing a computer program is much like performing an experiment. Unlike the physical objects in a conventional experiment, however, the objects in a computer experiment are not bound by the laws of nature. Instead they follow the laws embodied in the computer program, which can be of any consistent form. Computation thus extends the realm of experimental science: it allows experiments to be performed in a hypothetical universe. Computation also extends theoretical science. Scientific laws have conventionally been constructed in terms of a particular set of mathematical functions and constructs, and they have often been developed as much for their mathematical simplicity as for their capacity to model the salient features of a phenomenon. A scientific law specified by an algorithm, however, can have any consistent form. The study of many complex systems, which have resisted analysis by traditional mathematical methods, is consequently being made possible through computer experiments and computer models. Computation is emerging as a major new approach to science, supplementing the long-standing methodologies of theory and experiment.

For example, the magnetic field under investigation is specified by a set of numbers stored in a computer. The computer program applies an algorithm that simulates the motion of the electron by changing the numbers representing its position at successive times. Computers are now fast enough for the simulations to be carried out quickly, and so it is practical to explore a large number of cases. The investigator can interact directly with the computer, modifying various aspects of a phenomenon as new results are obtained. The usual cycle of the scientific method, in which hypotheses are formulated and then tested, can be followed much faster with the aid of the computer.

(www.stephenwolfram.com/publications/articles/general/)

List of words and expressions

simulation – моделирование; имитация; имитационное моделирование
to predict – предсказывать
complicated system – сложная система
procedure – программа-процедура; методика; порядок действий
to manipulate – обрабатывать; управлять

to deduce – выводить
embodied – реализованный; воплощенный
consistent – совместимый; согласованный; последовательный
realm – область, сфера
salient [‘seıljənt] – характерный
to resist – не поддаваться

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What is the computer program? 2. How can physical objects and mathematical structures be represented? 3. What causes the numbers and symbols to be modified in the way specified by the scientific laws? 4. Is executing a computer program like performing an experiment? Why? 5. What terms have scientific laws conventionally been constructed in? 6. What is the study of many complex systems being made possible through? 7. What are the advantages of simulation with the help of computers? 8. What can you say about peculiarities of executing a computer program?

Exercise 2. Read the text and translate the following equivalents:

scientific laws, procedures, to determine, a medium, physical objects, mathematical structures, to be executed, to be modified, specified by, consequences, to be deduced, to execute a computer program, to perform an experiment, unlike, conventional experiment, to be bound by, instead, consistent form, computation, to extend, realm, conventionally, constructs, simplicity, capacity, the salient features of a phenomenon, specified by, to emerge as a major new approach to science, to supplement, the magnetic field, to be carried out quickly, to interact.

Exercise 3. Find in the text the sentences corresponding to their Russian equivalents given below:

1. Выполнение программы для компьютера приводит к изменению чисел и символов в соответствии с научными законами. 2. Таким образом, вычисление расширяет сферу экспериментальной науки: оно позволяет проводить эксперименты в гипотетической области. 3. Изучение многих сложных систем, которые не поддавались исследованию традиционными математическими методами, становится невозможным с использованием компьютерных экспериментов и моделей. 4. Современные компьютеры обладают достаточным быстродействием, поэтому возможно изучение большого числа случаев.

Exercise 4. Translate the following definitions and memorize them

Program: A series of instructions or statements in a form acceptable to a computer, prepared in order to achieve a certain result.

Model: A mathematical representation of a process, device or concept.

Simulation: The representation of certain features of the behavior of a physical or abstract system; or a computer program that models a real situation.

Language Work

Exercise 1. Put the verbs in brackets into the Present Perfect tense (Active or Passive):

1. Many complex systems (to resist), analysis by traditional mathematical methods. 2. Many scientific calculations (to do) by conventional mathematical means. 3. The computer program (to apply) in both cases. 4. The numbers and symbols (to modify) in the way specified by the scientific laws. 5. They (to construct) already scientific laws in terms of a particular set of mathematical functions. 6. This mathematical structure (to represent) as numbers and symbols recently.

Exercise 2. Make the following sentences Passive:

1. When the computer program is executed, it causes the numbers and symbols **(to modify)** in the way specified by the scientific laws.
2. It thereby allows the consequences of the laws **(to deduce).**
3. The objects in a computer experiment are **(to bind)** by the laws of nature.
4. It allows experiments **(to perform)** in a hypothetical universe.
5. Scientific laws **(to construct)** conventionally in terms of a particular set of mathematical functions and constructs.
6. They **(to develop)** often as much for their mathematical simplicity as for their capacity to model the salient features of a phenomenon.
7. The magnetic field under investigation **(to specify)** by a set of numbers stored in a computer.
8. Computers are now fast enough for the simulations **(to carry out)** quickly, and so it is practical to explore a large number of cases.

Exercise 3. Ask questions to the parts of the sentence in bold:

1. **The computer program** is **a medium** in which the algorithms **can be expressed** and applied.
2. Physical objects and mathematical structures can be represented **as numbers and symbols in a computer.**
3. **Executing a computer program** is much **like performing an experiment.**
4. Computation thus **extends the realm** of experimental science.
5. **A scientific law** specified by an algorithm, however, **can have any consistent form.**
6. Computation **is emerging** as **a major new approach to science.**
7. For example, the magnetic field under investigation **is specified by a set of numbers stored in a computer.**
8. **Computers** are now fast enough for the simulations to be carried out **quickly.**
9. A program **can be written** to manipulate them **according to the algorithms**.
10. **A scientific law** specified by an algorithm, however, can have any consistent form.

Class Activity. Discussion

Exercise 1. Read the following text. Discuss its message

In developing an algorithm for computer algebra it is not necessary to follow the procedure that is most efficient in manual calculation. Delaunay proved several theorems that he then employed to simplify intermediate calculations. Although the theorems could be incorporated into a program, the effort necessary to express them in algorithmic form encouraged Deprit and his colleagues to search for a method more compatible with mechanized execution. The one they invented requires transformations that would have exceeded the abilities even of Delaunay, but the algorithm is easy to program and can be executed quickly with a computer. The development of new algorithms is one of the most active areas of investigation in computer algebra; it is largely because of such work that computer-algebra systems have been improved significantly in the past few years.

In order to represent an algebraic expression in a computer program, most systems seek to store the minimum information needed to specify the expression uniquely. Current representational schemes employ one of two basic approaches or a combination of the two. In one approach an expression is represented as an inverted treelike structure in which the leaves are the operands. For example, suppose one wished to represent the expression 2(x + 4) in a computer. The leaves of the tree would be the terms 2, x and 4, although they would appear at different levels. Both the x and the 4 would be connected by upward-moving branches to a plus sign. The symbol 2, however, would not be linked to the plus sign. Instead branches from the 2 and from the plus sign would meet at the top, or root, of the tree, which would be labeled with a multiplication sign. The representation makes more efficient the search for subordinate expressions of predetermined form.

In the second scheme "slots" are assigned in some definite order to represent the information carried by an expression. To represent a polynomial in one variable, for instance, one slot is assigned to the name of the variable, the next slot to the degree of the polynomial (the largest power of the variable that appears in the polynomial) and the following slots to the coefficients of descending powers of the variable. The set of information slots can be made a part of a tree-structure representation when more complicated expressions must be stored.

(From Richard Pavelle, Michael Rothstein and John Fitch "Computer Algebra")

Text 2. DATA STRUCTURES AND ALGORITHMS

> They are the basic elements of every computer program. The choice of data structures and the design of procedures to manipulate them hold the key to verifying that a program does what it is meant to do.
>
> *Niklaus Wirth*

Data structures and algorithms are the materials out of which programs are constructed. Furthermore, the computer itself consists of nothing other than structures and algorithms. The built-in data structures are the registers and memory words where binary values are stored; the hard-wired algorithms are the fixed rules, embodied in electronic logic circuits, by which stored data are interpreted as instructions to be executed. Thus at the most fundamental level a computer can work with only one kind of data, namely individual bits, or binary digits, and it can act on the data according to only one set of algorithms, those defined by the instruction set of the central processing unit.

The problems people undertake to solve with the aid of a computer are seldom expressed in terms of bits. Instead the data take the form of numbers, characters, texts, events, symbols and more elaborate structures such as sequences, lists and trees. The algorithms employed to solve the problems are even more varied; indeed, there are at least as many algorithms as there are computational problems. How can a vast spectrum of problems be solved by a single machine that always acts according to fixed rules? The explanation is that the computer is a truly general-purpose device, whose nature can be transformed altogether by the program given it. The underlying principle was first set forth by John von Neumann. A stream of information is at one moment data being processed by a program, and at the next moment the same information is interpreted as a program in its own right. Hence a program is formulated in terms of familiar notions convenient to the problem at hand; then another program, called an assembler or a compiler, maps those notions onto the facilities available in the computer.

In this way it is possible to construct systems of extraordinary complexity. The programmer sets up a hierarchy of abstractions, viewing the program first in broad outline and then attending to one part at a time while ignoring the internal details of other parts. The process of abstraction is not merely a convenience; it is a necessity, because programs of more than trivial size simply could not be created if one had to work with an undifferentiated, homogeneous mass of bits. Without higher level abstractions a program could not be understood fully even by its creator.

Among the facilities provided by almost all programming languages is the ability to refer to an item of data by assigning it a name, or identifier. Some of the named quantities are constants, which have the same value throughout the segment of the program in which they are defined; for example, *pi* might be assigned the value 3.14159. Other named quantities are variables, which can be assigned a new value by statements within the program, so that their value cannot be known until the program is run. The variables *diameter* and *circumference* might take on new values each time a calculation is done.

The name of a constant or a variable is a mnemonic aid to the programmer, but it has no meaning to the computer. The compiler that translates a program text into binary code merely associates each identifier with an address in memory. If an instruction calls for multiplying *diameter* by *pi,* the computer fetches whatever numbers are stored at the specified addresses and calculates the product; if the result is to become the new value of *circumference,* it is stored in memory at the address corresponding to that label.

The naming of constants and variables in programming is similar to the use of symbolic expressions in algebra, but for a computer to handle the process some additional information must be supplied. The information gives the «type» of each named quantity. A person working a problem by hand has an intuitive grasp of data types and the operations that are valid for each type; it is known, for example, that one cannot take the square root of a word or capitalize a number. One reason such distinctions are easily made is that words, numbers and various other symbols are represented quite differently. For the computer, however, all types of data ultimately resolve into a sequence of bits, and the type distinctions must be made explicit.

Suppose in the course of some operation the seven-bit binary value 1010011 has been read into a register in the central processing unit of a computer. How is the value to be interpreted? One possibility is that it represents a cardinal, or counting, number, in which case the equivalent in decimal notation would *be* 83. In many programming languages the value could also represent a signed integer equal to decimal — 45. The same binary data could encode not a number but a character; in the American Standard Code for Information Interchange (ASCII) binary 1010011 specifies the letter S. Several other possibilities exist. (Indeed, the binary code might not be data at all but an instruction to the computer; its interpretation would then depend on the particular processor.)

The data types recognized by common programming languages include cardinal numbers, integers, real numbers (approximated as decimal fractions), sets, characters and strings of characters. Information on each variable's type is needed not only to interpret the binary representation but also to set aside the correct amount of space in storage. In many modern computer systems a single character is allocated eight bits, or one byte, of memory, whereas a cardinal or an integer might be given two or four bytes and a real number might take up as many as eight bytes.

(Niklaus Wirth , Algorithms & Data Structures , Prentice-Hall (1986), 288 pp.
akps.ssau.ru/forth/pattern/pat4th-h.html)

List of words and expressions

to verify – проверять, контролировать; верифицировать
hard-wired algorithm – аппаратно-реализованный алгоритм
to be executed – которые нужно исполнять
undertake to solve – отважиться решить
computational problem – вычислительная задача; вычислительная проблема
altogether – в общем; в целом
to set forth – излагать, формулировать
familiar notion – привычное представление
at hand – под рукой; доступный
at a time – сразу, одновременно
trivial – незначительный
to assign – присвоить
circumference – окружность; периметр
by hand – ручным способом, вручную
grasp – понимание
to capitalize – печатать или писать прописными буквами
explicit – точный, явный
cardinal – количественный; кардинальный
decimal notation – десятичная система счисления
integer – целое число
strings of characters – строки символов
to set aside – не принимать во внимание; пренебрегать
to allocate – распределять, размещать

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What are the built-in data structures? 2. Where are binary values stored? 3. How can a computer act? 4. What form do the data take? 5. How many algorithms are there? 6. Whom was the underlying principle first set forth by? 7. What terms is a program formulated in? 8. In which case couldn’t a program be understood fully? 9. Are some of the named quantities constants? 10. What do constants have? 11. What can you say about variables? 12. What does the compiler that translates a program text into binary code associate each identifier with? 13. What is the naming of constants and variables in programming similar to? 14. Does a person working a problem by hand have an intuitive grasp of data types? 15. What do the data types recognized by common programming languages include? 16. How many bits is a single character allocated in many modern computer systems?

Exercise 2. Read the text and translate the following equivalents. Use the equivalents to render the text:

basic elements, the choice of data structures, the design of procedures, to manipulate, to verify, algorithms, furthermore, the built-in data structures, registers, binary values, to be embodied in electronic logic circuits, to be executed, to be defined by the instruction set, central processing unit, to undertake, to solve problems, instead, characters, elaborate structures, algorithms, at least, computational problems, general-purpose device, to be set forth, to be interpreted, hence, familiar notions, convenient, extraordinary complexity, a hierarchy of abstractions, to view the program first in broad outline, internal details, undifferentiated, homogeneous mass of bits, to refer to an item of data, by assigning it a name, an identifier, variables, circumference, a mnemonic aid to the programmer, compiler, to fetch, distinctions, to ultimately resolve, to be made explicit, a cardinal number, in decimal notation, ASCII, to specify the letter, to depend on the particular processor, common programming languages, strings of characters, decimal fractions, binary representation, the correct amount of space in storage, to be allocated, an integer.

Exercise 3. Read the text. Use a dictionary to translate it. Ask 5 questions to the text in writing:

Why algorithms are necessary: an informal definition

No generally accepted *formal* definition of "algorithm" exists yet. We can, however, derive clues to the issues involved and an informal meaning of the word from the following quotation from Boolos & Jeffrey (1974, 1999) (boldface added):

No human being can write fast enough, or long enough, or small enough to list all members of an enumerably infinite set by writing out their names, one after another, in some notation. But humans can do something equally useful, in the case of certain enumerably infinite sets: They can give **explicit instructions for determining the nth member of the set**, for arbitrary finite n. Such instructions are to be given quite explicitly, in a form in which **they could be followed by a computing machine**, or by a **human who is capable of carrying out only very elementary operations on symbols** (Boolos & Jeffrey 1974, 1999, p. 19/From Wikipedia).

The words "enumerably infinite" mean "countable using integers perhaps extending to infinity". Thus Boolos and Jeffrey are saying that an algorithm *implies* instructions for a process that "creates" output integers from an *arbitrary* "input" integer or integers that, in theory, can be chosen from 0 to infinity. Thus we might expect an algorithm to be an algebraic equation such as **y = m + n** – two arbitrary "input variables" **m** and **n** that produce an output **y**. As we see in Algorithm characterizations – the word algorithm implies much more than this, something on the order of (for our addition example):

Precise instructions (in language understood by "the computer") for a "fast, efficient, good" *process* that specifies the "moves" of "the computer" (machine or human, equipped with the necessary internally-contained information and capabilities) to find, decode, and then munch arbitrary input integers/symbols **m** and **n**, symbols **+** and **=** ... and (reliably, correctly, "effectively") produce, in a "reasonable" time, output-integer **y** at a specified place and in a specified format.

The concept of *algorithm* is also used to define the notion of decidability (logic). That notion is central for explaining how formal systems come into being starting from a small set of axioms and rules. In logic, the time that an algorithm requires to complete cannot be measured, as it is not apparently related with our customary physical dimension. From such uncertainties, that characterize ongoing work, stems the unavailability of a definition of *algorithm* that suits both concrete (in some sense) and abstract usage of the term.

(From Wikipedia)

Language Work

Exercise 1. Insert the prepositions:

1. The computer itself consists …… structures and algorithms. 2. Computation is establishing a new approach …… many problems. 3. The underlying principle was set forth …… John von Neumann. 4. The program is viewed …… broad outline. 5. …… higher level abstractions a program could not be understood fully. 6. This result is dependent only …… the error pattern. 7. For the computer all types of data ultimately resolve …… a sequence of bits.

Exercise 2. Complete these sentences with the correct form of the passive tense:

1. The nature of a general-purpose device (to transform) altogether by the program given it. (Present Simple).
2. A stream of information (to process) by a program. (Present Continuous)
3. The design (to specify) in terms of the facilities provided by the notation. (Present Simple).
4. An electronic device (to design) by drawing the symbols for basic circuit elements and their connections. (Present Simple).
5. New aspects of natural phenomena (to make) accessible to investigation. (Present Perfect).
6. The seven-bit binary value 1010011 (to read) into a register in the central processing unit of a computer. (Present Perfect).
7. Each identifier (to associate) with an address in memory. (Present Simple).

Exercise 3. Translate the following information into English. Use it in your summary as for Algebraic algorithms:

1. Алгоритм – это искусство счёта с помощью цифр.

2. Алгори́тм – это точный набор инструкций, описывающих последовательность действий некоторого исполнителя для достижения результата, решения некоторой задачи за конечное время.

3. Слово «алгоритм» происходит от имени учёного Абу Абдуллах Мухаммеда ибн Муса аль-Хорезми, который впервые дал описание придуманной в Индии позиционной десятичной системы счисления..

4. Понятие алгоритма необязательно относится к компьютерным программам. Однако чаще всего в качестве исполнителя выступает компьютер.

5. Различные определения алгоритма в явной или неявной форме содержат следующий ряд общих требований:

– *детерминированность* – определённость. В каждый момент времени следующий шаг работы однозначно определяется состоянием системы.

– *понятность* – алгоритм для исполнителя должен включать только те команды, которые ему (исполнителю) доступны, которые входят в его систему команд.

– *завершаемость* (конечность) – при корректно заданных исходных данных алгоритм должен завершать работу и выдавать результат за конечное число шагов.

– *массовость* – алгоритм должен быть применим к разным наборам исходных данных.

6. В последнее время активно разрабатываются параллельные алгоритмы, предназначенные для вычислительных машин, способных выполнять несколько операций одновременно.

7. В настоящее время теория алгоритмов развивается, главным образом, по трем направлениям.

8. Классическая теория алгоритмов изучает проблемы формулировки задач в терминах формальных языков, вводит понятие задачи разрешения, проводит классификацию задач по классам сложности P, NP и другим.

9. Теория асимптотического анализа алгоритмов рассматривает методы получения асимптотических оценок ресурсоемкости или времени выполнения алгоритмов, в частности, для рекурсивных алгоритмов. Асимптотический анализ позволяет оценить рост потребности алгоритма в ресурсах (например, времени выполнения) с увеличением объема входных данных.

10. Функции трудоёмкости, интервального анализа функций, поиска практических критериев качества алгоритмов, разработки методики выбора рациональных алгоритмов.

(From Wikipedia)

Discussion

Exercise 1. Speak on the problem of data structures and algorithms

Text 3. STRUCTURE AND DECODING OF BLOCK CODES

Shannon showed that the performance limit of codes with fixed code rate improves as the block length increases. As *n* and *k* increase, however, practical implementation requires that the mapping from message to code vector not be arbitrary but that an underlying structure to the code exist. The structures developed to date limit the error correcting capability of these codes to below what Shannon proved possible, on average, for a code with random codeword assignments. The search for good constructive codes continues.

A property which simplifies implementation of the coding operations is that of code linearity. A code is **linear** if the addition of any two code vectors forms another code vector, which implies that the code vectors from a subspace of the vector space of *n*-tuples. This subspace, which contains the all-zero vector, is spanned by any set of *k* linearly independent code vectors. Encoding can be described as the multiplication of the information *k*-tuple by a **generator matrix *G*,** of dimension *k*n*, which contains these basis vectors as rows. That is, a message vector $\boldsymbol{m}_i$ is mapped to a code vector $\boldsymbol{c}_i$ according to

$$\boldsymbol{c}_i = \boldsymbol{m}_i\boldsymbol{G}, \qquad i = 0, 1, \dots, q^k - 1,$$

where element wise arithmetic is defined in the **finite field** *GF*(*q*). In general, this encoding procedure results in code vectors with nonsystematic form in that the values of the message symbols cannot be determined by inspection of the code vector. However, if ***G*** has the form [$\boldsymbol{I}_k$ ***P***] where $\boldsymbol{I}_k$ is the *k*k* identity matrix and ***P*** is a *k*(n – k)* matrix of parity checks, then the *k* most significant symbols of each code vector are identical to the message vector and the code has **systematic** form.

For each generator matrix there is an *(n-k)*k* **parity check matrix H** whose rows are orthogonal to the rows in ***G***, i.e., $\boldsymbol{GH^{\tau} = 0}$**.** If the code is systematic, $\boldsymbol{H = [-P^{\tau}, I_{n-k}]}$. Since all codewords are linear sums of the rows in ***G***, it follows that $\boldsymbol{c_i H^{\tau} = 0}$ for all *i*, *i* = 0, 1, …, q^k – 1, and that the validity of the demodulated vectors can be checked by performing this multiplication.

If the error pattern is a code vector, the errors go undetected. For all other patterns, however, the syndrome is nonzero. Since there are q^{n-k} – 1 nonzero syndromes, q^{n-k} – 1 error patterns can be corrected. When these patterns include all those with *t* or fewer errors and no others, the code is said to be a **perfect code**. Few codes are perfect; most codes are capable of correcting some patterns with more than *t* errors. **Standard array decoders** use lookup tables to associate each syndrome with an error pattern but become impractical as the block length and number of parity symbols increases. Algebraic decoding algorithms have been developed for codes with stronger structure. These algorithms are simplified with imperfect codes if patterns corrected are limited to those with *t* of fewer errors, a simplification called **bounded distance decoding**.

