МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

МИКОЛИШИН Марія Петрівна

Програмно-апаратний засіб для оцінки та аналізу безпеки мобільних пристроїв / Software and Hardware Tool for Assessing and Analyzing Mobile Device Security

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконала студентка групи КБм -21
М.П. Миколишин

_____

Науковий керівник
д.т.н., професор М.М.Касянчук

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри

_____ В.В.Яцків

ТЕРНОПІЛЬ – 2024

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
МИКОЛИШИН Марія Петрівна

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Програмно-апаратний засіб для оцінки та аналізу безпеки мобільних пристроїв / Software and Hardware Tool for Assessing and Analyzing Mobile Device Security
керівник роботи: д.т.н., проф. М.М.Касянчук
затверджені наказом по університету 12 грудня 2023 року № 753
2. Строк подання студентом закінченої кваліфікаційної роботи
12 грудня 2024 р.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити

− порівняльний аналіз існуючих програмно-апаратних засобів для оцінки безпеки мобільних пристроїв;

− виявлення та класифікація основних загроз і вразливостей мобільних платформ (Android, iOS);

− розробка методів та алгоритмів для автоматизованого аналізу безпеки мобільних пристроїв;

− вибір інструментів, бібліотек та середовища для реалізації програмно-апаратного рішення;

− оцінка ефективності створеного засобу шляхом порівняння результатів з відомими підходами.

5. Перелік графічного матеріалу у роботі.

Архітектура SecuWear та вектори атак на носимі, мобільні та веб-сервіси.
Порівняльний аналіз компонентів SecuWear.
Захоплення пакетів SecuWear під час атаки відмови в обслуговуванні.
Рекламні пакети від Fitbit Charge HR та MetaWear.
Приклад пакета CONNECT_REQ від Fitbit під час безпечного сполучення.
Читання даних мобільним додатком Jawbone UP2.
Атака через ін'єкцію коду із передачею даних сенсорів на сервер.
Журнал аудиту подій, зібраний SecuWear.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання: 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Сучасний стан безпеки мобільних пристроїв	12.2023 р. – 03.2024 р.	
2	Теоретичні аспекти оцінки безпеки мобільних пристроїв	03.2024 р. – 06.2024 р.	
3	Використання SecuWear на практиці	06.2024 р. – 11.2024 р.	

Студент _____ Миколишин М.П.
(підпис)

Керівник роботи_____ д.т.н., проф. М.М.Касянчук
(підпис)

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Програмно-апаратний засіб для оцінки та аналізу безпеки мобільних пристроїв“ на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека та захист інформації“ освітньо-професійної програми «Кібербезпека» написана обсягом 83 сторінки і містить 22 ілюстрації, 1 таблицю та 39 джерел за переліком посилань.

Метою роботи є аналіз сучасного стану безпеки мобільних пристроїв та дослідження можливостей платформи SecuWear для оцінки їхньої безпеки.

Методи дослідження. Аналіз наявних загроз та вразливостей, огляд інструментів безпеки, теоретична оцінка ефективності платформи SecuWear, моделювання практичних сценаріїв атак.

Результати дослідження. Здійснено огляд основних загроз мобільних пристроїв, сучасних методів та засобів їхнього захисту. Проаналізовано інструменти для оцінки безпеки, а також характеристики та функціональність платформи SecuWear. Виконано оцінку ефективності SecuWear, включаючи аналіз типів атак і захисту в реальних сценаріях використання. Виявлено ключові вразливості платформи та розроблено рекомендації для покращення захисту мобільних пристроїв.

Результати роботи можуть бути використані для подальшого розвитку платформ безпеки мобільних та носимих пристроїв.

КЛЮЧОВІ СЛОВА: ЗАГРОЗИ БЕЗПЕЦІ, МОБІЛЬНІ ПРИСТРОЇ, АНАЛІЗ ВРАЗЛИВОСТЕЙ, ІНСТРУМЕНТИ БЕЗПЕКИ, НОСИМІ ПРИСТРОЇ, ВЕКТОРИ АТАК, КІБЕРБЕЗПЕКА.

ABSTRACT

Master’s qualification thesis on the topic "Software and Hardware Tool for Assessing and Analyzing the Security of Mobile Devices" for obtaining the degree of "Master" in the specialty 125 "Cybersecurity and information protection" of the educational-professional program "Cybersecurity" comprises 83 pages and includes 22 illustrations, 1 table and 39 references.

The purpose of the thesis is to analyze the current state of mobile device security and explore the capabilities of the SecuWear platform for assessing their security.

Research methods. Analysis of existing threats and vulnerabilities, review of security tools, theoretical evaluation of the SecuWear platform's efficiency, and modeling of practical attack scenarios.

Research results. The thesis provides an overview of the key security threats to mobile devices, modern methods, and tools for their protection. It analyzes tools for security assessment and evaluates the characteristics and functionality of the SecuWear platform. The platform's efficiency is assessed, including an analysis of attack types and protection in real-world scenarios. Key vulnerabilities of the platform are identified, and recommendations for improving mobile device security are proposed.

The results of the thesis can be applied to further development of security platforms for mobile and wearable devices.

KEYWORDS: SECURITY THREATS, MOBILE DEVICES, VULNERABILITY ANALYSIS, SECURITY TOOLS, WEARABLE DEVICES, ATTACK VECTORS, CYBERSECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

URL	універсальний покажчик ресурсу
MITM	“Людина посередині”, атака перехоплення даних
VPN	віртуальна приватна мережа
AES-256	стандарт шифрування з ключем довжиною 256 біт
BLE	енергозберігаючий протокол Bluetooth
IoT	інтернет речей
MDM	управління мобільними пристроями
MobSF	платформа для аналізу безпеки мобільних додатків
2FE	двофакторна аутентифікація
WEP	захист дротової еквівалентності (застарілий стандарт)
CSS	міжсайтовий скриптинг, тип веб-атаки
SSP	захищене просте сполучення Bluetooth

ВСТУП

Актуальність теми кваліфікаційної роботи зумовлена зростаючою кількістю загроз безпеці мобільних пристроїв, які стали невід'ємною частиною повсякденного життя сучасної людини. З кожним роком кількість кіберзагроз, спрямованих на мобільні пристрої, зростає, що вимагає розробки нових методів та засобів для захисту інформації. Таким чином, створення ефективного програмно-апаратного засобу для оцінки та аналізу безпеки мобільних пристроїв є важливим кроком для забезпечення конфіденційності, цілісності та доступності інформації в мобільному середовищі.

Мета роботи. Метою дослідження є розробка програмно-апаратного засобу для оцінки та аналізу безпеки мобільних пристроїв, що дозволить ефективно виявляти, аналізувати та реагувати на потенційні загрози.

Для досягнення цієї мети необхідно виконати такі **завдання**:

- аналіз існуючих методів оцінки та захисту мобільних пристроїв;
- визначення вимог до програмно-апаратного засобу;
- розробка архітектури та функціональних компонентів;
- реалізація прототипу та його тестування;
- оцінка ефективності розробленого рішення та рекомендації щодо його використання.

Об'єкт дослідження. Процеси оцінки та аналізу безпеки мобільних пристроїв, які виникають у зв'язку з кіберзагрозами.

Предмет дослідження. Програмно-апаратні засоби, що використовуються для забезпечення безпеки мобільних пристроїв.

Методи дослідження. Аналіз літературних джерел та наукових статей, методи моделювання загроз, розробку прототипу та експериментальне тестування з використанням засобів статистичного аналізу для оцінки ефективності запропонованих рішень.

Наукова новизна одержаних результатів.

1. Проведено огляд сучасних загроз та вразливостей мобільних пристроїв, що дозволило визначити основні проблеми безпеки та нові виклики в цій сфері.

2. Виконано аналіз інструментів для оцінки безпеки мобільних пристроїв, зокрема, досліджено функціональність та характеристики платформи SecuWear.

3. Оцінено ефективність платформи SecuWear шляхом аналізу її захисту від різних типів атак, включаючи атаки відмови в обслуговуванні та ін’єкції коду.

4. Виявлено ключові вразливості платформи SecuWear та запропоновано рекомендації для їх усунення.

5. Узагальнено практичні аспекти використання платформи SecuWear для забезпечення безпеки носимих пристроїв, що дозволяє підвищити її ефективність у реальних сценаріях використання.

Практичне значення одержаних результатів.

Можливість використання розробленого засобу в різних сферах, таких як корпоративна безпека, захист особистих даних, моніторинг безпеки мобільних пристроїв у реальному часі.

Проблемна задача, що розглядається у даній роботі, стосується підвищення рівня захисту мобільних пристроїв від загроз кібербезпеки шляхом розробки програмно-апаратного засобу. Для вирішення цієї задачі запропоновано модульну систему, що поєднує методи виявлення та аналізу загроз із можливістю їх миттєвого реагування. Система буде реалізована на основі програмної платформи Android та апаратних компонентів для забезпечення надійності та продуктивності.

Можливі сфери застосування отриманих результатів включають розробку інструментів для мобільної безпеки, використання у підприємствах для захисту корпоративних даних, а також забезпечення безпеки приватних користувачів мобільних пристроїв.

Публікації та апробація КР.

1. Миколишин М. Застосування штучного інтелекту для забезпечення безпеки мобільних додатків. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ-2024), Тернопіль, 2024. С.150-152.

2. Миколишин М. Розвиток стандартів безпеки для мобільних пристроїв. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2024. С.76-79.

1 СУЧАСНИЙ СТАН БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

1.1 Основні загрози безпеці мобільних пристроїв

У сучасному світі мобільні пристрої, такі як смартфони та планшети, стали невід'ємною частиною повсякденного життя людей. Вони забезпечують зручність у доступі до Інтернету, обміні інформацією, зберіганні даних та виконанні робочих завдань. Однак мобільні пристрої, як і інші цифрові технології, стають мішенню для кіберзлочинців, що створює нові загрози для безпеки даних користувачів. У цьому розділі розглянемо основні загрози, з якими стикаються мобільні пристрої, та можливі шляхи їхньої нейтралізації.

Вірусне програмне забезпечення та шкідливі додатки є одними з основних загроз для мобільних пристроїв. Вони можуть проникати на пристрій через заражені додатки, небезпечні вебсайти, або в результаті неперевірених завантажень. Коли такі програми потрапляють на пристрій, вони можуть красти особисту інформацію, контролювати мобільні функції або навіть використовувати пристрій у зловмисних цілях без відома користувача.

Зокрема, шкідливе програмне забезпечення, як-от трояни, шпигунські програми та ransomware, є найбільш розповсюдженими типами загроз. Трояни зазвичай маскуються під безпечні або корисні додатки, але насправді призначені для викрадення даних або передачі їх зловмисникам. Шпигунські програми часто слідкують за діяльністю користувача, реєструючи натискання клавіш, передаючи інформацію про місцезнаходження, а також інші особисті дані. Ransomware, у свою чергу, блокує доступ до пристрою або його файлів і вимагає викуп для їх відновлення.

Згідно з дослідженням компанії Symantec, кількість шкідливих додатків для мобільних пристроїв за останній рік зросла на 54%, що свідчить про постійне збільшення загроз у цій сфері [1]. Особливо вразливими є користувачі Android, оскільки через відкритість цієї операційної системи зловмисники можуть легко створювати та поширювати шкідливі додатки через сторонні магазини додатків. Ця проблема не обмежується тільки мобільними додатками:

зловмисники також можуть використовувати вразливості в веб сайтах, які відкривають шляхи для зараження пристроїв через браузери.

Однією з основних проблем є те, що багато користувачів мобільних пристроїв ігнорують важливість оновлення програмного забезпечення та операційної системи. Це призводить до того, що шкідливе програмне забезпечення може використовувати застарілі версії додатків для експлуатації вразливостей і проникнення на пристрій. Тому важливо регулярно оновлювати всі додатки та системи, щоб запобігти зараженню.

Шкідливе програмне забезпечення також може бути використане для збору конфіденційних даних, таких як фінансова інформація, паролі, або навіть особисті фотографії. Такі додатки часто маскуються під безпечні програми для підвищення ймовірності їх завантаження користувачами. Крім того, зловмисники можуть отримати контроль над пристроєм і використовувати його для злому інших акаунтів або систем, що може призвести до великих фінансових збитків або компрометації конфіденційної інформації.

Один із важливих аспектів захисту від шкідливого програмного забезпечення полягає в тому, що користувачі повинні бути обережними при завантаженні додатків з незнайомих джерел. Сторонні магазини додатків і необачне використання інтернет-ресурсів можуть призвести до зараження пристрою. Крім того, важливо перевіряти відгуки користувачів і рейтинги додатків, а також уважно читати дозволи, які запитують додатки перед їх встановленням.

У зв'язку з постійним розвитком шкідливих програм і зростанням загроз важливо мати на мобільному пристрої антивірусне програмне забезпечення, яке може виявити та нейтралізувати такі загрози на ранніх стадіях [2]. Мобільні антивірусні програми повинні бути оновлені та налаштовані для автоматичного сканування пристрою на предмет вірусів і шкідливих додатків.

Останні дослідження також показують, що зловмисники використовують нові методи маскування своїх шкідливих додатків і намагаються обдурити антивірусні програми, що робить виявлення та блокування таких загроз ще

складнішим. Зокрема, новітні форми ransomware використовують шифрування для приховування своїх дій, що дозволяє їм залишатися непоміченими до того часу, поки не буде досягнута мета.

Таким чином, для захисту від шкідливих програм необхідно дотримуватися комплексного підходу, який включає в себе використання антивірусного програмного забезпечення, регулярні оновлення пристроїв, обережність при завантаженні додатків та дотримання рекомендацій з кібербезпеки.

Фішинг та соціальна інженерія є одними з найпоширеніших методів атак, спрямованих на викрадення особистої інформації користувачів мобільних пристроїв. Фішинг передбачає створення фальшивих повідомлень, веб сайтів або електронних листів, які виглядають як легітимні, але насправді мають на меті обманом змусити користувача ввести свої конфіденційні дані, такі як паролі, номери кредитних карток або інші особисті відомості. Приклад фішингового повідомлення зображено на рисунку 1.1. Особливістю мобільних пристроїв є те, що мобільні браузери та електронна пошта часто відображають лише частину URL-адреси, що ускладнює визначення підробки. Це робить мобільні користувачі більш вразливими до фішингу, адже вони можуть не помітити несанкціоновані зміни в адресі веб сайту або підроблені повідомлення. Дослідження компанії Verizon показують, що мобільні пристрої є основною ціллю для фішингових атак, через те, що користувачі часто не звертають увагу на повну URL-адресу в браузерах мобільних пристроїв [3]. Більше того, зловмисники постійно вдосконалюють свої методи, роблячи фальшиві сайти майже ідентичними до справжніх, що значно ускладнює їх ідентифікацію навіть досвідченим користувачам.

Соціальна інженерія, у свою чергу, є інструментом, який використовують зловмисники для психологічного тиску на користувачів, щоб отримати доступ до їхніх конфіденційних даних. Зловмисники можуть видавати себе за офіційних представників компаній, державних установ або знайомих осіб і

таким чином змусити користувачів надати свою особисту інформацію або навіть дозволити доступ до мобільного пристрою.

Часто в таких атаках використовують емоційні маніпуляції, такі як створення паніки, погрози або пропозиції вигідних умов, що підвищує ймовірність того, що користувач надасть необхідні дані. Для прикладу, зловмисник може зателефонувати або надіслати повідомлення, в якому буде стверджувати, що є працівником банку, і попросить підтвердити особисті дані під приводом проведення перевірки безпеки. За статистикою Proofpoint, майже 88% організацій зазнають соціально-інженерних атак щонайменше один раз на рік, а мобільні пристрої є найбільш вразливою ланкою в цьому контексті [4].

Для захисту від фішингу та соціальної інженерії користувачі повинні навчитися розпізнавати підроблені повідомлення та сайти, уникати введення конфіденційних даних на сумнівних платформах і використовувати додаткові методи автентифікації, такі як двофакторна авторизація.

Рисунок 1.1 - Спам-повідомлення, надіслане у Facebook [5]

Дослідження показують, що кількість фішингових атак, спрямованих на мобільні пристрої, зростає. За даними компанії Symantec, кількість фішингових атак, що націлюються на мобільних користувачів, збільшилася на 50%

протягом останнього року, і цей тренд продовжує зростати [6]. У свою чергу, зростання кількості атак через соціальну інженерію також є свідченням того, що цей метод використовується все частіше, адже його важче виявити за допомогою стандартних заходів безпеки.

Щоб знизити ризики від таких атак, важливо регулярно оновлювати операційну систему мобільного пристрою, встановлювати антивірусні програми і бути особливо уважними до повідомлень, які надходять на пристрій. Крім того, використання двофакторної аутентифікації значно знижує ймовірність успішних атак, оскільки навіть якщо зловмисник отримає доступ до пароля, додаткове підтвердження за допомогою іншого каналу зв’язку все одно забезпечить захист [7].

Операційні системи (ОС) мобільних пристроїв, такі як Android та iOS, часто стають мішенню кіберзлочинців через вразливості у програмному забезпеченні. Одна з найсерйозніших загроз – це атаки типу "нульовий день" (zero-day attacks), які використовують невідомі розробникам вразливості. Уразливості можуть бути знайдені не лише у самій ОС, але й у додатках або бібліотеках, які використовуються операційною системою. Це надає зловмисникам можливість отримати доступ до конфіденційних даних користувачів або навіть взяти контроль над пристроєм без відома власника. Згідно з даними Symantec, атаки на основі "нульового дня" стають дедалі поширенішими через те, що зловмисники шукають нові шляхи обходу захисту систем [8].

