ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

ПОЯСНЮВАЛЬНА ЗАПИСКА

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Устінов В.О.
(прізвище та ініціали)
Керівник Борсуковський Ю.В.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер _____
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Устінову Валентину Олександровичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо застосування багатофакторної автентифікації в автоматизованих системах» керівник бакалаврської роботи Борсуковський Юрій Володимирович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24 » лютого_2023 року № 26.
2. Строк подання студентом бакалаврської роботи 28.05.2022 р.
3. Вихідні дані до бакалаврської роботи
автоматизована система;
програмний комплекс для багатофакторної автентифікації;
наукова та технічна література, експлуатаційна документація, нормативні документи.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми вибору рішень для використання багатофакторної автентифікації.
2. Зміст процесу реагування на загрози в автоматизованій системі.
3. Методи та засоби захисту автоматизованої системи за допомогою багатофакторної автентифікації.
4. Рекомендації щодо вибору рішення для захисту автоматизованої системи за допомогою багатофакторної автентифікації.
5. Перелік графічного матеріалу
1. Тема бакалаврської роботи.
2. Об'єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу змісту процесу вибору рішення для захисту автоматизованох систем.
4. Результати аналізу методів та засобів захисту багатофакторною автентифікацією.

5. Призначення та можливості захисту багатофакторної автентифікації.
6. Рекомендації щодо застосування методів та засобів забезпечення безпеки багатофакторною автентифікацією в автоматизованій системі.
7. Висновки за результатами роботи.
6. Дата видачі завдання 15.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми відсутності багатофакторної автентифікації в автоматизованих системах.	24.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	01.05.2023 р.	
3.	Аналіз методів та засобів захисту автоматизованої системи багатофакторною автентифікацією.	05.05.2023 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів багатофакторної автентифікації в автоматизованих системах.	08.05.2023 р.	
5.	Оформлення результатів дослідження.	15.05.2023 р.	
6.	Підготовка доповіді до захисту.	22.05.2023 р.	

Студент _____ Устінов В.О.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Борсуковський Ю.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА

студента Устінова Валентина Олександровича
на тему: «Дослідження шляхів та розробка рекомендацій щодо застосування багатофакторної автентифікації в автоматизованих системах»

Актуальність: Оскільки обсяг і складність загроз кібербезпеці неухильно зростають, зростає потреба в більш досконалих рішеннях багатофакторної автентифікації. Сучасні методи багатофакторної автентифікації розроблені для того щоб захистити данні в системах від несанкціонованого доступу. Для цього вони повинні співпрацювати один з одним та з іншими технологіями безпеки, щоб надати захист автоматизованих системах та запобігти вторгненню та витоку данних.

Позитивні сторони:
1. На основі проведеного аналізу в роботі було встановлено зміст процесу вибору рішення багатофакторної автентифікації в автоматизованих системах визначено місце щодо їх розслідування.
2. Було досліджено методи та засоби забезпення безпеки автоматизованої системи на прикладі рішення Google аккаунту.
3. Розроблення рекомендацій щодо застосування методів та засобів забезпечення багатофакторної автентифікації в автоматизованих системах.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:
1. У бакалаврській роботі слідувало б провести більш детальний опис принципів роботи багатофакторної автентифікації на базі інших автоматизованих систем.
2. Експеримент із застосуванням рішення Google аккаунту бажано було б показати на прикладі конкретного рішення.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Устінов В.О.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Устінов В.О. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо застосування багатофакторної автентифікації в автоматизованих системах.
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Устінов В.О. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент Устінов В.О. обрав тему роботи, метою якої було дослідження методів та засобів багатофатктрної автентифікації в автоматизованих системах. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Устінова В.О. показав добру теоретичну та практичну підготовку. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану бакалаврську роботу студента Устінова Валентина Олександровича на оцінку **«добре»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Борсуковький Ю.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Устінов В.О.
(прізвище та ініціали)
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 54 сторінок, 13 рисунків, 1 таблиця, 12 джерел.

Об'єкт дослідження – процес вибору найкращого методу захисту автоматизованої системи за допомогою багатофакторної автентифікації.

*Предмет дослідженн*я – види багатофакторної автентифікації для захисту автоматизованих систем.

Мета роботи – розробити рекомендацій щодо застосування багатофакторної автентифікації в автоматизованих системах.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, розробка рекомендацій для вибору рішення щодо захисту атоматизованих систем за допомогою багатофакторної автентифікації.

В роботі приведено основні відомості про автоматизовану систему, загрози багатофакторної автентифікації в автоматизованих системах.
Проаналізовано різні види багатофакторної автенntифікації та наведено їх класифікацію.
Досліджено методи та засоби щодо захисту багатофакторної автентифікації в автоматизованих системах.
Досліджено можливості багатофакторної автентифікації безпосередньо в системі.
На основі досліджень проведених в роботі розроблено рекомендації щодо вибору багатофакторної автентифікації в автоматизованих системаї.

Галузь використання – кібербезпека автоматизованих систем.

АВТОМАТИЗОВАНА СИСТЕМА, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, ЗАХИСТ СИСТЕМ, ВИБІР РІШЕННЯ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MFA - Multi-Factor Authentication

SFA - Single-Factor Authentication

2FA - Two-Factor Authentication

SSS - Shamir’s Secret Sharing

PIN - Personal Identification Number

ID - Identification Number

ATM - Automated Teller Machine

FAR - False Accept Rate

FRR - False Reject Rate

PPG - Photoplethysmography

RFID - Radio-Frequency Identification

NFC - Near-Field Communication

OCS - Occupant Classification Systems

ECG - Electrocardiography

EEG - Electroencephalography

GPS - Global Positioning System

FTE - Failure to Enroll

FTA - Failure to Acquire

CER - Crossover Error Rate

EER - Equal Error Rate

V2X - Vehicle-to-Everything

IAM - Identity and Access Management

ВСТУП

Сьогодні цифровізація рішуче проникає в усі сторони сучасного суспільства. Одним із ключових факторів забезпечення безпеки цього процесу є автентифікація. Вона охоплює багато різних сфер гіперзв'язаного світу, включаючи онлайн-платежі, комунікації, керування правами доступу тощо.

Актуальність теми дослідження полягає в тому, що відсутність багатофакторної автентифікації може сильно порушити безпеку автоматизованих систем, як до втрати даних власників самих систем так і клієтів що нею користуються. Тому дослідження шляхів та розробка рекомендацій щодо захисту автоматизованих систем за допомогою багатофакторної автентифікації є важливою задачею для будь-якої організації.

Об'єкт дослідження - процес вибору найкращого методу захисту автоматизованої системи за допомогою багатофакторної автентифікації.

*Предмет дослідженн*я - види багатофакторної автентифікації для захисту автоматизованих систем.

Мета роботи - розробити рекомендацій щодо застосування багатофакторної автентифікації в автоматизованих системах.

Методи дослідження - опрацювання літератури за даною темою, аналіз

експлуатаційної документації, міжнародних стандартів та їх порівняння, розробка рекомендацій для вибору рішення щодо захисту атоматизованих систем за допомогою багатофакторної автентифікації.

1. АНАЛІЗ АВТЕНТИФІКАЦІЇ ТА ПРОБЛЕМ ФУНКЦІОНУВАННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

1.1 Поняття автентифікація та її характеристика

Постійне зростання кількості інтелектуальних пристроїв і пов’язане з ними навантаження на зв’язок вплинуло на мобільні послуги, які безперешкодно пропонуються в будь-якій точці земної кулі[1]. У такому підключеному світі засобом забезпечення безпеки переданих даних є, насамперед, аутентифікація[2].

Автентифікація - це процес, у якому «користувач ідентифікує себе, надсилаючи щось, що підтверджує особу самого користувача системі. Система підтверджує його особу шляхом обчислення і перевіряє, що воно дорівнює збереженому значенню у системі автентифікації. Це визначення не зазнало істотних змін з часом, незважаючи на те, що простий пароль більше не є єдиним фактором для перевірки користувача з точки зору інформаційних технологій.

Автентифікація залишається фундаментальним запобіжним засобом проти нелегітимного доступу до пристрою чи будь-якої іншої конфіденційної програми, як офлайн, так і онлайн.

Раніше транзакції засвідчувалися переважно фізичною присутністю, тобто, наприклад, накладенням сургучної печатки. Ближче до наших днів і з розвитком нашої цивілізації стало зрозуміло, що перевірка, заснована лише на ідентифікації відправника, не завжди є адекватною в глобальному масштабі[3].

Спочатку для аутентифікації суб’єкта використовувався лише один фактор. На той час однофакторна автентифікація (SFA) була в основному прийнята спільнотою через її простоту та зручність.

Як приклад можна розглянути використання пароля (або PIN-коду) для підтвердження права власності на ідентифікатор користувача. Мабуть, це найслабший рівень аутентифікації. Втративши конфеденційність паролю, можна дуже швидко піддати свій обліковий запис несанкціонованому доступ.

Як правило, під час використання цього типу автентифікації слід враховувати вимоги до мінімальної складності пароля.

Крім того, було зрозуміло, що автентифікація лише з одним фактором не є надійною для забезпечення належного захисту через низку загроз безпеці.

В якості інтуїтивного кроку вперед було запропоновано двофакторну автентифікацію (2FA), яка поєднує репрезентативні дані (комбінація імені користувача/пароля) з фактором особистої власності, наприклад, смарт-карткою або телефоном.

На сьогодні доступні три типи груп факторів для зв'язку особи з встановленими повноваженнями:

1) Фактор знань - те, що користувач знає, наприклад пароль або просто «секрет»;

2) Фактор власності - щось, що є у користувача, наприклад картки, смартфони чи інші токени;

3) Біометричний фактор - те, чим є користувач, тобто біометричні дані чи модель поведінки;

Згодом було запропоновано багатофакторну автентифікацію (MFA) для забезпечення вищого рівня безпеки та сприяння постійному захисту комп'ютерних пристроїв, а також інших критичних служб від несанкціонованого доступу за допомогою використання більше двох категорій облікових даних. Здебільшого MFA базується на біометрії, яка є автоматизованим розпізнаванням осіб на основі їх поведінкових та біологічних характеристик. Цей крок запропонував покращений рівень безпеки, оскільки користувачі повинні були надати докази своєї особи, які ґрунтуються на двох або більше різних факторах.

Рис.1.1. Еволюція методів автентифікації.

Сьогодні очікується, що MFA буде використовуватися в сценаріях, де вимоги безпеки вищі, ніж зазвичай [4]. Розглянемо розпорядок дня зняття готівки в банкоматах. Тут користувач повинен надати фізичний токен (картку), що

представляє фактор власності, і підкріпити його PIN-кодом, який представляє фактор знань, щоб отримати доступ до особистого рахунку та зняття грошей. Цю систему можна було б легко зробити складнішою, додавши ще один фактор, як, наприклад, одноразовий пароль, який потрібно вводити після того, як картка та пароль користувача були надані У більш цікавому сценарії це можна було б зробити за допомогою методів розпізнавання обличчя. Багато ресурсів підтверджують MFA як надзвичайно перспективний напрямок еволюції автентифікації.