Cyclic codes are a subclass of linear block codes with an algebraic structure that enables encoding to be implemented with a linear feedback shift register and decoding to be implemented without a lookup table. As a result, most block codes in use today are cyclic or are closely related to cyclic codes. These codes are best described if vectors are interpreted as polynomials and the arithmetic follows the rules for polynomials where the element wise operations are defined in *GF*(*q*). In a cyclic code, all codeword polynomials are multiples of a **generator polynomial** *g(x)* of degree *n – k.*

The first step in decoding the demodulated word is to determine if the word is a multiple of *g(x).* This is done by dividing it by *g(x)* and examining the remainder. Since polynomial division is a linear operation, the resulting syndrome *s(x)* depends only on the error pattern. This is the principle of the **cyclic redundancy check** (CRC). It remains to determine the most likely error pattern that could have generated this syndrome.

Single error correcting binary code can use the syndrome to immediately locate the bit in error. More powerful codes use this information to determine the locations and values of multiple errors. The most prominent approach of doing so is with the iterative technique developed by Berlekamp.

Other decoding techniques, including Chase's algorithm and threshold decoding, are easier to implement with soft-decision input. Berlekamp's algorithm can be used in conjunction with transform-domain decoding, which involves transforming the received and block with a finite field Fourier-like transform and solving for errors in the transform domain. Since the implementation complexity of these decoders depends on the block length rather than the number of symbols corrected, this approach results in simpler circuitry for codes with high redundancy.

Other block codes have also been constructed, including product codes that extend the ideas to two dimensions, codes that are based on transform-domain spectral properties, codes that are designed specifically for correction of burst errors, and codes that are decodable with straightforward threshold or majority logic decoders.

(From Clark G.C. Jr.and Cain, J.B.
Error Correction Coding for Digital Communications.)

List of words and expressions

block codes – блочные коды

performance – эффективность
arbitrary – произвольный, независимый
assignment – предназначение, присвоение
random codeword assignment – присвоение случайного кодового слова
on average – в среднем
to simplify – упрощать
code linearity – линейность кода
code vector – кодовый вектор
subspace – подпространство
n-tuple [‘tju:pl] – набор n-величин
to be spanned – заполняться
to map – отображать; устанавливать соответствие
finite field – конечное поле; поле конечных размеров
parity check – контроль четности; контроль по четности
error pattern – ошибочная кодовая комбинация
coding – кодирование, программирование
perfect code – совершенный (исправляющий) код
lookup table – справочная таблица; таблица преобразования(соответствия)
imperfect code – несовершенный код
bounded distance decoding – декодирование с ограниченным расстоянием
cyclic code – циклический код
linear feedback shift register – линейный регистр сдвига с обратной связью
polynomial – многочлен, полином
remainder – остаток
burst error – пакетная ошибка; ошибка в линии передачи пакетных даных

Exercises

Comprehension Check

Exercise 1. Put down problem questions to the text

Exercise 2. Read the text and translate the following equivalents. Use them in your own sentences:

the performance limit of codes, as the block length increases, practical implementation, the mapping from message to code vector, random codeword assignments, to simplify implementation, code linearity, *n*-tuples, nonsystematic form, parity check matrix, the validity of the demodulated vectors, a perfect code, to be capable of correcting some patterns, standard array decoders, bounded distance decoding, to use lookup tables, cyclic codes, polynomials, the principle of the cyclic redundancy check, error pattern, the most prominent approach, iterative technique, threshold decoding, to be used in conjunction, the transform domain, dimensions, to be decodable with straightforward threshold.

Exercise 3. Read and translate the following defining terms

Defining terms

Bounded distance decoding: Limiting the error patterns which are corrected in an imperfect code to those with *t* or fewer errors.

Cyclic code: A block code in which cyclic shifts of code vectors are also code vectors.

Cyclic redundancy check: When the syndrome of a cyclic block code is used to detect errors.

Finite field: A finite set of elements and operations of addition and multiplication that satisfy specific properties. Often called Galois fields and denoted GF(q), where q is the number of elements in the field. Finite fields exist for all q which are prime or the power of a prime.

Generator matrix: A matrix used to describe a linear code. Code vectors equal the information vectors multiplied by this matrix.

Generator polynomial: The polynomial that is a divisor of all codeword polynomials in a cyclic block code; a polynomial that describes circuit connections in a convolutional encoder.

Hamming distance: The number of symbols in which codewords differ.

Linear code: A code whose code vectors form a vector space. Equivalently, a code where the addition of any two code vectors forms another code vector.

Parity check matrix: A matrix whose rows are orthogonal to the rows in the generator matrix of a linear code. Errors can be detected by multiplying the received vector by this matrix.

Perfect code: A t error correcting (n, k) block code in which $q^{n-k} - 1 = \sum_{i=1}^{t}\binom{n}{i}$.

Standard array decoding: Association of an error pattern with each syndrome by way of a lookup table.

Systematic code: A code in which the values of the message symbols can be identified by inspection of the code vector.

Vector space: An algebraic structure comprised of a set of elements in which operations of vector addition and scalar multiplication are defined. For our purposes, a set of n-tuples consisting of symbols from GF(q) with addition and multiplication defined in terms of elementwise operations from this finite field.

Language work

Exercise 1. Complete the statements using the words from the box:

smallest contradictory requirements error search impractical conjunction commonplace

1. There are two …… objectives of block codes.
2. The minimum distance $d_{\min}$ of the code is the …… Hamming distance between any two codewords.
3. The …… for good constructive codes continues.
4. TCM has become …… in transmission of data over voiceband telephone channels.
5. Standard array decoders become …… as the block length and number of parity symbols increases.
6. The Golay codes can correct more than one …… .
7. BCH (Bose-Chaudhuri-Hocquenghem) codes can be shortened to accommodate system …… by deleting positions for information symbols.
8. Berlekamp's algorithm can be used in …… with transform-domain decoding.

Exercise 2. Complete the following sentences using a relative pronoun (who, which, that):

1. A property …… simplifies implementation of the coding operations is that of code linearity.

2. The sequence of n-tuples has distance properties …… allow for detection and correction of errors.

3. Each node represents an encoding interval, from …… the upper branch is taken.

4. Chase …… elaborated other decoding techniques used algorithm and threshold decoding.

5. Other block codes have also been constructed including codes …… are designed specially for correction of burst errors.

6. This subspace …… contains the all-zero vector, is spanned by any set of k linearly independent code vectors.

Class Activity

Exercise 1. Discuss the problem of code linearity

Exercise 2. Binary linear codes (refer to formal definition above) are ubiquitous in electronic devices and digital storage media. For example the Reed-Solomon code is used to store digital data on a compact disc. Read the following text. Discuss it in class.

A Compact Disc (or CD) is an optical disc used to store digital data, originally developed for storing digital audio. The CD, available on the market since late 1982, remains the standard playback medium for commercial audio recordings to the present day.

Standard CDs have a diameter of 120 mm and can hold up to 80 minutes of audio. There is also the Mini CD, with diameters ranging from 60 to 80 mm; they are sometimes used for CD singles, storing up to 24 minutes of audio.

The technology was later adapted and expanded to include data storage (CD-ROM), write-once audio and data storage (CD-R), rewritable media (CD-RW), SACD, VCD, SVCD, PhotoCD, PictureCD, CD-i, and Enhanced CD. CD-ROMs and CD-Rs remain widely used technologies in the computer industry.

Compact Disc is made from a 1.2 mm thick disc of almost pure polycarbonate plastic and weighs approximately 16 grams. A thin layer of aluminium or, more rarely, gold is applied to the surface to make it reflective, and is protected by a film of lacquer. The lacquer is normally spin coated directly on top of the reflective layer. On top of that surface, the label print is applied. Common printing methods for CDs are screen-printing and offset printing.

CD data is stored as a series of tiny indentations (pits), encoded in a tightly packed spiral track molded into the top of the polycarbonate layer. The areas between pits are known as "lands". Each pit is approximately 100 nm deep by 500 nm wide, and varies from 850 nm to 3.5 μm in length.

The spacing between the tracks, the pitch, is 1.6 μm. A CD is read by focusing a 780 nm wavelength (near infrared) semiconductor laser through the bottom of the polycarbonate layer. The change in height between pits and lands results in a difference in intensity in the light reflected. By measuring the intensity change with a photodiode, the data can be read from the disc.

The pits and lands themselves do not directly represent the zeros and ones of binary data. Instead, Non-return-to-zero, inverted (NRZI) encoding is used: a change from pit to land or land to pit indicates a one, while no change indicates a zero. This in turn is decoded by reversing the Eight-to-Fourteen Modulation used in mastering the disc, and then reversing the Cross-Interleaved Reed-Solomon Coding, finally revealing the raw data stored on the disc.

While CDs are significantly more durable than earlier audio formats, they are susceptible to damage from daily usage and environmental factors. Pits are much closer to the label side of a disc, so that defects and dirt on the clear side can be out of focus during playback. Discs consequently suffer more damage because of defects such as scratches on the label side, whereas clear-side scratches can be repaired by refilling them with plastic of similar index of refraction, or by careful polishing. Early music CDs were known to suffer from "CD rot" or "laser rot" where the internal reflective layer itself degrades. When this occurs the CD may become unplayable.

(From Wikipedia)

Unit VI. CRYPTOGRAPHY
Text 1. CRYPTOGRAPHY

> "The mantra of any good security engineer is:
> "Security is not a product, but a process."
> It's more than designing strong
> cryptography into a system; it's designing
> the entire system such that all security
> measures, including cryptography , work
> together".
>
> Bruce Schneier,
> author of "Applied Cryptography"

Cryptography (or cryptology; derived from Greek κρυπτός kryptós "hidden," and the verb γράφω gráfo "write" or λεγειν legein "to speak") is the practice and study of hiding information. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography.

Until modern times, cryptography referred almost exclusively to encryption, the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e, ciphertext). Decryption is the reverse, moving from unintelligible ciphertext to plaintext. A cipher (or cypher) is a pair of algorithms which perform this encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. This is a secret parameter (ideally, known only to the communicants) for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks.

In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, code has a more specific meaning; it means the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, apple pie replaces attack at dawn). Codes are no longer used in serious cryptography–except incidentally for such things as unit designations (eg, 'Bronco Flight' or Operation Overlord) – since properly chosen ciphers are both more practical and more secure than even the best codes, and better adapted to computers as well.

Some use the terms cryptography and cryptology interchangeably in English, while others use cryptography to refer to the use and practice of cryptographic techniques, and cryptology to refer to the subject as a field of study. In this respect, English usage is more tolerant of overlapping meanings and word origins than are several European languages in which meanings of cognate words are more restricted.

(en.wikipedia.org/wiki/**Cryptography**)

List of words and expressions

to hide (hid; hidden) – прятать, скрывать
derived from – полученный от

to affiliate – объединять, присоединять

ATM card (Automated Teller Machine) – карточка банковского автомата

computer password – компьютерный пароль

encryption – зашифровывание

plaintext – простой текст

unintelligible gibberish – непонятная тарабарщина

ciphertext – зашифрованный текст

decryption – расшифровывание

authentication – аутентификация; проверка личности

integrity check – проверка на целостность

colloquial – разговорный (о словах, выражениях)

concealment – маскировка, укрытие

incidentally – случайно; между прочим

interchangeably – путем обмена (замены); взаимозаменяемо

overlapping meaning – частично совпадающее значение

cognate words – родственные слова

Exercises

Comprehension Check

Exercise 1. Write some problem questions to the text for class discussion

Exercise 2. Read and translate the following equivalents. Use them in your own sentences:

to derive from, to be considered, to be affiliated closely with information theory, technologically advanced societies, to depend on, until modern times, unintelligible gibberish, decryption, reverse, plaintext, cipher, communicants, a specific message exchange context, additional procedures, as authentication or integrity check, colloquial use, concealment of meaning, unit designations, to be tolerant of overlapping meanings, cognate words, restricted.

Exercise 3.Look at the table. Reread the text and find the corresponding ending of each of the sentences:

1. Codes	**A.** were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks.
2. Code	**B.** are no longer used in serious cryptography—except incidentally for such things as unit designations.
3. The term "code"	**C.** is often used to mean any method of encryption or concealment of meaning.
4. Ciphers	**D.** is the practice and study of hiding information.
5. A key	**E.** is a secret parameter (ideally, known only to the communicants) for a specific message exchange context.
6. A cipher	**F.** is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering.
7. Cryptography	**G.** has a more specific meaning; it means the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, apple pie replaces attack at dawn).

8. Cryptography **H.** referred almost exclusively to encryption, the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e, ciphertext).

9. Cryptography **I.** is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography.

10. Cryptography **J.** is a pair of algorithms which perform this encryption and the reversing decryption.

Language Work

Exercise 1. Choose the correct alternative in each of the following sentences:

1. Cryptography *is being / is* considered to be a branch of both mathematics and computer science.

2. I hope that the description of this ciphertext *will be / is being* performed next week.

3. Historically, ciphers *are / were* used for encryption or decryption.

4. Cryptography *will be / is* affiliated closely with information theory.

5. Ciphers *should have been / should be* properly chosen by the end of last week.

6. This secret parameter *is / has been* intended for a specific message exchange context.

7. Meanings of cognate words in several European languages *are / are being* more restricted.

8. Codes *are / have been* no longer used in serious cryptography.

Exercise 2. Make questions for which the following sentences would be answers. Ask about the words in bold:

1. **Cryptography** is the practice and study of hiding information.
2. **In modern times, cryptography** is considered to be a branch of both mathematics and computer science, and is affiliated **closely** with information theory, computer security, and engineering.
3. Cryptography **is used in** applications present in technologically advanced societies; **examples** include the security of ATM cards, computer passwords, and electronic commerce, which all **depend on** cryptography.
4. **A cipher** (or cypher) is a pair of algorithms which **perform** this encryption and the reversing decryption.
5. This is a secret parameter (ideally, **known only to the communicants**) for a specific message exchange context.
6. **Historically,** ciphers were often used directly for encryption or decryption, **without additional procedures** such as authentication or integrity checks.
7. In cryptography, code has **a more specific meaning.**
8. **Properly** chosen ciphers are both more practical and more secure than even the best codes, and **better adapted to** computers as well.
9. **Some** use the terms cryptography and cryptology **interchangeably** in English.

Exercise 3. Translate the following text from English. Use a dictionary if necessary. Give it a title. Make up a short oral summary and present it in class

Passwords, locks, access privileges, and even biometric devices do not always deter the determined intruder. A common tool like a protocol analyzer can be hooked up to the network and the intruder can watch all data, including passwords, pass by. Data encryption is the answer.

With encryption, data is scrambled before transmission, making it unreadable as it passes over the wire, even if it is intercepted. To scramble or encrypt this data, its bits must be transformed according to an algorithm. The data is transmitted, and at the receiving end, a system of keys is used to decode the bits into intelligible information. Keys are necessary for encoding and decoding.

Encryption usually requires extra hardware because of the processing power required. Hardware-based encryption schemes are more difficult to crack than software-based methods.

A common data encryption standard specified by the U.S. government is Data Encryption Standard (DES).

DES defines how the data should be encrypted and specifications for an electronic key. It uses one 64-bit key for encryption and decryption. This can cause problems because the key must be in the hands of the sender and receiver. The only way to get it from place to place is to transmit it. Transmitting the key introduces a security threat. The Public Key System, with matched public and private keys, is a solution.

Encryption may be done before data is stored or transmitted. Some networks only encrypt data when it is sent, which makes wire tapping more difficult but does not keep intruders from taking data from a disk. Other networks also encrypt data on the hard disk. Data is encrypted as it is written and decrypted as it is read from the disk. Having encryption working in both places keeps network data much more secure. Encrypting passwords is sometimes sufficient to deter the casual data thief.

To further enhance encryption's effectiveness, keys should be changed at random intervals. This prevents intruders from discovering either the key or the time the key is changed. Alternative keys should be available, too, in case the original set is compromised.

The best network encryption schemes hide much of the encryption hassle from end users by taking care of key management and encryption automatically.

(From LAN Magazine/Network Magazine. № 44.March.1992)

Class Activity

Exercise 1. Discuss this question

Why is cryptography considered to be a branch of both mathematics and computer science?

Text 2. HYSTORY OF CRYPTOGRAPHY AND CRYPTANALYSIS

Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) — conversion of messages from a comprehensible form into an incomprehensible one, and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely, the key needed for decryption of that message). In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs, and secure computation, amongst others.

The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or opponent literacy, required actual cryptography. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g. 'help me' becomes 'ehpl em' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the alphabet). Simple versions of either offered little confidentiality from enterprising opponents, and still don't. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. It was named after Julius Caesar who is reported to have used it, with a shift of 3, to communicate with his generals during his military campaigns, just like EXCESS-3 code in boolean algebra.

Encryption attempts to ensure secrecy in communications, such as those of spies, military leaders, and diplomats, but it has also had religious applications. For instance, early Christians used cryptography to obfuscate some aspects of their religious writings to avoid the near certain persecution they would have faced they had been less cautious; famously, 666 or in some early manuscripts, 616, the Number of the Beast from the Christian New Testament Book of Revelation, is sometimes thought to be a ciphertext referring to the Roman Emperor Nero, one of whose policies was persecution of Christians. There is record of several, even earlier, Hebrew ciphers as well. Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, concealed a message - a tattoo on a slave's shaved head - under the regrown hair. More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

Ciphertexts produced by classical ciphers (and some modern ones) always reveal statistical information about the plaintext, which can often be used to break them. After the discovery of frequency analysis by the Arab polymath al-Kindi in the 9th century, nearly all such ciphers became more or less readily breakable by an informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles. Essentially all ciphers remained vulnerable to cryptanalysis using this technique until the invention of the polyalphabetic cipher, most clearly by Leon Battista Alberti around the year 1467 (there is some indication of early Arab knowledge of them). Alberti's innovation was to use different ciphers (i.e., substitution alphabets) for various parts of a message (often each successive plaintext letter). He also invented what was probably the first automatic cipher device, a wheel which implemented a partial realization of his invention. In the polyalphabetic Vigenère cipher, encryption uses a key word, which controls letter substitution depending on which letter of the key word is used. In the mid 1800s Babbage showed that polyalphabetic ciphers of this type remained partially vulnerable to frequency analysis techniques.

Although frequency analysis is a powerful and general technique, encryption was still often effective in practice; many a would-be cryptanalyst was unaware of the technique. Breaking a message without frequency analysis essentially required knowledge of the cipher used, thus encouraging espionage, bribery, burglary, defection, etc. to discover it. It was finally recognized in the 19th century that secrecy of a cipher's algorithm is not a sensible or practical safeguard; in fact, any adequate cryptographic scheme (including ciphers) should remain secure even if the adversary knows the cipher algorithm itself. Secrecy of the key should alone be sufficient for confidentiality when under attack — for good ciphers. This fundamental principle was first explicitly stated in 1883 by Auguste Kerckhoffs and is generally called Kerckhoffs' principle; alternatively and more bluntly, it was restated by Claude Shannon as Shannon's Maxim — 'the enemy knows the system'.

Various physical devices and aids have been used to assist with ciphers. One of the earliest may have been the scytale of ancient Greece, a rod supposedly used by the Spartans as an aid for a transposition cipher. In medieval times, other aids were invented such as the cipher grille, also used for a kind of steganography. With the invention of polyalphabetic ciphers came more sophisticated aids. Early in the 20th century, several mechanical encryption/decryption devices were invented, and many patented, including rotor machines — most famously the Enigma machine used by Germany in World War II.

The development of digital computers and electronics after WWII made possible much more complex ciphers. Furthermore, computers allowed for the encryption of any kind of data that is represented by computers in any binary format, unlike classical ciphers which only encrypted written language texts, dissolving the utility of a linguistic approach to cryptanalysis in many cases. Many computer ciphers can be characterized by their operation on binary bit sequences (sometimes in groups or blocks), unlike classical and mechanical schemes, which generally manipulate traditional characters (i.e., letters and digits) directly. However, computers have also assisted cryptanalysis, which has compensated to some extent for increased cipher complexity. Nonetheless, good modern ciphers have stayed ahead of cryptanalysis; it is usually the case that use of a quality cipher is very efficient (i.e., fast and requiring few resources), while breaking it requires an effort many orders of magnitude larger, making cryptanalysis so inefficient and impractical as to be effectively impossible.

Extensive open academic research into cryptography is relatively recent — it began only in the mid-1970s with the public specification of DES (the Data Encryption Standard), and the public release of the RSA algorithm. Since then, cryptography has become a widely used tool in communications, computer networks, and computer security generally. The present security level of many modern cryptographic techniques is based on the difficulty of certain computational problems, such as the integer factorization problem or the discrete logarithm problem. In many cases, there are proofs that cryptographic techniques are secure if a certain computational problem cannot be solved efficiently. With one notable exception—the one-time pad—these proofs are contingent, and thus not definitive, but are currently the best available for cryptographic algorithms and protocols.

As well as being aware of cryptographic history, cryptographic algorithm and system designers must also sensibly consider probable future developments in their designs. For instance, the continued improvements in computer processing power have increased the scope of brute-force attacks when specifying key lengths. The potential effects of quantum computing are already being considered by some cryptographic system designers; the announced imminence of small implementations of these machines is making the need for this preemptive caution fully explicit.

Essentially, prior to the early 20th century, cryptography was chiefly concerned with linguistic patterns. Since then the emphasis has shifted, and cryptography now makes extensive use of mathematics, including aspects of information theory, computational complexity, statistics, combinatorics, abstract algebra, and number theory. Cryptography is also a branch of engineering.