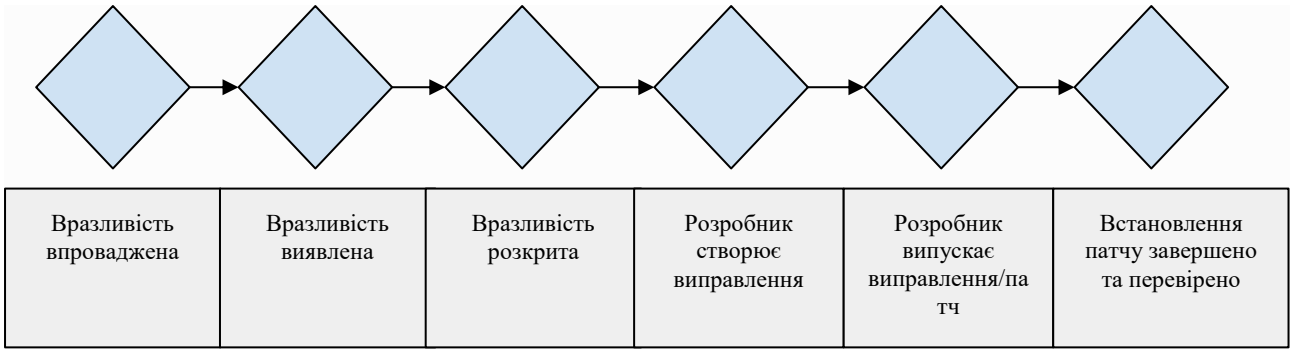

Рисунок 1.2 - Етапи життєвого циклу вразливості нульового дня

Дослідники з McAfee наголошують, що вразливості в ОС можуть бути використані не тільки для особистих атак, але й для масових кіберкомпаній проти компаній [9]. Особливо це стосується підприємств, які використовують мобільні пристрої для роботи з корпоративними даними. Наприклад, пристрої з застарілими версіями операційних систем часто не отримують важливі оновлення безпеки, що робить їх особливо вразливими до атак. Невчасне встановлення оновлень призводить до того, що навіть загальні уразливості залишаються відкритими для експлуатації.

На додачу, Zimperium вказує, що підвищення рівня складності шкідливого програмного забезпечення сприяє збільшенню кількості атак на ОС мобільних пристроїв [10]. Розробники ОС постійно працюють над виправленням цих вразливостей, але користувачі також повинні відповідально підходити до оновлення своїх пристроїв.

Варто зазначити, що компанія Google, розробник Android, активно працює над покращенням систем безпеки через регулярні патчі. Однак, як зазначає Verizon, значна частина користувачів Android не встановлює оновлення вчасно, що робить їх пристрої вразливими до нових типів атак. Тому важливо, щоб користувачі мобільних пристроїв уважно ставилися до оновлень ОС і завжди встановлювали останні версії програмного забезпечення [11].

Безпека мобільних пристроїв часто піддається загрозам через вразливості у бездротових мережах, особливо коли користувачі підключаються до незахищених публічних Wi-Fi мереж. Атаки типу "людина посередині" (MITM) є однією з найпоширеніших загроз, коли зловмисник може перехоплювати дані між мобільним пристроєм і сервером, через що стає можливим доступ до конфіденційної інформації, такої як паролі, фінансові дані або навіть дані для входу до банківських акаунтів.

Користувачі, що часто використовують відкриті мережі, наприклад, у кафе або на вокзалах, можуть наражати свої пристрої на ризик атак MITM, адже такі мережі зазвичай не використовують надійних засобів шифрування даних

[12]. Використання старих протоколів захисту, таких як WEP, суттєво підвищує ймовірність успішного перехоплення даних зловмисниками [13].

Одним з ефективних методів захисту є використання віртуальних приватних мереж (VPN). VPN створює зашифрований канал між пристроєм користувача та віддаленим сервером, роблячи перехоплення даних значно складнішим для зловмисників (див. рисунок 1.3). McAfee рекомендує користувачам активувати VPN, особливо під час підключення до публічних Wi-Fi, оскільки це знижує ймовірність несанкціонованого доступу до даних [12]. Додатково, багато сучасних операційних систем, таких як Android та iOS, мають вбудовані інструменти для відстеження безпеки з'єднань, попереджаючи користувачів про небезпечні або підозрілі мережі.

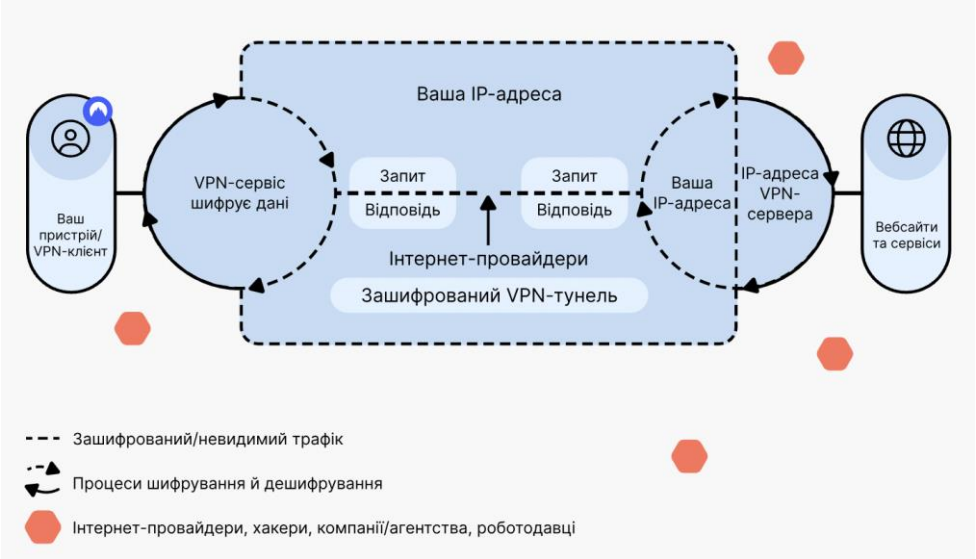

Рисунок 1.3 - Принцип роботи VPN [14]

Захист мобільних пристроїв також може включати в себе додаткові заходи, такі як використання двофакторної автентифікації та регулярні оновлення програмного забезпечення. Це дозволяє користувачам захистити не тільки сам пристрій, але й дані, що передаються через нього. Згідно з даними F-Secure, уразливості в бездротових мережах є одними з найчастіше використовуваних кіберзлочинцями через доступність публічних точок доступу та брак обізнаності серед користувачів щодо ризиків.

Однією з основних загроз для безпеки мобільних пристроїв є недостатнє шифрування даних. Шифрування є важливою частиною кібербезпеки, яка гарантує, що дані залишаться недоступними для сторонніх осіб навіть у випадку втрати чи крадіжки пристрою. Однак, згідно з дослідженням компанії Zimperium, близько 25% додатків на Android взагалі не використовують шифрування для захисту даних своїх користувачів, що створює значний ризик [15]. У той час, коли шифрування є стандартною практикою для багатьох додатків, ця статистика демонструє, що велика частина програм все ще не забезпечує належного захисту.

Недостатнє шифрування ставить під загрозу особисті та конфіденційні дані користувачів. Якщо зловмисник отримує доступ до незашифрованих даних, він може використовувати їх для викрадення ідентифікаційних даних, що призводить до фінансових втрат або інших негативних наслідків, таких як доступ до приватної інформації користувача. Symantec також підкреслює, що відсутність або неналежне використання шифрування може зробити користувачів вразливими до атак на мобільні пристрої, особливо під час використання публічних мереж Wi-Fi [16].

Шифрування не лише захищає локальні дані, збережені на пристрої, але й інформацію, що передається між додатками та серверами. Наприклад, Apple використовує наскрізне шифрування для даних, що передаються через iMessage або FaceTime, щоб запобігти доступу до них навіть на рівні серверів компанії. Водночас, застарілі додатки або системи, які не забезпечують сучасного рівня шифрування, можуть становити серйозну загрозу безпеці.

Ще один приклад потенційних ризиків стосується неправильно налаштованих програм. F-Secure відзначає, що навіть за наявності шифрування, неправильне налаштування або використання застарілих протоколів може зробити шифрування неефективним, відкриваючи дані для атак. Це демонструє, наскільки важливим є постійне оновлення та підтримка додатків з використанням сучасних алгоритмів шифрування, таких як AES-256, для захисту інформації.

Отже, відсутність шифрування даних або його неналежне використання залишається однією з основних вразливостей для мобільних пристроїв. Використання шифрування є критичним для захисту як локальних даних, так і інформації, що передається через мережі, що робить його важливим елементом у забезпеченні безпеки користувачів мобільних пристроїв.

Фізична крадіжка мобільного пристрою залишається однією з найбільших загроз для безпеки. Якщо пристрій не захищений паролем або іншими засобами автентифікації (наприклад, відбитками пальців або розпізнаванням обличчя), зловмисники можуть отримати доступ до всіх даних на пристрої. За даними дослідження, кожен п'ятий власник смартфона втрачає або стає жертвою крадіжки пристрою принаймні раз у житті.

Щоб запобігти несанкціонованому доступу в разі крадіжки, користувачам рекомендується використовувати багатофакторну автентифікацію, а також функції дистанційного блокування або видалення даних, такі як Find My iPhone або Android Device Manager.

1.2 Методи та засоби захисту мобільних пристроїв

Захист мобільних пристроїв від кіберзагроз є важливим елементом сучасної інформаційної безпеки, оскільки мобільні телефони та планшети все частіше використовуються для доступу до чутливої інформації, фінансових операцій і корпоративних даних. Вони є частинами глобальної інфраструктури і в той же час вразливими до атак з різних джерел. Через постійне вдосконалення кіберзлочинців, важливо розуміти основні методи та засоби захисту мобільних пристроїв, щоб мінімізувати можливі загрози.

Один із ключових способів захисту інформації на мобільних пристроях — це використання шифрування даних. Більшість сучасних смартфонів, як iOS, так і Android, мають вбудовані інструменти для повного шифрування даних, що забезпечує їхню недоступність без введення пароля або використання біометричних даних. Наприклад, використовуються відбитки пальців або

розпізнавання обличчя для доступу до зашифрованих даних на мобільному пристрої, що зображено на рисунку 1.4. Це особливо важливо в разі втрати чи крадіжки пристрою, оскільки шифрування допомагає зберегти конфіденційну інформацію захищеною від стороннього доступу [17].

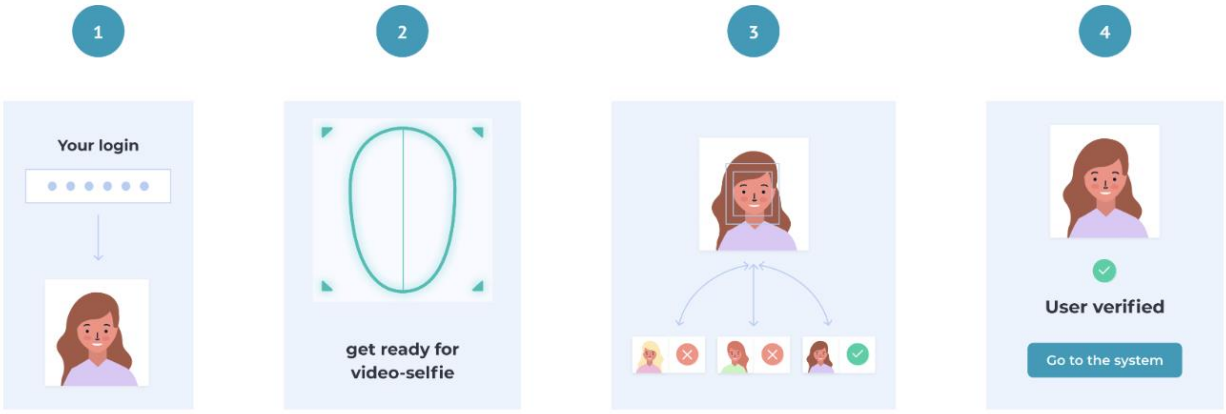

Рисунок 1.4 - Ідентифікація за обличчям для захисту доступу до даних [18]

Правильне використання шифрування є найкращим методом забезпечення захисту як збережених даних, так і комунікацій. Шифрування працює шляхом застосування математичних алгоритмів, які перетворюють дані у форму, що її можна розшифрувати лише за допомогою спеціального ключа. Це дозволяє користувачам захистити конфіденційну інформацію навіть під час передавання її через відкриті мережі [19].

Важливо також звертати увагу на те, які програми або сервіси використовуються для обміну зашифрованими повідомленнями, оскільки деякі компанії можуть розшифровувати інформацію на своїх серверах, що становить ризик доступу до цієї інформації з боку третіх осіб. До популярних програм, що підтримують наскрізне шифрування, належать Signal, WhatsApp, та Wire.

Крім того, варто бути уважними до законодавства щодо використання шифрування в різних країнах, оскільки деякі уряди обмежують або навіть забороняють його використання. Перед роботою в іншій країні або перетином кордонів варто ретельно оцінити ризики та провести необхідні дослідження.

Технології шифрування, такі як BitLocker для Windows і FileVault для Mac, також можуть використовуватися для захисту даних на комп'ютерах і зовнішніх носіях, таких як USB-накопичувачі. Це гарантує, що інформація залишається захищеною незалежно від того, де і як вона зберігається.

Важливим додатковим засобом для підвищення рівня безпеки є використання віртуальних приватних мереж (VPN). VPN забезпечують створення зашифрованого з'єднання між мобільним пристроєм та віддаленим сервером, що дозволяє користувачу уникнути спостереження за його інтернет-трафіком. Це особливо актуально під час використання незахищених Wi-Fi мереж у громадських місцях, таких як кафе, аеропорти чи торгові центри, де зловмисники можуть спробувати перехопити дані.

Завдяки VPN трафік між мобільним пристроєм і сервером проходить через захищений тунель, який запобігає його перехопленню, модифікації або відстеженню. Це дозволяє не лише захистити особисту інформацію користувача від хакерів, а й уникнути підслуховування чи зміни даних під час передачі через мережу. Крім цього, VPN маскує IP-адресу, яка може використовуватись для відстеження місця знаходження або онлайн-активності користувача. Завдяки приховуванню IP-адреси зменшуються ризики пов’язані з відстеженням дій з боку інтернет-провайдерів, урядових структур чи власників веб-сайтів, що дозволяє зберегти приватність користувача [20].

Додатково, використання VPN надає можливість обійти геообмеження і доступ до контенту, який може бути заблокований у певних країнах або регіонах. Це відкриває доступ до заблокованих ресурсів, таких як стримінгові сервіси, соціальні мережі або новинні сайти, що важливо для користувачів, які подорожують або працюють у країнах з обмеженим доступом до Інтернету.

Правильний вибір VPN також є важливим аспектом для забезпечення безпеки. Варто звертати увагу на рівень шифрування, адже VPN повинен використовувати сучасні протоколи, такі як AES-256, щоб гарантувати високий рівень захисту. Важливо також обирати провайдера VPN, який дотримується політики відсутності логів, щоб уникнути зберігання інформації про активність

користувача. Додатковими параметрами, які слід враховувати при виборі, є швидкість з’єднання, сумісність із мобільними операційними системами, наявність зрозумілого інтерфейсу та функція автоматичного роз'єднання у разі втрати VPN-з’єднання.

Таким чином, використання VPN як частини стратегії захисту мобільних пристроїв суттєво знижує ризики, пов’язані з кіберзагрозами, забезпечуючи користувачам не лише захист даних, а й приватність та свободу доступу до інформації в умовах сучасних викликів.

Ще одним важливим засобом забезпечення безпеки мобільних пристроїв є система двофакторної автентифікації (2FA). Вона додає додатковий рівень захисту, вимагаючи від користувача підтвердження його особи через другий канал, наприклад, за допомогою смс або спеціального додатку для генерації кодів. Це значно ускладнює несанкціонований доступ до облікових записів, навіть у разі, якщо пароль був скомпрометований. Оскільки кількість атак на акаунти через крадіжку паролів постійно зростає, використання 2FA стає надзвичайно важливим, особливо у корпоративному середовищі, де обсяги чутливої інформації значні.

Багато постачальників онлайн-сервісів наразі пропонують методи входу, які вимагають від користувача ідентифікації за допомогою другого фактора. Ці методи можуть бути представлені в різних формах: деякі додають другий фактор після введення пароля, інші ж поєднують два фактори для входу без використання пароля. Найбільш безпечними є апаратні методи, які використовуються як доповнення до (або замість) сильного пароля.

Зазвичай процес багатофакторної автентифікації починається з введення правильного пароля, після чого система перевіряє його правильність. Однак, на відміну від стандартних систем, користувач не переходить одразу до контенту, а потрапляє до другого бар'єру — додаткової перевірки. Це запобігає несанкціонованому доступу третіх осіб, навіть якщо пароль був вкрадений.

Після введення пароля багато систем 2FA звертаються до зовнішніх ресурсів для перевірки користувача. Це може бути, наприклад, код, який

надсилається на інший пристрій користувача, наприклад, смартфон. Іншим варіантом є використання біометрії, наприклад, відбитку пальця, або ж застосування USB-токена чи чип-картки. Лише в тому випадку, коли у користувача є цей додатковий засіб підтвердження особи, він зможе отримати доступ до запитуваного контенту.

Рисунок 1.5 - Приклад двофакторної автентифікації [21]

Також важливо, щоб фактори автентифікації належали до різних категорій, таких як знання (пароль, ПІН), володіння (чип-картка, генератор кодів) або біометрія (відбиток пальця). Окрім того, деякі методи комбінують кілька факторів безпосередньо, що підвищує рівень безпеки. Наприклад, при використанні німецької ID-картки функція eID (електронної ідентифікації) може працювати тільки в поєднанні з ПІН-кодом. У цьому випадку система аутентифікує користувача лише за наявності обох факторів одночасно, що є ще більш безпечним варіантом, ніж послідовне використання пароля та другого фактора [22].

Завдяки двофакторній автентифікації, навіть у разі компрометації пароля, ризик несанкціонованого доступу значно знижується, що робить її важливим елементом сучасних систем безпеки.

Регулярне оновлення програмного забезпечення є одним із найважливіших методів захисту мобільних пристроїв від кіберзагроз.

Оновлення, що регулярно випускаються для операційних систем і додатків, містять виправлення для вразливостей, які зловмисники можуть використати для несанкціонованого доступу. Виправлення безпеки допомагають значно знизити ризики компрометації пристроїв, адже вони усувають відомі вразливості, що можуть бути експлуатовані для атак.

Мобільні операційні системи, такі як Android і iOS, активно підтримують цей процес, адже оновлення є необхідними для забезпечення безпеки користувачів. Без своєчасного оновлення програмного забезпечення пристрій може бути вразливим до атак, що значно підвищує ризики зловживання особистою інформацією, фінансовими даними або навіть віддаленим контролем над пристроєм.

Без регулярних оновлень, програмне забезпечення може містити незахищені ділянки, які зловмисники використовують для проникнення в систему. Оновлення не тільки усувають ці вразливості, але й покращують загальну продуктивність пристроїв, роблячи їх більш ефективними та стабільними. Тому оновлення програмного забезпечення є важливою частиною стратегії кібербезпеки, яка допомагає зберігати захищеність особистих даних і запобігати кіберзлочинам.

Важливо також зазначити, що використання апаратних методів для оновлення, таких як вбудовані механізми безпеки в процесі оновлення програм, надає додатковий рівень захисту від можливих загроз. Ці методи включають в себе використання шифрування, цифрового підпису та інших технологій, які гарантують, що оновлення дійсно надходять від авторитетного постачальника і не були змінені чи скомпрометовані під час передачі.