Одним із цікавих трендів майбутнього можна вважати аутентифікацію між транспортним засобом та його власником або тимчасовим користувачем. Поточним методом автентифікації, який дозволяє запускати та використовувати автомобіль, є іммобілайзерний ключ. Багатофакторна автентифікація (MFA) може значно покращити доступ до більшості електронних пристроїв як з точки зору безпеки, так і з точки зору взаємодії з користувачем.

Загалом програми багатофакторної автентифікації можна розділити на три групи, пов’язані з ринком:

- Комерційні програми, тобто вхід до облікового запису, електронна комерція, банкомати, контроль фізичного доступу тощо;
- Державні заяви, тобто документи, що посвідчують особу, державне посвідчення особи, паспорт, водійські права, соціальне забезпечення, прикордонний контроль тощо;
- Застосування судово-медичної експертизи, тобто кримінальне розслідування, зниклі діти, ідентифікація трупів тощо.

Загалом, кількість сценаріїв, пов’язаних із автентифікацією, справді велика. Сьогодні MFA стає надзвичайно критичним фактором для:

1) Підтвердження ідентифікації користувача та електронного пристрою (або його системи);

2) Перевірка підключення інфраструктури;

3) Перевірка взаємопов’язаних пристроїв IoT, таких як смартфон, планшет, носимий пристрій або будь-який інший цифровий маркер (ключ-ключ)[5].

В даний час однією з головних проблем MFA є відсутність кореляції між ідентифікацією користувача та ідентичністю інтелектуальних датчиків в електронному пристрої/системі. Що стосується безпеки, ці відносини повинні бути встановлені таким чином, щоб тільки легітимний оператор, наприклад, той, чию особу підтверджено заздалегідь, міг отримати права доступую.

У той же час процес MFA має бути максимально зручним для користувача, наприклад:

1) Клієнти спочатку реєструються та автентифікуються в постачальника послуг, щоб активувати та керувати послугами, до яких вони бажають отримати доступ;

2) Після доступу до послуги користувач повинен пройти простий SFA з відбитком пальця/токеном, підписаним заздалегідь постачальником послуг;

3) Після початкового прийняття системою клієнт проходить автентифікацію, увійшовши в систему з тим самим іменем користувача та паролем, які були налаштовані раніше на порталі клієнта (або через соціальну мережу). Для додаткової безпеки платформа керування може ввімкнути вторинні фактори автентифікації. Після того, як користувач успішно пройде всі тести, фреймворк автоматично проходить автентифікацію на сервісній платформі;

4) Вторинна автентифікація відбувається автоматично на основі біометричного MFA, тому користувачеві буде запропоновано ввести додатковий код або надати пароль-токен лише у випадку помилки MFA.

Біометрія справді вносить значний внесок у схему MFA та може значно покращити підтвердження особи шляхом поєднання фактора знань із мультимодальними біометричними факторами, таким чином значно ускладнюючи злочинцю проникнути в систему, видаючи себе за іншу особу. Однак використання біологічних факторів має свої проблеми, пов’язані в основному з простотою використання, що значною мірою впливає на зручність використання системи MFA.

З точки зору взаємодії з користувачем, сканер відбитків пальців уже забезпечує найбільш широко інтегрований біометричний інтерфейс. В основному це пов’язано з його прийняттям постачальниками смартфонів на ринку. З іншого

боку, не рекомендується використовувати його як окремий метод автентифікації. Однак для використання будь-якої біометрії часто потрібен набір окремих датчиків. Використання вже інтегрованих дозволяє зменшити витрати на систему автентифікації та полегшити прийняття кінцевими користувачами. Фундаментальний компроміс між зручністю використання та безпекою є одним із критичних факторів при розгляді сучасних систем автентифікації.

Інша проблема полягає в тому, що використання біометрії базується на механізмі бінарного прийняття рішень. Це було добре вивчено протягом останніх десятиліть у класичній статистичній теорії прийняття рішень з точки зору автентифікації.

Існують різні можливі рішення для контролю невеликої невідповідності фактичних «виміряних» біометричних даних і даних, що зберігаються в попередньо взятих зразках. Двома широко використовуваними методами є: частота помилкових прийомів (FAR) і частота помилкових відхилень (FRR). Маніпуляції з критеріями прийняття рішень дозволяють коригувати структуру автентифікації на основі попередньо визначених витрат, ризиків і переваг. Операція багатофакторної автентифікації (MFA) сильно залежить від FAR і FRR, оскільки отримати нульові значення для обох показників майже неможливо. Оцінка більш ніж однієї біометричної ознаки для встановлення особистості може значно покращити роботу системи багатофакторної автентифікації (MFA).

1.2 Аналіз проблем функціонування MFA

Інтеграція нових рішень завжди була серйозною проблемою як для розробників, так і для менеджерів.Основні проблеми представлені на рисунку 2. По-перше, прийняття користувачами є критичним аспектом для прийняття сильної ідентифікації та багатофакторної автентифікації. Під час прийняття та розгортання рішень MFA необхідно дотримуватися обережного та ретельного підходу, коли більшість проблем виникає через можливості та потенційні вигоди.

Рис.1.2. Основні операційні виклики багатофакторної автентифікації.

1. Простота використання

Основні проблеми зручності використання, що виникають у процесі автентифікації, можна охарактеризувати з трьох точок зору:

1) Ефективність виконання завдання - час на реєстрацію та час на аутентифікацію в системі;

2) Ефективність завдання - кількість спроб авторизації в системі;

3) Уподобання користувача - чи надає користувач перевагу певній схемі автентифікації над іншою.

На додаток до підходів, які обговорювалися раніше, дослідники вже почали дослідження більш конкретних ефектів у процедурах автентифікації на основі різноманітних людських факторів. Є дослідження того, як вік користувача впливає на ефективність виконання завдань у випадках PIN-коду та механізмів доступу до графіки. Зроблено висновок, що молоде покоління може витрачати на 50 відсотків менше часу на проходження процедури аутентифікації в обох випадках. Інший напрям у юзабіліті механізмів аутентифікації пов’язаний з когнітивними властивостями обраної людини. Для більшості учасників використання графічних паролів вимагає більше часу, ніж текстових.

Однак когнітивні відмінності між користувачами, тобто вони вербальні чи зображення, значно впливають на виконання завдання. Підтверджено, що текстові паролі використовуються краще, ніж графічні.Крім того, велику роль у цьому процесі відіграють властивості пристрою аутентифікації. Було доведено, що

використання смартфона або іншого безклавіатурного обладнання для створення пароля погіршується порівняно зі звичайними персональними комп’ютерами.

Сьогодні більшість служб онлайн-автентифікації базуються на знаннях, тобто залежать від комбінації імені користувача та пароля. Більш складні системи вимагають від користувача взаємодії з додатковими маркерами (одноразовими паролями, генераторами кодів, телефонами тощо). Доповнюючи традиційні стратегії автентифікації, MFA неможливий без біометрії. Багато дослідників пропагували використання персональних портативних пристроїв для використання під час процедури багатофакторної автентифікації (MFA). Надзвичайно важлива проблема зручності використання MFA полягає в тому, що «не всі користувачі можуть використовувати будь-яку дану біометричну систему». Люди, які втратили кінцівку внаслідок нещасного випадку, можуть не мати змоги ідентифікувати себе за відбитком пальця. Люди з вадами зору можуть мати труднощі з використанням методів автентифікації на основі райдужної оболонки ока. Біометрична автентифікація вимагає інтеграції нових служб і пристроїв, що призводить до потреби в додатковому навчанні під час усиновлення, що стає складнішим для людей похилого віку та через проблеми зрозумілості. Один факт очевидний: досвід користувача відіграє важливу роль в успішному прийнятті MFA; деякі кажуть, що «користувач на першому місці» [9]. Сьогодні дослідження придатної для використання безпеки для автентифікації користувачів на основі знань знаходяться в процесі пошуку життєздатного компромісу між зручністю використання та безпекою.

2. Інтеграція

Навіть якщо всі проблеми зручності використання вирішено на етапі розробки, інтеграція приносить нові проблеми як з технологічної, так і з людської точки зору.

Загалом, «інтеграція фізичної та IT-безпеки може отримати значні переваги для організації, включаючи підвищену ефективність і відповідність, а також покращену безпеку». При розробці системи MFA слід ретельно враховувати біометричну незалежність, тобто слід дотримуватися критеріїв забезпечення

взаємодії. Фреймворк повинен мати функціональні можливості для обробки біометричних даних від датчиків, відмінних від початково розгорнутих. Слід також брати до уваги використання мультибіометрії, тобто одночасне використання більш ніж одного фактора.

Іншою серйозною проблемою взаємодії є залежність від постачальника. Корпоративні рішення зазвичай розробляються як автономні ізольовані системи, які пропонують надзвичайно низький рівень гнучкості. Інтеграція нещодавно виведених на ринок датчиків вимагатиме складних і дорогих оновлень, які, ймовірно, не скоро будуть розглядатися.

Крім того, слід зазначити, що більшість доступних на даний момент рішень MFA не є повністю/частково відкритими. Це ставить перед сторонніми постачальниками послуг питання достовірності та надійності. Вибираючи структуру MFA, насамперед слід брати до уваги доступний рівень прозорості, який надають постачальники обладнання та програмного забезпечення.

3. Безпека та конфіденційність

Будь-яка структура MFA є цифровою системою, що складається з критичних компонентів, таких як датчики, сховище даних, пристрої обробки та канали зв’язку.Усі вони, як правило, вразливі до різноманітних атак на абсолютно різних рівнях, починаючи від спроб відтворення до атак противника. Таким чином, безпека є необхідним інструментом для забезпечення та підтримки конфіденційності.

Якщо дозволити лише законному контролеру отримувати доступ до конфіденційних персональних даних і обробляти їх, спільнота наражається на основні ризики, пов’язані з безпекою MFA, перелічені далі.

Перший із ключових ризиків пов’язаний зі спуфінгом даних, який буде успішно прийнято системою багатофакторної автентифікації. Примітно, що через те, що біометрія використовується різноманітними фреймворками MFA, чудова можливість для зловмисника проаналізувати як технологію, що лежить в основі датчика, так і сам датчик. Це призводить до виявлення найбільш підходящих матеріалів для підробки. Основна мета архітекторів системи та апаратного

забезпечення - забезпечити або безпечне середовище, або, якщо це неможливо, заздалегідь розглянути відповідні можливості підробки. Ризик захоплення фізичних або електронних шаблонів і їх відтворення в системі MFA слід ретельно розглядати.

Традиційно захист від атак електронного відтворення вимагає використання позначки часу. На жаль, атаку біометричного спуфінгу досить просто здійснити. Незважаючи на те, що біометрія може покращити продуктивність системи MFA, вона також може збільшити кількість вразливостей, якими може скористатися зловмисник. Додатковим ризиком є крадіжка конфіденційних даних під час передачі між датчиком і блоком обробки/зберігання. Така крадіжка може відбуватися в першу чергу через незахищену передачу з пристрою введення через вилучення та зіставлення блоків до бази даних, і існує потенціал для атаки. Необхідні рівні безпеки даних повинні бути гарантовані, щоб протистояти цьому типу ризику.