(en.wikipedia.org/wiki/**Cryptography**)

List of words and expressions

Incomprehensible – несжимаемый

Interceptor – перехватчик; устройство перехвата

Eavesdropper – пассивный нарушитель; подслушивающий
integrity checking – проверка целостности (данных)
trivially – незначительно
confidentiality – конфиденциальность
Boolean algebra – булева алгебра, алгебра логики
to obfuscate – сбивать с толку
persecution – преследование, надоедание
caution – предосторожность
Revelation – апокалипсис (библ.)
Steganography – стеганография
Microdot – микроточка (многократно уменьшенная фотокопия документа)
to conceal – скрывать, маскировать
to reveal – обнаруживать, показывать
polymath – человек с энциклопедическими знаниями, эрудит
partially – частично
scytale (**skytale**) – сцитала /s təli/ – примитивное шифровальное устройство в Древней Греции и Спарте, состоящее из цилиндра и полосков кожи вокруг него, на которых писалось сообщение; устройство использовалось для транспозиционного шифра
grille – решетка
one-time pad – одноразовый шифровальный блокнот криптографический ключ одноразового использования
contingent – случайный, непредвиденный
brute-force attack – атака с применением грубой силы (силовая атака)
imminence – нависшая угроза
preemptive caution – упреждающая предосторожность

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What was cryptography concerned with before the modern era? 2. What has it included in recent decades? 3. Why did the earliest forms of secret require little more than local pen and paper analogs? 4. What are the main classical cipher types? 5. Whom was the Caesar cipher named after? 6. What can you say about the Caesar cipher? 7. Why did Julius Caesar use it? 8. Why did early Christians use cryptography? 9. When was steganography first developed? 10. What do ciphertexts always reveal? 11. When did all such ciphers become more or less readily breakable by an informed attacker? 12. What have you learned from the text about Alberti's innovation? 13. What did Babbage show in the mid 1800s? 14. Why is frequency analysis a powerful and general technique? 15. Why was encryption still often effective in practice? 16. When was it finally recornized that secrecy of a cipher's algorithm is not a sensible or practical safeguard? 17. What is called Kerckhoffs' principle? 18. When were several mechanical encryption/ decryption devices invented? 19. What made possible much more complex ciphers? 20. What can many computer ciphers be characterized by? 21. Have computers assisted cryptanalysis? Why? 22. When did extensive open academic research into cryptography begin? 23. Where has cryptography become a widely used tool since then? 24. What is the present security level of many modern cryptographic techniques based on? 25. Whom are the potential effects of quantum

computing being considered by? 26. What was cryptography chiefly concerned with prior to the early century? 27. How has the emphasis shifted since then?

Exercise 2. Reread the text to find the English equivalents for the following expressions:

быть связанной только с конфиденциальностью сообщений, преобразование сообщений в непонятную форму, нечитаемый, ключ, дешифровка, за последние десятилетия, проверка целостности сообщения, идентификация авторизированного отправителя, цифровая подпись, среди прочего, транспозиционные шифры, заместители, конфиденциальность, простой текст, избежать преследования, ранние рукописи, невидимые чернила, водяные знаки, скрывать информацию, головоломка, уязвимые, соответствующая криптографическая схема, устройства шифрования, в отличие от классических шифров, взломать шифр, стандартная кодировка данных, быть связанным главным образом с лингвистическими моделями, упреждающая предосторожность.

Language Work

Exercise 1. Complete the sentence with the correct Present perfect form of the verbs in the box:

compensate become use examine solve increase attempt

1. Cryptography ……. already …… a widely used tool in communications.
2. A certain computational problem …… (not) efficiently before.
3. Since then encryption …… to ensure secrecy in communication.
4. They …… the relationship between cryptographic problems and quantum physics so far.
5. The continued improvements in computer processing power …… the scope of brute-force attacks when specifying key lengths.
6. Cryptanalysis …… to some extent for increased cipher complexity.
7. Various physical devices …… to assist with ciphers.

Exercise 2. Translate and analyze the following sentences containing complex subject:

1. Encryption is known to ensure secrecy of military leaders and diplomats.
2. This manuscript is thought to be a ciphertext referring to the Roman Emperor Nero.
3. The results obtained are considered to be concerned solely with decryption .
4. Julius Caesar is reported to have used an early substitution cipher.
5. The invention of the polyalphabetic cipher is known to use different ciphers.
6. Frequency analysis is believed to be a powerful technique but uneffective in practice.
7. Secrecy of a cipher's algorithm was recognized in the 19th century not to be a sensible or practical safeguard.
8. The development of digital computers is assumed to have made possible much more complex ciphers.

Exercise 3. Read the following information and translate it into English. Use a dictionary if necessary:

1. Криптография – это набор методов защиты информационных взаимодействий от отклонений их нормального, штатного протекания, вызванных злоумышленными действиями различных субъектов, методов, базирующихся на секретных алгоритмах преобразования информации, включая алгоритмы, не являющиеся собственно секретными, но использующие секретные параметры.

2. Исторически первой задачей криптографии была защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, что нашло отражение в самом названии этой дисциплины, эта защита базируется на использовании "секретного языка", известного только отправителю и получателю, все методы шифрования являются лишь развитием этой философской идеи.

3. С усложнением информационных взаимодействий в человеческом обществе возникли и продолжают возникать новые задачи по их защите, некоторые из них были решены в рамках криптографии, что потребовало развития принципиально новых подходов и методов.

((C)iNFUSED BYTES On Line http://www.enlight.ru/ib)

Discussion

Exercise 1. Outline the main ideas of the text «History of cryptography and cryptanalysis» and write a summary. Search for some additional information. Present your report in class

Text 3. MODERN CRYPTOGRAPHY

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until 1976.

The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern embodiment of Alberti's polyalphabetic cipher: block ciphers take as input a block of plaintext and a key: and output – a block of ciphertext of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the mode of operations and must be carefully considered when using a block cipher in a cryptosystem.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken.

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on an internal state which changes as the cipher operates. That state's change is controlled by the key, and, in some stream ciphers, by the plaintext stream as well. RC4 is an example of a well-known stream cipher.

Cryptographic hash functions (often called message digest functions) do not necessarily use keys, but are a related and important class of cryptographic algorithms. They take input data (often an entire message), and output a short, fixed length hash, and do so as a one-way function. For good ones, collisions (two plaintexts which produce the same hash) are extremely difficult to find.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key is used to authenticate the hash value on receipt.

Symmetric-key cryptosystems typically use the same key for encryption and decryption, though this message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of establishing a secret key between two communicating parties, when a secure channel doesn't already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used – a public key and a private key. A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance".

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption. Diffie and Hellman showed that public-key cryptography was possible by presenting the Diffie-Hellman key exchange protocol.

In 1978, Ronald Rivest, Adi Shamir, and Len Adleman invented RSA, another public-key system.

In 1997, it finally became publicly known that asymmetric key cryptography had been invented by James H. Ellis at GCHQ, a British intelligence organization, in the early 1970s, and that both the Diffie-Hellman and RSA algorithms had been previously developed (by Malcolm J. Williamson and Clifford Cocks, respectively).

The Diffie-Hellman and RSA algorithms, in addition to being the first publicly known examples of high quality public-key ciphers, have been among the most widely used. Others include the Cramer-Shoup cryptosystem, ElGamal encryption, and various elliptic curve techniques.

In addition to encryption, public-key cryptography can be used to implement digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic that they are easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the content of the message being signed; they cannot be 'moved' from one document to another, for any attempt will be detectable. In digital signature schemes, there are two algorithms: one for signing, in which a secret key is used to process the message (or a hash of the message, or both), and one for verification, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (SSL/TLS, many VPNs, etc).

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie-Hellman and DSA are related to the discrete logarithm problem. More recently, elliptic curve cryptography has developed in which security is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems, in which a fast high-quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

(en.wikipedia.org/wiki/**Cryptography**)

List of words and expressions

symmetric-key cryptography – криптография с симметричным ключом
publicly – публично, открыто
block cipher – блочный шифр
stream cipher – поточный шифр
embodiment – конструктивное оформление; осуществление
knitting – соединение
successive blocks – последовательные блоки
to withdraw – удалять
deprecation – осуждение
triple – тройной
bit-by-bit – поразрядный; побитовый
character-by-character – по кодовым комбинациям
fixed length hash – хэш конечной длины
groundbreaking – делающий первые шаги в чем-либо
infeasible – неосуществимый
interrelated pair – взаимосвязанная пара
GCHQ – *воен., брит.* Government Communication Headquarters
воен. ШПС (Великобритания); штаб правительственной связи
reminiscent – напоминающий
to forge – подделывать, фальсифицировать
exponentiation – возведение в степень, потенцирование
public-key cryptoscheme – криптосхема с общедоступным ключом
to be digitally signed – быть подписаным электронным символом (подписью)
hash function –*безоп.* хэш-функция; функция хэширования

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. Which methods does symmetric-key cryptography refer to? 2. Do the sender and the receiver share the same key in these methods? 3. What does the modern study of symmetric-key ciphers deal with? 4. What is a block cipher? 5. Why must the methods be carefully considered when using a block cipher in a cryptogram? 6. Which designs have been designated cryptography standards? 7. Which standard was finally withdrawn? 8. Does this standard remain popular despite its deprecation as an official standard? 9. Where is the Data Encryption Standard used? 10. What do stream ciphers create in contrast to the 'block' type? 11. What is the state's change controlled by in some stream ciphers? 12. What can you say about cryptographic hash functions? 13. What is a significant disadvantage of symmetric ciphers? 14. Why is there the difficulty of establishing a secret key between two communicating parties? 15. Who proposed the notion of public-key cryptography? 16. What do you know about it? 17. Where is the public key typically used? 18. What is the difference between the public key and the private key? 19. When was another public-key system invented? 20. Which algorithms have been among the most widely used? 21. What can public-key cryptography be used for? 22. What is the digital signature reminiscent of? 23. Is it easy or difficult to forge a digital signature using public-key cryptography? Why? 24. How many algorithms are there in digital signature schemes? 25. What are digital signatures central to? 26. What are public-key algorithms based on? 27. Why do most public-key algorithms involve operations such as modular multiplication and exponentiation? 28. What is the difference between a fast high-quality symmetric-key encryption algorithm and the relevant symmetric key?

Exercise 2. Reread the text to find the meaning of the following equivalents. Translate them. Make up your own sentences:

symmetric-key cryptography, encryption methods, the sender and receiver, to share the same key, in an easily computable way, block ciphers, stream ciphers, a method of knitting together successive blocks, to be carefully considered, despite its deprecation, e-mail privacy, to be broken, a one-time pad, cryptographic hash functions, fixed length hash, collisions, message authentication codes, to authenticate the hash value on receipt, complex key management schemes, a considerable practical obstacle, public-key (asymmetric key) cryptography, infeasible from the other, an interrelated pair, polyalphabetic substitution, to emerge, the Diffie-Hellman key exchange protocol, respectively, various elliptic curve techniques, to implement digital signature schemes, to forge, to be based on the computational complexity, a number theory, modular multiplication, exponentiation, a fast high-quality symmetric-key encryption algorithm.

Language Work

Exercise 1. Complete the sentences using the words from the box:

document used block number cryptographic using quality

1. A …… cipher is a modern embodiment of Alberti's polyalphabetic cipher.
2. Many other block ciphers have been designed with considerable variation in …… .
3. Cryptographic hash functions are a related and important class of …… algorithms.

4. A secret is …… to authenticate the hash value on receipt.

5. The number of keys required increases as the square of the …… of network members.

6. Digital signatures cannot be ‘moved’ from one …… to another.

7. The relevant symmetric key is encrypted …… a public-key algorithm.

Exercise 2. Choose the correct alternative in each of the following sentences:

1. These block cipher designs *have / have been* designated cryptography standards by the US government.

2. The Data Encryption Standard *was / has* finally withdrawn.

3. Cryptographic hash functions *are being / are* often called message digest functions.

4. Digital signatures *must / can* also be permanently tied to the content of the message being signed.

5. A different key *can / must* be shared by each distinct pair of communicating parties.

6. In public-key cryptosystems, the paired private key *should / must* be used to remain secret.

7. The matching public key *is / has* used with the message to check the validity of the signature.

Exercise 3. Translate the following into English. Use a dictionary if necessary:

1. Криптография – это дисциплина, изучающая способы защиты процессов информационного взаимодействия от целенаправленных попыток отклонить их от условий нормального протекания, основанные на криптографических преобразованиях, то есть преобразованиях данных по секретным алгоритмам.

2. С давних времен вплоть до настоящего время важнейшей задачей криптографии является защита передаваемых по каналам связи или хранящихся в системах обработки информации данных от несанкционированного ознакомления с ними и от преднамеренного их искажения.

3. Криптография решает указанную задачу посредством шифрования защищаемых данных, что предполагает использование двух следующих взаимно обратных преобразований:

– перед отправлением данных по линии связи или перед помещением на хранение они подвергаются **зашифрованию;**

– для восстановления исходных данных из зашифрованных к ним применяется процедура **расшифрования.**

4. Каким же условиям должен удовлетворять шифр, не только обладающий необходимой стойкостью, но, вдобавок к этому удобный в реализации и использовании.

5. Операции за- и расшифрования должны быть близкими настолько, чтобы могли быть выполнены одним и тем же аппаратным или программным модулем – это диктуется требованием экономичности реализации.

6. Объем ключевой информации должен быть относительно небольшим.

7. Разумным является такой размер ключа, при котором невозможно его нахождение путем перебора по всему ключевому пространству, с определенным запасом на возможный прогресс электронной техники.

8. В настоящее время граница практической осуществимости подбора ключа находится где-то в районе 64-128 бит. Соответственно, разумным может считаться размер ключа 256-1024 бит. Данное требование вытекает из необходимости хранить ключи на любых носителях, включая нетрадиционные, например – на персональных миниатюрных магнитных карточках.

9. Реализация шифра (код программы и постоянные данные) должна быть достаточно компактной для того, чтобы "уместиться" на микроконтроллерах с относительно невысоким объемом запоминающего устройства – последнее требование также диктуется соображениями экономичности реализации.

((C)iNFUSED BYTES On Line http://www.enlight.ru/ib)

Discussion

Exercise 1. Learn the material about Data Encryption and Decryption Algorithms and speak about any algorithm you like

There are two kinds of cryptosystems: symmetric and asymmetric. Symmetric cryptosystems use the same key (a secret key) to encrypt and decrypt a message, and asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it, or vice versa. The following is a list of some popular cryptography algorithms:

DES – the Digital Encryption Standard was developed by IBM and the National Security Agency (NSA) of the USA in the 50s. DES uses a key of only 56 bits, and thus it is too weak and easy to be broken with today’s technology.

IDEA – International Data Encryption Algorithm (IDEA) is a cryptosystem developed by X. Lai and J. Massey in 1991 to replace the DES standard. It is a symmetric (same key for encryption and decryption) block cipher, operating on 8 bytes at a time, just like DES, but with a key of 128 bits.

RC4 – a cipher invented by Ron Rivest, a proprietary system by RSADSI, is used in a number of commercial systems like Lotus Notes and secure Netscape.

Unix Crypt – Many Unix systems come supplied with an encryption system called crypt. This routine should never be used for encrypting anything because there exist programs on the net for producing the decrypted text and the key.

RSA – a cipher/algorithm based on the concept of a trapdoor function, which is easily calculated, but whose inverse is extremely difficult to calculate. The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1997.

(From en. Wikipedia.org/wiki/Cryptography)

Exercise 2. Discuss the problems of modern cryptography

Text 4. CRYPTANALYSIS

The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion. Cryptanalysis might be undertaken by a malicious attacker, attempting to subvert a system, or by the system's designer (or others) attempting to evaluate whether a system has vulnerabilities, and so it is not inherently a hostile act. In modern practice, however, cryptographic algorithms and protocols must be carefully examined and tested to offer any assurance of the system's security (at least, under clear — and hopefully reasonable — assumptions).

It is a commonly held misconception that every encryption method can be broken. In connection with his WWII work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message. Most ciphers, apart from the one-time pad, can be broken with enough computational effort by brute force attack, but the amount of effort needed may be exponentially dependent on the key size, as compared to the effort needed to use the cipher. In such cases, effective security could be achieved if it is proven that the effort required (i.e., 'work factor' in Shannon's terms) is beyond the ability of any adversary. This means it must be shown that no efficient method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no such showing can be made currently, as of today, the one-time-pad remains the only theoretically unbreakable cipher.

There are a wide variety of cryptanalytic attacks, and they can be classified in any of several ways. A common distinction turns on what an attacker knows and what capabilities are available. In a ciphertext-only attack, the cryptanalyst has access only to the ciphertext (good modern cryptosystems are usually effectively immune to ciphertext-only attacks). In a known-plaintext attack, the cryptanalyst has access to a ciphertext and its corresponding plaintext (or to many such pairs). In a chosen-plaintext attack, the cryptanalyst may choose a plaintext and learn its corresponding ciphertext (perhaps many times); an example is gardening, used by the British during WWII. Finally, in a chosen-ciphertext attack, the cryptanalyst may choose ciphertexts and learn their corresponding plaintexts. Also important, often overwhelmingly so, are mistakes (generally in the design or use of one of the protocols involved).

Cryptanalysis of symmetric-key ciphers typically involves looking for attacks against the block ciphers or stream ciphers that are more efficient than any attack that could be against a perfect cipher. For example, a simple brute force attack against DES requires one known plaintext and 255 decryptions, trying approximately half of the possible keys, to reach a point at which chances are better than even the key sought will have been found. But this may not be enough assurance; a linear cryptanalysis attack against DES requires 243 known plaintexts and approximately 243 DES operations. This is a considerable improvement on brute force attacks.

Public-key algorithms are based on the computational difficulty of various problems. The most famous of these is integer factorization (e.g., the RSA algorithm is based on a problem related to factoring), but the discrete logarithm problem is also important. Much public-key cryptanalysis concerns numerical algorithms for solving these computational problems, or some of them, efficiently. For instance, the best known algorithms for solving the elliptic curve-based version of discrete logarithm are much more time-consuming than the best known algorithms for factoring, at least for problems of more or less equivalent size. Thus, other things being equal, to achieve an equivalent strength of attack resistance, factoring-based encryption techniques must use larger keys than elliptic curve techniques. For this reason, public-key cryptosystems based on elliptic curves have become popular since their invention in the mid-1990s.

While pure cryptanalysis uses weaknesses in the algorithms themselves, other attacks on cryptosystems are based on actual use of the algorithms in real devices, and are called side-channel attacks. If a cryptanalyst has access to, say, the amount of time the device took to encrypt a number of plaintexts or report an error in a password or PIN character, he may be able to use a timing attack to break a cipher that is otherwise resistant to analysis. An attacker might also study the pattern and length of messages to derive valuable information;

this is known as traffic analysis, and can be quite useful to an alert adversary. And, of course, social engineering, and other attacks against the personnel who work with cryptosystems or the messages they handle (e.g., bribery, extortion, blackmail, espionage, ...) may be the most productive attacks of all.

(en.wikipedia.org/wiki/**Cryptography**)

List of words and expressions

subversion – *зд.* незаконная деятельность
evasion – уклонение; обход
to subvert – разрушать
vulnerability – уязвимость; слабое место; степень защищенности
inherently – в своей основе
a hostile act – враждебный акт; враждебное действие
assurance – адекватность; гарантия, обеспечение
as opposed to – противопоставляя; противодействуя
to turn on – направлять на …
overwhelmingly – непреодолимо
side-channel attack – атака через побочный канал; нападение со стороны бокового канала
a timing attack – временная атака (позволяет вскрывать ключи путем замера времени)
traffic analysis – анализ информационного потока; анализ переписки; анализ трафика
an alert adversary – осторожный нарушитель; (противник)
bribery – взяточничество; подкуп
extortion – вымогательство
blackmail – шантаж

Exercises

Comprehension Check

Exercise 1. Put down problem questions to the text

Exercise 2. Find the equivalents for the following expressions in the text:

найти слабости либо бреши в криптографической схеме, дополнительный вариант, злонамеренный хакер, уязвимые стороны, враждебный акт, общепринятая неверная концепция, выбранный наугад, в отличие от одноразового криптографического ключа, в зависимости от размера ключа, могут быть классифицированы, блок шифры, дискретный логарифм, анализ информационного потока.

Language Work

Exercise 1. Match the words with the definitions:

Key words

cybercriminal, hacker, cyberterrorist, cryptosystems, the Internet, virtual, e-mail, attack

1. A criminal who uses the Internet.
2. A system where people can send messages(mail) to each other by computer.

3. Images produced by computers that surround the person looking at them and seem to be real.

4. Someone who uses computers for violent political demands.

5. Computer system that allows millions of people around the world to exchange information.

6. A person who enters other people's computer programmes without permission.

7. Systems where algorithms and assorted protocols are combined.

8. An attempt to cause damage to someone's data by unauthorized access.

Exercise 2. Put the words in the right order to make questions:

1. An attacker to subvert when attempt a system did?
2. That is who the one-time pad unbreakable proved cipher?
3. The one-time pad does what remain?
4. Long working have at this ciphertext been you how?
5. On is what based the RSA algorithm?
6. You these computational problems why yet solved haven't?

Exercise 3. Make questions for which the following would be answers. Ask about the words in bold:

1. The goal of cryptanalysis **is to find some weakness or insecurity** in a cryptographic scheme, **thus permitting its subversion or evasion.**

2. In modern practice, however, **cryptographic algorithms and protocols** must be **carefully examined and tested** to offer any assurance of the system's security.

3. **Most ciphers,** apart from the one-time pad, **can be broken** with enough computational effort **by brute force attack**, but the amount of effort needed may be exponentially dependent **on the key size**, as compared to the effort needed to use the cipher.

4. In connection with his WWII work at Bell Labs, **Claude Shannon** proved that **the one-time pad cipher** is unbreakable, **provided the key material is truly random**, **never reused, kept secret from all possible attackers, and of equal or greater length than the message.**

5. There are **a wide variety of cryptanalytic attacks**, and they can be classified **in any of several ways.**

6. **A common distinction** turns on what an attacker knows and what capabilities are available.