Компанії, які працюють з мобільними пристроями, часто впроваджують рішення для управління мобільними пристроями (MDM), що дозволяє централізовано керувати та забезпечувати безпеку цих пристроїв у корпоративному середовищі. Це рішення охоплює такі функції, як блокування пристроїв, видалення даних і відстеження місцезнаходження у випадку втрати або крадіжки. MDM є критично важливими для великих організацій, які

працюють з великими обсягами чутливої інформації, адже вони допомагають зменшити ризики витоку даних і забезпечити контроль над доступом.

MDM являє собою спеціалізоване програмне забезпечення для захисту, моніторингу, управління та виконання політик безпеки на мобільних пристроях співробітників. Це рішення працює через дві основні компоненти: сервер управління MDM, який зберігається в центрі даних компанії, і агент MDM, що отримує та реалізує політики на пристроях користувачів. Спеціально налаштовані політики, що визначаються IT-адміністраторами через консоль управління сервером, передаються агенту і застосовуються на мобільних пристроях. Цей процес дозволяє організаціям забезпечувати ефективний контроль над всіма мобільними пристроями, що підключаються до корпоративної мережі, і виконувати команди, спрямовані на підтримку безпеки [23].

Сучасні рішення MDM можуть автоматично визначати нові пристрої, які підключаються до мережі, і застосовувати політики або команди для забезпечення їхньої безпеки. Окрім управління інвентаризацією пристроїв, MDM також захищає додатки, дані і контент на пристроях, що використовуються в організаціях. Ці системи можуть включати різноманітні функції для забезпечення безпеки, такі як використання VPN, контролю доступу на основі ролей, а також відстеження GPS. Системи MDM також дозволяють компаніям моніторити поведінку та важливі дані на пристроях і захищати їх від шкідливого програмного забезпечення та інших кіберзагроз.

Таким чином, рішення MDM є важливим елементом для підтримки безпеки мобільних пристроїв в організаціях, оскільки вони забезпечують захист корпоративної інформації, контролюють доступ і оптимізують використання пристроїв.

Не менш важливою є роль антивірусного програмного забезпечення для мобільних пристроїв. Хоча мобільні операційні системи мають вбудовані механізми безпеки, такі як перевірка додатків перед їх встановленням, антивірусні програми здатні виявляти та блокувати шкідливе програмне

забезпечення, яке може проникнути через сторонні додатки або під час використання небезпечних мереж. Сучасні антивірусні рішення для мобільних пристроїв також можуть виявляти підозрілі програми, захищати від фішингових атак і допомагати у запобіганні несанкціонованого доступу.

Мобільний антивірус є програмним забезпеченням, яке призначене для захисту мобільних пристроїв, таких як смартфони, планшети чи ноутбуки, від шкідливих програм, таких як віруси, трояни, фішингові атаки, програми-вимагачі та інші форми зловмисного ПЗ. Враховуючи, що ми активно використовуємо смартфони та цифрові інструменти, мобільні антивіруси є важливою складовою кібербезпеки і виступають як цифрові охоронці ваших чутливих даних та операційної системи пристрою.

Мобільні антивіруси працюють аналогічно до традиційного антивірусного ПЗ для комп’ютерів. Вони постійно моніторять пристрій, скануючи нові та існуючі файли на предмет потенційних загроз і блокуючи їх згідно з заздалегідь налаштованими перевагами. Крім цього, вони також захищають від онлайн-шахрайства та крадіжки особистих даних, пропонуючи функції захисту від фішингу, захисту веб-ресурсів і електронної пошти, а також забезпечують безпечне серфінгування.

Сучасні мобільні антивіруси працюють в реальному часі, постійно моніторячи пристрій на наявність шкідливих програм або несанкціонованої активності, скануючи додатки на предмет інфекційного ПЗ. Вони здатні виявляти так звані "zero-day" уразливості, коли хакери використовують невідомі постачальникам вразливості системи для атак. Це підкреслює важливість мобільних антивірусів як критичної захисної лінії в умовах постійно змінюваного кіберпростору [24].

Мобільний антивірус також може виконувати додаткові функції, такі як віддалене блокування загублених пристроїв, автоматичне резервне копіювання, попередження користувача про небезпечні веб сайти та посилання, перевірка наявності витоків інформації, а також використання складних алгоритмів для боротьби з новими загрозами.

Хоча є певний скепсис щодо ефективності мобільних антивірусів, особливо для таких систем, як iOS, сучасні антивіруси мають можливість адаптуватися до швидко змінюваних умов кіберзагроз. Вони забезпечують додатковий рівень захисту і допомагають уникнути крадіжки особистих даних, паролів, кредитних карток і конфіденційної інформації.

Антивірусне ПЗ для мобільних пристроїв слід розглядати як невід'ємну частину кібер гігієни. Це не є розкішшю, а практичною інвестицією для тих, хто хоче захистити свої цифрові кордони і забезпечити свою безпеку в онлайн-середовищі.

Зважаючи на зростання загроз, важливо також звертати увагу на безпечне використання мобільних додатків. Зловмисники часто використовують фальшиві або неправильно налаштовані додатки для збору чутливої інформації або її продажу. Користувачі повинні завжди завантажувати додатки лише з офіційних магазинів, таких як Google Play або App Store, і стежити за правами доступу, які надаються додатку під час його установки. У багатьох випадках, для зменшення ризиків, рекомендується обмежувати доступ додатків до чутливих даних, таких як камера або місцезнаходження.

Загалом, захист мобільних пристроїв вимагає комплексного підходу, що включає не лише використання технічних засобів, але і підвищення обізнаності користувачів про можливі загрози. Лише за допомогою об'єднання технічних рішень та належної політики безпеки можна забезпечити високий рівень захисту мобільних пристроїв від сучасних кіберзагроз.

1.3 Проблеми безпеки та нові виклики

У сучасному світі мобільні пристрої, такі як смартфони, планшети та носимі гаджети, стали невід'ємною частиною нашого життя. Разом із цим їхнє використання супроводжується новими викликами та загрозами для безпеки і конфіденційності даних.

Проблеми конфіденційності даних є ще однією серйозною загрозою. Багато мобільних застосунків мають неналежно налаштовані політики безпеки, що дозволяє несанкціонованим програмам або користувачам отримувати доступ до чутливої інформації. Наприклад, дані користувачів можуть бути відкритими під час сполучення, що створює ризик їхнього викрадення. Згідно зі звітом MIT, безпека популярного носимого пристрою Fitbit викликала занепокоєння, оскільки хоча він використовує власний шифрувальний процес, його дані можуть бути доступними під час сполучення. Це підкреслює важливість забезпечення конфіденційності особистих даних для запобігання несанкціонованому доступу.

Дослідження, проведене Університетом Кембриджа, виявило, що численні популярні додатки без дозволу відстежують активність користувачів і передають зібрані дані. Це створює загрозу для особистої інформації, оскільки користувачі не завжди знають, які дані збираються та обробляються. У звіті Appthority зазначається, що близько 80% популярних мобільних застосунків мають вразливості, які можуть бути використані для збору особистих даних, таких як геолокація, контакти та інші чутливі дані [25].

Для забезпечення конфіденційності особистих даних важливо, щоб користувачі та розробники вживали активні заходи захисту. Це включає регулярні оновлення програмного забезпечення, впровадження політик шифрування та контроль за доступом, який надається мобільним застосункам. Користувачам слід уважно ставитися до наданого доступу, а також до даних, які вони дозволяють збирати, щоб уникнути несанкціонованого доступу та захистити свою приватність.

Атаки на Bluetooth Low Energy (BLE) можуть проявлятися у різних формах, включаючи прослуховування (eavesdropping), атаки на відмову в обслуговуванні (Denial of Service) та маніпуляції з даними. Однією з основних загроз є можливість прослуховування зв'язку між пристроями. Дослідження свідчать, що зловмисники можуть використовувати спеціалізовані пристрої, такі як Ubertooth One, для прослуховування BLE-з'єднань, що призводить до

серйозних зловживань, таких як викрадення особистих даних та шахрайство. Наприклад, дослідження, проведене експертами з безпеки, показало, що завдяки слабкому шифруванню і вразливостям у протоколах аутентифікації зловмисники можуть легко перехоплювати передачі даних між пристроями, отримуючи доступ до конфіденційної інформації користувачів [26].

Атаки на відмову в обслуговуванні можуть призвести до недоступності пристроїв або сервісів, що суттєво порушує роботу користувачів. Зловмисники можуть надсилати величезну кількість запитів до цільового пристрою, перевантажуючи його ресурси і роблячи його недоступним для легітимних користувачів. Такі атаки не лише призводять до втрат у користуванні пристроями, але й можуть мати серйозні економічні наслідки для компаній, які покладаються на безперервність роботи своїх сервісів .

Варто також зазначити, що зловмисники можуть використовувати BLE для атак на інші пристрої, взаємодіючи з ними в межах однієї мережі. Це може включати спроби отримати контроль над бездротовими гаджетами, такими як розумні годинники чи фітнес-трекери, що створює додаткові ризики для конфіденційності та безпеки даних користувачів.

Сучасні технології постійно еволюціонують, вносячи нові виклики у сферу безпеки мобільних пристроїв. Одним із значних факторів є зростаюча популярність Інтернету речей (IoT), що веде до збільшення кількості пристроїв, підключених до мережі та взаємодіючих між собою. Це створює нові вектори атак, оскільки зловмисники можуть використовувати вразливості не лише окремих пристроїв, а й усієї екосистеми IoT. Наприклад, атаки на смарт-годинники, термостати та інші побутові пристрої можуть відкривати доступ до домашніх мереж і викрадати конфіденційну інформацію [27].

Крім того, нові технології, такі як 5G, значно змінюють безпековий ландшафт. Хоча 5G пропонує вищу швидкість передачі даних і більшу ємність, це також створює нові можливості для зловмисників. За даними аналітиків, мережі 5G можуть бути вразливими до атак, які намагаються перезавантажити систему або отримати контроль над пристроями через недостатню безпеку в

нових протоколах. Дослідження показали, що у разі неналежного налаштування безпеки, злочинці можуть легко зламати пристрої, що використовують 5G, ставлячи під загрозу дані та конфіденційність користувачів.

Важливо також враховувати нові моделі атак, такі як зловживання штучним інтелектом (AI) та машинним навчанням. Зловмисники можуть використовувати AI для автоматизації атак, що робить їх більш ефективними і менш помітними. Наприклад, алгоритми можуть бути використані для виявлення вразливостей у системах безпеки, оптимізації методів зламування, а також для проведення фішингових атак, які стають все більш переконливими.

Підсумовуючи виклики та загрози безпеці мобільних пристроїв, стає очевидним, що постійне зростання складності систем, поява нових технологій, таких як 5G та IoT, а також все більше поширення атак на BLE і конфіденційність даних значно ускладнюють захист інформації. Зловмисники використовують все більш витончені методи атак, що вимагає постійного моніторингу та адаптації безпеки мобільних пристроїв до нових ризиків.

Це підкреслює важливість впровадження ефективних інструментів для тестування безпеки мобільних пристроїв. Такі інструменти допомагають виявляти вразливості та слабкі місця в системах ще до того, як ними скористаються зловмисники. Використання цих інструментів не лише аналізує безпеку на рівні програмного забезпечення, а й перевіряє надійність шифрування, стійкість до атак типу "людина посередині" та захист даних під час з'єднання.

Мета таких інструментів полягає в ідентифікації вразливостей, щоб запобігти повторенню помилок у майбутніх розробках і модифікувати існуючі носимі застосунки за допомогою ефективних патчів програмного забезпечення чи прошивки. Це дозволить не тільки поліпшити безпеку вже існуючих продуктів, але й забезпечити кращу основу для нових технологій, які з’являються на ринку.

2 ТЕОРЕТИЧНІ АСПЕКТИ ОЦІНКИ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

2.1 Інструменти для аналізу безпеки мобільних пристроїв

Постійний розвиток програмного забезпечення, нових функцій та підключень, таких як Bluetooth і Інтернет речей (IoT), створює нові виклики у забезпеченні безпеки. Для виявлення вразливостей і підвищення захисту даних використовуються різноманітні інструменти для аналізу безпеки мобільних пристроїв. У цьому підрозділі ми розглянемо кілька важливих інструментів, які допомагають в оцінці безпеки мобільних і носимих пристроїв, таких як MobSF, OWASP ZAP, Frida та SecuWear.

MobSF, або Mobile Security Framework, є одним із найпопулярніших інструментів для аналізу безпеки мобільних додатків, відомий своєю універсальністю та потужними можливостями. Цей фреймворк підтримує як статичний, так і динамічний аналіз для платформ Android та iOS, що робить його важливим інструментом для фахівців з безпеки.

Однією з ключових особливостей MobSF є його здатність виконувати статичний аналіз. Цей метод дозволяє оцінювати безпеку додатку, не запускаючи його. Статичний аналіз виявляє вразливості в коді та конфігураціях додатка, включаючи ненадійні API, використання застарілих бібліотек та неправильні налаштування конфігурацій. Такі дані надають розробникам можливість виявляти та усувати проблеми на ранніх етапах, зменшуючи ризик експлуатації вразливостей у фінальному продукті.

Динамічний аналіз, що підтримується MobSF, є ще одним важливим аспектом цього фреймворку. Він полягає у запуску додатку в контрольованому середовищі, що дозволяє спостерігати за його поведінкою в реальному часі. Це особливо корисно для виявлення проблем, пов'язаних із обробкою конфіденційних даних, інтеграцією з API, а також недоліками у зберіганні даних. Таким чином, динамічний аналіз забезпечує глибше розуміння безпеки програми, виявляючи проблеми, які можуть бути пропущені статичним аналізом.

MobSF також генерує детальні звіти про виявлені вразливості, включаючи конкретні рекомендації щодо їх усунення. Ці звіти є надзвичайно корисними для розробників, оскільки вони допомагають зрозуміти специфіку вразливостей і шляхи їх виправлення. Така документованість підвищує шанси на безпечний випуск програмного забезпечення.

Переваги MobSF:

1) універсальність: підтримка як Android, так і iOS платформ;

2) детальний аналіз: можливість статичного та динамічного аналізу, що забезпечує всебічний огляд безпеки;

3) автоматизовані звіти: генерація зрозумілих звітів з рекомендаціями щодо усунення вразливостей;

4) відкритий код: Як інструмент з відкритим вихідним кодом, MobSF дозволяє спільноті активно брати участь у його розвитку та удосконаленні;

5) інтеграція з CI/CD: Легкість в інтеграції у процеси безперервної інтеграції та доставки, що підвищує ефективність тестування на етапі розробки.

Недоліки MobSF:

1) ресурсоємність: динамічний аналіз може бути вимогливим до системних ресурсів, що ускладнює використання на старих або малопотужних пристроях;

2) складність налаштування: налаштування та використання MobSF може бути складним для новачків, що вимагає певного часу на навчання;

3) обмеження у динамічному аналізі: деякі вразливості можуть бути не виявлені в ході динамічного аналізу через обмеження середовища тестування;

4) необхідність оновлень: як і будь-який інший інструмент, MobSF потребує регулярних оновлень для підтримки актуальності та ефективності [28].

Важливо також враховувати, що MobSF активно розвивається, що відкриває нові можливості для покращення аналізу безпеки мобільних додатків. Користувачі можуть інтегрувати MobSF у свої CI/CD процеси, автоматизуючи

тести на безпеку, що значно підвищує ефективність тестування. Таке автоматичне тестування дозволяє швидко виявляти вразливості та надавати рекомендації, що допомагає розробникам оперативно реагувати на потенційні загрози.

OWASP ZAP, або Zed Attack Proxy, є безкоштовним інструментом з відкритим кодом, який був створений для тестування безпеки веб-додатків, але його функціонал також може бути застосовано до мобільних платформ. Інструмент пропонує багатий набір можливостей, які дозволяють фахівцям з безпеки проводити комплексні тести, виявляючи вразливості в додатках, зокрема ті, що пов'язані з конфіденційністю та безпекою даних.

Однією з основних функцій OWASP ZAP є інтерактивний тестувальник, який дозволяє користувачам у зручному режимі виконувати тестування безпеки. Цей інструмент підходить як для новачків, так і для досвідчених спеціалістів. З його допомогою користувачі можуть аналізувати запити та відповіді між клієнтом і сервером, що надає змогу виявляти вразливості, такі як SQL-ін'єкції або XSS-атаки.

Окрім інтерактивного тестувальника, OWASP ZAP також пропонує можливості автоматизації тестування. Користувачі можуть налаштувати сканування для регулярної перевірки безпеки, що є особливо корисним для проектів, що активно розвиваються. Плагіни, доступні для ZAP, дозволяють розширити його функціонал, додаючи нові можливості, такі як підтримка специфічних технологій або методів атаки.

ZAP активно підтримується спільнотою, що дозволяє постійно вдосконалювати інструмент відповідно до нових загроз і вразливостей. Відкритий характер ZAP означає, що кожен може внести свій внесок у його розвиток, що сприяє швидкій адаптації до нових викликів безпеки.

Проте, незважаючи на свої численні переваги, OWASP ZAP має й деякі недоліки. Одним з них є складність початкового налаштування, яка може бути викликом для новачків. Зокрема, зрозуміти, як правильно налаштувати проксі та інтегрувати ZAP у свій робочий процес може вимагати певного часу та

зусиль. Також, через широкий спектр функцій, деякі користувачі можуть відчувати, що інтерфейс інструменту є перевантаженим і не таким інтуїтивно зрозумілим, як хотілося б.

Переваги OWASP ZAP:

1) безкоштовність і відкритість: ZAP є безкоштовним інструментом з відкритим кодом, що робить його доступним для всіх;

2) широкий набір функцій: інтеграція різних функцій для тестування безпеки, включаючи автоматизацію та плагіни, надає користувачам гнучкість у використанні;

3) активна підтримка спільноти: постійне оновлення та вдосконалення завдяки внескам з боку спільноти;

4) підтримка навчання: OWASP ZAP є чудовим інструментом для навчання нових спеціалістів у сфері безпеки.

Недоліки OWASP ZAP:

1) складність налаштування: початкове налаштування та інтеграція можуть бути складними для новачків;

2) перевантажений інтерфейс: широкий набір функцій може призвести до відчуття перевантаження інформацією для деяких користувачів;

3) обмеження в мобільному тестуванні: хоча ZAP може бути використаний для мобільних платформ, його основна функціональність зосереджена на веб-додатках, що може обмежувати можливості тестування специфічних мобільних вразливостей [29].