Ще одна можливість атакувати систему MFA - захоплення зразка секретних даних. Для факторів знань система буде негайно скомпрометована, якщо не використовуватимуться рішення з нульовим знанням. Особливий інтерес приділяється взяттю біометричного зразка, який неможливо оновити або змінити з часом. Отже, захист біометричних даних вимагає більш високого рівня безпеки під час захоплення, передачі, зберігання та обробки фаз.

Наступний ризик пов'язаний з крадіжкою зі сховища даних. Традиційно бази даних зберігаються централізовано, що забезпечує єдину точку відмови. У той же час, деякі з віддалених систем, які звертаються до бази даних, не завжди мають законний доступ до збережених персональних даних. Щоб захистити дані від крадіжки на додаток до використання необоротного шифрування, потрібен високий рівень ізоляції. Подальший ризик пов’язаний з атаками, пов’язаними з розташуванням. Сигнал GPS може бути вразливим до фіксації позиції (перешкод) або до подачі в приймач неправдивої інформації, так що він обчислює помилковий час або місцезнаходження. Подібні методи можуть бути застосовані до служб визначення місцезнаходження на основі стільникового зв’язку та WLAN.

Нарешті, будучи системою інформаційних технологій, структура MFA повинна забезпечувати відносно високі рівні «пропускної здатності», що відображає здатність системи задовольняти потреби своїх користувачів з точки зору кількості спроб введення за період часу. Навіть якщо біометричні дані вважаються придатними з усіх інших аспектів, але система може виконувати лише, наприклад, один збіг на основі біометричних даних на годину, тоді як потрібно працювати зі 100 зразками на годину, таке рішення не слід вважати можливим . Рекомендується вибрати відповідне апаратне забезпечення обробки для сторони сервера/захоплення.

Структура безпеки MFA також повинна підтримувати панель тестування на проникнення для оцінки її потенційних недоліків. Сьогодні розробники часто проводять зовнішній аудит для оцінки ризиків і діють на основі такої оцінки для більш ретельного планування. Таким чином, систему MFA слід оцінити для забезпечення більш безпечного середовища.

4. Стійкість до робочого середовища

Навіть якщо аспекти безпеки та конфіденційності повністю вирішені, біометричні системи, головним чином зняття відбитків пальців, не відповідали вимогам «надійності» з самого початку свого шляху. Це сталося в основному через те, що робочі випробування проводилися в лабораторних умовах замість польових. Одним із яскравих прикладів є розпізнавання голосу, яке було дуже надійним у тихій кімнаті, але не змогло перевірити користувача в міських ландшафтах.

Подібна проблема стосується ранніх методів розпізнавання обличчя, які не працювали без належного освітлення, якісної камери тощо. Зворотною стороною медалі була необхідність постійного спостереження за обстежуваним. Навіть сьогодні є або деякі поради щодо того, куди дивитися/покласти пальці, або є візуальна допомога під час перевірки безпеки. Відсутність досвіду взаємодії між машиною та людиною зазвичай аналізується за показниками невдач зареєструватися (FTE), а також невдало придбати (FTA). Вони обидва залежать від самих користувачів, а також від додаткового шуму навколишнього середовища.

Оскільки значна частина MFA сильно залежить від біометрії, її можна класифікувати як імовірнісну за своєю природою. Основа біометричної автентифікації лежить в області зіставлення шаблонів, яка, у свою чергу, спирається на наближення. Приблизне збігання є критично важливим фактором у будь-якій системі MFA, оскільки різниця між користувачами може бути вирішальною через низку факторів і невизначеність. Зображення, отримане під час сканування відбитків пальців, буде відрізнятися кожного разу, коли його спостерігатимуть через кут представлення, тиск, бруд, вологість або диференціацію датчиків, навіть якщо знімати ту саму людину.

Дві важливі частоти помилок, які використовуються для кількісної оцінки продуктивності біометричної системи автентифікації, це FAR і FRR. FAR - це відсоток самозванців, яких невірно дозволено вважати справжніми користувачами. Він визначається як відношення кількості помилкових збігів до загальної кількості спроб самозванців. FRR - це кількість справжніх користувачів, яким було відмовлено у використанні системи, яка визначається як відношення кількості помилкових відмов до загальної кількості спроб справжнього збігу.

Література також рекомендує використовувати частоту помилок кроссовера (CER) на додаток до раніше обговорених показників. Цей параметр визначається як ймовірність перебування системи в стані, де FAR дорівнює FRR. Чим нижче це значення, тим краще працює система. Відповідно до, «вищий FAR є кращим у системах, де безпека не має першочергового значення, тоді як більший FRR є кращим у додатках із високим рівнем безпеки». Точка рівності між FAR і FRR називається рівною частотою помилок (EER). На підставі вищесказаного можна ще раз зробити висновок, що систему, яка використовує виключно біометричні дані, не можна вважати бажаною структурою MFA.

Аналізуючи перераховані вище виклики, можна оцінити та оцінити всю систему MFA. Нижче ми пропонуємо підхід, який дозволить увімкнути MFA для автомобільної інтеграції на основі наявності великої кількості датчиків у сучасних автомобілях.

2. ДОСЛІДЖЕННЯ МЕТОДІВ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ЇХ ВИКОРИСТАННЯ ДЛЯ ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ

2.1 Дослідження сучасних та потенційніх джерела MFA

В даний час системи аутентифікації вже використовують величезну кількість датчиків, які дозволяють ідентифікувати користувача. Розглянемо фактори, придатні для MFA, відповідні датчики, доступні на ринку, і пов'язані з цим проблеми. Крім того, ми надаємо додаткові відомості про ті, які потенційно планується розгорнути найближчим часом.

1) Захист паролем

Традиційним способом аутентифікації користувача є запит PIN-коду, пароля тощо. Секретна парольна фраза традиційно представляє фактор знань. Для автентифікації користувача потрібен лише простий пристрій введення (принаймні одна кнопка).

2) Наявність маркера

Потім пароль може бути доповнений фізичним маркером, наприклад, карткою, яка рекомендована як друга факторна група — право власності. З точки зору апаратного забезпечення, користувач може пред'явити смарт-карту, телефон, носимий пристрій тощо, які делегувати складніше. У цьому випадку система повинна бути оснащена радіоінтерфейсом, що дозволяє здійснювати двосторонній зв'язок з токеном. З іншого боку, найбільш відомим програмним маркером є одноразовий програмно-генерований пароль. Основним недоліком вищесказаного є проблема неконтрольованого тиражування.

3) Біометрія голосу

Більшість сучасних інтелектуальних електронних пристроїв оснащено мікрофоном, який дозволяє використовувати розпізнавання голосу як фактор для MFA. Водночас розвиток технологій завтрашнього дня може дозволити спеціальним агентствам не тільки розпізнавати тих, хто говорить, але й імітувати їхні голоси, включаючи інтонацію, тембр тощо, що є серйозним недоліком використання голосу як основного методу автентифікації.

4) Розпізнавання обличчя

Наступним кроком може бути розпізнавання обличчя. На початку свого розвитку технологія базувалася на аналізі орієнтирного зображення, яке було відносно легко відтворити, надаючи системі фото. Наступним етапом було ввімкнення тривимірного розпізнавання обличчя, тобто просіння користувача рухати головою під час процесу автентифікації певним чином. Нарешті, розвиток цієї системи досяг точки розпізнавання фактичних виразів користувачів. Для можливості розпізнавання обличчя необхідно оснастити систему принаймні одним пристроєм виведення та камерою.

5) Окулярна методологія

Методи розпізнавання райдужної оболонки ока існують на ринку більше 20 років. Цей підхід не вимагає, щоб користувач знаходився близько до пристрою захоплення під час аналізу колірної моделі людського ока. Аналіз сітківки є ще одним привабливим методом. Тут тонка тканина, що складається з нейронних клітин, розташованих у задній частині ока, захоплюється та аналізується. Завдяки складній структурі капілярів, які постачають сітківку кров'ю, сітківка кожної людини унікальна. Найпомітнішими проблемами в цих методах є потреба у високоякісному пристрої захоплення та надійній математичній техніці для аналізу зображення.

6) Геометрія руки

Деякі системи використовують аналіз фізичної форми руки для автентифікації користувача. Спочатку для валідації суб'єкта використовували прив'язки, але зручність використання таких методів була низькою. Далі планшетний сканер використовувався для отримання зображення без необхідності фіксації руки користувача в одному певному положенні. Сьогодні в деяких системах використовуються звичайні камери, які не потребують близького контакту з поверхнею захоплення. Цей підхід, однак, не дуже стійкий до навколишнього середовища. Деякі постачальники застосовують так звану фотоплетизмографію (PPG), щоб визначити, чи носійний пристрій (наприклад,

розумний годинник) зараз знаходиться на зап’ясті користувача чи ні. Процес подібний до того, який виконується при вимірюванні частоти серця.

7) Розпізнавання вен

Удосконалення сканерів відбитків пальців також дає можливість отримати зображення вени пальця. Більш складні пристрої використовують розпізнавання відбитка долоні для отримання та збереження форми/руху всієї руки. На поточному етапі розвитку біометрія вен все ще вразлива до атак підробки.

8) Сканер відбитків пальців

Використання сканера відбитків пальців як основного механізму автентифікації зараз просувається більшістю виробників смартфонів/персональних комп’ютерів [6]. Це рішення є інтуїтивно зрозумілим у використанні, але залишається надзвичайно простим у виготовленні — головним чином завдяки тому факту, що наші відбитки пальців можна отримати практично з усього, до чого ми торкаємося. Інтеграційний потенціал цього методу дійсно високий, хоча його також не рекомендується використовувати як окремий підхід аутентифікації. Більшість виробників смартфонів встановлюють додаткову камеру для отримання відбитків пальців замість більш безпечного розпізнавання вен.

9) Розпізнавання теплових зображень

Подібно до розпізнавання вен, термосенсор використовується для реконструкції унікального теплового зображення кровотоку в тілі поблизу. Багато проблем із цим методом автентифікації можуть виникнути через умови користувача: хвороба чи емоції можуть суттєво вплинути на сприйняті цифри.

10) Географічне положення

Використання географічного розташування пристрою та користувача для перевірки того, чи можна надати доступ до пристрою/сервісу, є окремим випадком автентифікації на основі місцезнаходження. Важливо, що сигнал GPS може бути легко заглушений або вважатися несправним через властивості розповсюдження; таким чином, рекомендується використовувати принаймні два джерела визначення місцезнаходження, наприклад, GPS та ідентифікатор комірки бездротової мережі.

Смартфон можна використовувати для підтримки MFA з точки зору визначення місцезнаходження.

2.2 Аналіз майбутніх інтеграцій багатофакторної автентифікації (MFA) для більшої надійсності захисту

Прискорене впровадження в багатьох галузях, а також збільшення доступності біометричних послуг у широкому діапазоні доступних споживчих товарів підштовхує концепцію тісної інтеграції MFA. В даний час дослідники та перші користувачі технологій намагаються інтегрувати нові датчики для використання в системах MFA.