7. A linear cryptanalysis attack against DES **requires 243 known plaintexts** and approximately 243 DES operations.

8. For this reason, public-key cryptosystems **based on elliptic curves** have become popular **since their invention in the mid-1990s.**

9. **If a cryptanalyst has access to,** say, the amount of time the device took to encrypt a number of plaintexts or report an error in a password or PIN character, **he** may be able to use a timing attack to break a cipher that is otherwise resistant to analysis.

10. **Social engineering, and other attacks against the personnel** who work with cryptosystems or the messages they handle (e.g., bribery, extortion, blackmail, espionage, ...) may be the most productive attacks of all.

Exercise 4. Choose the correct linker:

1. The efficiency survey gave no useful results, offered no suggestions. __________ , it was a complete waste of time.

a) Otherwise b) Incidentally c) In any case d) In short

2. In modern practice, ____________ , cryptographic algorithms and protocols must be carefully tested.

a) despite b) however c) although d) owing to

3. __________ there are no more questions to discuss, we can choose this plaintext.

a) As b) So that c) Because d) Unless

4. _______________ , the public-key cryptosystems have become popular since their invention.

a) Instead b) Because c) For this reason d) In short

5. Most ciphers can be broken with enough computational effort by brute force attack, ___________ the amount of effort needed may be dependent on the key size.

a) but b) despite c) in fact d) although

6. ____________ frequency analysis is a powerful technique, encryption was still often effective in practice.

a) In other words b) Nevertheless c) Although d) In spite of

7. The present security level of many modern cryptographic techniques is based on the difficulty of certain computational problems, ___________ the integer factorization problem or the discrete logarithm problem.

a) especially b) such as c) including d) e.g.

Class Activity

Exercise 1. Speak about a variety of cryptanalytic attacks. Use the word-combinations given below:

a wide variety of; a common distinction; to be immune to; to have access to; to choose ciphertexts.

Text 5. CRYPTOGRAPHIC PRIMITIVES

Much of the theoretical work in cryptography concerns cryptographic primitives — algorithms with basic cryptographic properties — and their relationship to other cryptographic problems. For example, a one-way function is a function intended to be easy to compute but hard to invert. In a very general sense, for any cryptographic application to be secure (if based on such computational feasibility assumptions), one-way functions must exist. However, if one-way functions exist, this implies that P ≠ NP. Since the P versus NP problem is currently unsolved, it is not known if one-way functions really do exist. More complicated cryptographic tools are then built from these basic primitives. For instance, if one-way functions exist, then secure pseudorandom generators and secure pseudorandom functions exist.

Complex functionality in an application must be built in using combinations of these algorithms and assorted protocols. Such combinations are called cryptosystems and it is they which users will encounter. Examples include PGP and its variants, ssh, SSL/TLS, all PKIs, digital signatures, etc.

Other cryptographic primitives include the encryption algorithms themselves, one-way permutations, trapdoor permutations, etc.

In many cases, cryptographic techniques involve back and forth communication among two or more parties in space (e.g., between the home office and a branch office) or across time (e.g., cryptographically protected backup data). The term cryptographic protocol captures this general idea.

Cryptographic protocols have been developed for a wide range of problems, including relatively simple ones like interactive proof systems, secret sharing, and zero-knowledge, and much more complex ones like electronic cash and secure multiparty computation.

When the security of a good cryptographic system fails, it is rare that the vulnerability leading to the breach will have been in a quality cryptographic primitive. Instead, weaknesses are often mistakes in the protocol design (often due to inadequate design procedures, or less than thoroughly informed designers), in the implementation (e.g., a software bug), in a failure of the assumptions on which the design was based (e.g., proper training of those who will be using the system), or some other human error. Many cryptographic protocols have been designed and analyzed using ad hoc methods, but they rarely have any proof of security. Methods for formally analyzing the security of protocols, based on techniques from mathematical logic, and more recently from concrete security principles, have been the subject of research for the past few decades. Unfortunately, to date these tools have been cumbersome and are not widely used for complex designs.

(en.wikipedia.org/wiki/**Cryptography**)

List of words and expressions

primitive – примитив (функция или оператор)
a one-way function – однонаправленная функция
intended to be – предназначенный быть
to compute – вычислять, подсчитывать
to invert - инвертировать
feasibility – выполняемость; технические возможности
versus – в противовес; против
pseudorandom – псевдослучайный
to encounter – наталкиваться
PGP – Pretty Good Privacy – «Довольно хорошая секретность» (программа шифрования)
SSL – Secure Sockets Layer – протокол защищенных сокетов (криптографический протокол)

TLS – Transport Layer Security – протокол защиты транспортного уровня
PKI – Public Key Infrastructure – инфраструктура открытых ключей
permutation – [pɜːmjʊˈteɪʃ(ə)n] – перестановка; подстановка (математическая операция, изменяющая порядок следования компонентов вектора)
пермутация, перестановка групп каналов
trapdoor – лазейка; потайной ход (слабое место в шифросистеме)
backup data – дублирующие данные
proof system – система доказательств
breach – прорыв; брешь; дыра
a software bug – закладка
ad hoc methods – специальные методы (на данный случай)
cumbersome – обременительный; громоздкий
to date – исчисляться

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What does much of the theoretical work in cryptography concern? 2. What is a one – way function? 3. In which case isn't it known if one –way functions really exist? 4. What are more complicated tools built from? 5. Do secure pseudorandom generators and secure pseudorandom functions exist if one –way functions exist? 6. How must complex functionality in an application be built? 7. What do cryptographic techniques involve? 8. What problems have cryptographic protocols been developed for? 9. Where are often weaknesses mistakes? 10. Have many cryptographic protocols been designed and analyzed using ad hoc methods? 11. What methods have been the subject of research for the past few decades?

Exercise 2. Read and translate the following equivalents. Use them in your own sentences:

to concern cryptographic primitives, basic cryptographic properties, a one-way function, a function intended to be easy to compute, for any cryptographic application to be secure, to be based on computational feasibility assumptions, complicated cryptographic tools, secure pseudorandom generators, secure pseudorandom functions, to exist, assorted protocols, one-way permutations, trapdoor permutations, to capture this general idea, to have been developed for a wide range of problems, interactive proof systems, secret sharing, secure multiparty computation, to fail the security of a good cryptographic system, inadequate design procedures, implementation, to use ad hoc methods, complex designs.

Exercise 3. Complete the sentences with the missing words and expressions:

concerns, to be secure, must exist, built from, include, cases, techniques, among, captures, for, cryptographic, designed and analyzed, rarely, based on, more recently, the subject of research.

1. …….protocols have been developed ….. a wide range of problems.
2. For any cryptographic application ………… (if based on such computational

feasibility assumptions), one-way functions……….

3. In many….., cryptographic……. involve back and forth communication …… two or more parties in space (e.g., between the home office and a branch office) or across time (e.g., cryptographically protected backup data).

4. Methods for formally analyzing the security of protocols, ……. techniques from mathematical logic, and….. from concrete security principles, have been…….. for the past few decades.

5. Other cryptographic primitives……… the encryption algorithms themselves, one-way permutations, trapdoor permutations, etc.

6. More complicated cryptographic tools are then …… these basic primitives.

7. Much of the theoretical work in cryptography………….. cryptographic primitives — algorithms with basic cryptographic properties.

8. The term cryptographic protocol…… this general idea.

9. Many cryptographic protocols have been………. using ad hoc methods, but they ……have any proof of security.

Language Work

Exercise 1. Insert the prepositions:

1. More complicated cryptographic tools are built … these basic primitives.

2. Historically , ciphers were often used … encryption and decryption.

3. Steganography was first developed … ancient times.

4. Cipher-texts always reveal statistical information … the plaintext.

5. Many computer ciphers can be characterized … their operation on binary bit sequences.

6. A significant disadvantage … symmetric ciphers is the key management necessary to use them securely.

7. Public – key algorithms are most often based … the computational complexity of "hard" problems.

Keys : of , for , on , from ,by , in , about.

Exercise 2.Insert the missing words into the gaps. Use your grammar skills:

to concern, to compute, to invert, to be secure, to exist, secure, one-way, to be built, to include, permutations, techniques, to involve, to develop, to be designed, to be the subject of research

1. Much of the theoretical work in cryptography …… cryptographic primitives and their relationship to other cryptographic problems.

2. A one-way function is a function intended to be easy …… but hard ….. .

3. In a very general sense, for any cryptographic application…., one-way functions must …..

4. If functions …..exist, then …. pseudorandom generators and secure pseudorandom functions exist.

5. Complex functionality in an application must ….. in using combinations of these algorithms and assorted protocols.

6. Other cryptographic primitives ….. the encryption algorithms themselves, one-way……, trapdoor permutations, etc.

7. In many cases, cryptographic …… ….. back and forth communication among two or more parties in space or across time.

8. Cryptographic protocols……… for a wide range of problems.

9. Many cryptographic protocols …… and analyzed using ad hoc methods, but they rarely have any proof of security.

10. Methods for formally analyzing the security of protocols, based on techniques from mathematical logic, and more recently from concrete security principles, ……of research for the past few decades.

Discussion

Exercise 1. Collect all the information about problems of the encryption of any kind of data and write down a short abstract

Exercise 2. Speak on the problems mentioned in your abstract

Unit VII. NETWORK AND SYSTEM SECURITY

Text 1. SECURITY

Many operating systems include some level of security. Security is based on the two ideas that

The operating system provides access to a number of resources, directly or indirectly, such as files on a local disk, privileged system calls, personal information about users, and the services offered by the programs running on the system.

The operating system is capable of distinguishing between some requesters of these resources who are authorized (allowed) to access the resource, and others who are not authorized (forbidden). While some systems may simply distinguish between "privileged" and "non-privileged", systems commonly have a form of requester *identity*, such as a user name. Requesters, in turn, divide it into two categories.

Internal security: an already running program. On some systems, a program once it is running has no limitations, but commonly the program has an identity which it keeps and is used to check all of its requests for resources.

External security: a new request from outside the computer, such as a login at a connected console or some kind of network connection. To establish identity there may be a process of *authentication*. Often a username must be quoted, and each username may have a password. Other methods of authentication, such as magnetic cards or biometric data might be used instead. In some cases, especially connections from the network, resources may be accessed with no authentication at all.

In addition, to the allow/disallow model of security, a system with a high level of security will also offer auditing options. These would allow tracking of requests for access to resources (such as, "who has been reading this file?").

Security of operating systems has long been a concern because of highly sensitive data held on computers, both of a commercial and military nature. The United States Government Department of Defense (DoD) created the *Trusted Computer System Evaluation Criteria* (TCSEC), which is a standard that sets basic requirements for assessing the effectiveness of security. This became of vital importance to operating system makers, because the TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information.

Internal security can be thought of as protecting the computer's resources from the programs concurrently running on the system. Most operating systems set programs running natively on the computer's processor, so the problem arises of how to stop these programs doing the same task and having the same privileges as the operating system (which is after all just a program too). Processors used for general purpose operating systems generally have a hardware concept of privilege. Generally less privileged programs are automatically blocked from using certain hardware instructions, such as those to read or write from external devices like disks. Instead, they have to ask the privileged program (operating system kernel) to read or write. The operating system therefore gets the chance to check the program's identity and allow or refuse the request.

Internal security is especially relevant for multi-user systems; it allows each user of the system to have private files that the other users cannot tamper with or read. Internal security is also vital if auditing is to be of any use, since a program can potentially bypass the operating system, inclusive of bypassing auditing.

Typically an operating system offers (hosts) various services to other network computers and users. These services are usually provided through ports or numbered access points beyond the operating systems network address. Typically services include offerings such as file sharing, print services, email, web sites, and file transfer protocols.

At the front line of security are hardware devices known as firewalls. At the operating system level, there are a number of software firewalls available. Most modern operating systems include a software firewall, which is enabled by default. A software firewall can be configured to allow or deny network traffic to or from a service or application running on the operating system. Therefore, one can install and be running an insecure service, such as Telnet or FTP, and not have to be threatened by a security breach because the firewall would deny all traffic trying to connect to the service on that port.

(From Wikipedia, the free encyclopedia)

List of words and expressions

local disk – локальный диск
requester – лицо, сделавшее запрос
login – 1) начало сеанса (*работы с терминалом*)
2) вход в систему
3) регистрационное имя (*сообщаемое пользователем при входе в систему*)
console – консоль, пульт (управления)
authentication – аутентификация
a running program – выполняемая программа
an auditing option – опция введения аудита (контроля)
concurrently – параллельно, одновременно
natively – естественным образом
kernel –ядро
to tamper with – подделывать что-либо
auditing – аудит; проверка, введение контроля
firewall – брандмауэр
by default – по умолчанию
to deny – отрицать, отвергать
FTP (File Transfer Protocol) – протокол передачи файлов
port – порт; многоразрядный вход; (выход) устройства
a security breach – брешь в системе защиты
privileges – права (доступа); полномочия; привилегии

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What is security based on? 2. What does the operating system provide? 3. Is the operating system capable of distinguishing between several requesters? 4. What is internal security? 5. What is external security? 6. Which process may there be to establish identity? 7. What options will a system with a high level of security offer? 8. Why has security of operating systems been a concern? 9. What sets basic requirements for assessing the effectiveness of security? 10. Why did this standard become of vital importance to operating system makers? 11. How can internal security be thought of? 12. What does the problem of

most operating systems arise of? 13. Do processors used for general purpose operating systems have a hardware concept of privilege? 14. Which programs are automatically blocked from using certain hardware instructions? 15. What systems is internal security relevant for? 16. What does it allow each user of the system? 17. What are various services provided through? 18. Where are there a number of software firewalls available? 19. Do most modern operating systems include a software firewall? 20. What can a software firewall be configured for?

Exercise 2. Read and translate the following equivalents. Use them in your own sentences:

Operating systems, level of security, a number of resources, indirectly, privileged system calls, the programs running on the system, to be capable of distinguishing, authorized (allowed) to access, not authorized (forbidden), requester identity, internal security, to have no limitations, to check all of its requests for resources, external security, a login, a console, to establish identity, a process of authentication, to be quoted, biometric data, instead, the allow/disallow model of security, to offer auditing options, a concern, highly sensitive data, of a commercial and military nature, the Trusted Computer System Evaluation Criteria (TCSEC), to set basic requirements, to assess the effectiveness of security, storage and retrieval of sensitive or classified information, the programs concurrently running on the system, external devices, operating system kernel, to check the program's identity, relevant, to tamper with, to bypass, to host, file transfer protocols, firewalls, by default, a security breach, to deny all traffic.

Exercise 3. Reread the text to find the corresponding ending for each of the sentences:

1. Many operating systems	– is an already running program that can be thought of as protecting the computer's resources from the programs concurrently running on the system and is especially relevant for multi-user systems.
2. The operating system	– there may be a process of *authentication*.
3. The operating system	– offers various services to other network computers and users.
4. Internal security	– provides access to a number of resources.
5. External security	– include some level of security.
6. To establish identity	– is capable of distinguishing between some requesters of these resources who are authorized (allowed) to access the resource, and others who are not authorized (forbidden).
7. An operating system	– would deny all traffic trying to connect to the service on that port.
8. Hardware devices known firewalls	– can be configured to allow or deny network traffic to or from a service or application running on the operating system.
9. A software firewall	– is a new request from outside the computer.
10. The firewall	– are at the front line of security.

Language work

Exercise 1. Complete the following sentences using the correct preposition:

for at by to of with on in

1. Most current operating systems are capable ……… using TCP/IP networking protocols.

2. An identity is used to check all of its requests ………. resources.

3. Network security consists of the provisions made ………. an underlying computer network infrastructure and policies adopted ……. the network administrator.

4. Security of operating systems has long been concern because of highly sensitive data held ……… computers.

5. Typically an operating system offers various services …….. other network computers and users.

6. A computer host's security is vulnerable to users ……… higher access privileges.

7. ……….. the front line of security are hardware devices known as firewalls.

Exercise 2. Rewrite the following sentences without changing the meaning, using **have to, can't, can, could, must:**

Example: To remember this information, it's necessary to review it several times.
To remember this information, *you have to* review it several times.

1. You are not allowed to share resources such as files, printers, and scanners using either wired or wireless connections.
You ……………. share resources such as files, printers, and scanners using either wired or wireless connections.

2. Some requesters were authorized to access the resource.
Some requesters ………. access the resource.

3. To protect the network, the network administrator is obliged to adopt policies.
To protect the network, the network administrator ……….. adopt policies.

4. These services are allowed to be accessed by the network users.
These services ……….. be accessed by the network users.

5. He said it was possible for us to check all the requests for resources.
He said we …….. check all the requests for resources.

6. Is it necessary to refuse the request?
Do you ……… refuse the request?

Exercise 3. Write out all examples with the Passive Voice from the text. Translate the sentences:

Exercise 4. Translate into English.

Зачем нужен брандмауэр?

Брандмауэр защищает компьютер от проникновения хакеров или вредоносных программ (например, червей) по сети или через Интернет. Брандмауэр также помогает предотвратить отправку программ на другие компьютеры.

Даже если вы считаете, что на компьютере нет ничего интересного для посторонних, вредоносные программы (сетевые черви) могут сделать ваш компьютер полностью неработоспособным, а также кто-то может воспользоваться им для рассылки подобных программ или вирусов другим компьютерам без вашего ведома.

Class activity
Exercise 1. Outline the main ideas of the text:

Text 2. HOW DIFFERENT IS NETWORK SECURITY FROM COMPUTER SECURITY?

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together.

Securing network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense. Computer security is more like providing means of self-defense to each individual citizen of the country. The former is better and practical to protect the civilians from getting exposed to the attacks. The preventive measures attempt to secure the access to individual computers the network itself thereby protecting the computers and other shared resources such as printers, network-attached storage connected by the network. Attacks could be stopped at their entry points before they spread. As opposed to this, in computer security the measures taken are focused on securing individual computer hosts. A computer host whose security is compromised is likely to infect other hosts connected to a potentially unsecured network. A computer host's security is vulnerable to users with higher access privileges to those hosts.

Network security starts from authenticating any user. Once authenticated, firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network. An intrusion prevention system (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.

(From Wikipedia, the free encyclopedia)

List of words and expressions

network administrator	администратор сети
policy	политика, стратегия
unauthorized access	несанкционированный доступ (НСД)
entry point	точка входа
preventive measures	предупредительные меры

network-attached storage (NAS) – сетевая система хранения (данных);
сетевые устройства хранения (данных)
computer worms – компьютерные черви (вирусы)
an intrusion prevention – предотвращение вмешательства
malware – *комп.* вредоносные программы вторжений (например, вирусы, трояны, их цель – нарушение нормальной работы ПК).
suspicious – подозрительный
denial of service – отказ от обслуживания
honey pot – *Интернет* "ловушка" (программа, сервис, система, компьютер, задачей которого является «принять удар на себя», т.е.”honey pot” – это специально подготовленный для взлома компьютер).
decoy – ловушка, приманка, ложная цель

Exercises

Comprehension Check

Exercise 1. Put down problem questions to the text. Ask each other in class to get the true answers

Exercise 2. Translate the following equivalents into English using the text:

безопасность сети, условия, компьютерная сетевая инфраструктура, лежащая в основе, доступные через сеть ресурсы, неразрешенный доступ, применять соответствующую защиту, превентивные меры, таким образом, остановка атаки в пункте ввода, распространяться, в отличие от, уязвимый, сервер, авторизация пользователя, потенциально вредная информация, компьютерные вирусы, отказ в обслуживании, информация может быть закодирована, ловушки, приманки, наблюдение, улучшать безопасность.

Language Work

Exercise 1. Write the question tags for the statements:

1. He hasn’t read the program yet, *has he*?
2. The preventive measures attempt to secure the access to individual computers, ______?
3. Crimeware can wait for the user to log into their account at a financial institution, ____?
4. Crimeware represents a growing problem in network security, __________?
5. This policy wasn’t adopted by the network administrator, _________?
6. This system will protect the network from attacks such as denial of service, ________?
7. Complexity theory seeks to determine the minimum number of components needed for these systems, __________?
8. Much attention, both theoretical and practical, has been given to the design, _____?
9. This standard wasn’t used to evaluate computer systems being considered for the data processing, ______________?

Exercise 2. Unjumble the sentences:

1. The in consists computer network an made network of security infrastructure underlying provisions.
2. Suspicious network anomalies for network also protect to for contents, and the attacks as volume denial such of service IPS monitors traffic from.
3. Authenticating starts any security network from user.
4. Be network maintain two privacy encrypted using to between communication could the hosts.
5. A deployed resources early-warning in as and network-accessible and network decoy tools surveillance could be honeypots.
6. (IPS) such prevention intrusion prevent detect helps system and malware an.
7. Individual are taken computer on measures security hosts the in focused securing computer.

Exercise 3. Complete these sentences with the correct preposition:

1. This securing network infrastructure is very different ……….. that one.
2. Network security consists ………the provisions made in an underlying computer network infrastructure.
3. Who is responsible ……. this detection system?
4. This can allow hackers to break ………networks for malicious purposes.
5. The measures are focused …………securing individual computer hosts.
6. Communication ………..two hosts could be encrypted to maintain privacy.
7. Cybercriminals use a variety of techniques to steal confidential data ……….. crimeware.

Discussion

Exercise 1. Speak about the difference of network security from computer security

Text 3. DATA LOSS PREVENTION

Data Loss Prevention (**DLP**) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Also referred to by various vendors as **Information Leak Detection & Prevention** (**ILDP**), **Information Leak Prevention** (**ILP**), **Content Monitoring and Filtering** (**CMF**) or **Extrusion Prevention System** by analogy to Intrusion-prevention system.

Today’s security professionals face a daunting challenge: Protecting the organization’s most valuable asset, its information, amidst widespread investment in new, more efficient communication technologies. As organizations invest in new business systems and processes to exchange critical information to, from and about customers, partners, and employees in real time, more opportunity exists for information leaks. Data breaches are rapidly becoming the forerunner of IT security concerns, in part because of the increase in both the frequency and severity of such breaches. For security professionals, the pressure to provide data security is influenced by three factors: 1) regulatory compliance, 2) protecting confidential data, and 3) mitigating the risk and associated cost of a breach.