Frida - це потужний інструмент для динамічного інструментування, який дозволяє дослідникам безпеки взаємодіяти з програмами під час їх виконання. Завдяки своїй гнучкості та підтримці різних платформ, включаючи Android, iOS, Windows та macOS, Frida став популярним вибором серед фахівців з безпеки для тестування мобільних додатків і проведення реверс-інжинірингу.

Однією з основних переваг Frida є його здатність виконувати скрипти на JavaScript для динамічного інструментування додатків. Це дозволяє користувачам змінювати поведінку програм, а також виводити важливу

інформацію про їх внутрішню структуру. Дослідники можуть використовувати Frida для модифікації запитів до серверів, зміни значень у пам'яті, або виявлення вразливостей без необхідності змінювати вихідний код додатку.

Frida забезпечує гнучкість, що дозволяє користувачам зосередитися на специфічних аспектах безпеки, таких як аутентифікація, шифрування даних або вразливості у веб-сервісах. Завдяки підтримці різних платформ, Frida може бути використаний для тестування як мобільних, так і десктопних додатків, що робить його універсальним інструментом у руках дослідників безпеки.

Проте, ефективне використання Frida вимагає певних технічних знань та досвіду. Оскільки інструмент є досить потужним, він також вимагає від користувача розуміння роботи системи, з якою він працює, а також знань про JavaScript. Це може стати викликом для менш досвідчених користувачів, які можуть зіштовхнутися з труднощами під час налаштування інструменту та написання власних скриптів.

Переваги Frida:

1) гнучкість: підтримка різних платформ і можливість динамічного інструментування програм;

2) потужний API: дозволяє взаємодіяти з додатками на низькому рівні, модифікувати їх поведінку та виводити внутрішні дані;

3) скриптування на JavaScript: Легкість написання скриптів для автоматизації та модифікації.

Недоліки Frida:

1) технічні вимоги: вимагає певного рівня технічних знань, що може бути складним для новачків;

2) налагодження: налаштування та інтеграція Frida можуть потребувати часу та зусиль, особливо при роботі з мобільними платформами;

3) безпека: використання Frida для злочинних цілей може піддавати користувачів правовим ризикам, оскільки маніпуляція з додатками може порушувати їх ліцензійні угоди [30].

SecuWear є прогресивним інструментом, розробленим для забезпечення безпеки мобільних та носимих пристроїв. Він спирається на п'ять основних відкритих технологій, що забезпечують глибокий аналіз безпеки. Однією з найважливіших рис SecuWear є його здатність виявляти вразливості в реальному часі, що дозволяє розробникам оперативно реагувати на загрози. У сучасному середовищі, де кіберзагрози постійно еволюціонують, ця функція є надзвичайно важливою.

Важливим аспектом SecuWear є його відкритий код, що сприяє активному залученню спільноти розробників і користувачів до вдосконалення інструменту. Це дозволяє швидко адаптувати SecuWear до нових загроз і вразливостей, оскільки користувачі можуть вносити зміни та поліпшення, які допомагають у боротьбі з новими формами атак.

SecuWear підтримує широкий спектр платформ, включаючи не лише мобільні додатки, а й носимі пристрої, такі як смарт-годинники та фітнес-трекери. Це робить його універсальним інструментом для дослідників безпеки, які працюють в різних сферах.

Проте, незважаючи на всі переваги, SecuWear має свої недоліки. Одним із викликів є те, що для його ефективного використання можуть знадобитися певні технічні знання. Менш досвідчені користувачі можуть зіткнутися з труднощами під час налаштування та інтеграції SecuWear у свої процеси тестування.

Однією з основних причин, чому SecuWear випереджає інші інструменти, є його здатність до реального моніторингу вразливостей. Це дозволяє розробникам своєчасно реагувати на загрози, що суттєво знижує ризик успішних атак. Інші інструменти, такі як MobSF, хоча й забезпечують статичний та динамічний аналіз, не завжди демонструють таку оперативність у виявленні загроз.

SecuWear, побудований на основі відкритого коду, користується підтримкою активної спільноти, що забезпечує швидку реакцію на нові виклики безпеки. Хоча MobSF також є відкритим проектом, його розвиток не

завжди відбувається так швидко, як у випадку SecuWear, що дозволяє останньому залишатися на передовій у сфері безпеки [31].

Цей інструмент забезпечує великий спектр платформ для аналізу, що робить його універсальним для дослідників, які працюють в різних галузях. У порівнянні з OWASP ZAP, який здебільшого орієнтується на веб-додатки, SecuWear надає розширені можливості для тестування мобільних та носимих технологій.

Доступний інтерфейс SecuWear робить його зручним для широкого кола користувачів, включаючи новачків у сфері безпеки. Інструменти, як-от Frida, хоч і потужні, можуть вимагати від користувачів значних технічних знань, що може стати бар'єром для тих, хто тільки починає свій шлях у тестуванні безпеки.

SecuWear також генерує докладні звіти про виявлені вразливості, що допомагає розробникам зрозуміти, які саме аспекти потребують покращення. На відміну від OWASP ZAP, звіти SecuWear надають глибокий аналіз, що полегшує процес виправлення вразливостей.

Таким чином, SecuWear поєднує в собі моніторинг загроз у реальному часі, відкритий код, універсальність, простоту використання та детальну аналітику. Це робить його найкращим вибором серед існуючих інструментів для аналізу безпеки мобільних і носимих пристроїв. Ці переваги забезпечують не лише ефективність у виявленні вразливостей, але й безперервне вдосконалення, що дозволяє SecuWear залишатися на передовій технологій захисту від кіберзагроз. У наступному розділі ми детально розглянемо цей інструмент.

2.2 Характеристики та функціональність SecuWear

SecuWear є інструментом, який можуть використовувати дослідники з безпеки та розробники додатків для тестування, аналізу та усунення вразливостей у носимих пристроях. Його основна мета — забезпечити

прозорість і відкритість, надаючи дослідникам повний контроль над компонентами архітектури носимих пристроїв для кращого розуміння та оцінки вразливостей.

SecuWear побудований на п’яти ключових відкритих технологіях: MetaWear (пристрій), Apache Cordova (для швидкого прототипування мобільних додатків) на платформах Android та iOS, Ubertooth One (для атак між смартфоном і носимим пристроєм) та Django (фреймворк для ведення журналів даних з мобільного додатка).

Ці технології охоплюють три ключові домени: носимі пристрої, мобільні пристрої та веб-сервіси. SecuWear дозволяє дослідникам аналізувати безпекові виклики кожного з цих доменів окремо та в контексті їхньої взаємодії. У носимому домені основним питанням є те, як збираються дані та як вони передаються на мобільні пристрої. У мобільному домені існує загроза витоку даних до менш безпечних додатків, що можуть зловживати такими даними. В області веб-сервісів можуть виникати проблеми, пов’язані з атаками, такими як Cross-Site Scripting (CSS) та SQL-ін'єкції, або з розкриттям особистої інформації через неправильне агрегування даних [32].

Однією з важливих особливостей є аналіз ризиків у зоні взаємодії між носимим пристроєм та мобільним додатком. Дані передаються через Bluetooth Low Energy (BLE), що піддає їх ризикам, таким як перехоплення та атаки Man-in-the-Middle (MiTM).

Протидія ризикам безпеки та конфіденційності в носимих пристроях є ключовою задачею. Головний принцип дизайну платформи SecuWear — це надання дослідникам можливості відійти від конкретних пристроїв чи додатків і розглядати вразливості в більш загальному контексті, охоплюючи різні домени взаємодії. SecuWear підтримує дослідження, що охоплюють три домени: носимі пристрої (програмне і апаратне забезпечення), мобільні пристрої (додатки на смартфонах та планшетах) та веб-додатки (компоненти, що з'єднуються з мобільним доменом).

Тестування в SecuWear є роздільним для кожного домену, що дозволяє дослідникам ізолювати проблеми і узагальнювати виявлені вразливості для інших продуктів. Наприклад, якщо вразливість виявлена у мобільному домені, дослідники можуть опублікувати свої результати, що дозволить інженерам безпеки з інших організацій оцінити їхній вплив на власні продукти. Такий підхід узгоджується з існуючими зусиллями каталогізації вразливостей, як-от Common Weakness Enumeration (CWE) та Common Vulnerabilities and Exposures (CVE). SecuWear використовує п'ять основних відкритих технологій:

1) MetaWear – це платформа з відкритим кодом, що включає апаратне та програмне забезпечення, розроблене компанією MbientLab. Пристрій має компактний розмір, близький до розміру американської монети у 25 центів, і важить лише 4 грами, враховуючи акумулятор. До складу MetaWear входить невеликий процесор ARM Cortex-M0, здатний обробляти прості інструкції, а також різні датчики, такі як яскравий світлодіод, термодатчик, тривісний акселерометр, кнопка та контакти для підключення додаткових сенсорів або пристроїв через GPIO. Це може бути оптичний пульсометр або мініатюрний вібромотор для тактильного зворотного зв'язку. Також на платі розміщені USB-зарядний пристрій і антена для зв'язку через Bluetooth LE. MetaWear надає розробникам та компаніям масштабовану платформу, яка дозволяє швидко виводити на ринок нові носимі пристрої. Крім того, у комплекті з апаратним забезпеченням йде вбудоване програмне забезпечення, яке через відкритий API BLE для Android та iOS передає дані з сенсорів на мобільні пристрої.

SecuWear отримує значні переваги від функціональних можливостей і відкритості MetaWear. Вбудовані функції дають можливість дослідникам безпеки аналізувати різні сценарії використання, які часто зустрічаються в комерційних і медичних носимих пристроях. Відкритість MetaWear, завдяки доступності коду та детальній документації, забезпечує прозорість роботи програмного забезпечення носимих пристроїв, що є важливим для оцінки й аналізу можливих вразливостей;

2) Apache Cordova — для швидкого створення мобільних додатків на Android та iOS. Мобільний додаток SecuWear створений за допомогою платформи Cordova. Це гібридний мобільний додаток, що дозволяє без труднощів працювати на різних платформах, таких як Android та iOS. За допомогою Cordova додаток побудований як веб-додаток, який використовує HTML5, CSS та JavaScript, і обгорнутий у нативний контейнер для забезпечення доступу до функцій пристрою, таких як акселерометр, Bluetooth тощо. Використання цієї платформи у SecuWear дає дослідникам можливість вивчати вразливості додатків на різних апаратних засобах та операційних системах, створюючи ефективний інструмент для вивчення безпеки носимих пристроїв;

3) Ubertooth One — для аналізу атак по повітрю між мобільним і носимим доменами. Це відкритий апаратно-програмний інструмент, що дозволяє аналізувати радіочастотний спектр у діапазоні 2,4 ГГц (ISM). Він працює як Bluetooth-антена і дає можливість досліджувати мережеві вразливості, що використовуються у носимих пристроях. Використовуючи Ubertooth, можна вловлювати пакети даних, передані через Bluetooth, і аналізувати їх у програмі Wireshark. Це дозволяє дослідникам оцінювати потенційні загрози у каналах між мобільними додатками та носимими пристроями, а також проводити атаки "людина посередині";

4) SecuWear також використовує веб-сервіс на основі Django, який надає RESTful API для збереження даних з мобільного додатку та Ubertooth у форматі JSON. Django є фреймворком для створення веб-додатків на Python і дозволяє зберігати та аналізувати дані, отримані під час досліджень. Сервіс зберігає отримані пакети даних і події в панелі адміністратора для подальшого аналізу вразливостей і поведінки носимих пристроїв [33].

На рисунку 2.1 продемонстровано зв'язки між цими доменами (носима електроніка, мобільний додаток і веб-сервіси), канали передачі даних і можливі вектори атак. Ліворуч представлено домен носимих пристроїв з MetaWear, у центрі — мобільний додаток SecuWear, а праворуч — веб-додаток на Django.

Ця структура дозволяє точно відстежувати та аналізувати усі загрози в кожному домені.

SecuWear є потужним інструментом для всебічного аналізу безпеки носимих пристроїв, надаючи дослідникам можливість зануритися в комунікаційні процеси між носимими сенсорами та мобільними додатками. Він здатен записувати та аналізувати дані, що передаються через Bluetooth, вивчаючи потенційні загрози, такі як атаки "людина посередині" та інші види кіберзагроз, що стосуються перехоплення інформації. Відкритий доступ до інструменту стимулює розвиток дослідницької спільноти, яка спільними зусиллями адаптує платформу до нових викликів у сфері кібербезпеки.

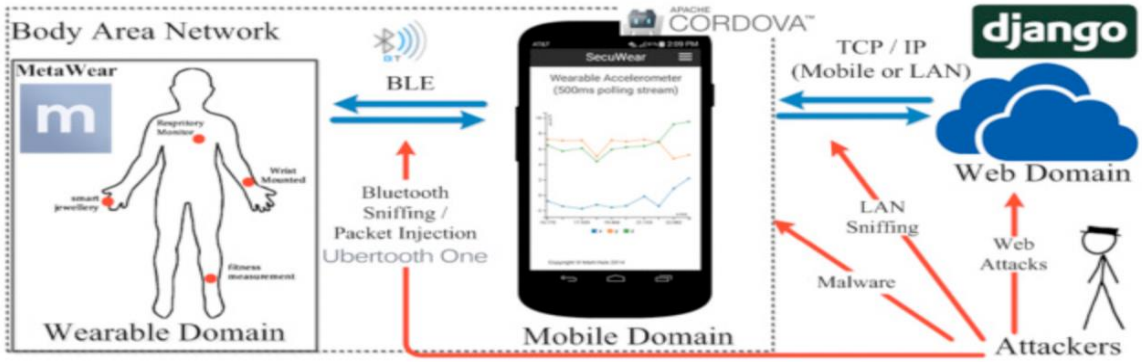

Рисунок 2.1 - Архітектура SecuWear та вектори атак на різні домени (носимі, мобільні та веб-сервіси) [34]

2.3 Оцінка ефективності платформи SecuWear

У порівняльному аналізі компонентів SecuWear важливо критично оцінити його переваги та недоліки в контексті інших варіантів дослідження безпеки носимих пристроїв. SecuWear прагне об'єднати різні домени використання носимих пристроїв та представляє їх у загальному вигляді, що дозволяє дослідникам узагальнювати результати оцінки вразливостей. Цей підхід відрізняється від багатьох стратегій оцінки вразливостей, які зосереджуються на конкретних апаратних чи програмних рішеннях, але узгоджується з зусиллями категоризувати та класифікувати загальні проблеми

безпеки в системах CVE та CWE. Серед основних переваг SecuWear можна виділити:

- сприяння оцінці вразливостей, що охоплюють різні домени;
- опис категоричних (загальних) проблем, які можуть впливати на декілька апаратних або програмних продуктів;
- ідкритий код компонентів та прозорість взаємодії;
- наявність кількох потоків збору даних для багатофакторного аналізу та звітності, що допомагає виявити і ізолювати визначені проблеми.

Однак існують і недоліки:

- виробники носимих пристроїв можуть не сприймати результати, оскільки їх продукти не є предметом конкретних досліджень;
- виявлені вразливості все ще потребують додаткового аналізу у контексті комерційних продуктів, щоб визначити їх застосовність;
- вразливості можуть бути специфічними для обраних компонентів з відкритим кодом, що може призводити до помилкових позитивних результатів.

Важливо розуміти, що SecuWear не має на меті замінити специфічні оцінки продуктів, а слугує першим етапом для виявлення та класифікації вразливостей безпеки носимих пристроїв. Візія полягає в тому, що дослідники можуть загалом вивчати проблеми з SecuWear і поширювати результати за методом, подібним до CVE/CWE, а потім виробники та інші дослідники можуть здійснити подальші специфічні оцінки продуктів для кращої класифікації та контекстуалізації інформації [35].

У таблиці 2.1 наведено переваги та недоліки використання вибраних компонентів SecuWear у порівнянні з конкурентами. Всі доступні варіанти в доменах носимих та мобільних технологій SecuWear представлені у стовпцях, а кожну характеристику закодовано кольорами: від коричневого (погано) до жовтого (прийнятно) та зеленого (добре). Варіантні клітинки білого кольору. Оскільки веб-сервіс надає лише REST API, конкуренти не аналізуються детально.

Серед носимих продуктів, які були проаналізовані, - Adafruit Flora, електронна плата, сумісна з Arduino для функціональності GPIO, WARP, платформа для розробки додатків IoT та носимих пристроїв, а також типові комерційні продукти, такі як Apple Watch, Fitbit, Pebble, Jawbone UP, Samsung Gear і Nike + Sportbands. Також у таблиці порівнюються різні технології розробки мобільних додатків відповідно до бажаних характеристик.

Таблиця 2.1 - Порівняльний аналіз компонентів SecuWear

Носимий пристрій	**MetaWear**	**Flora**	**WARP**	**Комерційні продукти**
Тип прошивки	Закрита, настроювана	Програмована	Закрита	Закрита
Розмір спільноти	Середня	Середня	Мала	Велика
Bluetooth	BLE	BLE (заплановано)	BLE	Різні
Простота використання	Легка	Легка	Н/Д	Різні
Кількість сенсорів	Висока	Висока	Середня	Різні
Відкритий код	Так	Так	Заплановано	Ні
Платформи	iOS, Android	Arduino	Всі	Одинарна
Вартість	$39	$20 + $70 (сенсори)	$149	$100+
Мобільний додаток	**Cordova**	**iOS**	**Android**	**Веб**
Кросс-платформність	Так	Ні	Ні	Так
Незалежність від пристрою	Так	Ні	Ні	Так
Час розробки	Середній	Високий	Високий	Низький
Продуктивність	Помірна	Висока	Висока	Повільна
Доступ до функцій	Всі	Всі	Всі	Деякі

Прошивка вважається програмованою, якщо розробники отримують доступ до її вихідного коду від виробника пристрою. Вона вважається закритою, якщо виробники не надають доступу до коду і не готові налаштовувати прошивку за запитом розробників. Якщо ж вихідний код недоступний, і виробники не планують надати налаштування для альтернативних застосувань, прошивка вважається закритою.

Розмір спільноти оцінюється за кількістю користувачів мобільних додатків у Google Play та Apple App Store для кожного типу пристрою, а також за кількістю активних учасників, завантажень та активності на GitHub. На момент написання мобільний додаток, що використовується для Flora — Adafruit Bluefruit LE connect, має близько 10 тисяч завантажень у Play Store та невідому кількість на iOS. MetaWear має приблизно 8 тисяч завантажень на GitHub, Play Store та App Store, а також активні репозиторії вихідного коду. На момент написання інформація про кількість додатків для WARP не була доступна, а активність на GitHub була обмеженою.