1) Виявлення поведінки

У минулому розпізнавання поведінки використовувалося для аналізу ритму друку військового телеграфіста для відстеження переміщення військ. Сьогодні жести для цілей автентифікації можуть варіюватися від звичайних до «важко імітованих», оскільки моторно-запрограмована навичка призводить до організації руху перед фактичним виконанням.

Сучасним прикладом такої ідентифікації є процес контакту з екраном смартфона. Цей підхід можна легко поєднати з будь-якими методами автентифікації введення тексту, оскільки шаблон набору унікальний для кожної людини. У випадку, якщо система багатофакторної автентифікації (MFA) спеціально розроблена для попередньо визначеного аналізу жестів, користувач повинен відтворити раніше вивчений рух, утримуючи сенсорний пристрій. Природним кроком аутентифікації для широко використовуваних кишенькових і переносних пристроїв є використання відбитків пальців акселерометра. Наприклад, кожен власник смартфона може бути перевірений на основі моделі ходи шляхом постійного моніторингу даних акселерометра, які майже неможливо підробити іншій людині.

Очікується, що для автентифікації в транспортному засобі інтегрована система відстежуватиме специфічні характеристики водія, які можна аналізувати з двох точок зору:

- Специфічна поведінка автомобіля: датчик кута повороту, датчик швидкості, датчик гальмівного тиску тощо;
- Людські фактори: музика, що звучить, зроблені дзвінки, присутність людей у машині тощо;

Ще одним важливим блокатором-фактором є алкогольний датчик. Функція запуску двигуна може бути заблокована, якщо рівень алкоголю в салоні перевищує допустиму норму.

2) Технології формування променя

З точки зору телекомунікацій, методи радіочастотної ідентифікації (RFID) і комунікації ближнього поля (NFC) вже отримали широке впровадження та визнання в суспільстві. Останні тенденції безпеки на фізичному рівні стверджують, що використання бездротових рішень із кількома входами та кількома виходами для визначення джерела сигналу може стати значним проривом у перевірці маркера на тілі користувача.

3) Системи класифікації пасажирів (OCS)

Деякі автомобільні системи вже мають рішення OCS, інтегровані в споживчі автомобілі [7]. Система датчиків може визначити, хто зараз перебуває на пасажирському/водійському сидінні, використовуючи, наприклад, вагу чи позу, і автоматично регулюючи транспортний засіб відповідно до особистих потреб.

4) Електрокардіографічне (ECG) розпізнавання

Дані (ECG) можна зібрати зі смарт-годинника користувача або трекера активності та порівняти з індивідуально збереженим шаблоном. Основна перевага використання цього фактора для автентифікації полягає в тому, що сигнали (ECG) постають як потенційна біометрична модальність з перевагою в тому, що їх важко (або майже неможливо) імітувати. Єдиним способом є використання наявного особистого запису.

5) Електроенцефалографічне (EEG) розпізнавання

Це рішення ґрунтується на аналізі мозкових хвиль і може розглядатися з фундаментального філософського положення «Cogito ergo sum» Р. Декарта, або «Я мислю, отже я існую». Це дозволяє отримати унікальний зразок патерну мозкової активності людини. Раніше збір даних електроенцефалографічний (EEG) можна було виконувати лише в клінічних умовах за допомогою інвазивних зондів під черепом або вологих гелевих електродів, розташованих на шкірі голови. Сьогодні простий електроенцефалографічний (EEG) збір можливий за допомогою доступних на ринку пристроїв розміром з гарнітуру.

6) Розпізнавання ДНК

Клітинні лінії людини є важливим ресурсом для досліджень, який найчастіше використовується у зворотних генетичних підходах. Це також джерело унікальної інформації про відбитки пальців ДНК [8]. Незважаючи на те, що цей процес трудомісткий і дорогий, він потенційно може бути використаний для попередньої авторизації користувача в високозахищеному об’єкті разом з іншими факторами.

У таблиці наведено порівняння основних показників для вже розгорнутих і нових факторів:

Фактори/сенсори оцінюються на основі наступних параметрів:

Фактор	Універсальність	Унікальність	Колекційність	Продуктивність	Прийнятність	Спуфінг
Пароль	n/a	L	H	H	H	H
Токен	n/a	M	H	H	H	H
Голос	M	L	M	L	H	H
Лице	H	L	M	L	H	M
Опитч.	H	H	M	M	L	H
Відбиток	M	H	M	H	M	H
Геометрія руки	M	M	M	M	M	M

Фактор	Універсальність	Унікальність	Колекційність	Продуктивність	Прийнятність	Спуфінг
Локація	n/a	L	M	H	M	H
Вени	M	M	M	M	M	M
Розпізнавання теплових зображень	H	H	L	M	H	H
Поведінка	H	H	L	L	L	L
Пучковоутворювальні	n/a	M	L	L	L	H
OCS	n/a	L	L	L	L	M
ECG	L	H	L	M	M	L
EEG	L	H	L	M	L	L
DNA	H	H	L	H	L	L

Таб 2.1 Порівняння відповідних факторів для MFA: H—високий; M—середній; L—низький; n/a — недоступний.

- Універсальність означає наявність чинника в кожній людині;
- Унікальність показує, наскільки добре фактор відрізняє одну людину від іншої;
- Збірність вимірює, наскільки легко отримати дані для обробки;
- Продуктивність вказує на досяжну точність, швидкість і міцність;
- Прийнятність означає ступінь прийняття технології людьми в їх повсякденному житті;
- Підробка вказує на рівень складності захоплення та підробки зразка.

Однак під час інтеграції багатофакторної автентифікації (MFA) для кінцевих користувачів потрібно вирішити багато інших проблем. У наступному розділі ми

детально розглянемо ці проблеми та оформимо рекомендації щодо полегшення інтеграції.

2.3 Дослідження гнучкої роботи MFA

У цій роботі ми розглянемо нову схему автентифікації, яка зосереджена на сценаріях транспортного засобу до всього (V2X), оскільки сучасні автомобілі вже оснащені декількома датчиками, які потенційно можуть бути використані для MFA. Традиційно користувач має ім’я користувача/пароль/PIN-код/токен і додатково буде запропоновано використати біометричний фактор, такий як риси обличчя або відбитки пальців. Загальний огляд, підкріплений подальшим обговоренням, наведено на малюнку.

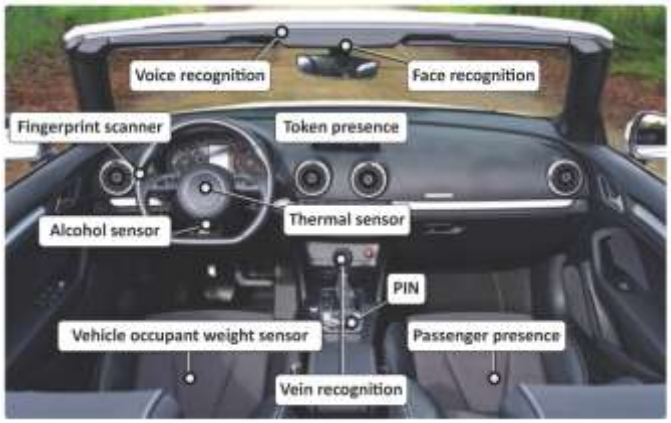

Рис.2.1. Нинішні та нові датчики MFA для транспортних засобів.

Якщо процедура автентифікації не може встановити доступ за допомогою цієї комбінації факторів, тоді користувачеві буде запропоновано автентифікуватися за допомогою іншого раніше зареєстрованого фактора або набору цих факторів. . Ця система MFA може не тільки перевіряти точність введення користувача, але й визначати, як користувач взаємодіє з пристроями, тобто аналізувати поведінку. Чим більше користувач взаємодіє з біометричною системою, тим точнішою стає її робота.

Іншою особливістю обговорюваного сценарію є реальна придатність датчика у разі взаємодії з автомобілем. Якщо використовується датчик (наприклад, пристрій для зчитування відбитків пальців), і цей пристрій недоступний з того

місця, де користувач намагається ввійти або отримати доступ, досвід використання стає негодящим. Наявність пристрою подвійного призначення — смартфона або смарт-годинника, який користувач уже має у своєму розпорядженні — як додаткового фактора MFA робить обидві системи вартість і зручність використання більш резоні [10].

Наявність великої кількості даних датчиків підводить нас до логічного наступного кроку його застосування в MFA. Крім того, ми передбачаємо потенційне використання відповідних факторів для автентифікації користувача без впровадження спеціального «верифікатора» з фактичними біометричними даними, за винятком тих, що збираються в режимі реального часу.

1. Традиційний підхід

Традиційний підхід до автентифікації базується на використанні одного фактора для підтвердження ідентичності користувача. Цей підхід використовує щось, що користувач знає (наприклад, пароль) або щось, що користувач має (наприклад, фізичний пристрій, такий як токен або смарт-карта).

Основний принцип традиційного підходу до автентифікації полягає в тому, що користувач надає ідентифікуючі дані (такі як ім'я користувача та пароль) для перевірки його ідентичності. Ці дані порівнюються зі збереженими даними в базі даних аутентифікації. Якщо дані співпадають, користувачу надається доступ до системи.

Основні компоненти традиційного підходу до автентифікації включають:

1) Ідентифікатор користувача: це унікальне ім'я або ідентифікатор, який відрізняє одного користувача від іншого. Наприклад, ім'я користувача або електронна адреса можуть використовуватись як ідентифікатор.

2) Пароль: це конфіденційна інформація, яку знає тільки користувач. Пароль використовується для перевірки ідентичності користувача. При введенні пароля він порівнюється зі збереженим хешем (криптографічною перетворенням) пароля, який зберігається в базі даних.

3) Аутентифікаційний сервер: це сервер, який виконує процес перевірки ідентичності користувача. Він отримує ідентифікатор та пароль користувача,

перевіряє їх на співпадіння зі збереженими даними і надає або відмовляє в доступі до системи.

Традиційний підхід до автентифікації має свої переваги, такі як простота реалізації і зрозумілість для користувачів. Однак він також має свої обмеження, такі як вразливість до атак перехоплення паролю, складності управління паролями та відсутність можливості додаткового захисту.

2. Запропонована зворотна методологія

Запропонована зворотна методологія автентифікації є інноваційним підходом, який змінює звичайну послідовність автентифікаційного процесу. Замість того, щоб користувач надавав свої ідентифікуючі дані для перевірки, система автоматично визначає характеристики користувача та засновано на цих характеристиках визначає його ідентичність.

Основні етапи роботи запропонованої зворотної методології автентифікації можуть включати наступне:

1) Збір характеристик: В цьому етапі система автоматично збирає різноманітні характеристики користувача, такі як динаміка набору тексту, голосові характеристики, особливості впливу пальців на сенсорних пристроях тощо. Ці характеристики можуть бути зібрані за допомогою різних сенсорів або аналізу специфічних взаємодій користувача з пристроєм.

2) Аналіз характеристик: Зібрані характеристики користувача аналізуються для виявлення унікальних шаблонів або особливостей, які можуть бути використані для ідентифікації користувача. Цей аналіз може включати використання алгоритмів машинного навчання, штучного інтелекту або статистичних методів для розпізнавання шаблонів і класифікації користувачів.