Information leaks are not solely relegated to organizations with customer data or regulatory requirements; many non-regulated companies share a need to secure sensitive data. Intellectual Property (IP), M&A plans, and other critical assets are strategic to many organizations’ success and competitive advantage. These organizations are as concerned about leaks (both external and internal) as regulated companies because of the strategic nature of the information they manage and the frequency with which they fall victim to leaks.

Over the years, organizations have spent a tremendous amount of resources in hopes of protecting their information. However, their efforts have been focused on preventing outsiders from hacking into the organization, educating employees, and securing data at rest. According to analyst firms, the majority of all leaks are the result of unintentional information loss from employees and partners, both external and internal leaks.

Gateway-based systems are usually dedicated hardware/software platforms, typically installed on the organization's internet network connection, that analyze network traffic to search for unauthorized information transmissions. They have the advantage that they are simple to install, and provide a relatively low cost of ownership. Because decoding network traffic at high speed is extremely complex and difficult (transmitted objects are broken into small parts, often encoded, and then mixed with other traffic), Network based systems typically integrate with or include technologies to discover information 'at rest' while it is stored in file systems and databases. Discovering sensitive data at rest is far simpler and less time critical, thereby allowing greater levels of accuracy. Taking 'signatures' of data identified at rest, and then looking for such signatures as data passes over the network boundary, is a technique favored by virtually all Network system vendors to improve accuracy, and to identify sensitive data that would otherwise be missed. The technique does suffer from the disadvantage that it must have previously been scanned at rest in order to be identified, and therefore newly created data, for example typed directly into an email message, is often missed.

Network systems have the disadvantage that they can only monitor external communications, and therefore cannot consider internal leaks - between departments for example, and that they are easily defeated by encryption, or even compressing sensitive data in a Zip (file format) or similar archive.

Host Based ILD&P systems run on end-user workstations or servers in the organization. Since they are not limited to operation at the network boundary, host based systems can address internal as well as external communications, and can therefore be used to control information flow between groups or types of users (eg 'Chinese walls').

Workstation systems have the advantage that they can monitor and control access to physical devices (such as USB keys, iPods etc) and in some cases can access information before it has been encrypted. Workstation systems can also provide granular application controls to block attempted transmissions of confidential information, and provide immediate feedback to the user. They have the disadvantage that they need to be installed on every workstation in the network, cannot be used on mobile devices (eg Blackberry), or where they cannot be practically installed (for example on a workstation in an internet café using Outlook Web Access to send corporate email).

Server based systems, for example on email or file servers, have the advantage that they only need to be installed on a relatively small number of machines, but provide protection for a full range of corporate email clients (eg Blackberry and Web clients). They do however require deep integration with messaging and file systems, and few vendors provide them.

The most comprehensive protection is provided by solutions where both Network and Host based systems are combined, preferably within a single management platform where rules are defined centrally and distributed automatically, and where results are gathered and presented in a single console. This approach is endorsed by industry analysts.

(From Wikipedia, the free encyclopedia)

List of words and expressions

information leak – утечка информации
to endorse – одобрять; аттестовать
daunting – пугающий
amidst – в середине
real time – фактическое время; интерактивный режим работы
security concern – важность защиты
severity – серьёзность, опасность
regulatory compliance – регулярная уступчивость
mitigating the risk – уменьшающий риск
to relegate – передавать, направлять
at rest – в покое
granular – гранулированный

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. Which systems does Data Loss Prevention refer to? 2. Why is there the problem of information leaks? 3. What factors is the pressure to provide data security for professionals influenced by? 4. Are information leaks solely relegated to organizations with customer data or regulatory requirements? Why not? 5. Why are these organizations as concerned about leaks as regulated companies? 6. What have organizations' efforts been focused on? 7. What are the majority of all leaks according to analyst firms? 8. Where are gateway-based systems typically installed? 9. Why do they analyze network traffic? 10. What advantage do these systems have? 11. What do network based systems deal with? 12. What disadvantage does this technique suffer from? 13. What can you say about host based ILD&P systems? 14. Can workstation systems monitor and control access to physical devices? 15. What disadvantage do they have? 16. What advantage do server based systems have? 17. Which approach is endorsed by industry analysts?

Exercise 2. Read and translate the following equivalents. Use them in your own sentences:

data loss prevention, to refer to, to prevent the unauthorized transmission of information, various vendors, Information Leak Detection, Content Monitoring and Filtering, Extrusion Prevention System, to face a daunting challenge, the most valuable asset, amidst, widespread investment, data breaches, regulatory compliance, to mitigate, to share a need to secure sensitive data, to spend a tremendous amount of resources, unintentional information loss, gateway-based systems, to analyze network traffic, ownership, to decode network traffic at high speed, over the network boundary, to monitor external communications, to compress sensitive data in a Zip (file format), to run on end-user workstations or servers, to monitor and control access to physical devices, USB keys, iPods, to provide granular application controls, the most comprehensive protection, within a single management platform, to gather and present results in a single console, to be endorsed, to provide something currently.

Language Work

Exercise 1. Write these adjectives with all the nouns they can go with. Add more adjectives to each list:

reliable compact easy to use convenient various efficient confidential competitive unintentional

a person____

a system____

a vendor____

technology____

data____

protection____

Exercise 2. Give your own definition to the following terms and put them down:

data loss prevention; information loss; sensitive data; gateway - based systems; network traffic; disadvantage; confidential information; external communication.

Exercise 3. Read the text and define the italicized verb forms:

data corruption *refers* to errors in computer data that occur during transmission or retrieval, *introducing* unintended changes to the original data. Computer storage and transmission systems use a number of measures *to provide* data integrity, the lack of errors.

Data corruption during transmission has a variety of causes. Interruption of data transmission causes information loss. Environmental conditions can interfere with data transmission, especially when *dealing* with wireless transmission methods.

When data corruption behaves as a Poisson process, where each bit of data has an independently low probability of *being changed*, data corruption can generally *be detected* by the use of checksums, and can often be corrected by the use of error correcting codes.

If an uncorrectable data corruption *is detected*, procedures such as automatic retransmission or restoration from backups can be applied. RAID disk arrays, store and evaluate parity bits for data across a set of hard disks and can reconstruct *corrupted* data upon of the failure of a single disk.

If appropriate mechanisms are employed *to detect* and remedy data corruption, data integrity *can be maintained.* This is particularly important in banking, where an undetected error can drastically affect an account balance, and in the use of *encrypted* or *compressed* data, where a small error can make an extensive dataset unusable.

(From http://en.wikipedia.org/wiki/Data_corruption)

Oral Practice

Exercise 1. Reproduce the text in your own words

Text 4. SECURITY AND PERFORMANCE MANAGEMENT

Security management tools allow the network manager to restrict access to various resources, from the applications and files to the entire network itself; these generally offer password-protection schemes that give users different levels of access to different resources.

For instance, a user in marketing could be allowed to view, or read a data file in accounting but not be permitted to change or write to it.

Security management is also important in managing the network itself – for instance, only certain individuals (such as network administrators) should be permitted to change configuration settings on a server or other key network devices.

Performance management tools produce real-time and historical statistical information about the network's operation: how many packets are being transmitted at any given moment, the number of users logged into a specific server, and utilization of internetwork lines. As already noted, this type of information can help network administrators pinpoint areas or network segments that pose potential problems.

Most network operating systems (NOSs) provide some level of network management capabilities; in particular, almost all the leading NOSs offer password-protection schemes that limit users' access to network resources. Novell, for instance, implements its NetWare management schemes through user profiles, which define not only the user's access rights, but the users' classifications (supervisor, workgroup manager, console operator, or user), which also determine the resources they can access.

In this scheme, a supervisor has access rights that allow reconfiguring and upgrading the entire system. The workgroup manager, available with NetWare 3.X, controls only the resources of a single user or user group. This concept allows a supervisor to distribute some of the responsibility for maintaining the network to others around a large network.

A user with console operator access rights can run NetWare's FCONSOLE utility, which allows monitoring and controlling a variety of network performance criteria, such as print queues. The user can access only those resources allowed by the supervisor (or workgroup manager with NetWare 3.X). Although users can access the NetWare management utilities, their rights to actually perform management functions are severely limited.

Although other NOSs' access schemes may differ in specific features from NetWare's, they all offer similar resource-restriction capabilities that give the network managers control over their networks.

(From mk:@MSIT Store:C:\Documents)

List of words and expressions

security management – управление защитой (безопасностью)

to log – записывать (регистрировать)

internetwork line – межсетевая линия

to pinpoint – точно определить

user profile – *безоп.* профиль пользователя

комп. параметры (профиль) пользователя,

upgrading – модернизация, совершенствование

console – пульт (управления); консоль; пульт оператора

queue – очередь; очередность, список очередности

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What allows the network manager to restrict access to various resources? 2. What do

password-protection schemes give users? 3. Is security management important in managing the network itself? 4. What information do performance management tools produce? 5. Can this type of information help network administrators pinpoint areas or network segments? 6. What do most network operating systems concern with? 7. Can user profiles define only the user's access rights? 8. What is the workgroup manager available with? 9. Which resources can the user access? 10. What gives the network managers control over the network?

Exercise 2. Use the text to translate the following equivalents. Use them in your own sentences:

Инструменты управления безопасностью, ограничивать доступ к различным ресурсам, вся сеть полностью, предлагать схемы защиты при помощи паролей, предоставлять пользователям различные уровни доступа, не разрешается изменять файлы, изменять установки, информация в режиме реального времени, быть подключенным к определенному серверу, выделять области и сегменты сети, представлять потенциальные проблемы, классифицировать пользователя, позволять реконфигурацию и обновление всей системы, различаться в определенных технических характеристиках.

Language Work

Exercise 1. Complete the statements using the words from the box:

report *software* *data* *access* *important* *supervisor*

1. A user in marketing could not be permitted to change or write to a …… file.
2. Security management is also …… in managing the network itself.
3. A file server might …… the number of users logged in.
4. Password-protection schemes limit users' …… to network resources.
5. A …… has access rights that allow reconfiguring and upgrading the entire system.
6. Configuration management applications deal with installing, initializing, booting, modifying, and tracking the configuration parameters or options of network hardware and …… .

Exercise 2. Choose the best alternatives in the following sentences:

1. Crimeware *represents / is represented* a growing problem in network security as many malicious code threats seek to pilfer confidential information.
2. Cybercriminals *are used / use* a variety of techniques to steal confidential data through crimeware.
3. Individual events *are tracked / track* for audit purposes and for a later high level analysis.
4. Hacking and system cracking *appeared / were appeared* with the first electronic computers.
5. Any deviations from the Inspection technologies, server operating software and applications *require / are required.*
6. This standard *applied / was applied* to protect packets both between hosts and between network security gateways like routers or firewalls.

Class Activity

Exercise 1. Speak about Network and Systems management. Make a short oral

summary. Present it to the class

Text 5. NETWORK SECURITY AND BACKUP SYSTEMS

Prevention is the key when it comes to network security. Identifying and stopping intrusion – in all its forms – is what security is all about. But identifying a potential intrusion is not always obvious, or likely. The usual security suspects – CIA agents, and industrial espionage – make great headlines, but they don't pose real risks to the average company. However, just because you're not building the next secret weapon doesn't mean that you're not at risk from security breaches. Far more often, security risks come from acts committed out of human error, greed, malcontent, or machine error.

Physical theft, electronic tampering, and unauthorized access are just three of the more obvious threats to network equipment and data. Physical theft includes people stealing computers, taking floppies with data, and tapping into the cable to siphon off information. Electronic tampering covers computer viruses and other malicious reprogramming. Unauthorized access, the most common threat to security, usually occurs when people see information they shouldn't.

Networks seriously increase access to your information, and with access comes the responsibility of restriction and control. In addition to the usual sources of security breaches—people taping passwords to their monitors and using scanners to electronically eavesdrop—networks invite a whole host of other vulnerabilities. It's easy enough to drop another workstation or server on the network or add another application. Add the ability to dial into the network system, and you pose an even greater risk.

There is no simple formula for calculating your security needs. The amount of security depends upon the threat you perceive. In some cases, the need for security is clear: banks, airlines, credit card companies, and insurance companies. In other cases, the risks may be less obvious. Allowing any worker to examine the payroll file makes for disgruntled employees. Your personal calendar indicates when you are out of town. The following are some of the more common risks to network security.

Your network can be a danger to itself. Being made of mechanical components, a network can do itself damage when disk heads crash, servers fail, and power supplies blow. Tape and disk platters get old and go bad. Bugs, such as in an out-of-control operating system process or one with a faulty memory mapping, destroy data. Monitor mechanical equipment for wear. For critical components, keep spares onsite or, if warranted, online.

Your network is physically vulnerable. Thieves and other intruders can physically break into your building, wiring closet, or server room and steal or vandalize equipment and data. When a file is erased, very often it physically remains on disk or tape – only the entry to the directory structure is removed. Sensitive documents may be printed out and left lying around the office, waiting for prying eyes or thieving hands.

Your first line of defense is the simplest: Use locks, guards, and alarms to protect against these physical vulnerabilities. Lock servers in a room and lock wiring closets, permitting access to only those with a key. Sensitive data must be completely wiped off the media when deleted. Shred all sensitive printouts. Bolt expensive equipment to the floor or to a desk. A slew of products exist to prevent intruders from physically taking equipment. Most involve locking equipment with metal bars, in steel cabinets, or with large chains. Others sound loud alarms to deter the thief. These products can help to keep your equipment from being physically stolen (it also makes them difficult to move from one station to another). If your security needs are extreme, you might employ biometric devices.

Biometric devices use a physical aspect of people, such as their fingerprints, to verify their identity.

The next step is to secure the cable. Copper cable gives off electromagnetic radiation, which can be picked up with listening devices, with or without tapping into the cable. One solution is to fiber-optic cable, which does not emit electromagnetic signals and is more difficult to tap without detection.

Diskless PCs are a popular security measure. A diskless PC lacks floppy and fixed drives. Users must boot the computers off the file server. With no drives, no way to remove data physically exists. However, be aware that diskless PCs with serial and parallel ports and expansion slots are insecure. A user can insert a removable disk into an expansion slot and remove data. Or the user can attach a printer.

Another step is to physically limit access to data sources. Use the keyboard lock on PCs and file servers. Lock file servers in closets or computer rooms, thus preventing direct access and forcing intruders to circumvent network security. Rooms with doors and locks are good places for printers and other output devices since printed data may be as sensitive as electronic data.

Viruses are potentially one of the most dangerous and costly types of intrusion. Although they are relatively rare to a well-kept network, the penalties inflicted by a virus can be severe. Your network is vulnerable at any point it contacts the outside world, from floppy drives to bridges to modem servers. At these external contacts, your network's messages can be intercepted or misrouted. Workers take notebooks on the road and may come into contact with a virus-infected computer. Users may take work home, where their home computers are infected. Demonstration programs, bulletin boards, and even shrink-wrapped software may have viruses.

Protecting your network against a computer virus is much the same as protecting it from unauthorized access. If intruders can't access the network, they can't unleash a virus. However, many viruses are introduced by unwitting authorized users. Any new software should be suspected of having viruses. Although programs from bulletin boards may sometimes be infected, several software companies have shipped shrink-wrapped software that was infected with a virus. While specialized programs can look out for viruses and limit the havoc they wreak, no program can prevent a virus. It can only deal with the symptoms.

Intentional threats are also potentially damaging. Employees and outsiders pose intentional threats. Outsiders – terrorists, criminals, industrial spies, and crackers – pose the more newsworthy threats, but insiders have the decided advantage of being familiar with the network. Disgruntled employees may try to steal information, but they may also seek revenge by discrediting an employee or sabotaging a project. Employees may sell proprietary information or illegally transfer funds. Employees and outsiders may team up to penetrate the system's security and gain access to sensitive information.

Workstation file systems present a threat to the network. DOS is easy to circumvent. Intruders can use the many available programs to get at a hard disk and remove data, even if security programs are at work. For this reason, high security installations may want to use a different operating system, one with a different file system. Unix has sophisticated file security, and additional programs are available for even more protection.

Your network radiates electromagnetic signals. With an inexpensive scanner, experienced electronic eavesdroppers can listen in on your network traffic and decode it. Shielded cable, such as coax and shielded twisted pair, radiates less energy than unshielded cable, such as telephone wire. Fiber-optic cable radiates no electromagnetic energy at all – since it uses light instead of electrical signals to transmit—and it's relatively easy to detect taps into a fiber cable, since these decrease the light level of the cable. If your installation demands maximum security, Tempest-certified equipment shields electromagnetic emissions.

By far the most common network intrusion is unauthorized access to data, which can take many forms. The first line of defense against unauthorized access should be the workstation interface. Login passwords are a must. Nearly all network operating systems will not give workstation users access to network resources without the correct password. To make passwords more effective, the administrator should assign them and change them at random intervals. Don't let users post their passwords on their monitors or desk blotters. Use mnemonic passwords to help users remember.

Software is available to blank a user's screen or lock the keyboard after a certain definable period of inactivity. Other software will automatically log a user out of the network. In either case, a password is required to renew activity. This prevents the casual snooper, but not a determined one.

A more secure method to stop unauthorized access is an add-in card for each workstation. This card forces the workstation to boot up from a particular drive every time. It can also enforce some kind of user validation, like a password. If the card is removed, the workstation is automatically disabled.

Your network administrators present yet another risk. If you give them free rein over the applications and data, you're exposing your network to unnecessary risks. Your network administrators manage the network, not the data on it. Administrators should not have access to payroll information, for example. Similarly, don't fall victim to the fallacy that the department heads should have complete access to the network and its information just because they are in charge.

Finally, your network is subject to the whims of nature. Earthquakes, fires, floods, lightning, and power outages can wreak havoc on your servers and other network devices. While the effects of lightning and power outages can be minimized by using uninterruptible power supplies, you'll need to store backups of important data (and perhaps even equipment) offsite to deal with large-scale disasters.

(From mk:@MSIT Store:C:\Documents)

<u>List of words and expressions</u>

headline – заголовок, шапка

electronic tampering – *безоп.* умышленная подделка информации с применением электронных средств; электронное вмешательство

siphon off information – «скачать» информацию; «слить» информацию

to eavesdrop – подслушивать

to perceive – понимать, осознавать

disgruntled employees – недовольные служащие

platter –пластина

bug – неисправность; закладка; «жучок»

prying – пытливый

printout – распечатка; вывод (данных) на печатающее устройство

slew – *разг.* множество, масса

to deter – удерживать, отпугивать

expansion slot – дополнительный разъем; разъем (слот) расширения

inflicted penalties – налагаемые наказания; назначенные наказания

floppy – гибкий магнитный диск; дискеты

drive – дисковод; накопитель
havoc – опустошение, разорение; разрушение
to wreak – причинять ущерб
shielded cable – экранированный кабель
login password – пароль регистрационного имени
casual snooper – случайный человек, сующий нос не в свое дело
to be disabled – стать непригодным, быть поврежденным
to be in charge – руководить; быть ответственным
fallacy – ошибка, заблуждение
to unleash – развязать, дать волю (чему-либо)
unwitting – непреднамеренный
head crash – авария (плавающих) головок (соприкосновение плавающих магнитных головок с поверхностью жесткого диска приводит к порче данных или отказу накопителя)
sensitive documents – критические документы
to tap – перехватывать (сообщение), подслушивать

Exercises

Comprehension Check

Exercise 1. Write some problem questions to text 4 for class discussion

Exercise 2. Suggest the word-combinations equivalent in their meaning to those given in Russian:

защита сети; доступ к Вашей информации; неуправляемая операционная система; защитить от уязвимости; кабель с медными проводами; блокирующая аппаратура; параллельный порт (многоразрядный вход); экранированная скрученная пара проводов; случайный интервал; правильный пароль.

Language Work.

Exercise 1. Complete the following sentences using parts from the right-hand column. Translate them:

1. The encrypted stream of traffic forms a secure tunnel	of authentication and encryption protocols.
2. Internet Protocol Security is a set	to encrypt and decrypt a message.
3. There is no formula for	than unshielded cable.
4. Symmetric cryptosystems use the same key	across an otherwise unsecured IP network.
5. Deep inspection technology has detectors which are built	calculating your security needs.
6. Shielded cable radiates less energy	on TCP / IP protocol specifications.

Class Activity

Exercise 1. Be ready to talk on the following topics:

1. Networking is a risky business.
2. Network protecting against a computer virus is as important as protecting it from unauthorized access.

Text 6. THREE FORMS OF DATA SECURITY AND SECURITY PROBLEMS

Information security entails making sure the right people have access to the right information, that the information is correct, and that the system is available. These aspects are referred to as confidentiality, integrity, and availability.

Information stored on a network often needs to be confidential, and a secure network does not allow anyone access to confidential information unless they are authorized. The network should require users to prove their identities by providing something they know, such as a password, or by providing something they possess, such as a card key. Most network operating systems and many applications packages use passwords.

In government circles, this aspect of security hinges on secrecy; access to information is granted according to security clearance. In commercial circles, this aspect of security comes more from confidentiality, where only users who need to know the private information have access.

Guarding access to information is one aspect of security; the security system must also guarantee the information itself is accurate, referred to as data integrity. In providing data integrity, for example, a network ensures that a $14,000 bank account balance isn't really supposed to be $14 million. The system must verify the origin of data and when it was sent and received. Network operating systems grant users access to files and directories on a read, write, create, open, and delete basis. Word processors lock files so more than one user cannot modify the same file at the same time. Databases use record locking to provide a finer granularity of access control.

The third aspect of security is network availability. Although not commonly thought of as part of security, a secure network must also ensure that users can access its information. The network must continue to work, and when a failure occurs, the network devices must recover quickly.

Whatever type of security you implement, diligent watchfulness is important to its success. To help, network operating systems include audit trails that track all network activity, including which workstation has tried to log in to a file server three times unsuccessfully or which files have been changed when they should not have been altered.