Комерційні носимі пристрої мають величезний діапазон завантажень — від мільйонів (наприклад, 10 мільйонів для Fitbit) до сотень або тисяч в залежності від продукту. Простота використання стосується легкості, з якою розробники можуть працювати і писати код для своїх додатків, використовуючи продукт. Flora та MetaWear є простими у використанні завдяки добре задокументованим API та модульному дизайну, в той час як комерційні продукти можуть бути складнішими через відсутність або недостатню документацію.

Кількість сенсорів вважається високою, якщо пристрій має 4 або більше сенсорів, середньою — якщо 2 або 3 сенсори, і низькою, якщо тільки 1 сенсор. Комерційні продукти варіюються за цим показником, більшість з них має середню або високу кількість сенсорів.

2.4 Типи векторів атак у SecuWear

У цьому розділі ми розглядаємо вразливості Bluetooth-пристроїв, виявлені в рамках досліджень, проведених з використанням платформи SecuWear. Bluetooth став невід'ємною частиною сучасних технологій, які спрощують бездротову комунікацію між пристроями. Однак це також створює можливості для зловмисників, які прагнуть скористатися цими вразливостями. Розглядаються два основні типи атак: прослуховування та атаки відмови в обслуговуванні (DoS).

Атаки прослуховування на Bluetooth-пристрої можна класифікувати за кількома сценаріями, що зазвичай зустрічаються в носимих пристроях, які використовують Bluetooth для бездротового з'єднання. У нашому дослідженні були вивчені три основні сценарії:

1) сценарій реклами: носимий пристрій постійно транслює рекламні пакети, сигналізуючи про свою доступність для смартфонів з підтримкою Bluetooth Low Energy (BLE). Коли компонент MetaWear увімкнено та готовий до підключення, він постійно передає пакети реклами. Як показано на рисунку 2.2, пакет реклами (тип ADV_IND) містить MAC-адресу та ім'я пристрою. Хоча це не є особливо шкідливим, інформація все ж може бути використана зловмисниками. SecuWear здатна захоплювати релевантні дані атак для оцінки в цьому випадку. Щоб запобігти таким оголошенням, користувачі можуть:
a) здійснити парування пристрою перед входом у публічний простір бездротового зв'язку (наприклад, парування вдома);
b) помістити пристрій у Faraday-купол для запобігання зовнішнім комунікаціям;
c) вимкнути пристрій;

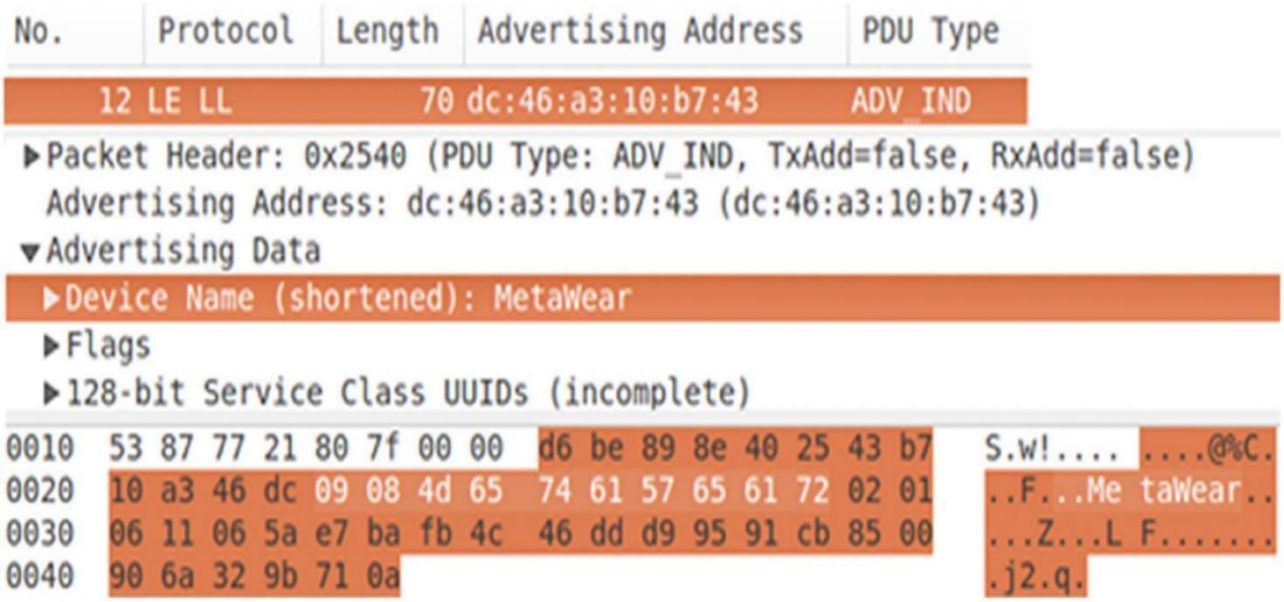

Рисунок 2.2 - Пакет, захоплений під час процесу реклами GAP

2) сценарій парування: у цьому випадку смартфон, що виконує додаток SecuWear, здійснює парування з MetaWear. Додаток отримує рекламні пакети та надсилає запит на сканування (SCAN_REQ), щоб отримати більше інформації, такої як Bluetooth-адреса та годинник пристрою. Коли MetaWear отримує запит, він відповідає пакетом SCAN_RES, використовуючи той самий канал. Наступним кроком є вибір користувачем опції "Підключити", що генерує запит на з'єднання (CONNECT_REQ). SecuWear, використовуючи Ubertooth, захоплює всі три типи пакетів, як показано на рисунку 2.3. Це дозволяє дослідникам зрозуміти атаку з трьох перспектив: джерела, призначення та атакуючого. Ця атака цікава, оскільки зловмисник може продовжувати прослуховувати дані навіть під час стрибків каналів [35];

Рисунок 2.3 - Пакети, отримані під час процесу парування

3) сценарій передачі даних: остання атака прослуховування, яку ми розглянули, полягає в перехопленні даних, що передаються після успішного захоплення CONNECT_REQ. Користувач надсилає сигнали на носимий пристрій (через парований мобільний додаток) для активації функцій або носимий пристрій передає дані на парований мобільний додаток для перегляду. Як видно на рисунку 2.4, пакети сигналізують MetaWear про передачу даних, таких як температура. Ця інформація може бути доступна для будь-кого, хто прослуховує канал під час передачі.

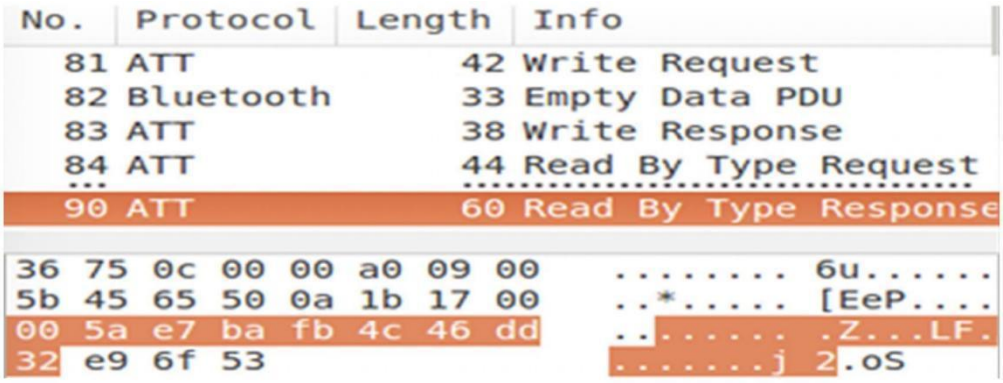

Рисунок 2.4 - Пакети, що активують термометр і передають дані

Окрім прослуховування, ми також дослідили атаки відмови в обслуговуванні (DoS), які можуть серйозно порушити функціонування Bluetooth-пристроїв. Ми проаналізували два конкретні типи DoS-атак:

1) спам запитів на підключення: перший тип атаки полягає у надсиланні великої кількості запитів на підключення до будь-якого пристрою, що рекламує свої можливості. Це заважає легітимним додаткам підключатися до пристроїв. У цьому випадку зловмисник може використовувати USB Bluetooth-адаптер разом із Python-скриптом для швидкого сканування та підключення до будь-якого доступного пристрою [36].

Як показано на рисунку 2.5, SecuWear зафіксувала з'єднання між комп'ютером-зловмисником та пасивними Bluetooth-навушниками LG HBS800. Перші два рядки показують сигнали (beacon packets), які надсилаються

навушниками, після чого йдуть запити на з'єднання (AUX1) та обмін пакетами для синхронізації частотних стрибків (FHS). Як тільки синхронізація завершена, починається нормальна робота пристрою, і зловмисник може залишатися підключеним або відключитися і знову підключитися;

2) атака на багатокористувацькі з'єднання: другий, більш цікавий тип DoS-атаки полягає у спробі перевищити ліміт підключень до пристроїв, які дозволяють підключення кількох додатків одночасно. Bluetooth-пристрої зазвичай підтримують до семи активних з'єднань одночасно через обмеження 3-бітного простору адрес. Використовуючи модифікований скрипт, можна створити до 7 одночасних з'єднань, однак жоден із протестованих носимих пристроїв (Pebble, Jawbone UP2, MetaWear та Fitbit) не підтримує кілька одночасних підключень. Тому поки що невідомо, чи можливо завадити легітимному використанню пристрою з багатьма підключеннями.

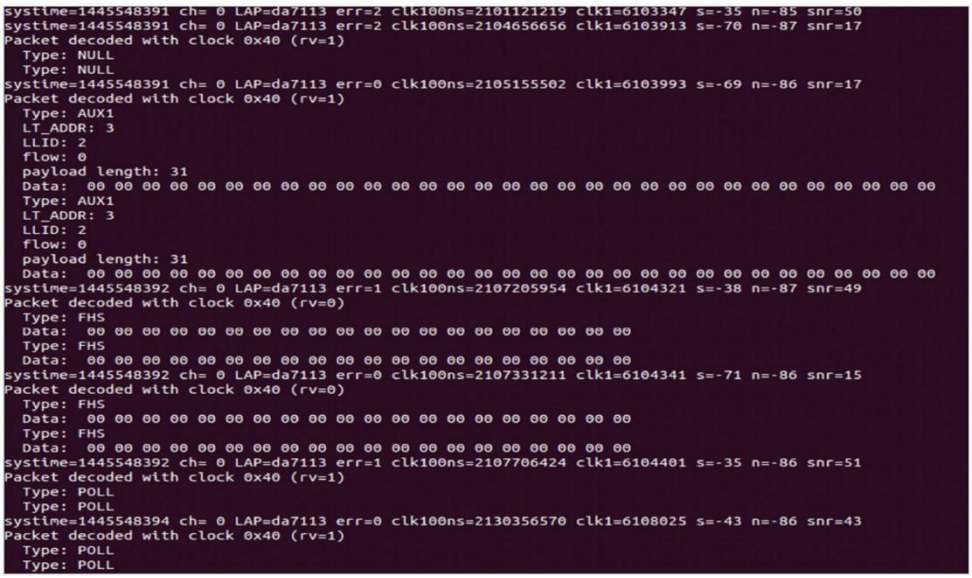

Рисунок 2.5 - Захоплення пакетів SecuWear, що демонструє атаку відмови в обслуговуванні, виконану за допомогою Python-скрипта

Важливо зазначити, що такі атаки можуть бути проблематичними для Bluetooth-пристроїв, які отримують оновлення прошивки через свої додатки. Зловмисник може заважати легітимному використанню пристрою,

завантажувати шкідливу прошивку або заволодіти пристроєм після підключення.

На основі наших досліджень можемо зробити висновок, що атаки DoS на Bluetooth є реальними, і платформа SecuWear може зафіксувати важливу інформацію для ідентифікації таких атак. Це підкреслює необхідність запровадження ефективних заходів безпеки для захисту від можливих загроз.

3 ВИКОРИСТАННЯ SECUWEAR НА ПРАКТИЦІ

3.1 Аналіз процесу забезпечення безпеки носимих пристроїв

Носимі пристрої, такі як фітнес-браслети, смарт-годинники, медичні монітори та інші гаджети, стають важливими елементами повсякденного життя. Вони забезпечують зручність, підвищують рівень здоров'я користувачів і навіть підтримують в реальному часі важливі біометричні дані. Однак, з ростом використання носимих технологій зростає і кількість вразливостей, які можуть бути використані для несанкціонованого доступу або маніпулювання даними. Враховуючи це, забезпечення безпеки таких пристроїв є важливою частиною розвитку та впровадження нових технологій.

SecuWear є спеціалізованим інструментом, що дозволяє забезпечити належний рівень безпеки носимих пристроїв. Він надає всебічний підхід до виявлення та усунення вразливостей, що дає змогу розробникам, постачальникам та незалежним тестувальникам проводити глибокий аналіз безпеки носимих пристроїв, створюючи процеси для фіксації уражень, їх тестування та виправлення [37].

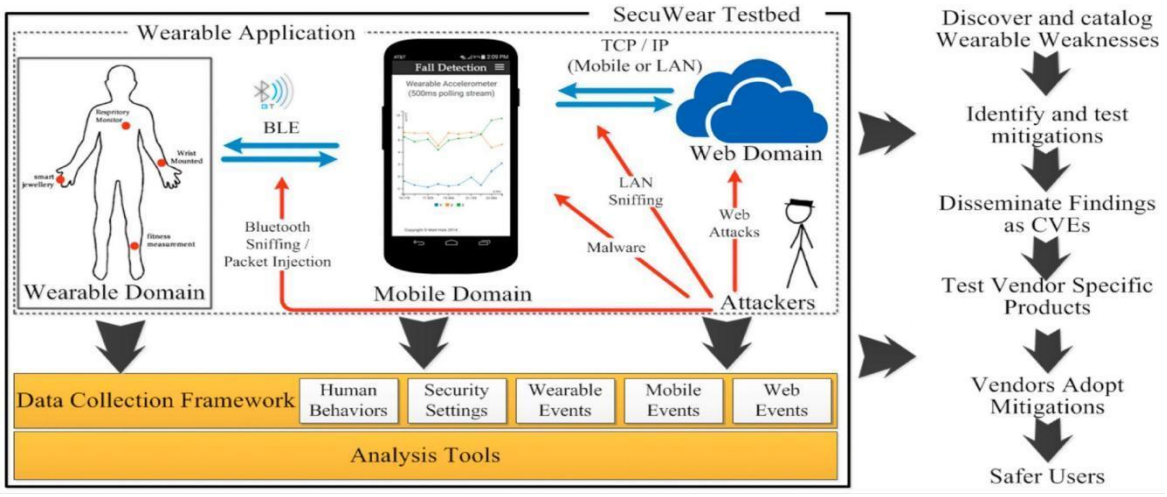

Рисунок 3.1 - Процес застосування SecuWear для забезпечення безпеки носимих пристроїв [35]

Розглянемо детальніше п’ятиступеневий процес застосування SecuWear, який наочно представлений на рисунку 3.1:

1) виявлення і каталогізація вразливостей носимих пристроїв;

2) тестування та розробка засобів для боротьби з вразливостями;

3) поширення результатів через CVE до постачальників;

4) тестування та коригування продуктів постачальниками;

5) випуск патчів для усунення вразливостей.

Першим етапом в рамках застосування SecuWear є виявлення вразливостей у носимих пристроях. Це може включати різні техніки тестування, такі як статичний аналіз коду, динамічне тестування, тестування на проникнення (penetration testing), а також перевірку на уразливості, що виникають через неправильну конфігурацію програмного забезпечення або взаємодію з іншими пристроями в мережі. Виявлені вразливості реєструються та класифікуються у каталог, що дозволяє систематизувати та структурувати інформацію для подальшої роботи.

Згідно з рисунком 3.1, цей етап є основою для подальших дій. SecuWear використовує різноманітні методи тестування для забезпечення широкого охоплення потенційних загроз. Наприклад, один із можливих способів виявлення вразливостей — це тестування на предмет уразливостей в апаратних компонентах пристроїв (сензори, мікропроцесори, антени). У разі виявлення уразливості, SecuWear фіксує її в базі даних, що дозволяє вести детальний облік усіх знайдених проблем і полегшує процес їх усунення.

Наступний етап полягає в розробці та тестуванні засобів для боротьби з виявленими вразливостями. Після того як вразливість була виявлена, необхідно протестувати різні методи її усунення. Це може включати в себе використання засобів криптографії, забезпечення безпеки передачі даних через мережу, а також використання безпечних протоколів для автентифікації користувачів. Для кожної вразливості SecuWear пропонує набір рекомендацій і можливих шляхів її усунення, після чого проводиться тестування на ефективність цих заходів.

Процес тестування включає в себе використання як автоматизованих інструментів SecuWear, так і ручних перевірок з боку досвідчених фахівців. Наприклад, після усунення вразливості можуть бути проведені повторні тестування для переконання в тому, що виправлення не викликало нових проблем або вразливостей. Крім того, на цьому етапі можуть бути розроблені додаткові інструменти для тестування пристроїв у більш різноманітних умовах, таких як зміни навколишнього середовища або інтеграція з іншими технологіями.

Після того як вразливість була виявлена та розроблені мітапи для її усунення, наступним етапом є поширення цієї інформації через систему CVE (Common Vulnerabilities and Exposures). Цей етап дуже важливий, оскільки він дозволяє стандартизувати інформацію про вразливості, що надається постачальникам пристроїв для подальшої роботи. Важливо зазначити, що на даному етапі також існують різні механізми, якими SecuWear забезпечує поширення інформації про вразливість серед постачальників.

Як показано на рисунку 3.1, SecuWear автоматично генерує запис CVE, що містить детальну інформацію про вразливість і можливі способи її усунення. Це дозволяє постачальникам пристроїв швидко отримувати необхідну інформацію та впроваджувати відповідні зміни. Процес фіксації та поширення CVE може бути здійснений через сертифіковані організації, такі як CERT/CC, US-CERT, або інші міжнародні організації, що відповідають за координацію вразливостей. Важливо, що SecuWear спрощує цей процес, роблячи його доступним для ширшого кола користувачів, включаючи невеликі компанії і академічні організації.

На наступному етапі, після того як постачальники отримали інформацію про вразливість через CVE, вони повинні провести додаткове тестування своїх продуктів з метою підтвердження існуючих проблем і виправлення вразливостей. Цей етап може включати в себе використання як внутрішніх тестувальних інструментів постачальників, так і інструментів SecuWear для перевірки на ефективність застосованих мітапів.

Рисунок 3.1 демонструє, як цей процес тісно пов'язаний з попередніми етапами і показує, як важливо, щоб постачальники активно тестували свої продукти і впроваджували виправлення. Враховуючи можливі різноманітні варіації пристроїв і їх апаратних компонентів, цей етап є критично важливим для забезпечення належного рівня безпеки.