3) Визначення ідентичності: На основі аналізу характеристик система приймає рішення щодо ідентичності користувача. Якщо отримані результати вказують на відповідність ідентифікаційним шаблонам, користувачу надається доступ до системи.

4) Адаптація та навчання: Запропонована зворотна методологія може бути здатна до адаптації до зміни характеристик користувача в часі. Вона може

включати навчання системи для визначення нових шаблонів ідентифікації або адаптації до зміни поведінки користувача.

5) Забезпечення безпеки: Для забезпечення безпеки використовуються різні методи, такі як шифрування даних характеристик користувача, захист передачі даних між пристроями, контроль доступу до характеристик і т.д.

3. Пропоноване рішення MFA для програм V2X

Пропоноване рішення MFA (багатофакторна автентифікація) для програм V2X (Vehicle-to-Everything) передбачає використання декількох факторів для підтвердження ідентичності та забезпечення безпеки комунікації між автомобілями та іншими елементами інфраструктури.

Основні етапи роботи пропонованого рішення MFA для програм V2X можуть включати наступне:

1) Фактори автентифікації: Рішення MFA використовує різні фактори для підтвердження ідентичності користувача або автомобіля. Ці фактори можуть включати:

- Що-то, що знає: Наприклад, пароль, PIN-код або секретне запитання, на яке може відповісти тільки правильний користувач.
- Що-то, що має: Наприклад, фізичний об'єкт, такий як смарт-карта, ключ або мобільний пристрій.
- Що-то, що є унікальним: Наприклад, біометричні характеристики, такі як відбиток пальця, розпізнавання голосу або сканування обличчя.

2) Процес автентифікації: При комунікації між автомобілями та інфраструктурою, пропоноване рішення виконує процес автентифікації на основі зазначених факторів. Зазвичай, користувач або автомобіль надають ідентифікаційні дані та фактори автентифікації, а система перевіряє ці дані на відповідність ідентичності.

3) Захист даних: Пропоноване рішення також може включати захист даних шляхом використання шифрування та інших методів захисту. Це допомагає забезпечити конфіденційність та цілісність передаваних даних під час комунікації між автомобілями та інфраструктурою.

4) Менеджмент автентифікації: Пропоноване рішення може включати також систему управління автентифікацією, яка дозволяє керувати правами доступу, встановлювати політики безпеки та керувати процесом автентифікації для різних користувачів та автомобілів.

4. Невідповідність факторів

Невідповідність факторів в пропонованому рішенні MFA для програм V2X означає ситуацію, коли надані фактори автентифікації не відповідають очікуваним або зазначеним критеріям для підтвердження ідентичності користувача або автомобіля. Це може стати причиною відмови у доступі до системи або обмеженням привілеїв користувача.

У пропонованому рішенні MFA для програм V2X можуть бути використані різні фактори автентифікації, такі як паролі, біометричні характеристики, фізичні токени тощо. Якщо надані фактори не відповідають очікуваним, то процес автентифікації може вважатись невдалим, а доступ до системи або привілеї обмеженими.

Наприклад, якщо користувач надає неправильний пароль, не виконує вимоги біометричного сканування або не має фізичного токена, то система може вважати його ідентичність недостовірною та відмовити у доступі до функцій V2X або надати обмежені привілеї.

Невідповідність факторів може бути спричинена помилками введення, використанням недійсних або викрадених факторів, технічними несправностями або шахрайськими діями. Для забезпечення надійності системи MFA важливо ретельно перевіряти та перевіряти відповідність наданих факторів перед наданням доступу та виконанням привілеїв.

5. Хмарна допомога

У пропонованому рішенні MFA для програм V2X хмарна допомога може використовуватись для забезпечення автентифікації та керування доступом в хмарному середовищі. Основна ідея полягає в тому, що частину процесу автентифікації та перевірки ідентичності можна виконати в хмарі замість локального пристрою або інфраструктури.

Процес роботи хмарної допомоги включає наступні кроки:

1) Запит на автентифікацію: Користувач або автомобіль, які намагаються отримати доступ до системи V2X, ініціюють запит на автентифікацію. Запит може містити інформацію про ідентичність користувача або автомобіля.

2) Передача запиту до хмари: Запит на автентифікацію передається до хмарного середовища, де знаходиться інфраструктура для обробки автентифікаційних запитів.

3) Аналіз запиту: У хмарі здійснюється аналіз запиту на автентифікацію. Це може включати перевірку коректності запиту, перевірку даних ідентичності та виконання інших безпечних перевірок.

4) Взаємодія з іншими системами: Хмарна допомога може взаємодіяти з іншими системами або службами для перевірки ідентичності, наприклад, базами даних користувачів або іншими джерелами інформації.

5) Надання результату: Після аналізу запиту хмарна допомога генерує результат автентифікації, який може бути переданий назад до автомобіля або іншого пристрою. Результат може вказувати на успіх або невдачу автентифікації, а також додаткову інформацію про привілеї доступу.

6) Дії на локальному пристрої: Залежно від результату автентифікації, локальний пристрій, наприклад, автомобіль, може прийняти відповідні дії. Якщо автентифікація пройшла успішно, доступ до функцій V2X може бути наданий. У разі невдачі автентифікації можуть застосовуватись обмеження або відмова в доступі.

6. Методи оцінки потенціалу

Методи оцінки потенціалу в автентифікації використовуються для визначення рівня достовірності або потенційних ризиків, пов'язаних з ідентифікацією користувача або сутності, яка намагається отримати доступ до системи. Ці методи дозволяють оцінити, наскільки надійно можна впевнитись у тому, що особа або пристрій, які намагаються отримати доступ, є дійсними і мають необхідні привілеї.

Існує кілька методів оцінки потенціалу в автентифікації, серед яких можуть бути:

1) Аналіз ризиків: Цей метод оцінки включає оцінку ризиків, пов'язаних з конкретною транзакцією або доступом до системи. Враховуються різні фактори, такі як ідентичність користувача, тип транзакції, контекст отримання доступу та інші. Ризик може бути оцінений на основі історичних даних, статистики або аналізу відхилень від звичайних поведінкових моделей.

2) Оцінка привілеїв: Цей метод оцінки використовується для визначення привілеїв або прав доступу, які пов'язані з ідентичністю користувача або сутності. Враховуються атрибути, такі як роль, рівень авторизації, привілеї, що надаються певній ідентичності. Оцінка привілеїв може здійснюватись на основі встановлених політик безпеки або ролей.

3) Аналіз поведінки: Цей метод оцінки враховує поведінкові аспекти користувача або сутності. Збираються дані про типові дії, звички, стилі поведінки та інші атрибути, які можуть бути унікальними для конкретної ідентичності. Ці дані порівнюються зі звичайними моделями поведінки, і в разі виявлення відхилень можуть застосовуватись додаткові заходи або обмеження.

4) Використання біометричних даних: Цей метод оцінки використовує фізичні атрибути користувача, такі як відбитки пальців, розпізнавання обличчя, сканування рітини ока тощо. Біометричні дані можуть бути використані для порівняння з попередньо збереженими даними або шаблонами, що дозволяють підтвердити ідентичність особи.

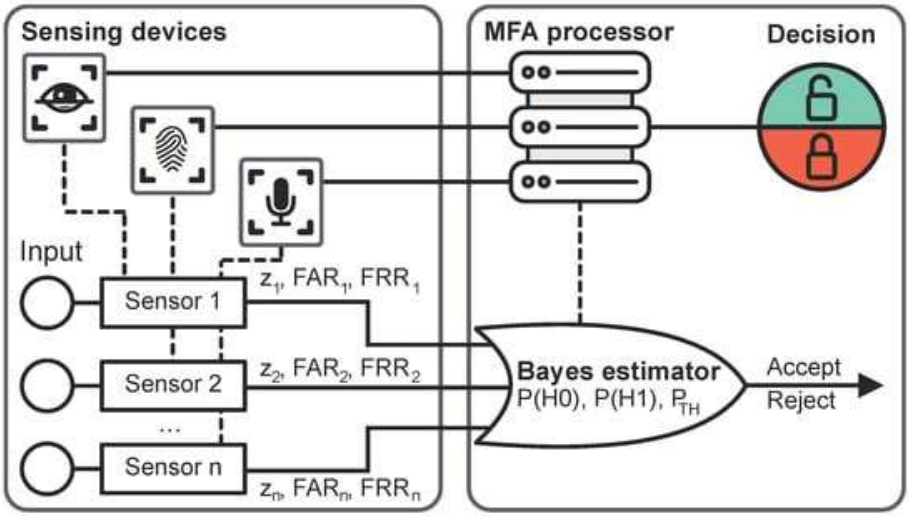

Рис.2.2. Режим системи MFA.

Ці методи можуть використовуватись окремо або комбінуватись для отримання більш надійних результатів автентифікації. Вибір конкретного методу залежить від вимог безпеки, типу системи та доступних технологій.

7. Строга методологія прийняття рішень

Строга методологія прийняття рішень в методах оцінки потенціалу автентифікації включає систематичний підхід до процесу оцінки, аналізу та прийняття рішень щодо потенційних ризиків та достовірності ідентифікації. Вона базується на залежних від даних протоколах, критеріях та алгоритмах, що використовуються для прийняття обґрунтованих рішень.

Основні етапи строгої методології прийняття рішень включають:

1) Зібрання даних: Спочатку збираються відповідні дані, які включають інформацію про ідентичність користувача, контекст доступу, атрибути безпеки та інші фактори, які можуть вплинути на процес автентифікації.

2) Аналіз ризиків: Зібрані дані аналізуються для визначення потенційних ризиків, пов'язаних з ідентифікацією користувача або сутності. Враховуються фактори, такі як конфіденційність, цілісність, доступність та вплив можливих загроз.

3) Вибір методів оцінки: На основі аналізу ризиків обираються відповідні методи оцінки потенціалу автентифікації. Це можуть бути методи, згадані раніше, такі як аналіз ризиків, оцінка привілеїв, аналіз поведінки, використання біометричних даних або комбінація декількох методів.

4) Розробка протоколів та критеріїв: На основі вибраних методів розробляються протоколи та критерії, які визначають процес оцінки та прийняття рішень. Ці протоколи та критерії враховують усі потенційні фактори ризику та встановлюють механізми для прийняття обґрунтованих рішень.

5) Виконання оцінки: Здійснюється оцінка потенціалу автентифікації на підставі розроблених протоколів та критеріїв. Це включає зіставлення збережених даних зі зібраними даними, порівняння з правилами та алгоритмами, а також використання відповідних аналітичних інструментів.

6) Прийняття рішень: На основі результатів оцінки приймаються рішення щодо автентифікації користувача або сутності. Це можуть бути рішення про надання доступу, вимоги додаткових перевірок або відхилення доступу на підставі визначених критеріїв та обґрунтувань.

Ці кроки забезпечують систематичний підхід до оцінки потенціалу автентифікації та прийняття рішень, з метою забезпечення високого рівня безпеки та достовірності процесу ідентифікації.