Some audit trails can sound alarms when certain events take place. For example, the system manager may want to know when certain files are open, or when unusual traffic takes place. Audit trails will also keep a running log of all that takes place, so the network manager may be able to detect a pattern of intrusion.

Protecting against internal threats requires you to control access to files and applications on a need-to-know basis. Only grant access if users present valid reasons to access the application or data. Use the network operating system's security features to restrict access. Keep audit trails of who accesses what files and when. Enforce the use of passwords.

Such access privileges may be assigned by file, by user or a combination of both. For example, users with a certain security level may read and write to certain files. Those with lower security levels might be restricted to reading these files.

The network manager should create a profile of access privileges for each user. This profile, which is executed when the user logs on, restricts the user to authorized data and devices. Profiles may also be set up for data and devices, limiting their access to only authorized users. Profiles make managing security easier since they provide a consistent method of assigning and maintaining network privileges.

Once a user has workstation and network access, other security barriers can be put in place. Most network operating systems have many levels of access control that limit what resources are available, which data can be accessed, and what operations can be performed. These include restricting who can read and write to certain files, directories, applications, servers, and printers.

To reduce the risk, limit connections to the outside world. When you must make connections, use callback modems, encryption, and virus-detection software. With call-back modems, users must dial into the system, verify their identity, then the modem calls the user back at a predetermined telephone number to establish the connection. Encryption scrambles data into an unreadable format so even if the packets are intercepted, the message remains nonsensical. Upon receipt of the message, only the people who know the private code, or key, can unscramble the data. Virus-detection software will identify many viruses and disable them if possible.

Biometric devices are a rather drastic security measure. Biometric devices use a person's physical characteristics to verify an identity. The verifying physical characteristic varies. Some use fingerprints, others use voice recognition, others scan a person's retina. Biometric devices are quite costly and are for highly secure environments.

(From mk:@MSIT STORE:C\Documents)

List of words and expressions

to entail – влечь за собой; вызывать
to hinge on – зависеть от
security clearance – допуск к секретным материалам; категория допуска; уровень защиты данных
guarding access – строгий доступ; охрана доступа
data integrity – целостность данных
availability – готовность, наличие
to recover – восстанавливать
to log in – вносить (записывать), регистрировать
audit trail – след контроля (аудита); контрольная запись (элемент системы управления безопасностью. Журнал, в котором регистрируются события, кто имел доступ к системе, какие операции выполнял).
a running log – проводимая регистрация (запись)
to enforce – заставлять
a profile – профиль; параметры пользователя
to log on – входить в систему; начало сеанса
to scramble data – зашифровывать (скремблировать) данные
to intercept – перехватывать, вмешиваться
nonsensical – бессмысленный, абсурдный
to disable – запрещать; отключать; блокировать
drastic – решительный
threat – угроза

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What does information security entail? 2. What aspects of information security do you know? 3. Why does information stored on a network need to be confidential? 4. How does the network prove users' identities? 5. What does this aspect of security hinge on in government circles? 6. What does this aspect of security come from in commercial circles? 7. What basis do network operating systems grant users access to files and directories on? 8. When cannot more than one user modify the same file at the same time? 9. What does the third aspect of security concern with? 10. Is diligent watchfulness important to success of security? Why? 11. When can audit trails sound alarms? 12. How may the network manager be able to detect a pattern of intrusion? 13. What does protecting against internal threats require? 14. May users with a certain security level read and write to a certain file? 15. What can you say about users with lower security levels? 16. Which profile restricts the user to authorized data and devices? 17. Do most network operating systems have many levels of access control? 18. What can you do with call – back modems? 19. Why do biometric devices use person's physical characteristics? 20. How does the verifying physical characteristic vary?

Exercise 2. Read the following equivalents and translate them. Make up your own sentences:

the right people have access to the right information, confidentiality, integrity, availability, to prove identities, a card key, many applications packages, to hinge on secrecy, to verify the origin of data, to grant users access to files and directories, to provide a finer granularity of access control, network availability, a failure, to recover quickly, to implement, diligent watchfulness, to log in to a file server, to alter, to sound alarms, to keep a running log of all that takes place, to detect a pattern of intrusion, on a need-to-know basis, to restrict access, to enforce the use of passwords, to be assigned by file, to create a profile of access privileges for each user, to restrict the user to authorized data and devices, to provide a consistent method of assigning and maintaining network privileges, to limit connections to the outside world, to use callback modems, encryption, and virus-detection software, to dial into the system, a predetermined telephone number, to scramble data in to an unreadable format, to remain nonsensical, to verify an identity, to use fingerprints, to use voice recognition, to scan a person's retina, quite costly, highly secure environments.

Language Work

Exercise 1. Put the nouns below into three groups:

a) countable b) uncountable c) countable or uncountable

data, information, network, security, aspect, access, integrity, type, user, profile, time, success, code, virus – detection, encryption, level, software, intrusion, traffic, experience, research.

Exercise 2. Complete the statements using words from the box:

modems *the origin* *for* *naming* *biometric*
to restrict *sent*

1. Passwords, locks, access privileges, and even …….. devices do not always deter the determined intruder.
2. The system must verify ……… of data and when it was sent and received.
3. You must start the planning process by ……. a security administrator.
4. We usually use the network operating system's security features ………… access.
5. Some networks encrypt data when it is …… .
6. With call – back ………. , users must dial into the system.
7. Biometric devices are ….. highly secure environment.

Exercise 3. Put the verbs in brackets into the Past Continuous or Past Simple Tense:

1. This security system (guarantee) data integrity.
2. He (not listen), so he missed what a security administrator said.
3. ………………. intruders from discovering either the key or the time the key was changed? (this measure prevent)
4. While audit trails (keep) a running log of all that took place, the network manager (detect) a pattern of intrusion.
5. Why …… the origin of data? (the system not verify).
6. The security administrator (work) with the department heads all the afternoon to develop a security plan.

Class Activity

Exercise 1. Collect all the material about network security problems and write down a short abstract. Present it to your class

Unit VIII. DATA SECURITY TECHNOLOGIES

Text 1. NETWORK SECURITY TECHNOLOGIES AND PROTOCOLS: AAA, VPN and FIREWALL

Network security covers issues such as network communication privacy, information confidentiality and integrity over network, controlled access to restricted network domains and sensitive information, and using the public network such as Internet for private communications. To address those issues, various network and information security technologies are developed by various organizations and technology vendors. Here is a summary of the technologies:

AAA: Authorization, Authentication and Accounting is a technology for intelligently controlling access to network resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The authorization process determines whether the user has the authority to access certain information or some network sub-domains. Accounting measures the resources a user consumes while using the network, which includes the amount of system time or the amount of data a user has sent and/or received during a session, which could be used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities. A dedicated AAA server or a program that performs these functions often provides authentication, authorization, and accounting services.

VPN: Virtual Private Network is a technology allowing private communications by business and individuals, such as remote access to corporate network, using a public telecommunication infrastructure, such as the Internet. A virtual private network can also be a specially configured network over the public network infrastructure that is only used by one organization. Various network-tunneling technologies such as L2TP are developed to reach this goal. Using encryption technologies such as IPsec could further enhance information privacy over public network and virtual private network.

Firewall: It is a software program or hardware device that filters the information coming through the Internet connection into a private network or computer system. Firewalls use one or more of three methods to control traffic flowing in and out the network:

- Packet filtering - Packets are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- Stateful inspection - compares certain key parts of passing through packets to a database of trusted information. Outgoing information from inside the firewall is monitored for specific defining characteristics, and then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Packet Filtering is the process a piece of software or device takes to selectively control the flow of data to and from a network. Packet filters allow or block packets, usually while routing them from one network to another (most often from the Internet to an internal network, and vice-versa). To accomplish packet filtering, you set up rules that specify what types of packets are to be allowed and what types are to be blocked.

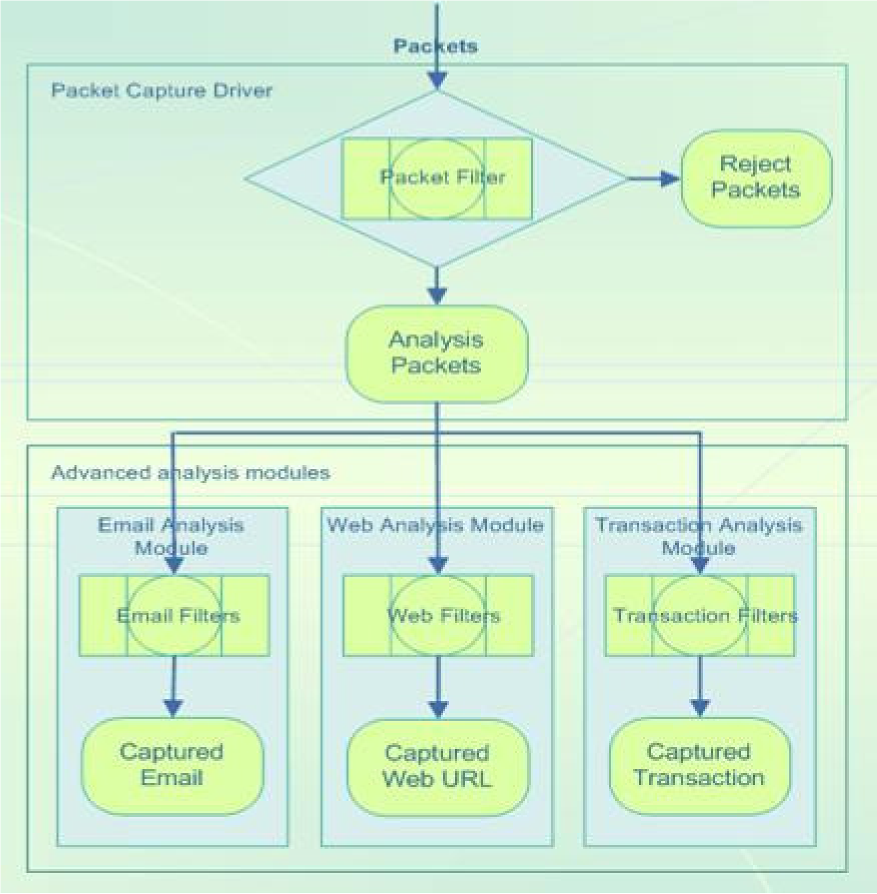
A packet filter examines all packets that pass in and out of it to prevent packets from passing through that do not conform to the configurable rules that are defined. A packet filter can filter packets based upon several criteria:

- the protocol that the packet belongs to (TCP, UDP, and so forth);
- the originating address;
- the destination address;
- the port number of the destination resource (application type);
- the packet direction, out to the Internet or into the local network;
- the signature of a pre-defined packet in database.

Packet Filtering is often a feature incorporated into routers and bridges to limit the flow of information. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate e-mail domains, and perform many other traffic control functions.

Packet filter is one of the key features implemented in a firewall's to examine IP packet headers to determine a packet's origin or destination address and the network transport service used. Traditional packet filters are static and use rule sets to allow or deny packets based solely on header content. Intrusion Detection Systems (IDS) use Packet Filtering techniques to analyze packets by matching certain pre-defined signatures and then alert possible network hackers and intruders.

Packet Filter is also a critical tool in network sniffing, protocol analyzer or packet analyzer tools. Many network sniffing tools have multiple filter types allowing users to filter and view traffic accordingly.



Packet Filtering

(From www.rsasecurity.com)

List of words and expressions

network security – сетевая безопасность, защита сети

UDP – (User Datagram Protocol) – протоколы передачи пользовательских дейтограмм

L2TP-Layer 2 – Tunneling Protocol – сетевой протокол туннелирования канального уровня

IDS (Intrusion Detection System) – система обнаружения (сетевых) атак (вторжений)

TCP (Transmission Control Protocol) – протокол управления передачей

privacy – секретность

restricted domains – ограниченные домены (области)

sensitive information – критическая информация; важная информация

authorization – авторизация; предоставление права на доступ; разрешение

authentication – аутентификация; проверка подлинности

accounting – учет

billing – биллинг; рассылка счетов

virtual private network – виртуальная частная сеть

public telecommunication infrastructure – открытая телекоммуникационная инфраструктура

requesting system – система запроса

to discard – отвергать, отказываться

packet filtering – фильтрация пакетов

proxy service –прокси-сервер; сервер полномочий

to retrieve – выбирать, разыскивать

stateful inspection – *сеть.* технология инспекции пакетов с учетом состояния протокола; метод контроля (проверки) трафика

to conform to – соответствовать

router – маршрутизатор, программа прокладки маршрута

bridge – мост; устройство сопряжения

packet header – заголовок пакета

intruder – злоумышленник; нарушитель

sniffing tools – *безоп.* сниффинг программных сред (прослушивание сетевого трафика путем передач сетевого интерфейса в режим приема всех пакетов)

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. What does network security cover? 2. Are various network and information security technologies developed by various organizations and technology vendors? 3. What kind of technology is AAA? 4. Which process determines whether the user has the authority to access certain information or some network sub-domains? 5. What does authentication provide? 6. What is the function of accounting? 7. What does Virtual Private Network deal with? 8. Can a virtual private network also be a specially configured network over the public network infrastructure? 9. Why are various network-tunneling technologies such as L2TP developed? 10. What do you know about firewall? 11. Why do firewalls use one or more of three methods? 12. What are packets analyzed against? 13. How are packets sent to the requesting system? 14. What is the role of Proxy-service? 15. How can stateful inspection be defined? 16. What is outgoing information from inside the firewall monitored for? 17. Is incoming information compared then to these characteristics? 18. When is the information allowed through? 19. What can you say about packet filtering? 20. What

examines all packets? 21. What do you set up to accomplish packet filtering? 22. What criteria do you know upon that a packet filter can filter packets? 23. What do packet filters let the administrator? 24. What is the role of Intrusion Detection Systems?

Exercise 2. Read and translate the following equivalents. Use them in your own sentences:

To cover the issues, network communication privacy, information confidentiality,

restricted network domains, to address, vendors, Authorization, Authentication, Accounting, enforcing policies, auditing usage, to enter a valid user name, to access some network sub-domains, authorization control, billing, trend analysis, resource utilization, capacity planning activities, VPN: Virtual Private Network, to use a public telecommunication infrastructure, various network-tunneling technologies, a remote access to corporate network, to reach the goal, to enhance information privacy over public network and virtual private network, firewall, to filter the information, to control traffic flowing in and out the network, packet filtering, to discard files, proxy service, to retrieve information, stateful inspection, trusted information, to monitor information for specific defining characteristics, to yield a reasonable match, to rout packets from one network to another, vice-versa, to set up rules, to specify, configurable rules, the originating address, the destination address, the signature of a pre-defined packet in database, a feature incorporated into routers, to limit the flow of information, to isolate e-mail domains, to examine IP packet headers, static, header content, to alert possible network hackers and intruders, network sniffing, to view traffic accordingly.

Exercise 3. Find the corresponding definitions of notions in the left column:

1.	Network security	**A** performs these functions often provides authentication, authorization, and accounting services.
2.	AAA	**B** measures the resources a user consumes while using the network.
3.	The authorization process	**C** network is a technology allowing private communications by business and individuals, such as remote access to corporate network, using a public telecommunication infrastructure, such as the Internet.
4.	Accounting	**D** determines whether the user has the authority to access certain information or some network sub-domains.
5.	A dedicated AAA server	**E** is a technology for intelligently controlling access to network resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.
6.	VPN	**F** covers issues such as network communication privacy, information confidentiality and integrity over network, controlled access to restricted network domains and sensitive information.
7.	Stateful inspection	**G** packets are analyzed against a set of filters.

8. Firewall **H** is a software program or hardware device that filters the information coming through the Internet connection into a private network or computer system.

9. Packet filtering: **I** examines all packets that pass in and out of it to prevent packets from passing through that do not conform to the configurable rules that are defined.

10. Proxy service: **J** compares certain key parts of passing through packets to a database of trusted information.

11. A packet filter **K** information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.

Exercise 4. Complete the sentences with the words from the box:

end use firewall the operating system sending performs information

1. Port scan is the process of …… data packets to potential target computers to see what network services each one offers.
2. Traditional packet filters …… rule sets to allow or deny packets based solely on header content.
3. Deep Inspection firewall …… all the Stateful Inspection functions such as packet filtering, tracking communications packets and sessions over a period of time.
4. Deep Inspection ……is going to provide all the protections of a stateful firewall as well as whatever signatures are loaded into it.
5. If the comparison doesn't yield a reasonable match, the …… is discarded.
6. The encapsulated data is received by the IPsec VPN gateway at the other ……, unwrapped, decrypted, and routed to the recipient.
7. Browsers are presently the most attacked software, so it is imperative that browsers take full advantage of the defenses offered by …….

Exercise 5. Give definitions of the following notions: ***Network security, AAA, VPN, Firewall, Packet filtering, Proxy service, Stateful inspection.*** **Learn them by heart.**

Language work.

Exercise 1. Ask questions to the words in bold to get the information you are interested in:

1. **Various network and information security technologies are developed** by various organizations and technology vendors.
2. Authorization, Authentication and Accounting is a technology **for intelligently controlling access to network resources,** enforcing policies, auditing usage, and **providing the information** necessary to bill for services.
3. **Virtual Private Network** is a technology allowing private communications **by business and individuals.**
4. A virtual private network **can also be a specially configured network** over the public network infrastructure that **is only used by one organization.**

5. Firewall **is a software program or hardware device** that **filters** the information **coming through the Internet** connection **into a private network or computer system**.

6. **To accomplish packet filtering**, you **set up** rules that **specify what types of packets are to be allowed and what types are to be blocked.**

Exercise 2. Choose a sentence from the text to ask all types of questions.

Exercise 3. Write these sentences as First Conditionals. Put the verbs in brackets in the correct form:

1. I (give) you the information if you (telephone) me tomorrow.
2. If the recipient (receive) the message early, he (try) to decrypt it.
3. If you (go) to that website, you (find) some interesting information about Internet Protocol Security.
4. If I (receive) a packet from the CE equipment, I must use the forwarding table to determine the routing for the data.
5. What will happen if a security domain (encapsulate) a packet by wrapping another packet around it?
6. If an intruder (steal) or (guess) an employee's password, that intruder can access your company's network.
7. Unless ensuring packets (be received) from a customer, they (not be placed) on the correct VPN.
8. If you have specified the traffic that needs protection, it (be protected).

Exercise 4. Translate into English

Что такое брандмауэр?

Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет поступить в компьютер.

Разрешение программе работать через брандмауэр, иногда называемое разблокированием, дается при создании исключения, разрешающего определенной программе передавать данные через брандмауэр в компьютер или из него. Также можно разрешить программе работать через брандмауэр, открыв один или несколько портов.

Class Activity

Exercise 1. Speak about Network Security Technologies

Text 2. SCHEMES FOR INTRUSION DETECTION

The importance of information system security, particularly as it applies to the Internet, is obvious. Each day the news media report yet another security breach – sometimes a localized single crime or prank; at others, a denial-of-service attack affecting millions of people. As electronic commerce becomes increasingly pervasive, the subject can only become more critical.

One of the more interesting techniques for enhancing information system security is detecting that an intrusion has taken place. Although intrusion-detection systems have been a part of the information security landscape for over 25 years, their proper role in the overall security picture is often misunderstood. As their very name implies, they are not preventative security measures. Most often, they are used as active security mechanisms in conjunction with other (passive) information assurance processes like firewalls, smart cards, and virtual private networks.

In practice, an intrusion-detection system (IDS) attempts to detect attacks or attack preparations by monitoring either the traffic on a computer network or the application or operating system activities within a computer. Once such behavior is detected, the IDS may alert a security administrator or it may invoke an automated response (such as closing down external communication paths or initiating a mechanism to trace the source of an attack), in which case it would more properly be called an intrusion detection *and response* system. If an IDS detects attack behavior soon enough, it might be able to invoke a response to thwart the attack.

In many instances, the information they provide can help a system security administrator learn what systems were attacked and exactly how the attacks were made. With this information, often damage control can be performed on the affected systems. For example, it may be possible to remove software planted by the attacker to facilitate later access to the system.

Analysis of the attack method may also enable an administrator to fix the security problems that allowed the attacks to happen. That may sound like closing the barn door after the horse has run away, but there may be more horses in the barn – and the farmer may have other barns.

Often, the data collected by an IDS aids in tracing the source of the attack, which may prove helpful in identifying the attacker. IDS logs, for instance, could provide forensic evidence if legal action is taken against an attacker. So, even if an IDS does not detect an attack early enough to help prevent it, it may be of considerable value.

Experience has shown that it is difficult to prevent many kinds of attacks. So, during the latter half of the 1990s, security-conscious organizations like the U.S. Department of Defense (DOD) began putting more emphasis on detection, with the intent that responses triggered by detection would ultimately result in more secure systems, even in the absence of better preventative security measures. The DOD adopted a three-word security mantra that emphasized the role of intrusion-detection systems: “Prevent, Detect, Respond.”

Unfortunately, some have interpreted the “detect” role in the triad to imply that an IDS will be capable of catching all attacks that are not thwarted by system’s preventative security measures. This is certainly not the case today, and it is not clear that it ever will be. The effectiveness of most of these systems is not as good as might be imagined, given the reliance placed upon them.

Installing an IDS often provides a security administrator with an immediate sense of accomplishment because installation is usually followed by a voluminous stream of data indicating *possible* attacks against a variety of target systems. Unfortunately, not all the indicated attacks are real. Moreover, not all actual attacks generate alarms. Over time, in fact, the security administrator may come to view the stream of alarms generated by the IDS more as a burden than as a revelation.

An IDS is an important element – but only an element – of a comprehensive, defense-in-depth, security architecture. The defense-in-depth paradigm currently in vogue calls for using multiple defensive technologies to thwart attacks. Although each defensive barrier is understood to be imperfect, the strategy assumes that all will not be equally vulnerable to the same sort of attacks. Therefore, the reasoning goes, an attacker will either be unable to overcome all of the barriers or, at least, will take longer to overcome them, and will therefore be more readily detectable by an IDS.