Останній етап включає в себе випуск патчів або оновлень для усунення вразливостей. Після того, як постачальники протестували свої пристрої та впровадили відповідні виправлення, ці патчі розповсюджуються серед кінцевих користувачів через механізми автоматичних оновлень. Це дозволяє знизити ризики для кінцевих споживачів і підвищити безпеку носимих пристроїв на глобальному рівні.

На цьому етапі важливою частиною є зворотний зв'язок між користувачами та постачальниками пристроїв. Наприклад, користувачі можуть повідомляти про ефективність виправлень або виявлені нові проблеми, що допомагає постачальникам своєчасно реагувати на нові загрози [38].

3.2 Узагальнення вразливостей SecuWear

SecuWear є платформою для тестування безпеки пристроїв носимої електроніки, що дозволяє виявляти уразливості, які виникають внаслідок взаємодії між пристроями, мобільними додатками та онлайн-сервісами. У цьому контексті дослідження показують, що комерційно доступні пристрої носимої електроніки можуть мати ті ж самі вразливості, які були виявлені в SecuWear. Для підтвердження цієї гіпотези було проведено тестування кількох відомих пристроїв носимої електроніки, таких як Fitbit Charge HR, Pebble Steel і Jawbone UP2, що дозволило порівняти уразливості, що виявляються на платформі SecuWear, з уразливостями цих комерційних пристроїв.

Для аналізу використовувалися ці пристрої разом із відповідними мобільними додатками, доступними в Google Play (Android), а також онлайн-API, що обробляють і зберігають зібрані дані. Деякі з цих API не надають

доступу до функціоналу пристрою, але лише до даних, які збираються ним. Для збору інформації з Bluetooth-з’єднань використовувався інструмент Ubertooth, що дозволяє захоплювати передачу даних по Bluetooth.

Усі три досліджувані пристрої демонструють рекламні пакети, які мають структуру, схожу на пакети, що використовуються платформою SecuWear. Наприклад, на рисунку 3.2 показано SCAN_REQ та ADV_IND пакети, що передаються від Fitbit Charge HR, і ці пакети за структурою схожі з тими, що генеруються платформою SecuWear (рисунок 2.2). Подібно, рисунки 3.3 та 3.4 показують пакети від Jawbone UP2 і Pebble Steel.

Рекламні пакети (ADV_IND) передаються Bluetooth-пристроєм, коли він перебуває в режимі активного сканування або прослуховування. Це дає можливість іншим пристроям (наприклад, мобільним телефонам) виявляти їх і з’єднуватися. Однак, при такій передачею інформації зловмисник може перехопити ці пакети і отримати дані про пристрій, такі як його ідентифікаційні дані (MAC-адреса, тип пристрою, модель тощо), навіть без підключення.

Такі рекламні пакети можуть стати потенційною уразливістю безпеки для пристроїв. Наприклад, зловмисник може використовувати перехоплені пакети для визначення пристроїв, які знаходяться в радіусі дії, і скласти профіль пристроїв, що використовуються для подальших атак або збору інформації. Це може включати фішинг-атаки або навіть фізичні атаки, якщо зловмисник має доступ до місця, де перебувають ці пристрої.

Таким чином, хоча рекламні пакети є важливим елементом для виявлення пристроїв і їх взаємодії, вони також створюють серйозні ризики для конфіденційності та безпеки користувачів. Важливим є розуміння цих ризиків та впровадження заходів безпеки, таких як шифрування рекламних пакетів або використання змінних ідентифікаторів (MAC-адрес), щоб знизити ймовірність їх перехоплення.

Важливим аспектом дослідження є з'єднання між пристроєм та мобільним додатком, яке, зокрема, включає безпечне спрощене з’єднання (Secure Simple Pairing, SSP) — технологію, що використовується для встановлення з’єднання

по Bluetooth з використанням криптографічних алгоритмів для забезпечення безпеки. В даному випадку ми перевіряли, як ці пристрої застосовують SSP для забезпечення захищеного з'єднання.

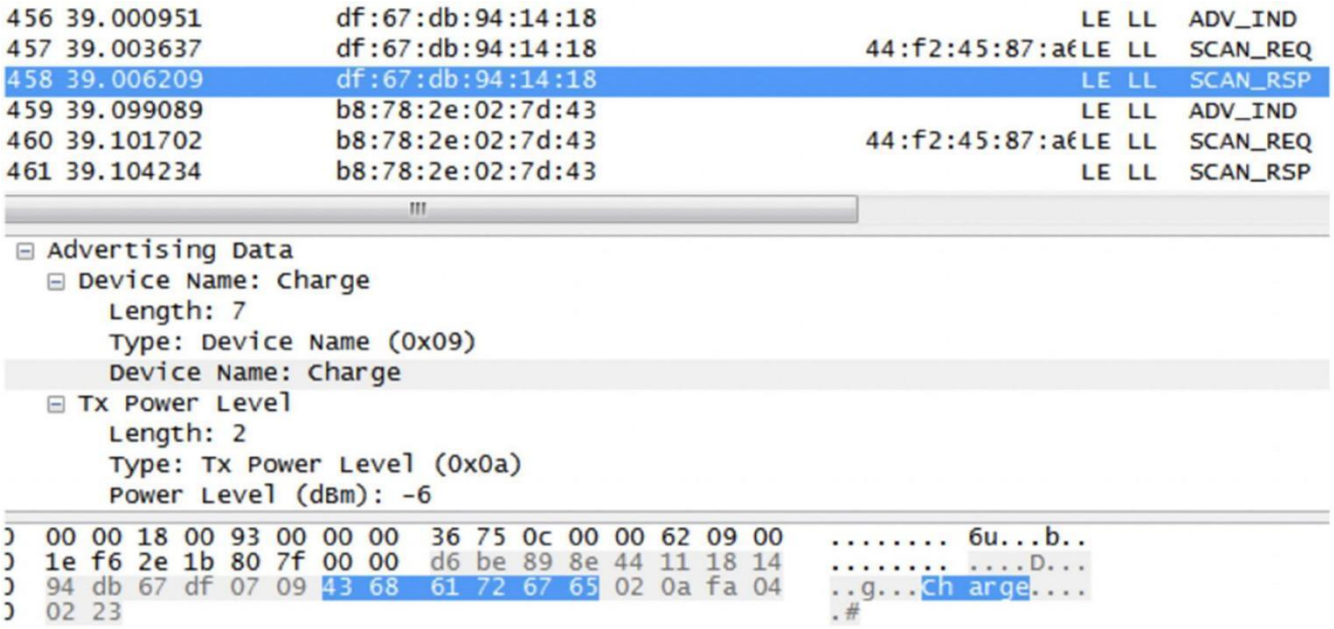

Рисунок 3.2 - Рекламні пакети від Fitbit Charge HR, які показують значну схожість з даними, отриманими за допомогою MetaWear

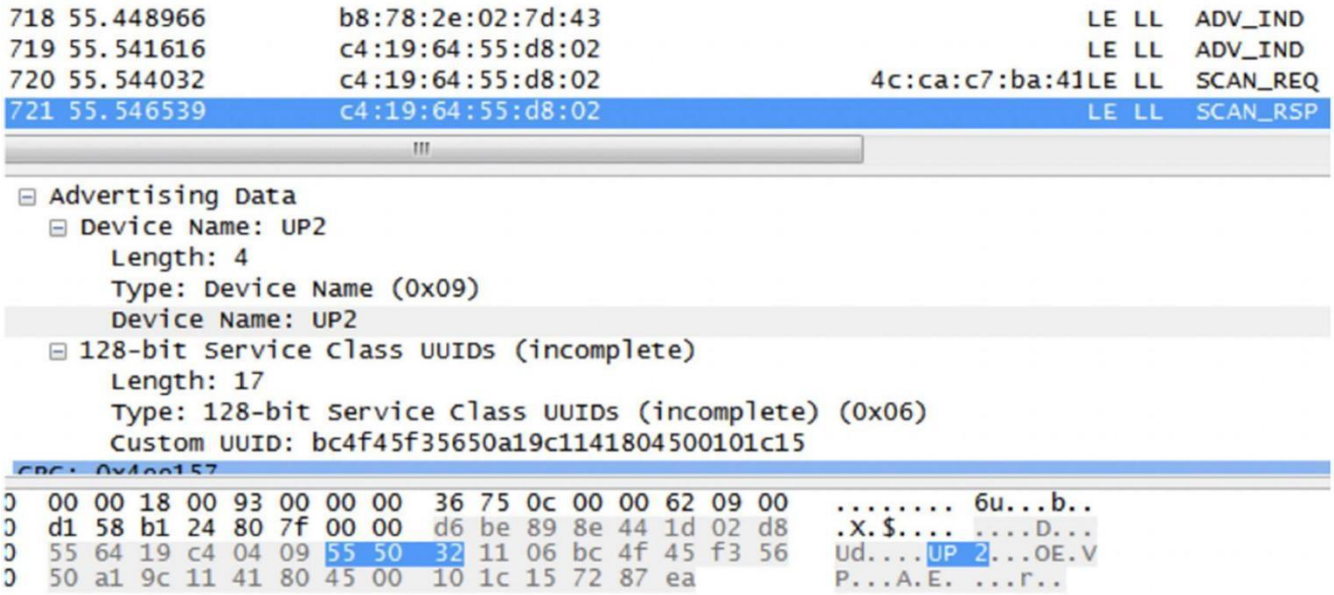

Рисунок 3.3 - Приклад аналогічного типу пакета, отриманого з пристрою Jawbone UP2

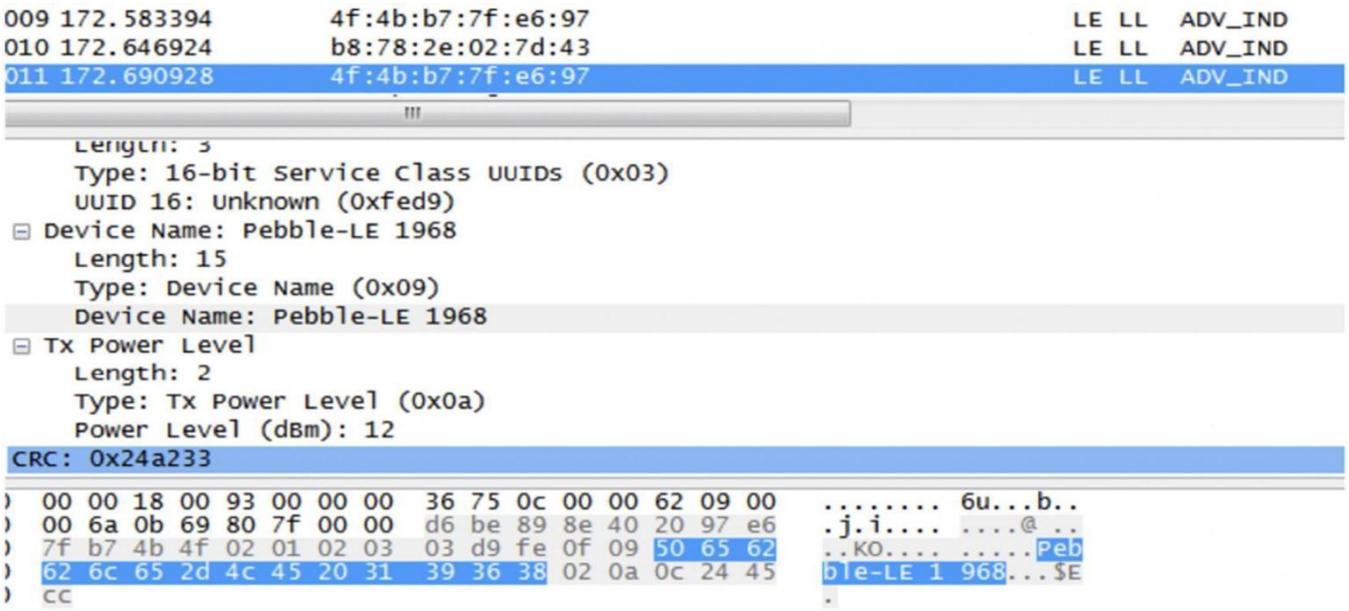

Рисунок 3.4 - Схожий ADV_IND пакет, отриманий з пристрою Pebble

Наприклад, рисунок 3.5 демонструє пакет CONNECT_REQ від Fitbit Charge HR, який використовується для ініціації з’єднання між пристроєм і мобільним додатком. Рисунки 3.6 та 3.7 аналогічно показують з'єднання від Jawbone UP2 та Pebble Steel.

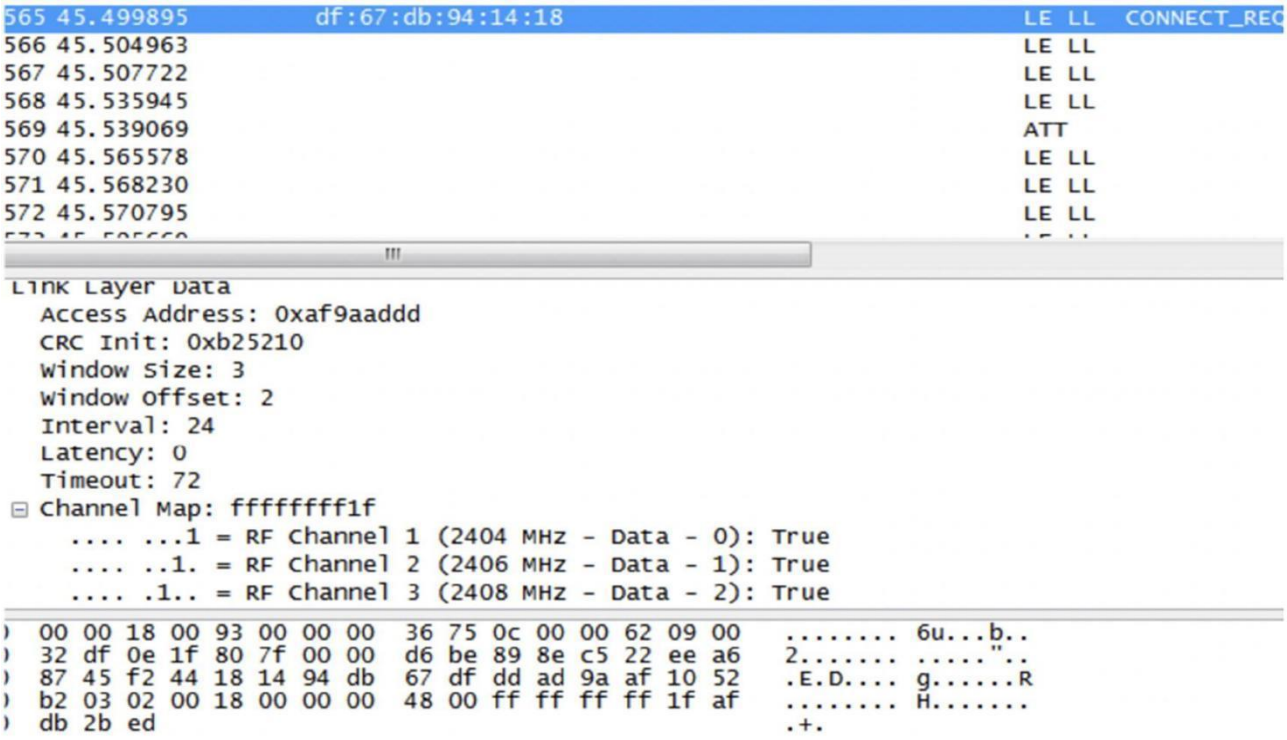

Рисунок 3.5 - Пакет CONNECT_REQ від Fitbit, перехоплений під час використання стратегії безпечного сполучення Secure Simple Pairing з введенням пароля

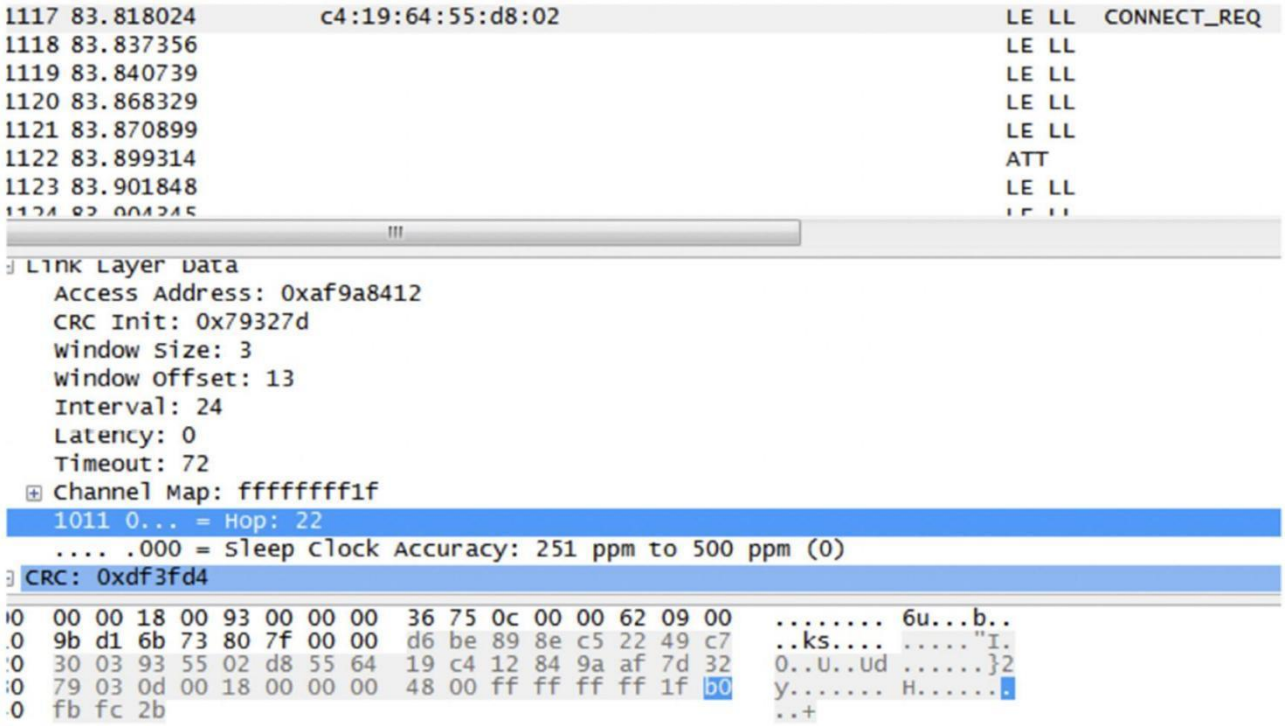

Рисунок 3.6 - Подібний пакет від Jawbone, перехоплений при використанні стратегії безпечного сполучення Secure Simple Pairing (Just Works)