8. Методологія імовірнісного рішення

Методологія імовірнісного рішення в методах оцінки потенціалу автентифікації базується на використанні статистичних методів та імовірнісних моделей для аналізу та оцінки ризиків ідентифікації. Цей підхід дозволяє оцінити ймовірність того, що конкретний користувач або сутність є легітимними.

Основні кроки методології імовірнісного рішення включають:

1) Зібрання даних: Збирання релевантних даних про користувачів, сутності та їхню ідентичність. Ці дані можуть включати історичні дані про взаємодії користувача з системою, логи автентифікації, атрибути безпеки та інші фактори, що впливають на ідентифікацію.

2) Побудова моделей: Розроблення імовірнісних моделей, які відображають поведінку та характеристики користувачів та сутностей. Ці моделі можуть базуватися на статистичних методах, машинному навчанні або комбінації обох. Вони допомагають визначити імовірності різних подій, таких як легітимність або фальсифікація ідентичності.

3) Аналіз ризиків: Використовуючи моделі імовірності, аналізується ризик, пов'язаний з ідентифікацією користувачів або сутностей. Враховуються фактори, такі як історія взаємодії, несподівані атрибути, зміни поведінки та інші відхилення від норми.

4) Визначення порогів: Встановлення порогових значень для прийняття рішень на підставі аналізу ризиків. Ці пороги вказують на межу між легітимними та підозрілими/небезпечними ідентифікаціями. Наприклад, якщо імовірність підозрілої ідентифікації перевищує певний поріг, можуть застосовуватись додаткові перевірки або блокування доступу.

5) Прийняття рішень: На основі аналізу ризиків та визначених порогів приймаються рішення стосовно автентифікації. Це можуть бути рішення про надання доступу, запит додаткових перевірок, відхилення доступу або інші дії відповідно до встановлених правил та процедур.

Методологія імовірнісного рішення дозволяє враховувати багатофакторність і комплексність процесу автентифікації, а також забезпечує більш гнучкий і індивідуальний підхід до прийняття рішень, забезпечуючи високий рівень безпеки та зручності для користувачів.

9. Оцінка

Оцінка в методах оцінки потенціалу автентифікації використовується для визначення ефективності різних методів або факторів, що використовуються в процесі автентифікації. Цей процес включає оцінку та порівняння різних параметрів, щоб визначити, наскільки добре вони задовольняють вимоги безпеки, зручності використання та інших факторів.

Оцінка може включати наступні кроки:

1) Визначення критеріїв оцінки: Встановлення критеріїв, які будуть використовуватись для оцінки різних методів або факторів автентифікації. Ці критерії можуть включати безпеку, зручність використання, вартість, масштабованість та інші фактори, які важливі для конкретної системи або сценарію.

2) Зібрання даних: Збирання релевантних даних про різні методи або фактори автентифікації. Ці дані можуть включати результати попередніх досліджень, статистику використання, відгуки користувачів та інші джерела інформації.

3) Аналіз та порівняння: Проведення аналізу та порівняння різних методів або факторів на основі зібраних даних та визначених критеріїв. Це може включати оцінку безпеки, швидкості, складності, зручності використання та інших характеристик.

4) Вибір найкращого рішення: На основі аналізу та порівняння різних методів або факторів вибирається найкраще рішення, що задовольняє визначені критерії оцінки. Це може бути один метод або комбінація різних методів, залежно від потреб і вимог системи.

Оцінка допомагає визначити, які методи або фактори автентифікації є найефективнішими та найпідходящішими для конкретної системи або сценарію. Це дозволяє покращити безпеку та зручність використання автентифікаційних методів і забезпечити оптимальне рішення для потреб організації чи системи.

3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ТА ОГЛЯД ВИДІВ ТА НАЛАШТУВАНЬБАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

3.1 Аналіз налаштування та функцій багатофакторної автентифікації

Authenticator – це мобільний додаток або окремий пристрій для створення кодів двоетапної автентифікації.

Двоетапна аутентифікація забезпечує надійніший захист вашого облікового запису: щоб входити до нього, потрібно не тільки пароль, але і код підтвердження

Токен (також апаратний токен, USB-ключ, криптографічний токен) — компактний пристрій, призначений для забезпечення інформаційної безпеки користувача, також використовується для ідентифікації його власника, безпечного віддаленого доступу до інформаційних ресурсів і т. д. Зазвичай, це фізичний пристрій, що використовується для спрощення аутентифікації. Також цей термін може відноситися і до програмних токенів, які видаються користувачеві після успішної авторизації і є ключем для доступу до служб.

Токени призначені для електронного посвідчення особи (наприклад, клієнта, який одержує доступ до банківського рахунку), при цьому вони можуть використовуватися замість або разом з паролем. У певному сенсі токен — це електронний ключ для доступу до чого-небудь.

Зазвичай апаратні токени мають невеликий розмір, що дозволяє носити їх у кишені або гаманці, часто вони мають вигляд, як брелоки.

Розглянемо налащтування багатофакторної автентифікації на прикладі Google аккаунту:

Створимо Google аккаунт для демонстрацій налаштувань.

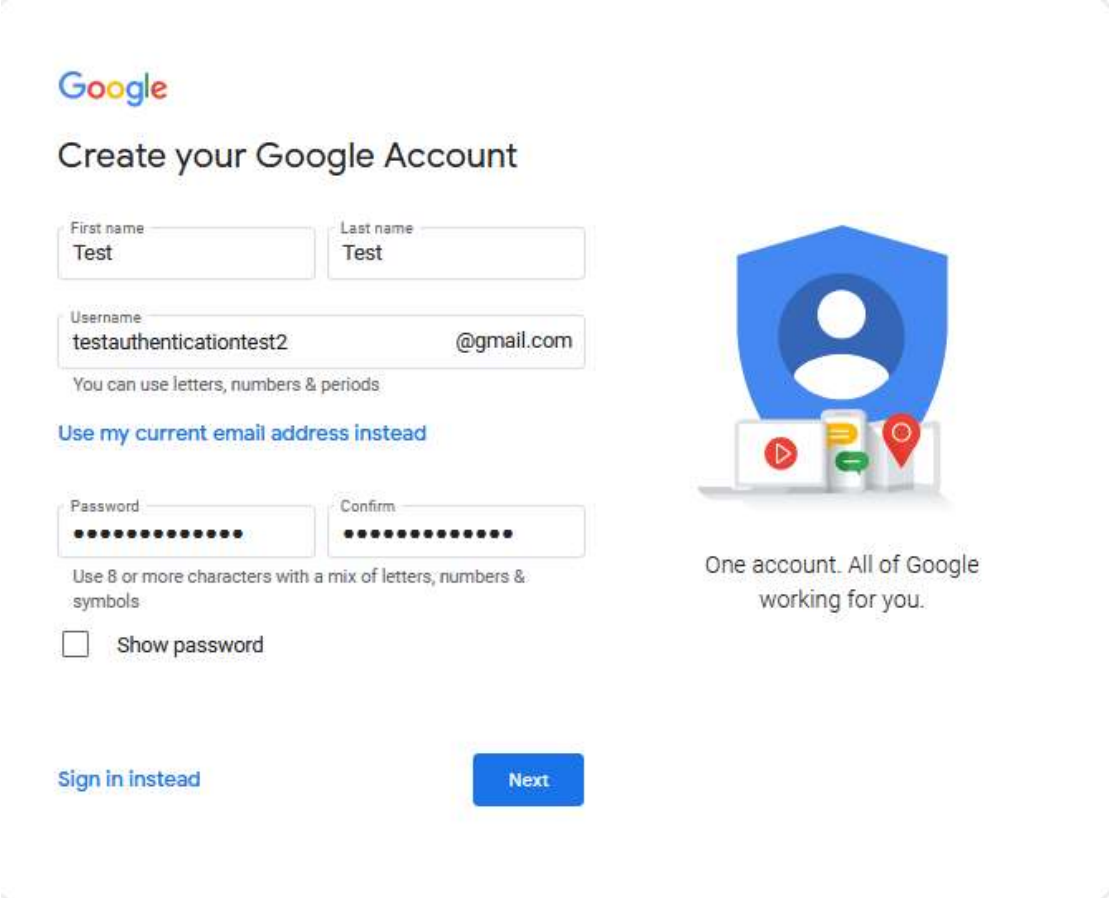

Рис.3.1. Підготовка до огляду видів автентифікації на основі Google аккаунту.

Після створення переходимо у вкладку “Безпека”. Тут ми можемо спостерігати варіанти які нам пропонують нам для підключення. Нас цікавить пункт Двухфакторна автентифікація (2-Step Verification).

Рис.3.2. Огляд видів автентифікації.

Підключаємо один із видів двухфакторної автентифікації, а саме надходження SMS коду або надходження вхідного дзвінка для входу в систему після введення паролю.

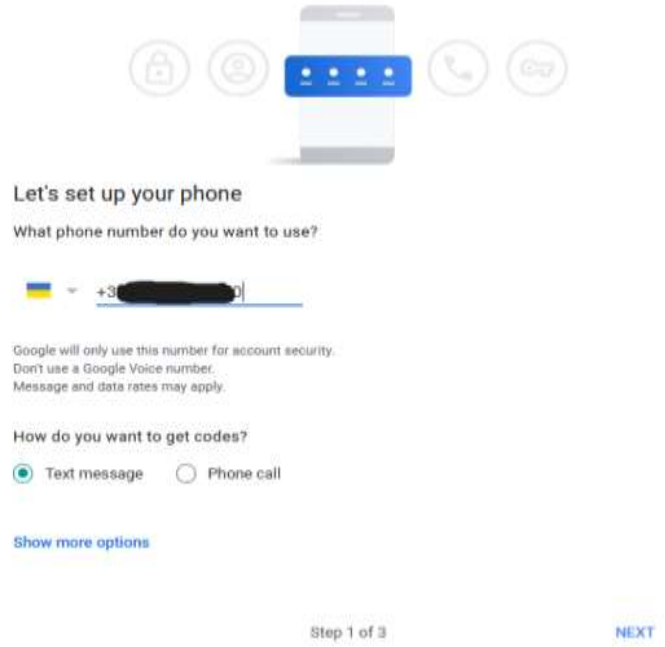

Рис.3.3. Додавання двухфакторної автентифікації.

На рисунку ми можемо побачити що процес підключення був успішним. Але такий метод я вважаю надійним чим наступні.