While the defense-in-depth strategy sounds good, it is hard to implement. No engineering methodology for designing a system to execute this strategy exists today. Moreover, as the capabilities of attackers increase, deployed security architectures must be reevaluated to determine whether they remain effective.

In principle, using one or more IDSs can help in the continuing evaluation of system security. Detecting new attacks might alert system security administrators to the need for upgrading selected defenses, for instance. But many IDSs are especially poor at detecting new attacks, so this potential is rarely realized in practice.

(By Stephen Kent. From “IEEE Spectrum”, December 2000)

List of words and expressions

intrusion [ɪn’tru:ʒən] – вторжение, вмешательство, проникновение

breach – нарушение

prank – выходка, проделка

denial-of-service – отказ от обслуживания

pervasive – распространяющийся

to be misunderstood – быть неправильно понятым

smart card – интеллектуальная карта; смарт-карта

to invoke – призывать; обращаться

an automated response – автоматизированный отклик (реакция)

to trace – трассировать (программу); отслеживать

to thwart the attack [Θwo:t] – расстраивать нападение

conscious – осознанный; понимающий

triggered – запущенный

preventative security measures – планово-предупредительные (профилактические) меры безопасности

to imply – подразумевать; означать

revelation – раскрытие (тайны и т.п.)

in vogue – модно

imperfect – несовершенный

vulnerable – уязвимый, слабый

upgrading –модернизация; совершенствование

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. Why is information system security important? 2. Is the role of intrusion-detection systems in the overall security picture misunderstood? 3. How does an intrusion-detection system attempt to detect attacks or their preparations in practice? 4. When is it possible to remove software planted by the attacker? 5. What has experience shown? 6. What did the U.S. Department of Defense adopt? 7. Is the effectiveness of most of these systems as good as might be imagined? Why? 8. Why is the defense-in-depth strategy hard to implement?

Exercise 2. Read the text to find the English equivalents for the following:

важность безопасности информационных систем, услуга отказа в доступе, электронная коммерция, усиление безопасности информационных систем, должная роль, активные механизмы безопасности, частные виртуальные сети, наблюдать за информационным потоком через компьютерные сети, спровоцировать автоматическую реакцию, закрытие внешних трактов, обнаружить источник атаки, система обнаружения и реагирования, удалить программное обеспечение, способствовать доступу к системе в дальнейшем, может оказаться полезным, может быть достаточно важным, уделять больше внимания обнаружению, «предотвращать, обнаруживать, реагировать», эффективность большинства современных систем, понятная с глубокими защитными механизмами архитектура безопасности информации, отражать атаки, преодолеть все барьеры, тяжело внедрять, должны быть переоценены, не часто реализуется на практике.

Exercise 3. Disagree with the following statements. Begin your sentences with: ***Sorry, but I can't agree with you; I don't think so; it seems to me you are wrong***

1. Electronic commerce doesn't become increasingly pervasive. 2. Intrusion-detection systems have been a part of the information security landscape for over 10 years. 3. The information cannot help a system security administrator learn what systems were attacked. 4. Experience has shown that it isn't difficult to prevent many kinds of attacks. 5. All the indicated attacks are real. 6. The defense-in-depth strategy is easy to implement.

Language work

Exercise 1. Insert the prepositions:

1. One of the more interesting techniques … enhancing information system security is detecting that an intrusion has taken place. 2. They are used as active security mechanisms … conjunction with other information assurance processes. 3. … this information, often damage control can be performed on the affected systems. 4. The data collected … an IDS aids in tracing the source of the attack. 5. … the latter half of the 1990s, security-conscious organizations began putting more emphasis on detection. 6. An attacker will either be unable to overcome all … the barriers or will take longer to overcome them.

Keys: With, during, for, of, by, in.

Exercise 2. Put in the correct forms of the Simple Past tense Passive of the verbs in brackets:

1. The source of an attack (to trace) … . 2. Preventative security measures (to use) … as active security mechanisms. 3. Attacks (to detect) … by monitoring the traffic on a computer network. 4. A three-word security mantra (to adopt) … by the U.S. Department of Defense. 5. Each defensive barrier (to understand) … to be imperfect. 6. Alarms (not/to generate) … by all actual attacks.

Exercise 3. Translate the following information into English

Сети Петри – математический аппарат для моделирования динамических дискретных систем. Впервые описаны Карлом Петри в 1962 году.

Сеть Петри представляет собой двудольный ориентированный граф, состоящий из вершин двух типов – позиций и переходов, соединённых между собой дугами, вершины одного типа не могут быть соединены непосредственно. В позициях могут размещаться метки (маркеры), способные перемещаться по сети.

Событием называют срабатывание перехода, при котором метки из входных позиций этого перехода перемещаются в выходные позиции. События происходят мгновенно, разновременно при выполнении некоторых условий.

Основными свойствами сети Петри являются:

– ограниченность – число меток в любой позиции сети не может превысить некоторого значения K.

– безопасность – частный случай ограниченности, K = 1;

– сохраняемость — постоянство загрузки ресурсов, постоянная. Где N_i – число маркеров в i-й позиции, A_i – весовой коэффициент.

– достижимость – возможность перехода сети из одного заданного состояния (характеризуемого распределением меток) в другое.

– живость – возможностью срабатывания любого перехода при функционировании моделируемого объекта.

В основе исследования перечисленных свойств лежит анализ достижимости.

(From Wikipedia)

Class Activity

Exercise 1.Discuss pros and cons of the schemes presented to you in class. Suggest your own schemes for intrusion detection.

Text 3. MIXING FEATURES

Historically, IDSs have been characterized as either signature-detection systems or anomaly-detection systems. Today more and more commercial products include features from both types of systems. The signature system detects attacks by matching observed parameters of network traffic or of computer operations against a database of known attack characteristics, called signatures. The anomaly system compares such parameters against *normal* network traffic or computer behavior patterns, looking for deviations from the norm. Each class of system has its pros and cons.

An IDS can also be characterized as either network-based or host-based. The distinction depends on whether the set of parameters the IDS examines is network data or computer operations data. Here, too, a product may incorporate both host- and network-based components. Most of the IDSs deployed today are signature-detection systems, and many are network-based.

In general, a signature-detection IDS will do well in detecting attacks in its signature database although it may miss some mounted by sophisticated attackers who have taken steps to conceal them, as described below. The database for these systems is compiled – and periodically updated – by experts who attempt to extract the essence of an attack from the set of parameters monitored by the system. A good signature database allows an IDS to minimize the likelihood of false alarms and to perform detection quickly – in real time or nearly so.

The database is general, not site-dependent, which increases its value. But where there is a database, there is the possibility of gaining access to it. It is wise to assume that capable adversaries will eventually do so and thus will be able to create attack tools and test them against the database. That upfront testing will, of course, give them the opportunity to refine their methods, thereby reducing the likelihood of detection during a real attack.

Examples of network-based, signature-driven IDS products include Network Flight Recorder’s eponymous product, Haystack’s NetStalker, Harris Corp.’s StakeOut, and CyberCop from Network Associates. The ISS RealSecure product incorporates both network- and host-based signature components.

Suppose someone on the Internet carried out an attack by transmitting malicious code as a part of a very large argument, or input, to an application. Processing the Internet traffic carrying this overlarge argument triggers a buffer overflow in the application, which allows the malicious code to be executed on the targeted computer. Aware of this attack scenario, a network-based signature-driven IDS might examine packets addressed to the targeted application and search for the malicious code in those packets.

As a countermeasure, the attacker might purposely employ a modified transmission control protocol (TCP) implementation to break the malicious code into several overlapping TCP packets before transmission, and then to transmit the packets out of order. The attacker can rely upon TCP (in the target system) to reorder the packets and to discard the overlapping data when it reassembles the packets.

However, an IDS may omit part of the TCP processing in an effort to keep up better with LAN traffic, and that may allow malicious code to get through undetected. Aware of this possibility, the creator of the IDS may choose to look for smaller parts of the malicious code. But that strategy may cause the IDS to match innocuous packets incorrectly.

(By Stephen Kent. From “IEEE Spectrum”, December 2000)

List of words and expressions

signature-detection system – система обнаружения сигнатуры
anomaly – аномалия; неправильность
pro and con [‘prouənd’kon] – «за» и «против»
host-based components – компоненты на основе центрального компьютера
deployed – развернутый
to conceal – скрывать, утаивать
to update – модернизировать, обновлять
false alarm – ложная тревога
to discard – браковать, выбрасывать
upfront testing – честное (открытое) тестирование
adversary – соперник; противник
to refine – вносить улучшения (во что-либо); доработать
malicious – предумышленный
to trigger – запускать, инициировать
overlapping – наложение
to omit – упускать (что-либо); не включать
aware of – сознающий что-либо; осведомленный
innocuous packets – безобидные (безвредные) пакеты
signature-driven IDS products – продукты с системой обнаружения вмешательства на основе сигнатуры

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. How have IDSs been historically characterized? 2. What does the signature system detect? 3. What does the anomaly system deal with? 4. Whom is the database for these systems compiled by? 5. What does a good signature database allow an IDS? 6. What increases the value of the database? 7. What might the attacker employ as a countermeasure? 8. In which case may an IDS omit part of the TCP processing?

Exercise 2. Read the text and translate the following equivalents. Use them in your own sentences:

signature-detection systems, anomaly-detection systems, to detect attacks by matching observed parameters of network traffic, attack characteristics, to compare parameters against *normal* network traffic, computer behavior patterns, to look for deviations from the norm, can be characterized as either network-based or host-based, a product may incorporate both host- and network-based components, IDSs deployed today, to do well in, to miss sophisticated attackers, false alarms, likelihood, not site-dependent, it is wise to assume, capable adversaries, upfront testing, to refine methods, to transmit malicious code, overlarge argument, a countermeasure, to employ a modified transmission control protocol, to reorder the packets and to discard the overlapping data, to omit, to match innocuous packets incorrectly.

Exercise 3. Complete the statements using words given below:

protocol code features the database the possibility

1. Today more and more commercial products include ……… from both types of systems.
2. ……… for these systems is compiled by experts.
3. There is ……… of gaining access to a database.
4. The attacker might purposely employ a modified transmission control ……… implementation.
5. The creator of the IDS may choose to look for smaller parts of the malicious ……… .

Exercise 4. Think of some more questions of your own and suggest possible answers

Language Work.

Exercise 1. Choose the correct alternative in each of these sentences:

1. IDSs *have characterized / have been characterized* as either signature-detection systems or anomaly-detection systems.
2. The distinction *depends / is depending* on whether the set of parameters is network data or computer operations data.
3. Capable adversaries *will be able / will have been able* to create attack tools.
4. The signature system *is detected / detects* attacks by matching observed parameters of network traffic.
5. The system *monitors / is monitored* the set of parameters.

Exercise 2. Read and translate the following defining terms

Defining terms

Anomaly detection: a kind of detection that infers a hacker attack is taking place by recognizing deviations from the normal behavior of a computer or network. Contrast with signature detection.

Host-based intrusion detection: intrusion detection in which the examined parameters are computer operations data; also called computer-based intrusion detection.

IDS: intrusion-detection system.

Network-based intrusion detection: intrusion detection in which the examined parameters are network data.

Signature detection: a kind of detection that recognizes an attack on the basis of known attack characteristics or signature; also called attack detection. Contrast with anomaly detection.

TCP: transmission control protocol, the robust protocol used by most Internet applications.

Class Activity

Exercise 1. Make up a short oral summary of the text. Present it in class. Be ready to discuss some important aspects of the problem with your classmates

Text 4. SECURITY CAMERAS

All of the cameras are divided up into genres that best describe their specifications and fixtures. Black and White security surveillance cameras are widely used in the security surveillance field.

Infrared Security Cameras are designed for optimum security and especially increased protection at night. With Infrared Security Cameras, we can see in total darkness, and they are great cameras for extremely low or non-lighted areas. The Day Night Infrared Security surveillance equipment section contains a variety of high tech CCTV(closed circuit TV) security surveillance cameras including Bullet and IR instrumentation.

Dome Security Cameras are ideal for use in building entrances, stores, and shopping malls. A Dome Camera offers high security and an increased surveillance capacity because of its non-invasive qualities. The Dome Security surveillance Cameras are a great way to achieve all your security surveillance needs in an effective way. The different kinds available are vandal proof exview high resolution, Sanyo day and night, Sony ruggedized day and night, Surveilux fixed lens, Vitek day/night vandal resistant dome, Vitek varifocal dome, indoor mini dome, dual voltage color surveillance cameras, auto iris camera lens, and alpha series indoor domes. Most CCTV security surveillance cameras are high resolution and of the best quality.

Bullet Security Cameras are a special type of a small and sleek camera that is ideal for both indoor and outdoor installation. Sealed in cylinders and totally protected, they are impermeable to water and are totally weatherproof. Mountable on the ceiling or on the wall, they provide sharp, detailed video images while maintaining low profile visibility and an unobtrusive presence.

Pan/Tilt/Zoom (PTZ) and Controllable Cameras are of the highest quality security surveillance cameras in the security surveillance field. PTZ and Controllable Cameras are designed to be controlled by remote or through a DVR. They have the ability to move up and down as well as right and left. You can pan, tilt, and zoom in or out. You have all the control you want over these cameras, and they provide excellent surveillance and security. Bosch AutoDome indoor CCTV security systems have optical zoom range varying from 26x to 18x and 12x digital zoom.

Hidden Security Cameras are concealed cameras that allow you discrete surveillance in places where it best suites you. These include Accel security EXIT sign black and white camera, alarm clock radio, Astrotel B&W purifier camera, black and white clock surveillance camera, smoke detector, discreet emergency light camera, mini ball, GE security PIR, and KJB book surveillance cameras.

Zoom Security surveillance Cameras have the ability to zoom in on whatever you want to give you more visibility on specific objects. Examples include KT&C 18x power zoom, KT&C zoom color surveillance camera, and Sanyo super high resolution Day and Night Camera.

Mini, Board, and Covert Cameras: Just as they sound, mini cameras are small, tiny cameras that come in wireless options and can be used for increased discrete security. Board cameras are tiny mini cameras set in small, flat housing, and are also highly useful in situations calling for more security and extremely low visibility. Like the mini and board cameras, covert cameras are intended for use for those that need increased security and a totally unobtrusive camera.

Wireless Security cameras are very essential to the CCTV industry. These cameras serve a very practical purpose, they allow you to setup the camera wirelessly so you will not have to go through all the hassle that come along with wires and cables. This equipment includes KJB color wireless clock radio, Toshiba wireless network, videocomm 4 channel security system color pinhole cam and rx kit, and black and white pinhole surveillance cameras.

Dummy Security Cameras can also serve your security purposes. Fake security cameras, or dummy cameras, are non-functional surveillance cameras designed to fool intruders, or anyone who it is supposedly watching. Those cameras are intentionally placed in a noticeable place, so passing people notice them and believe the place to be monitored by CCTV. These include 1-800 Dummy surveillance cameras with AC adaptors, outdoor housing, Dummy surveillance cameras with no led, mini dome surveillance cameras, motion detector dummy security cameras, outdoor dummy housing, and VITEK Dummy dome surveillance cameras.

Web/ Storage Cameras are top quality, high resolution security equipment for your CCTV security surveillance system. They include BOSCH digital network surveillance cameras, crow memocam PIR security cameras with storage, JVC digital networks, IP addressable LAN or Web fixed surveillance camera system, Panasonic network monitoring or day/night video surveillance equipment, Sanyo digital surveillance CCTV camera system with built in hard disk, or video server.

(From http://www.iso)

List of words and expressions

surveillance camera – камера наблюдения

varifocal – разнофокусный

vandal proof exview – антивандальное наблюдение

mall – архит. торговый центр (так называемый "молл", по сути – пешеходная аллея, иногда крытая, по сторонам которой расположены магазины, рестораны, кафе и т.п.)

non-invasive quality – нераспространяющееся (неинвазивное) качество

vandal proof – доказательство хулиганства

fixed lens – закреплённый объектив

dome security camera – купольная камера безопасности

sleek – отполированный; гладкий

impermeable – непроницаемый; герметичный

DVR – тех. digital video recording – цифровая видеозапись, ЦВЗ;

digital video recorder – цифровой видеомагнитофон, ЦВМ

GE security PIR – инфракрасные камеры безопасности компании General Electric сокр., Passive InfraRed (sensor)

ruggerized – повышенной прочности
Bullet security cameras – направленные камеры безопасности
Auto iris camera lens – автоматические линзы с ирисовой диафрагмой
Pinhole camera – общ. – камера или фотографический аппарат с малым отверстием
выч. – камера с точечной диафрагмой
тех. – камера-обскура
Pan/Tilt/Zoom – безоп. – поворотная камера с увеличительным объективом, камера с приводом наклона/поворота и увеличительным объективом "лупой"
optical zoom range – фото. оптическое увеличение, оптическое приближение
board camera – бортовая телекамера
crow memocam – мачтовая камера, хранящая информацию
covert camera [‘kΛvət ‘kæmərə] – срытая камера
resolution – разрешающая способность
hassle – драка; стычка
dummy cameras – ложные камеры

Exercises

Comprehension Check

Exercise 1. Put down problem questions to the text

Exercise 2. Find in the text English equivalents for the following words and expressions:

технические характеристики, камеры наблюдения, инфракрасные камеры, созданы для ночного наблюдения, не освещенные участки, камеры для внутреннего наблюдения, высокая разрешающая способность, тонкие камеры, пригодные для внутреннего и внешнего наблюдения, водонепронициаемые, не подвергающиеся воздействие погодных условий, монтировать, предоставлять четкое детальное видеоизображение, ненавязчивое присутствие, скрытие камеры, иметь возможность увеличивать изображение, беспроводные камеры, ложные камеры, видеосервер.

Exercise 3. Fill in the missing words in the sentences:

DVR, increased discrete security, PTZ and Controllable Cameras, Infrared Security Cameras, discrete, optimum security, wireless options, , essential, to set up the camera, high resolution security equipment, special type of small and sleek camera, concealed cameras, are divided up into, Dummy Security Cameras, ideal for use in building entrances, an installation, have the ability to zoom, visibility, a very practical purpose, hassle, to fool intruders, specifications and fixtures

1. All of cameras………… genres that best describe their………..

2. …………….are designed for ……….. and especially increased protection at night.

3. Dome Security Cameras are ……….., stores, and shopping malls.

4. Bullet Security Cameras are ……….. that is ideal for both indoor and outdoor ……..

5. …………..are designed to be controlled by remote or through a…….. .

6. Hidden Security Cameras are ………… that allow you ……… surveillance in places where it best suites you.

7. Zoom Security surveillance Cameras ………. in on whatever you want to give you more ….. on specific objects.

8. Mini, Board, and Covert Cameras are small, tiny cameras that come in ….. and can be used for ……….

9.Wireless Security cameras are very …… to the CCTV industry and serve ……….. they allow you ……… wirelessly so you will not have to go through all the …. that come along with wires and cables.

10. …….are non-functional surveillance cameras designed ………, or anyone who it is supposedly watching.

11.Web/ Storage Cameras are top quality, ………. for your CCTV security surveillance system.

Language Work

Exercise 1. Make compound words by matching one word from each list.

Example	*well-known*
well	cam
surveillance	known
non-lighted	proof
shopping	camera
outdoor	purpose
vandal	mall
pinhole	installation
security	area

Exercise 2. Complete the statements using the words from the box:

Employed the tapes switch to monitor the criminal appropriate equipped designed

1. Security cameras are able …….. your home or business operations and ensure safety.
2. Good dummy cameras come …….. with a cable and a blinking light.
3. Hidden units will catch criminals and …….. can be used as evidence in court.
4. Most companies offer communication with the …….. authorities in the case of a fire or other emergency.
5. The most basic alarm system involves a supply of power, a line, an on and off …….. , a bulb and a power supply.
6. Infrared security cameras are …….. for increased protection at night.
7. Covert surveillance systems have long been …….. by professionals.
8. Vandal-proof cameras will not prevent ……. from spray painting the lens or cutting the wires of the camera or system.

Exercise 3. Write these sentences as Second Conditionals. Put the verbs in brackets into the correct tenses:

1. If I (not belong) to this union I couldn't get a job in this private company.
2. Users (have) the same, continuous access to the network if they were physically connected .
3. If you could type, you (be able) to operate a computer.
4. Traffic coming from the gateway (be handled) if it came from any user within the LAN.
5. If we (improve) security mechanisms, we would avoid some attacks.
6. If I could understand the problem, I (find) a solution related to data integrity.

7. You wouldn’t have so much trouble with data if you (use) the IPSec protocol to encapsulate it.

8. If they (rely) on additional cryptography techniques they would not make so many mistakes.

9. If data corruption could be detected by the use of checksums, it (be corrected) by the use of error correcting codes.

10. If you had a Dome Security surveillance Camera you (achieve) all your security surveillance needs in an effective way.

Class Activity

Exercise 1. Speak about advantages of different types of closed circuit surveillance cameras

Text 5. USING COVERT SURVEILLANCE

There are countless uses for covert surveillance in the corporate environment. Hidden cameras are commonly employed to protect intellectual property, watch over high-value items and warehouse areas, provide an added element of personal security, and monitor employee behavior and productivity. The mere mention that hidden cameras are installed somewhere on business premises often dissuades employees from conducting themselves improperly during business hours.

Employee productivity is a huge concern for many small and large businesses. Dips in worker productivity can be a result of any number of distractions, including employees spending their work hours on personal phone calls, surfing the Internet, or other non-productive activity. It is accepted that people will act differently when they know they are being watched. Covert cameras can be employed to observe an employee's true behavior and work habits, and empower the employer to identify and address any problems that would otherwise become a distraction in the workplace.

Covert video can be particularly effective in business environments requiring higher levels of security. Virtually all banking institutions install visible cameras to deter crime and capture physical evidence should a robbery occur. However, many banks have found it necessary to have a few extra cameras stationed throughout the premises, particularly those that customers and even employees are not aware of. In addition to the visible cameras aimed at bank tellers' stations, bank administrators often install covert cameras that capture a glimpse of each customer's face during a transaction. And some banks are now fitting covert pinhole cameras into the chained-down penholders at each teller station as an added security element.