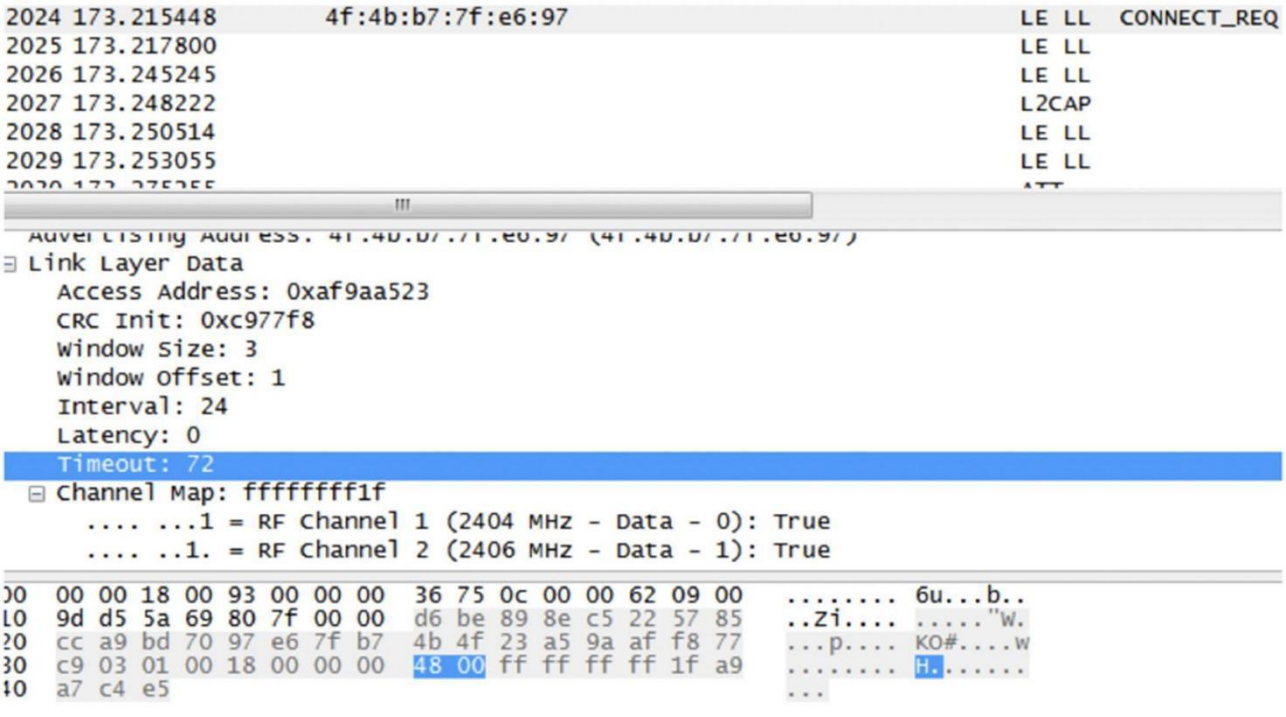

Рисунок 3.7 - Подібний пакет від Pebble, зафіксований під час використання числового порівняння у Secure Simple Pairing

Проте, незважаючи на застосування SSP, всі пристрої демонструють схожі проблеми безпеки. Наприклад, Jawbone використовує метод "just works", що є найменш безпечним серед варіантів SSP, оскільки він не передбачає додаткових заходів для перевірки автентичності пристроїв. Pebble Steel і Fitbit використовують більш безпечні методи, такі як введення паролю або числове порівняння, але всі ці методи все одно піддаються атакам на з'єднання через спостереження за початковими пакетами.

Після встановлення з'єднання пристрої демонструють значні відмінності у способах передачі зібраних даних. Наприклад, пристрій Fitbit використовує власний протокол шифрування для захисту даних після встановлення з'єднання. У процесі дослідження було виявлено специфічні Bluetooth-обробники (handles), які працюють подібно до регістрів у низькорівневих архітектурах процесорів, де зберігаються дані. Однак ці дані зашифровані, і розкриття методу шифрування не входить до меж цього дослідження, оскільки це потребує значних ресурсів та глибокого аналізу криптографічних алгоритмів.

Як показано на рисунку 3.8, ми зафіксували зміну в обробнику даних, що підтверджує наявність зашифрованої інформації. Це свідчить про високий рівень захисту даних на етапі передавання, але вимагає додаткової уваги з боку фахівців з безпеки для виявлення потенційних вразливостей.

При розгляді пристрою Jawbone UP2 було виявлено, що він також використовує власний протокол шифрування для захисту переданих даних. З огляду на практичний досвід зворотного інженерії, було доведено, що цей протокол шифрування може бути зламаний. Так, існують модифікації сторонніх мобільних додатків, які здатні контролювати пристрій, але для цього необхідно відновити алгоритм шифрування, що підтверджує, що безпека цього методу не є абсолютною. Як показано на рисунку 3.9, ми зафіксували зчитування даних через певний Bluetooth-обробник. Дані, ймовірно, були зашифровані, але ми не проводили їх подальшого аналізу.

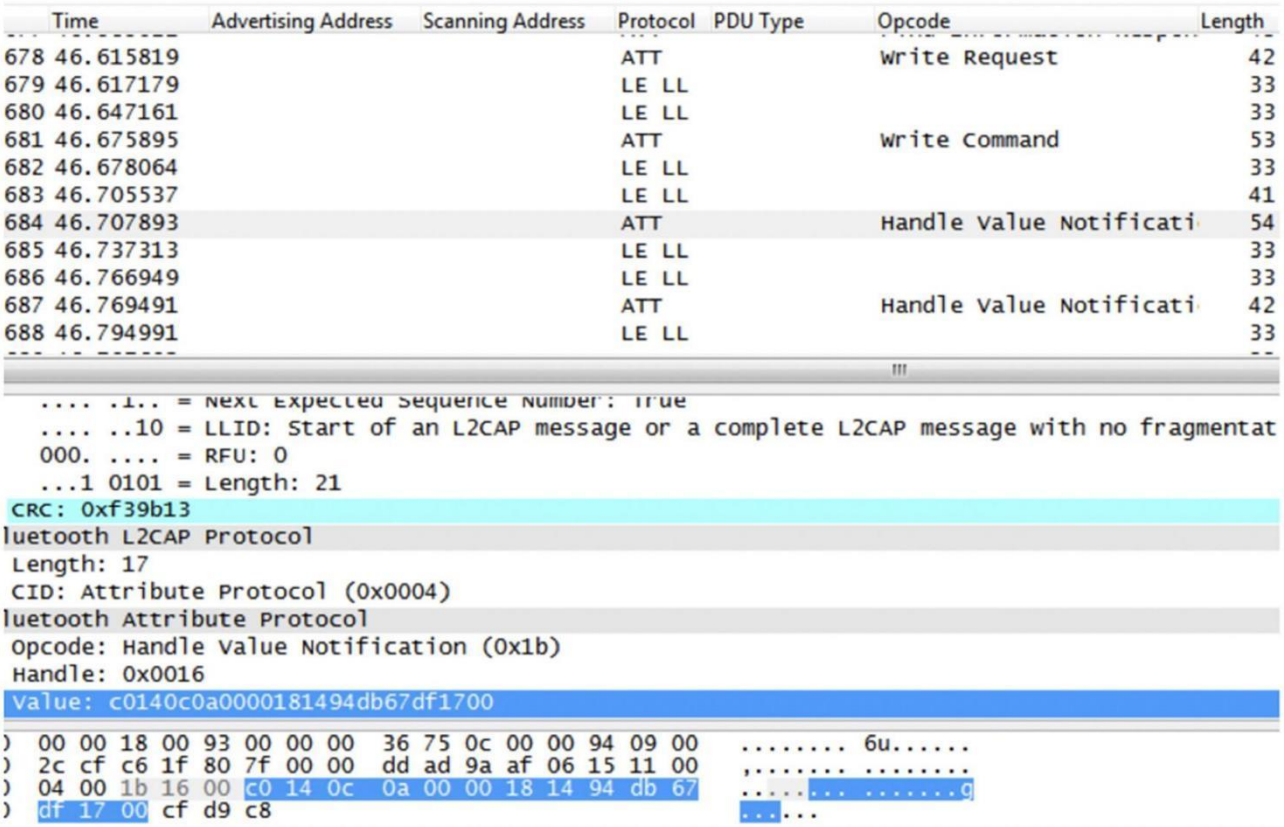

Рисунок 3.8 - Дані обробника, що передаються Fitbit до мобільного додатка

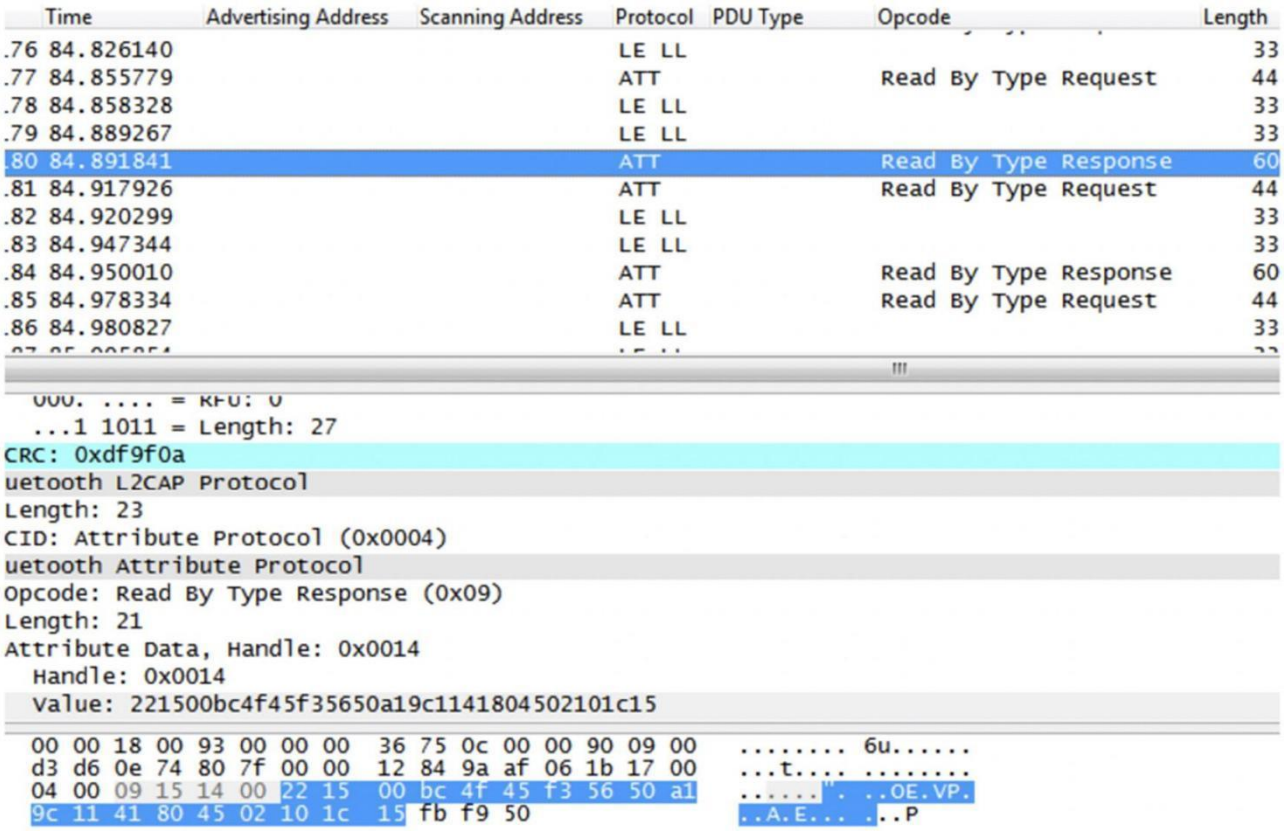

Рисунок 3.9 - Читання даних мобільним додатком Jawbone UP2 з парованого пристрою

Щодо Pebble Steel, то цей пристрій також використовує шифрування для передачі даних, що є стандартною практикою для забезпечення конфіденційності інформації. Однак проблема полягає в ненадійній ініціалізації ключів шифрування, що дозволяє потенційним зловмисникам спробувати декодувати передану інформацію навіть після завершення парування. Рисунок 3.10 ілюструє захоплення даних з Bluetooth-обробників після встановлення з'єднання, зокрема фіксацію початкового значення імені пристрою. Це демонструє, що хоча передача даних здійснюється із застосуванням шифрування, вразливість на етапі ініціалізації ключів може дозволити зловмисникам здійснювати спроби дешифрування. Незважаючи на те, що дані виглядають зашифрованими, ця уразливість знову підтверджує важливість удосконалення процесів безпеки при ініціалізації з'єднання та обміну даними між пристроями.

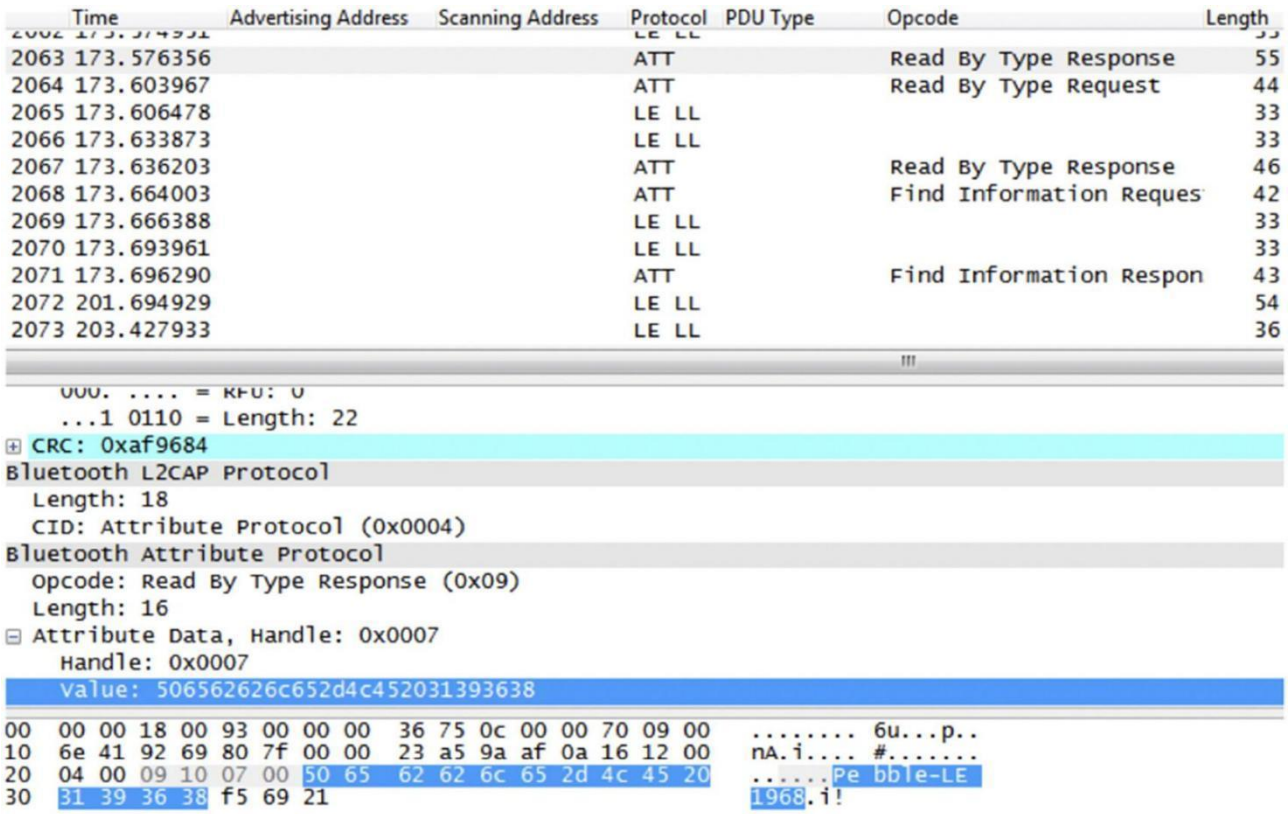

Рисунок 3.10 - Налаштування початкових обробників після парування на пристрої Pebble Steel

Загалом, усі три пристрої демонструють схожі вразливості у використанні шифрування та захисту даних, що вказує на важливість використання спеціалізованих платформ для тестування безпеки, таких як SecuWear. Платформи для тестування безпеки, що дозволяють імітувати атаки, можуть виявляти потенційні загрози, які не завжди видно в процесі звичайного користування пристроями. Виявлення таких проблем на етапі тестування допомагає розробникам вдосконалювати протоколи безпеки і забезпечувати більшу стійкість пристроїв до атак.

Застосування SecuWear для тестування пристроїв дає змогу не лише виявляти уразливості, але й формувати нові стандарти безпеки, що можуть бути застосовані до широкого спектра носимих пристроїв. Ретельне тестування на ранніх етапах розробки є критично важливим для зниження ризиків для кінцевих користувачів і підвищення рівня безпеки в цілому. Це дозволяє виробникам пристроїв своєчасно реагувати на виявлені загрози, підвищуючи довіру користувачів і підтримуючи конкурентоспроможність на ринку.

3.3 Приклад аналізу SecuWear у реальному використанні

Для демонстрації всіх можливостей інструменту SecuWear необхідно розглядати не лише один конкретний випадок, а й більш широкий спектр ситуацій. Тому ми обираємо для аналізу приклад атаки «від початку до кінця», що представлений на рисунку 3.11. У цьому випадку ми використовуємо пристрій MetaWear, який збирає дані про фізичну активність, зокрема дані про ходу та серцевий ритм. Мобільний додаток, розроблений за допомогою платформи Cordova, взаємодіє з сервісом збору даних і рекламним сервісом.

Сервіс збору даних просто акумулює та агрегує інформацію, що надходить від мобільного додатка та його супутнього носимого пристрою. Рекламний сервіс показує рекламу в додатку. В реальному сценарії цей рекламний сервіс зазвичай інтегрується через сторонні сервіси. У нашому випадку рекламний сервіс виявився вразливим до атаки типу Cross Site Scripting

(CSS). Зловмисник експлуатував цю вразливість для того, щоб впровадити атаку, яка відображалася в мобільному додатку на платформі Cordova.