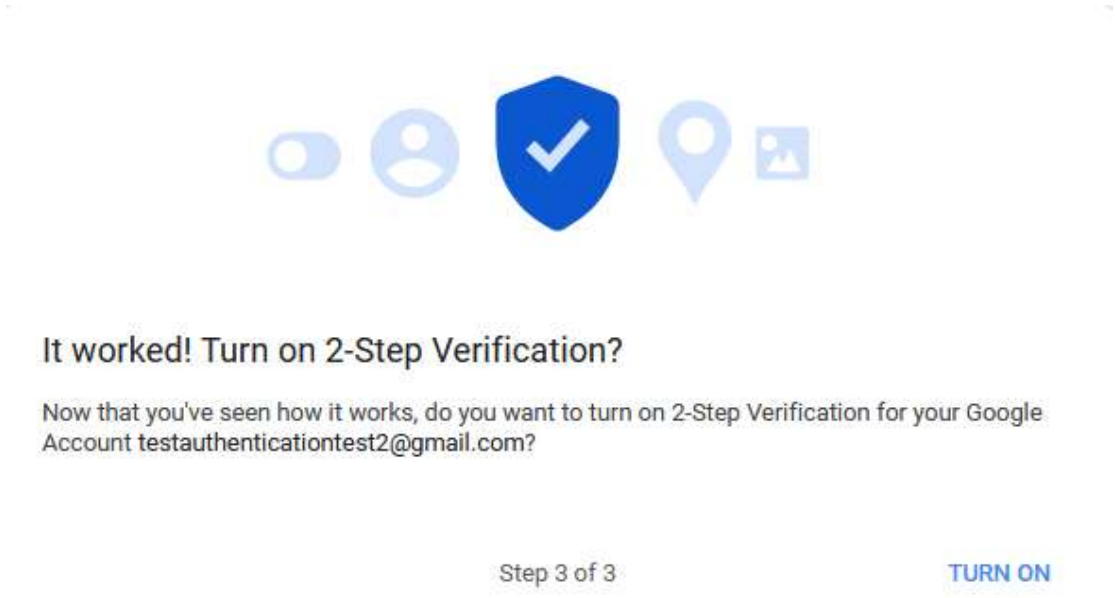

Рис.3.4. Демонстрація успішної прив’язки.

Після підключення ми можемо спостерігати, що нам відкрилось більш гнучке налаштування автентифікації. Нас цікавить пункт Программа для автентифікації (Authenticator app).

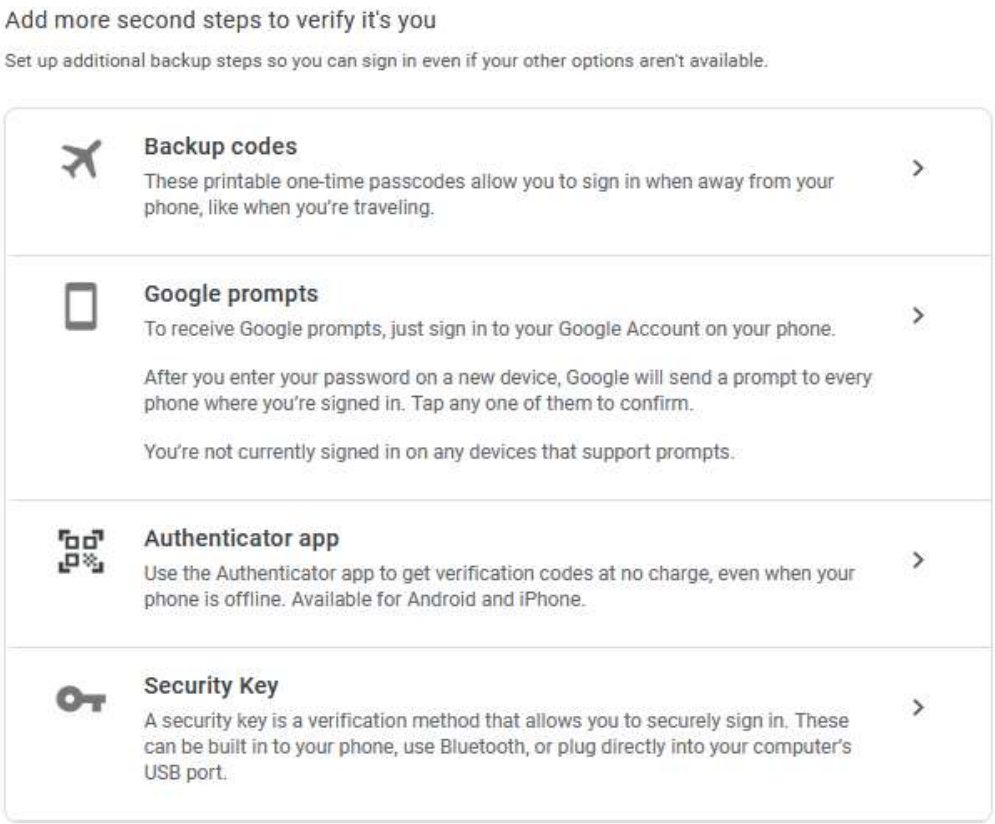

Рис.3.5. Демонстрація більш гнучкого налаштування автентифікації.

Для того щоб підключити цей метод автентифікації нам потрібно завантажити додаток для підключення кодів верифікації для двухфакторної автентифікації. Моя рекомендація використовувати Microsoft Authenticator, так як він використовує вбудовану автентифікацію по біометрії, яку можна підкріпити паролем для додатків які вбудовані в сучасних смартфонах.

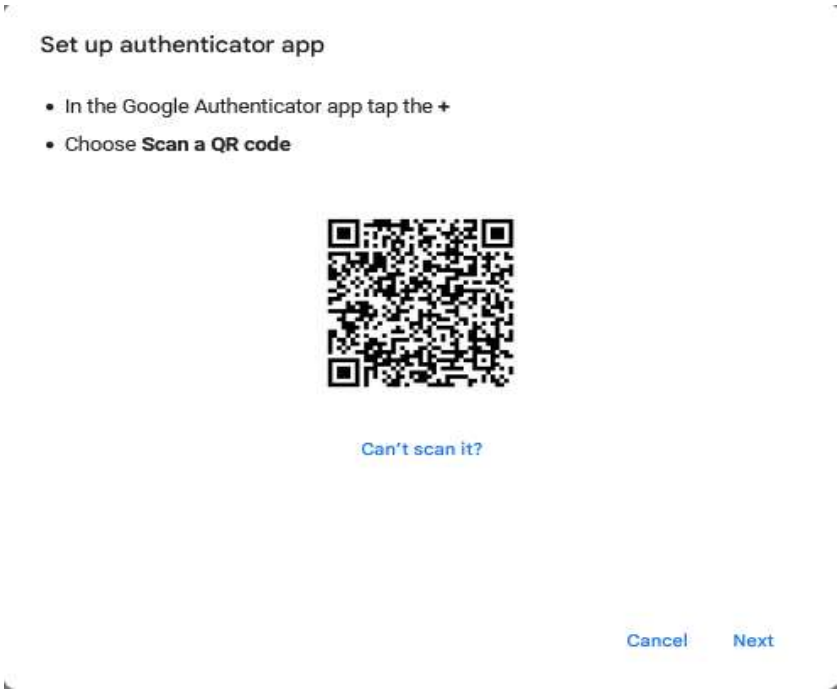

Рис.3.6. Прив'язка додатку для генерації кодів доступу.

Рис.3.7. Успішність прив'язки додатка.

Розглянемо методи які залишились. Резервні коди (Backup codes), цей метод підходить якщо був втрачений доступ до додатку двухфакторної автентифікації. Сповіщення від Google (Google prompts), я вважаю цей метод не таким надійним як генерація кодів доступу так як він потребує просто підтвердеження входу з пристрою на якому вже була проведенна авторизація, але все ж плюс в цьому є так як пристрій повинен пройти повний вхід в систему. Ключ доступу (Security key), дозволяє використати токен для входу в систему, можна скомбінувати зі всіма методами для забезбечення найбільшої безпеки.

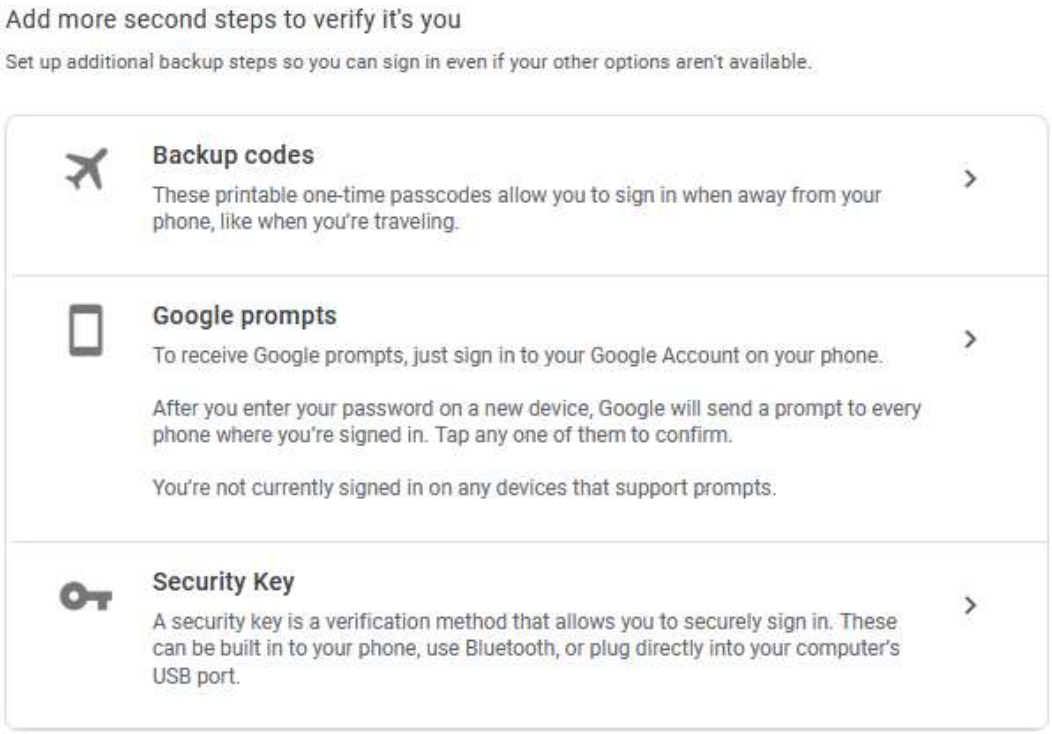

Рис.3.8. Методи автентифікації які залишились.

Ключ безпеки – це один із найбільш надійних других етапів автентифікації. Ви можете додати фізичний ключ або скористатися вбудованим у телефон.

Для його використання потрібно:

1. Отримайте ключі.

- Скористатися ключем безпеки, вбудованим у сумісний телефон.
- Купити ключі безпеки Titan у Google Store.
- Замовити сумісний ключ безпеки в надійного продавця.

2. Додайте ключ в обліковий запис.

- Відкрийте сумісний веб-переглядач, наприклад Chrome, FireFox або Safari (13.0.4 чи новішої версії).
- Зареєструйте ключ безпеки. Увійдіть в обліковий запис, якщо буде потрібно.

3. Увійдіть за допомогою ключа

Ключ безпеки – це один із найбільш надійних других етапів автентифікації. Якщо ви налаштували інший другий етап, використовуйте ключ безпеки для входу в обліковий запис, коли це можливо.