Because covert systems have the capability to work both indoors and outdoors, homeowners often use these cameras to catch vandals in the act of damaging their homes, yards, vehicles and mailboxes.

While some covert surveillance equipment can be incredibly high-tech and somewhat complex, many solutions are very user-friendly, and in many cases the user needs only to place a complete and self-contained covert security system in the preferred environment. Standard or custom-designed covert systems can also be easily integrated in to an existing security system. When considering covert cameras for these or any application, answering the following three questions will make finding the right solution easy.

1. How will you power your cameras?

The first concern for any covert security solution, is determining an effective source to power both the camera and recording device. Integrating a covert camera into an existing system will typically require that the user pull cabling to transfer the video signal and deliver power to the camera. This solution has its advantages, providing a permanent source of power for longer surveillance periods and a reliable means of transferring the captured video back to the video recorder. However, wires will typically need to be concealed or disguised in such applications. Covert cameras hidden within common fixtures, such as a wall clock or thermostat, can often draw power from that device or from a local wall outlet, providing a permanent solution as well. Once the equipment is plugged in, and cameras are positioned appropriately, customers can begin the surveillance process immediately, without need to conceal existing wiring.

For covert applications requiring extreme discretion, where wiring would appear unnatural, or where external power is not available, users must turn to battery-operated solutions. Typical examples include body-worn covert, outdoor, remote, or temporary surveillance operations. Although battery-powered devices can only operate for a limited period of time, the use of motion detection can be employed to minimize power consumption and maximize the utilization of storage capacity of these covert systems.

2. How will you extract the video?

There are a number of means to record data captured by your covert surveillance system, including wired and wireless applications, and self-contained solutions with micro recording devices. Wired applications provide a permanent and reliable means of transferring video back to the video recorder, but again requires additional cabling, which must typically be disguised. This is a relatively easy solution for common appliances such as speaker cameras, motion detectors, or utility boxes, that are affixed to a wall and already require wiring for power.

Wireless solutions are most practical for devices that cannot be hardwired, where video cables cannot be exposed, and perfect for applications that require quick and/or temporary installation. Typical wireless devices include tissue boxes, flowers, calculators, cell phones, and body worn covert gear. Limitations to wireless include range and quality of the transmitter / receiver pair, and wireless does introduce a potential to lose critical evidence, as transmitted signals aren't always dependable. Another common concern with wireless is the ability of others to capture transmitted video, which is why users commonly turn to local covert recording devices.

Micro DVRs eliminate concerns of losing transmitted video signals, do not need cables, and are a great option for surveillance needs that require capture and replay for instant feedback. Primary limitations include battery life and storage capacity, but most micro DVRs offer up to 4 hours recording time of full motion video. However, if a micro DVR is discovered and lost or destroyed, users run the risk of losing both a valuable piece of surveillance equipment and more importantly, the video evidence! Latest technologies, including the World's Smallest Micro DVR recently developed by Supercircuits, now enable the integration of both concealed video cameras and miniature capture devices in even the smallest of objects. Cameras and micro DVRs concealed together are far less detectable, and eliminate concerns of other detecting or stealing video transmissions.

(From http://www.its)

List of words of expressions

DVR (Digital Video Recorder) – цифровой видеомагнитофон
to dissuade [dis'weid] – не советовать ; отговаривать
mere mention – случайное упоминание
to empower – давать возможность
robbery – кража ; вор
tellers' station – место кассира

incredibly – неправдоподобно
to be concealed – быть скрытым (о проводке или монтаже)
to be disguised – быть замаскированным
wall outlet – сетевая розетка; настенная штепсельная розетка
to plug in – включать; вставлять в контактное гнездо
existing wiring – существующая проводка, монтаж
cabling – кабельная сеть; монтаж кабельной проводки
utility box – сервисная коробка
tissue box – коробка из ткани
body-worn gear – старый корпус (устройство)

Exercises

Comprehension Check

Exercise 1. Answer the following questions:

1. Where are hidden cameras commonly employed? 2. What dissuades employees from conducting themselves improperly during business hours? 3. How will people act when they know they are being watched? 4. Why do all banking institutions install visible cameras? 5. What systems do homeowners use? 6. Can standard covert systems be easily integrated in to an existing security system? What does integrating a covert camera into an existing system require? 8. Will wires need to be concealed or disguised in such applications? 9. Why must users turn to battery – operated devices? 10. Are there a number of means to record data captured by a covert surveillance system? 11. What do wired applications provide? 12. What devices are wireless solutions most practical for? 13. What can you say about DVRs? 14. Do latest technologies enable the integration of both concealed video cameras and miniature capture devices in even the smallest of objects?

Exercise 2. Read the following equivalents and translate them. Make up your own sentences:

covert surveillance, corporate environment, hidden cameras, to be commonly employed, to watch over high-value items, warehouse areas, to provide an added element of personal security, to monitor employee behavior and productivity, business premises, to dissuade, employee productivity, a huge concern, distractions, to surf the Internet, to empower the employer, to identify, particularly effective, to install visible cameras, to capture physical evidence, to deter crime, the premises, to aim at, bank tellers' stations, the chained-down penholders, to work both indoors and outdoors, vehicles, incredibly high-tech, to determine an effective source to power, to transfer the video signal, to have advantages, need to be concealed or disguised in such applications, hidden within common fixtures, a local wall outlet, once the equipment is plugged in, to require extreme discretion, to turn to battery-operated solutions, motion detection, self-contained solutions with micro recording devices, to be affixed to a wall, hardwired, body-worn covert gear, to be dependable, to turn to, to replay for instant feedback, to run the risk, to be far less detectable.

Language Work

Exercise 1. Choose the correct word from the brackets:

1. This strategy is commonly used to capture criminal activity (on/by) covert cameras.
2. Covert surveillance systems allow owners to monitor the activities (by/of) their employees.

3. Some banks are fitting covert pinhole cameras (in / into) the chained-down penholders at

each teller station.

4. Covert cameras can be employed to identify and address any problems that would otherwise become a distraction (in/to) the workplace.

5. The first concern (for/by) any covert security solution is determining an effective source

to power both the camera and recording device .

6. The use of motion detection can be employed to minimize power consumption and maximize the utilization (by/of) storage capacity of these covert systems.

Exercise 2. Translate into English:

1. Сетевые системы контроля и управления доступом устанавливаются на больших предприятиях.
2. Сетевые контроллеры объединяются в сеть.
3. В одноуровневой сети все контроллеры доступа имеют равные права.
4. В каждом контроллере необходимо иметь полную базу данных, например список пользователей, их прав и т.д.
5. Если сеть контроллеров работает по принципу произвольного доступа, недостаток отсутствует.
6. Существует много типов видеокамер.
7. Инфракрасные камеры безопасности разработаны для оптимальной защиты в ночное время.

Exercise 3. Write these sentences as Third Conditionals. Put the verbs in brackets in the correct form:

1. If we (know) the facts, we would have installed a traditional 4-camera system.
2. If he (manage) to install a hidden camera earlier, he could have monitored employee behavior and productivity.
3. She might have made a bad mistake, if she (not/read) the instruction of this equipment.
4. If you had placed covert cameras in these areas, you (capture) the criminal activity.
5. He (lose) thousands of dollars without a covert backup.
6. It (be) very difficult to detect and prove his illegal activity without being caught.
7. If you (set up) a wireless home security camera you would have increased the level of security of your building.
8. If I (have) micro DVR it could have eliminated concerns of other detecting or stealing video transmissions.

Class Activity

Exercise 5. Describe the covert video camera you bought recently. Are you satisfied with it? Why? Why not?

Text 6. SCANNER SYSTEMS

Most fingerprint scanner systems compare specific features of the fingerprint, generally known as minutiae. Typically, human and computer investigators concentrate on points where ridge lines end or where one ridge splits into two (bifurcations). Collectively, these and other distinctive features are sometimes called typica.

The scanner system software uses highly complex algorithms to recognize and analyze these minutiae. The basic idea is to measure the relative positions of minutiae, in the same sort of way you might recognize a part of the sky by the relative positions of stars. A simple way to think of it is to consider the shapes that various minutia form when you draw straight lines between them. If two prints have three ridge endings and two bifurcations, forming the same shape with the same dimensions, there's a high likelihood they're from the same print.

To get a match, the scanner system doesn't have to find the entire pattern of minutiae both in the sample and in the print on record, it simply has to find a sufficient number of minutiae patterns that the two prints have in common. The exact number varies according to the scanner programming.

A retinal scan is a biometric technique that uses the unique patterns on a person's retina to identify them. It is not to be confused with another ocular-based technology, iris recognition.

The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is so complex that identical twins do not even share a similar pattern.

Although retinal patterns may be altered in cases of diabetes, glaucoma, retinal degenerative disorders or cataracts, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the retina appears to be the most precise and reliable biometric. Advocates of retinal scanning have concluded that it is so accurate that its error rate is estimated to be only one in a million.

A biometric identifier known as a retinal scan is used to map the unique patterns of a person's retina. The blood vessels within the retina absorb light more readily than the surrounding tissue and are easily identified with appropriate lighting. A retinal scan is performed by casting an undetectable ray of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light outlines a circular path on the retina. Because retinal blood vessels are more sensitive to light than the rest of the eye, the amount of reflection fluctuates. The results of the scan are converted to computer code and stored in a database.

The idea for retinal identification was first conceived by Dr. Carleton Simon and Dr. Isodore Goldstein and was published in the New York State Journal of Medicine in 1935.The ides was a little before its time, but once technology caught up, the concept for a retinal scanning device emerged in 1975. In 1976, Robert "Buzz" Hill formed a corporation named EyeDentify, Inc., and made a fulltime effort to research and develop such a device. In 1978, the idea of a retinal scanner was patented, followed by a practical working prototype in 1981.

Retinal scanners are typically used for authentication and identification purposes. Retinal scanning has been utilized by several government agencies including the FBI, CIA, and NASA. However, in recent years, retinal scanning has become more commercially popular. Retinal scanning has been used in prisons, for ATM identity verification and the prevention of welfare fraud.

There are some advantages of retinal scanning:

- low occurrence of false negatives;
- extremely low (almost 0%) false positive rates;
- highly reliable because no two people have the same retinal pattern;
- speedy results: Identity of the subject is verified very quickly;

Disadvantages of retinal scanning are as follows.

- measurement accuracy can be affected by diseases such as cataracts and glaucoma;
- scanning procedure is highly invasive;

– not very user friendly;
– limited government, corporate, and other funding;
– subject being scanned must focus on the scanner from about three inches away;
– high equipment costs;
– poor lighting can affect results;
– retinal vessel pattern can change with systematic and other ocular disease, especially diabetes and hypertension.

(From Wikipedia, the free encyclopedia)

List of words and expressions

fingerprint scanner system – система сканирования отпечатка пальца; система дактилоскопического сканирования
minutiae [maɪ’nju:ɪi] – мелочи, детали
ridge – край
to split into – распадаться на
bifurcation – бифуркация, разветвление
dimension – измерение
retinal scan – сканирование сетчатки глаза
to be confused – смутить; поставить в тупик
tissue – ткань (биол.)
neural cell – нервная клетка
posterior – последующий
circular path – кровеносный путь
blood vessels – кровеносные сосуды
to conceive – постигать, понимать
fraud – обман; мошенничество; злоумышленное использование
by casting a ray – направляя луч

Exercises

Comprehension Check

Exercise 1. Ask your own problem questions to text 6

Exercise 2. Read the following expressions and find equivalents to translate them in the text:

Fingerprint scanner systems, minutiae, ridge lines, bifurcations, typica, the scanner system software, to recognize and analyze these minutiae, to consider the shapes, the same dimensions, a high likelihood, to get a match, to find the entire pattern of minutiae, a retinal scan, not to be confused with another ocular-based technology, iris recognition, the human retina, the complex structure of the capillaries, unique, the network of blood vessels, to share a similar pattern, a thin tissue, neural cells, in the posterior portion of the eye, to be the most precise and reliable biometric, error rate, to map, to absorb light, the beam of light, to outline a circular path on the retina, to be first conceived by, to emerge, a fulltime effort, ATM identity verification, prevention of welfare fraud, highly invasive, hypertension.

Exercise 3. Multiple choice:

Using the entire fingerprint image in comparative analysis uses a lot of…. :

a) firewalls;
b) processing power;
c) covert surveillance systems.

A retinal scan is a …… technique:

a) dangerous;
b) cryptographic;
c) biometric.

In 1935 the idea for retinal identification was first published in ………:

a) TCP/IP protocol specifications;
b) The New York state journal of Medicine;
c) The Network dictionary.

The result of the scan are converted to…… :

a) computer code;
b) error correcting codes;
c) randomly chosen words.

Exercise 4. Give your own definitions of the following terms.

the scanner system software, fingerprint images, a biometric technique, retinal scanning

Language work

Exercise 1. Translate the following sentences containing Complex Object:

1. We consider retinal scanners to be used for authentication and identification purposes.
2. Dr. Carleton Simon and Dr. Isodare Goldstein supposed the idea for retinal identification to be true.
3. He estimated the error rate of retinal scanning to be only one in a million.
4. They expect a security camera outside their home to deter criminals from robbing their place.
5. I know him to have interest in fake security cameras.
6. I want you to install a security camera.
7. We expect the vendor's ability to assist with installation and any technical challenges.
8. He found retinal scanning to be commercially popular.
9. You expect me to believe that complicated explanation.

Exercise 2. Make up your own sentences with Complex Object based on the context of the text

Class activity

Exercise 1.Speak on the problem solved by Dr. Carleton Simon and Dr. Isodore Goldstein

Text 7. RETINOGRAPHY

Retinography is a sophisticated means for identifying people by the pattern of blood vessels on the retina (the innermost coat of the back part of the eye). It requires the use of a special scanner about the size of a shoe-box that can map the unique pattern of blood vessels on the retina. The pattern is so complex that even identical twins do not have the same blood vessel configuration. Those who favor its use claim retinography has an error rate of only one in a million.

There are currently a number of biometric devices in use, machines that can identify people by their physical characteristics. Some examples include fingerprint scanners and devices that can recognize a particular voice, hand, or signature. The retinal scanner is another addition to the identification tool kit.

A retinal scanner uses infrared light for mapping. As a person looks into the eyepiece, an invisible beam of low-energy infrared light traces a circular path on the retina at the back of the eye. The blood-filled capillaries absorb more of the infrared light than the surrounding tissue. Because of this, there is a variation in the intensity of the reflection. The scanner measures this reflection at 320 points along the beam path. It then assigns an intensity grade between zero and 4,095. The resulting numbers are compressed into an 80-byte computer code. This code can then be compared with patterns that have already been entered into the computer’s data base.

Retina scans are already in use in government and corporate organizations where people need to be identified before they can enter an area. New concerns about security from terrorism and bank and credit card fraud caused many organizations to think seriously of using retina scans or other biometric means to identify people at airports and ATM machines.

Some states require that truck and bus drivers be mapped by retinography. This information is used by state agencies to prevent bad drivers from holding licenses in several states to hide their driving records. A proposed and more controversial use of retina scans is to develop a worker registry, where everyone is scanned to make sure that they are legal citizens of the country, and thus eligible for employment. Critics of this proposal are concerned about possible invasions of privacy and violations of other personal rights.

Retinal scanners have several advantages over fingerprinting and voice recognition systems. They do not require as much computer memory as a fingerprint scan, and they are not subject to contamination from dirt or finger misplacement. Unlike voice recognition systems, retinal scanners are not distracted by background noise or changes in voice caused by illness.

The main disadvantage of the retinal scanner is that the person has to focus on the scanner from about three inches away. This restriction makes the device difficult for ATM use because a person using a cash machine rarely focuses on one area very long and is never close enough. A new device called an iris scanner may prove more useful for these casual transactions, since the scanning camera can be farther away and only has to scan the pattern of the iris (colored portion) of the eye, a procedure which does not require focusing on the camera.

(From Wikipedia, the free encyclopedia)

List of words and expressions

Retinography – ретинография
innermost coat of the back part of the eye – самая отдалённая оболочка заднего (внутреннего) поля глаза
tool kit – набор инструментов
mapping – отображение
to trace – проследить
beam path – траектория пучка
to assign – определять; устанавливать
concerns – забота
controversial [ˌkontrə’və:ʃ(ə)l] – спорный
voice recognition – распознавание голоса
contamination – загрязнение; заражение
misplacement – плохое (неудачное) расположение (размещение)

to distract – сбивать с толку; отвлекать
inch – дюйм
iris – радужная оболочка
ATM - банкомат

Exercises

Comprehension Check

Exercise 1. How much can you remember? Check your answers:

1. What is retinography? 2. What does it require? 3. Why is the pattern complex? 4. Which an error rate does retinography have? 5. What are biometric devices? 6. Which scanner uses infrared light for mapping? 7. What is the principle of its functioning? 8. How does the scanner measure the reflection? 9. How does it assign an intensity grade? 10. What code are resulting numbers compressed into? 11. Can the code then be compared with patterns that have already been entered into the computer's data base? 12. Where are retina scans in use now? 13. What has caused many organizations to think seriously of using retina scans or other biometric means? 14. Why do a few states require that truck and bus drivers be mapped by retinography? 15. Who is concerned about possible invasions of privacy and violations of other personal rights? 16. What advantages do retinal scanners have? 17. What aren't retinal scanners distracted by? 18. What do you know about the main disadvantage of the retinal scanner? 19. How is a new device called? 20. Why may an iris scanner be more useful for casual transactions?

Exercise 2. Read the text to translate the following words and expressions:

Сложный способ, размером с коробку из-под обуви, уникальное расположение кровеносных сосудов сетчатки, предпочитать, вероятность ошибки, различные биометрические устройства, идентифицировать людей по их физическим характеристикам, распознавать голос, руку, подпись; невидимый поток маломощных инфракрасных лучей, ткань, отражение, сжимать в 80-байтовый компьютерный код, вводить в базу данных, мошенничество с кредитными картами, неоднозначный, нарушение личных прав человека, иметь преимущества над, системы распознавания голоса, не подвергаться загрязнениям, ограничение.

Exercise 3. Disagree with the following statements avoiding the simple negation:

1. Retinography is a sophisticated means for identifying people by gastric juice analysis.

2. Biometric devices can identify people by using the RSA public key cypher.

3. The blood-filled capillaries absorb more of the cathode light than the surrounding tissue.

4. The scanner measures this reflection at 220 points along the beam path.

5. Retina scans are not in use in government organizations.

6. Retinal scanners do not have advantages over fingerprinting systems.

7. The resulting numbers are compressed into a 50-byte computer code.

8. The advantage of the retinal scanner is that a person has to focus on the scanner from about three inches away.

Language Work

Exercise 1. Choose the proper verb form and translate the text into Russian

Electronic devices

The principal methods by which motion can be electronically … are optical detection and acoustical detection. Infrared light or laser technology … for optical detection. Motion detection devices, such as motion detectors, … sensors that detect movement and … signals to a sound device that … an alarm or switch on an image recording device. There … motion detectors which employ cameras … to a computer which … and manages captured images to be viewed later or viewed over a computer network.

The chief applications for such detection are (a) detection of unauthorized entry, (b) detection of cessation of occupancy of an area … lighting and (c) detection of a moving object which … a camera to record subsequent events. The motion detector is thus a linchpin of electronic security systems, but is also a valuable tool in … the illumination of unoccupied spaces.

A simple algorithm for motion detection by a fixed camera … the current image with a reference image and simply … the number of different pixels. Since images … due to factors such as varying lighting, camera flicker, and CCD dark currents, pre-processing is useful to reduce the number of false positive alarms.

More complex algorithms are necessary to detect motion when the camera itself …, or when the motion of a specific object … in a field containing other movement which can be ignored. An example might be a painting … by visitors in an art gallery.

Keys: compares, stores, send, identified, is moving, are, triggers, surrounded, produces, counts, must be detected, have, to extinguish, will differ, may be used, connected, preventing.

Exercise 2. Render into English

Стационарный сканирующий приёмник AR 5000

Стационарный профессиональный сканирующий приёмник фирмы AOR обеспечивает высококачественную обработку сигнала, высокую чувствительность, широкий диапазон частот от 10 кГц до 2600 МГц. Благодаря использованию микропроцессорного управления приёмник имеет 1000 каналов памяти, 20 банков поиска, режим быстрого сканирования «Cyber Scan», смещение частоты, установка шага и другие функции.

Этот сканирующий приёмник имеет автоматический электронный преселектор в диапазоне от 500 кГц до 999,99 МГц и полосовыми фильтрами.

Exercise 3. Join each of the following pairs of sentences, using a perfect participle (having done):

1. I had added this security camera. I increased the level of security.
2. We sensed a pattern by using a number of photodetectors. We created a binary number.
3. He had used more advanced encryption algorithm in this standard. He made it securer for high sensitivity information.
4. We determined a random error. We could reduce it by signal processing, such as filtering.
5. I had implemented electronic sensing devices. I prevented any mechanical intervention, such as “cutting the wire”.
6. They had focused a large aperture lens by a servo system. They determined the distance to an in-focus scene element by this lens setting.

Class Activity

Exercise 1. Share your opinions of retinography. Make use of text 7

Учебное пособие

Воробиенко Петр Петрович
Веретенникова Валентина Петровна
Кузнецова Галина Петровна

СЕТЕВАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ

Учебник

Издательство ОНАС им. А.С. Попова
(свидетельство ДК № 3633 от 27.11.2009 г.)

Сдано в набор 3.03.09. Подписано к печати 2.03.10.
Формат 60х90/16. Тираж 300.
Усл. печ. л. 16,9. Заказ № 4051.
Отпечатано с готового оригинал-макета в типографии
Одесской национальной академии связи им. А.С. Попова
Г. Одесса, ул. Старопортофранковская, 61
Тел. (048) 720-78-94