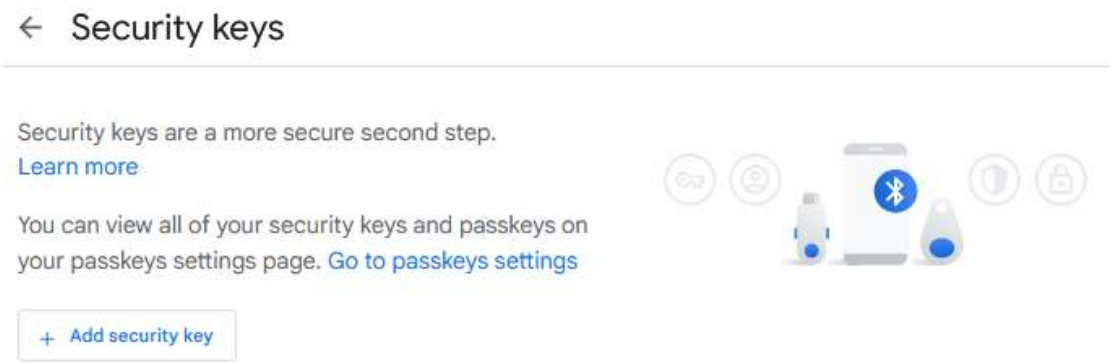

Рис.3.9. Метод ключ доступу.

3.2 Переваги використання токенів та генерації кодів

Спільною перевагаю є те що це додатковий фактор безпеки.Це надає додатковий фактор безпеки, який може бути використаний разом з іншими факторами, такими як пароль або відбиток пальця. Це підвищує безпеку, оскільки зловмисник повинен мати окремий пристрій з одним з методів, так і знати інші фактори автентифікації, щоб отримати доступ.

Якщо розглядати окремі плюси у цих двох методів, то токена це:

1) Віддалена автентифікація: Токени автентифікації можуть бути використані для здійснення віддаленої автентифікації. Вони можуть бути вбудовані в мобільні додатки або використовуватись через спеціальні програми для доступу до системи з віддаленої локації. Це зручно для користувачів, які працюють з віддалених місць або використовують хмарні послуги.

2) Висока стійкість до атак: Фізичні токени мають високу стійкість до атак, таких як фішинг або підміна. Токени можуть бути захищені паролями, PIN-кодами або біометричними данними, що робить їх важкими для зламу.

3) Універсальність: Багато токенів автентифікації сумісні з різними системами та сервісами. Це означає, що ви можете використовувати один токен для автентифікації в різних системах, що спрощує процес управління і забезпечення безпеки.

4) Можливість відновлення: У разі втрати або крадіжки токену автентифікації, його можна замінити новим без необхідності зміни паролів або інших факторів автентифікації. Це зручно та забезпечує високий рівень безпеки.

У генерації кодів це:

1) Одноразовість кодів: Генеровані коди є одноразовими, що означає, що вони дійсні лише на короткий період часу і не можуть бути повторно використані. Це зменшує ризик підміни або перехвату кодів зловмисниками, оскільки вони будуть некорисними поза обмежений часовий проміжок.

2) Зручність використання: Генерація кодів може бути зручним інструментом для автентифікації. Користувачі можуть отримувати коди через мобільні додатки, SMS-повідомлення або апаратні пристрої, такі як токени автентифікації. Це робить процес автентифікації легким і доступним у різних ситуаціях.

3) Додатковий рівень захисту: Генерація кодів може використовуватись як додатковий рівень захисту для критичних систем або транзакцій. Використання додаткового коду, який змінюється з кожним входом, допомагає ускладнити атаки і зменшити ризик несанкціонованого доступу.

4) Сумісність з різними платформами: Генерація кодів може бути підтримувана на різних платформах і пристроях, таких як мобільні телефони, комп'ютери або спеціалізовані пристрої. Це дає можливість користувачам використовувати зручний для них метод генерації кодів безпеки.

5) Масштабованість: Генерація кодів може бути легко масштабована для великої кількості користувачів і систем. Можна використовувати централізовані рішення для генерації і управління кодами, що полегшує впровадження і керування багатокористувацькими середовищами.

На додаток кожен з цих методів можна захистити за допомогою методів біометрії які були розглянуті раніше.

3.3 Розробка рекомендацій щодо застосування багатофакторної автентифікації в автоматизованих системах

Відштовхуючись від досліджень проведених раніше можна розробити такі рекомендації щодо застосування багатофакторної автентифікації в автоматизованих системах:

1) Використовуйте різноманітні фактори: Застосовуйте комбінацію різних факторів автентифікації, таких як щось, що користувач знає (наприклад, пароль), щось, що користувач має (токен або смарт-карта) і щось, що користувач є (біометричні дані, такі як відбиток пальця або розпізнавання обличчя). Це забезпечить більшу безпеку, оскільки зловмиснику буде складніше отримати доступ до всіх необхідних факторів.

2) Враховуйте контекст: Використовуйте інформацію про контекст, таку як місцезнаходження користувача, IP-адресу, пристрій тощо, для додаткової перевірки автентичності користувача. Наприклад, якщо автентифікація проводиться з незвичайного місця або з незвичайного пристрою, можна вимагати додаткові фактори для підтвердження ідентичності.

3) Використовуйте адаптивну автентифікацію: Застосовуйте адаптивні методи автентифікації, які враховують ризики та загрози в реальному часі. Наприклад, якщо система виявляє підозрілу активність або незвичайні дії користувача, може бути вимагана додаткова перевірка, така як введення одноразового пароля або відсканування відбитку пальця.

4) Забезпечте належну безпеку факторів: Зверніть особливу увагу на безпеку факторів автентифікації. Застосовуйте криптографічні методи для захисту паролів та інших конфіденційних даних. Використовуйте надійні пристрої для зберігання та обробки біометричних даних або інших факторів, що вимагають фізичного зберігання.

5) Передбачте можливість відновлення доступу: Враховуйте можливість відновлення доступу у випадку втрати або компрометації факторів автентифікації. Забезпечте механізми для відновлення паролів, блокування пристроїв або скасування токенів у разі необхідності.

6) Забезпечте зручність використання: Розробляючи систему багатофакторної автентифікації, забезпечте її зручне використання для користувачів. Мінімізуйте кількість кроків та складність процесу автентифікації, щоб уникнути відчуття незручності та підвищити прийняття користувачами.

7) Регулярно аудитуйте та оновлюйте систему: Проводьте регулярні аудити та оновлюйте систему багатофакторної автентифікації для виявлення та виправлення потенційних слабкостей та вразливостей. Слід слідкувати за новими технологіями та рекомендаціями безпеки для забезпечення найвищого рівня захисту.

ВИСНОВКИ

Сьогодні автентифікація важлива, ніж будь-коли. У цифрову епоху більшість користувачів покладатимуться на біометричні дані в питаннях безпеки систем і авторизації як доповнення до звичайних паролів. Незважаючи на те, що проблеми з конфіденційністю, безпекою, зручністю використання та точністю залишаються актуальними, MFA стає системою, яка обіцяє безпеку та легкість використання, необхідні сучасним користувачам під час отримання доступу до конфіденційних даних.

Без сумніву, біометрія є одним із ключових рівнів, які забезпечують майбутнє MFA. Ця функція часто розглядається не як окрема, а як доповнення до традиційних підходів автентифікації, таких як паролі, смарт-картки та PIN-коди. Очікується, що поєднання двох або більше механізмів автентифікації забезпечить вищий рівень безпеки під час перевірки користувача. Очікувана еволюція до MFA базується на синергетичних біометричних системах, які дозволяють значно покращити взаємодію з користувачем і пропускну здатність системи MFA, що було б корисним для різних програм. Такі системи будуть інтелектуально поєднувати всі три типи факторів, а саме знання, біометрію та власність.

Оскільки звичайні однофакторні системи сьогодні базуються лише на одному параметрі, якщо на його отримання будь-яким чином вплинути (будь то шум чи збої), загальна точність погіршиться.

Одним із найперспективніших напрямків у MFA є поведінкова біометрія, що забезпечує абсолютно нові способи аутентифікації користувачів.

Усі розглянуті сценарії MFA вимагають значних ресурсів пам’яті для статистичного аналізу вхідних даних і зберігання біометричних зразків, навіть якщо використовуються різні методи оптимізації.

Підводячи підсумок, біометричні технології є визначним напрямком розвитку ринку мобільних пристроїв.

Ця робота забезпечила систематичний огляд сучасного стану як технічних питань, так і питань зручності використання, а також основних проблем у

доступних на даний момент системах MFA. В першу чергу увага була зосереджена на факторах MFA, які становлять сучасний стан, майбутні можливі напрямки, відповідні виклики та перспективні рішення [11].

ПЕРЕЛІК ПОСИЛАНЬ

1. VNI Cisco Global Mobile Data Traffic Forecast 2016–2021. White Paper. 2017. Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf (accessed on 4 January 2018).

2. Dworkin, M.J. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. Special Publication (NIST SP)-800-38B 2016. Available online: https://www.nist.gov/publications/recommendation-block-cipher-modes-operation-cmac-mode-authentication-0 (accessed on 4 January 2018).

3. Danny, T. MFA (Multi-Factor Authentication) with Biometrics. 2017. Available online: https://www.bayometric.com/mfa-multi-factor-authentication-biometrics/ (accessed on 4 Jaurnay 2018).

4. SC Media UK. 68% of Europeans Want to Use Biometric Authentication for Payments. 2016. Available online: https://www.scmagazineuk.com/68-of-europeans-want-to-use-biometric-authentication-for-payments/article/530818/ (accessed on 4 January 2018).

5. Rossi, B. Connected car security: why identity should be in the driving seat. 2016. Available online: http://www.information-age.com/connected-car-security-why-identity-should-be-driving-seat-123461078/ (accessed on 4 January 2018).

6. Titcomb, J. Why Your Smartphone's Fingerprint Scanner Isn't as Secure as You Might Think. 2017. Available online: http://www.telegraph.co.uk/technology/2017/04/11/smartphone-fingerprint-scanners-could-easily-fooled-fake-prints/ (accessed on 4 January 2018).

7. Mercedes-Benz SUV Operation Manual. Occupant Classification System (OCS). 2017. Available online: http://www.mersuv.com/mbread-149.html (accessed on 4 January 2018).

8. Reid, Y.; Storts, D.; Riss, T.; Minor, L. Authentication of Human Cell Lines by STR DNA Profiling Analysis. Eli Lilly & Company and the National Center for Advancing Translational Sciences, 2013. Available online: https://www.ncbi.nlm.nih.gov/books/NBK144066/ (accessed on 4 January 2018).

9. NetworkWorld. Solving the Challenge of Multi-Factor Authentication Adoption. 2017. Available online: https://www.networkworld.com/article/3197096/lan-wan/solving-the-challenge-of-multi-factor-authentication-adoption.html (accessed on 4 January 2018).

10. SC Media UK. Making the Case for the Use of Biometrics in Multi-Factor Authentication. 2016. Available online: https://www.scmagazineuk.com/making-the-case-for-the-use-of-biometrics-in-multi-factor-authentication/article/545395/ (accessed on 1 January 2018).

11. Biometrics Research Group, Inc. Mobile Biometric Applications. 2017. Available online: http://chicagopolicyreview.org/2014/03/04/biometrics-and-artificial-neural-networks-how-big-data-collection-works-in-your-favor/ (accessed on 4 January 2018).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)