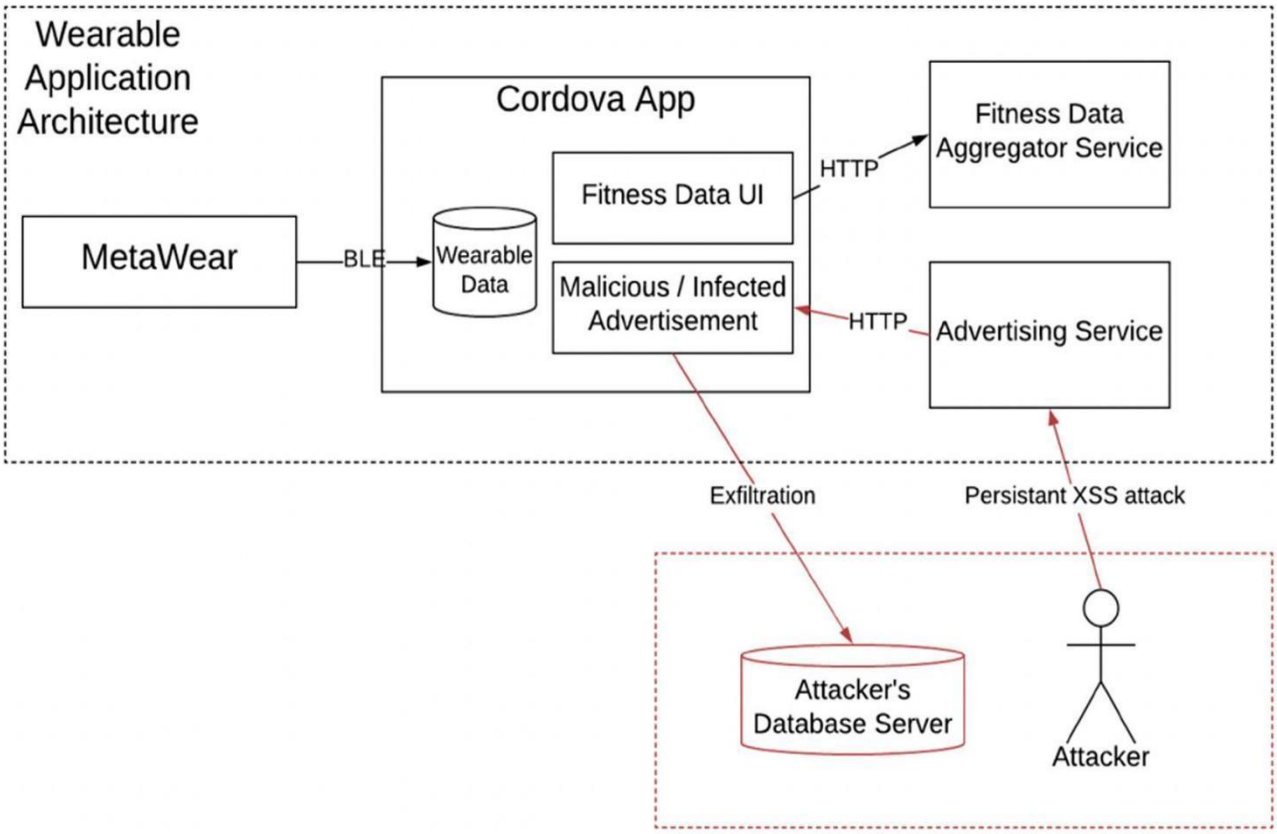

Рисунок 3.11 - Атака через ін'єкцію коду дозволяє зловмисному JavaScript передавати дані сенсорів на сервер атакуючого [39]

При завантаженні додатку дані про фізичну активність користувача починають передаватися в локальну базу даних на мобільному телефоні та відображатися в інтерфейсі користувача. Однак на цьому етапі додаток також завантажує рекламу з рекламного сервісу, який містить шкідливий CSS-код. Припустимо, що додаток Cordova не дотримується принципу найменших привілеїв і надає веб-переглядачу реклами дозвіл взаємодіяти з усіма даними в додатку. У такому разі виконується CSS-атака, що дозволяє ексфільтрувати дані з додатка та передавати їх на сервер зловмисника.

Цей випадок є яскравим прикладом, який підкреслює важливість використання таких інструментів, як SecuWear. SecuWear збирає події з MetaWear, мобільного додатка, пов'язаних сервісів та інтерфейсів зв'язку. У

результаті початкової CSS-атаки формується запис в журналі аудиту HTTP POST, який містить саму атаку в рекламному сервісі. Далі платформа захоплює мережевий запит, зроблений мобільним додатком до рекламного сервісу з шкідливим вантажем реклами. SecuWear також може фіксувати внутрішні події додатку Cordova, коли виявляється аудиторський хук. Окрім цього, можна захопити мережевий трафік, який йде на сервер бази даних зловмисника. Такий журнал аудиту дозволяє виявляти уразливості безпеки, які можуть охоплювати різні домени і взаємодії між різними компонентами системи.

Для дослідження цього сценарію ми реалізували кожен компонент архітектури і використали SecuWear для збору даних і аналізу журналу аудиту. Просте моделювання сервісів здійснювалось через WireMock, щоб забезпечити збір і передачу даних, як показано на рисунку 3.12. Той самий додаток MetaWear, описаний у розділі 2, був модифікований для включення нового веб-переглядача, що робить запит до рекламного сервера для завантаження реклами. Для реалізації цього випадку ми надаємо веб-переглядачу повний доступ до всіх даних додатку Cordova, включаючи його сховище даних. Частину журналу аудиту, яку зібрав SecuWear, показано на рисунку 3.12.

Як видно з фрагмента журналу аудиту, у додатку Cordova, де відображалася реклама, спостерігається аномальна поведінка. Після того, як реклама завантажується, програма починає передавати дані з носимого пристрою на сервер зловмисника. Така діяльність виявляється завдяки використанню аудитного хуку в додатку, що дає змогу точно зафіксувати момент і місце виникнення атаки. У фрагменті журналу не показано інші події, такі як зчитування чи запис даних на носимому пристрої після здійснення атаки, проте SecuWear здатна фіксувати такі дані також.

Цей приклад чітко показує, як важливо використовувати інструменти на кшталт SecuWear для виявлення безпекових уразливостей, які можуть виникнути через інтеграцію різних компонентів системи в реальних умовах. SecuWear дозволяє не тільки відслідковувати поведінку пристроїв, але й взаємодії між ними, що може стати важливим для виявлення і нейтралізації

потенційних загроз безпеки. Така можливість особливо важлива, оскільки інструмент дає змогу помічати загрози, які можуть бути непомітні при традиційному тестуванні безпеки. Він охоплює весь ланцюг взаємодій між пристроями і програмним забезпеченням.

Origin	Event	Captured By
<attacker IP>	HTTP POST – malicious XSS attack	Web service audit hook on Advertising service
MetaWear	Device advertisement	Ubertooth
Cordova App	Pairing request	Cordova App audit hook, Ubertooth
MetaWear	Pairing response	Ubertooth
Cordova App	Connection successful	Ubertooth, Mobile App audit hook
Cordova App	Turn accelerometer sensor on	Cordova App audit hook, Ubertooth
MetaWear	Sensor on acknowledgement	Ubertooth
MetaWear	Sensor data begins streaming	Ubertooth, Mobile App audit hook
Cordova App	HTTP POST - Authenticate to fitness data aggregator	Cordova App audit hook, network tap, Web service audit hook on Fitness data aggregator service
Fitness data aggregator	HTTP POST Response – return token	Web service audit hook on Fitness data aggregator service, network tap, Cordova App audit hook
Cordova App	HTTP POST - Data streaming to fitness data aggregator	Cordova App audit hook, network tap
Cordova App	HTTP GET to advertising service	Cordova App audit hook, network tap
Advertising Service	HTTP GET Response containing malicious advertisement	Web service audit hook on Advertising service, network tap, Cordova App audit hook
Cordova App	Render Advertisement (XSS attack)	Cordova App audit hook
Cordova App	Access local wearable data store	Cordova App audit hook
Cordova App	HTTP POST to <attacker server>	Cordova App audit hook
…	…	…
Cordova App	Access local wearable data store	Cordova App audit hook
Cordova App	HTTP POST to <attacker server>	Cordova App audit hook

Рисунок 3.12 - Журнал аудиту подій, зібраний SecuWear на основі сценарію дослідження випадку

Зокрема, SecuWear дозволяє виявити аномалії в роботі додатка, коли він взаємодіє з рекламними сервісами, і це допомагає знайти несанкціонований доступ до даних носимого пристрою. Такі загрози не тільки можна локалізувати, але й зібрати важливу інформацію для покращення системи безпеки. Детальні аудиторські записи, що фіксуються програмою, дають змогу точно визначити, де і коли почалася атака, а також відслідковувати подальші зміни в системі після її виконання.

Відтак, SecuWear є надзвичайно корисним інструментом для виявлення уразливостей у реальних умовах, особливо коли йдеться про інтеграцію мобільних додатків з зовнішніми сервісами, де можуть виникнути неочевидні загрози. Це дозволяє не лише вчасно зафіксувати саму атаку, але й здійснити детальний моніторинг її впливу на всю систему, що в свою чергу дає можливість швидко реагувати на потенційні ризики для безпеки.

ВИСНОВКИ

У роботі розглянуто проектування та ефективність платформи SecuWear, яка є універсальним інструментом для тестування безпеки носимих пристроїв. SecuWear дозволяє досліджувати безпеку носимих додатків, збираючи дані та симулюючи атаки на програмне й апаратне забезпечення з метою виявлення вразливостей. Платформа має широкий спектр можливостей для досліджень, що дозволяє оцінювати безпеку носимих пристроїв з різних аспектів та ідентифікувати потенційні ризики для користувачів.

У роботі було порівняно компоненти SecuWear з іншими рішеннями на ринку, що допомогло визначити їхні переваги й недоліки, а також вибрати найкращі технічні рішення для конкретних завдань. Експерименти показали, як різні вектори атак проявляються у додатках для носимих пристроїв і як SecuWear дозволяє збирати важливу інформацію для виявлення таких атак. Дослідження допомогли точніше ідентифікувати проблеми, які можуть виникнути при використанні носимих технологій у реальних умовах.

Аналіз атак на комерційно доступні пристрої підтвердив, що ті ж вектори атак, досліджені за допомогою SecuWear, присутній у широко використовуваних носимих пристроях, що демонструє ефективність платформи в реальних умовах. Висновки роботи свідчать, що SecuWear є важливим кроком вперед у виявленні вразливостей безпеки в сфері носимих технологій. Платформа має великий потенціал для подальшого вдосконалення та застосування у тестуванні безпеки пристроїв, що дозволить знизити ризики для користувачів і підвищити рівень захисту персональних даних. Очікується, що в майбутньому SecuWear стане важливою частиною процесу розробки та тестування носимих пристроїв, що забезпечують безпеку та захист від атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Symantec. Internet Security Threat Report. Symantec, 2024. 281 p.
2. McAfee. Mobile Threat Report. McAfee, 2024. 210 p.
3. Verizon. Data Breach Investigations Report. Verizon, 2024. 318 p.
4. Proofpoint. Human Factor Report. Proofpoint, 2024. 463 p.
5. Костащук А. Що таке фішинг і фішингова атака. Hostkoss, 2024. 317 с.
6. Symantec. Internet Security Threat Report. Symantec, 2023. P. 34-35.
7. Symantec. How Two-Factor Authentication Stops Cyber Attacks. Symantec, 2023. 42 p.
8. Symantec. Zero-Day Attacks: What You Need to Know. Symantec, 2023. 56 p.
9. McAfee. The Threat Report. McAfee, 2024. 112 p.
10. Zimperium. Mobile Security Trends. Zimperium, 2024. 87 p.
11. Verizon. Mobile Security Index. Verizon, 2024. 223 p.
12. A. Saeed, A. Ahmadinia, A. Javed, H. Larijani. Intelligent Intrusion Detection in Low-Power IoTs. ACM Trans. Internet Technol., Vol.16(4), 2016. P.1-25.
13. E. Benkhelifa, T. Welsh, W. Hamouda. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Commun. Surv. Tutorials, Vol.20(4), 2018. P.3496-3509.
14. NordVPN. How Does a VPN Work? 2024. 229 p.
15. Zimperium. Mobile Threat Report, 2023. 312 p.
16. Symantec. Mobile Security: Risks of Unencrypted Data. 2022. 143 p.
17. K. Chen. Mobile Device Security and Data Encryption. Mobile Security Journal, 2023. P. 34.
18. Evergreen. Introducing Face ID — A System for Biometric Authentication of Your Employees. 2024. 105 p.

19. S. Kumar. The Importance of Encryption for Mobile Applications. Journal of Cybersecurity, 2022. P. 45.

20. Розуміння мобільних VPN: Простий посібник для підвищення безпеки в Інтернеті. Lebara UK Blog, 2023. 291 с.

21. Secret Double Octopus. What is Two-Factor Authentication. 2024. 119 p.

22. Ваншкевич І.І., Олійник О.В., та ін. Основи захисту інформації: навчальний посібник. Львів: ЛНУ ім. Івана Франка, 2020. 320 с.

23. Smith J. Mobile Device Management: Practical Solutions for Security and Efficiency. New York: TechPress, 2021. P. 123–125.

24. Malwarebytes. Mobile Security for Android and iOS, 2024. 117 p.

25. Smith A., Thompson M. Privacy and Security Risks in Mobile Applications: A Study of User Data Tracking. Cambridge University Press, 2022. P. 112-125.

26. Lee W., Kwon J. Vulnerabilities and Exploits in Bluetooth Low Energy. Springer International Publishing, 2021. P. 45-57.

27. Zhang Y., Liu X., Zhao X. Security Challenges in the Internet of Things (IoT): A Survey. Springer, 2023. P. 45-59.

28. Iqbal S.S., Khan M.A. Mobile Application Security Testing using MobSF Framework. Springer. 2020. P. 155-168.

29. Molyneux M., Douglas A. OWASP ZAP: The Open Web Application Security Project’s Tool for Penetration Testing. Wiley, 2021. P. 89-101.

30. Matsumoto A., Yamada Y. Security Testing for Mobile Devices with Frida and Dynamic Instrumentation. Elsevier, 2022. P. 72-80.

31. Hammad M., Simoens P. SecuWear: A Security Framework for Wearable Devices. Springer, 2019. P. 50-65.

32. Wang X., Sun Y. Testing Wearables: Integrating Security with Mobile and IoT Systems. IEEE Transactions on Mobile Computing, 2022. Vol.21(3). P.457-472.

33. Gajek S., Neumann S. Security of Bluetooth-Based Wearable Devices. Journal of Information Security and Applications, 2020. Vol. 21(3). P. 143-149.

34. Hale M.L., Lotfy K., Gamble R.F., Walter C., Lin J. Developing a Platform to Evaluate and Assess the Security of Wearable Devices. Digital Communications and Networks, 2019. Vol. 5(3). P. 147-159.

35. Hale M.L., Ellis D., Gamble R., Walter C., Lin J. SecuWear: An Open Source, Multi-Component Hardware/Software Platform for Exploring Wearable Security. IEEE International Conference on Mobile Services, 2015. P. 97-104.

36. Yu Z., Sood A.K., Sampalli S. Wearable Device Security: Vulnerabilities and Attacks. International Journal of Computer Applications, 2018. Vol.13(7). P.192-207.

37. Chen S., Zhang Y., Liu W. A Study on the Security of Wearable Devices and Its Countermeasures. Security and Privacy, 2020. Vol. 19(2). P.84-98.

38. Chien S., Wu M. Securing Wearable Devices: Strategies and Techniques. Springer Briefs in Computer Science, 2020. 295 p.

39. Zhao K., Liu J. Security and Privacy of Wearable Devices in Healthcare: A Survey. Computers, Materials & Continua, 2020. Vol. 64(1). P. 408.

ДОДАТОК А

Копії публікації

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2024)

науково-практична конференція
молодих вчених, аспірантів та студентів

26–28 серпня 2024
Тернопіль

Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. - 160 с.

Адреса редакції:
Західноукраїнський національний університет, кафедра кібербезпеки,
вул. Олени Теліги 8, м. Тернопіль 46003
Контакти:
*e-mail:*conferencekb@gmail.com

УДК 004.89

Марія МИКОЛИШИН

Західноукраїнський національний університет

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ

Вступ. Сучасні мобільні пристрої відіграють важливу роль у житті кожного користувача, адже саме вони зберігають величезну кількість приватної інформації, від особистих фотографій до банківських даних та ділової інформації. Кількість мобільних додатків, які використовують люди, стрімко зростає, так само, як і ризики, пов'язані з їх використанням.

Впровадження штучного інтелекту у забезпечення безпеки різноманітних мобільних додатків дозволяє значно підвищити захист користувацьких даних та знизити вразливість перед кібератаками, що і визначає актуальність даної роботи.

Мета: аналіз методів використання штучного інтелекту для підвищення безпеки мобільних додатків, виявлення ключових переваг застосування ШІ у цій галузі та наведення практичних прикладів інтеграції технологій ШІ у мобільні платформи.

1. Прогнозування кіберзагроз за допомогою штучного інтелекту

Штучний інтелект (ШІ) відкриває нові можливості для передбачення і прогнозування кіберзагроз, що є надзвичайно важливим для безпеки мобільних додатків. Технології машинного навчання та аналізу даних дозволяють системам безпеки мобільних додатків автоматично виявляти аномалії та потенційно небезпечні патерни, навіть ще до того, як вони можуть призвести до серйозних загроз.

Використовуючи алгоритми, ШІ може обробляти величезні обсяги інформації про попередні атаки, виявляти схожі моделі і створювати прогнози для майбутніх загроз, що дозволяє мобільним додаткам ефективно реагувати на можливі атаки в реальному часі.

Одним із основних аспектів є можливість ШІ ідентифікувати відхилення від звичайної поведінки користувачів або аномалії в мережевому трафіку. Наприклад, система може зафіксувати спроби входу з нових локацій, нестандартну активність або надмірну кількість транзакцій, що можуть свідчити про спробу злому або шахрайства.

Такий підхід дозволяє не тільки виявляти загрози, але й здійснювати превентивні заходи, знижуючи можливі збитки і зменшуючи час, необхідний для реагування на інциденти безпеки. У поєднанні з іншими методами, такими як аналіз великих даних, прогнозування на основі історичних атак забезпечує значно кращу захист мобільних додатків від кіберзагроз.

Використання ШІ для прогнозування кіберзагроз (рисунок 1) є особливо корисним в умовах, коли традиційні методи безпеки, як-от статичні алгоритми виявлення загроз, можуть бути недостатньо ефективними для боротьби з новими, раніше невідомими атаками.

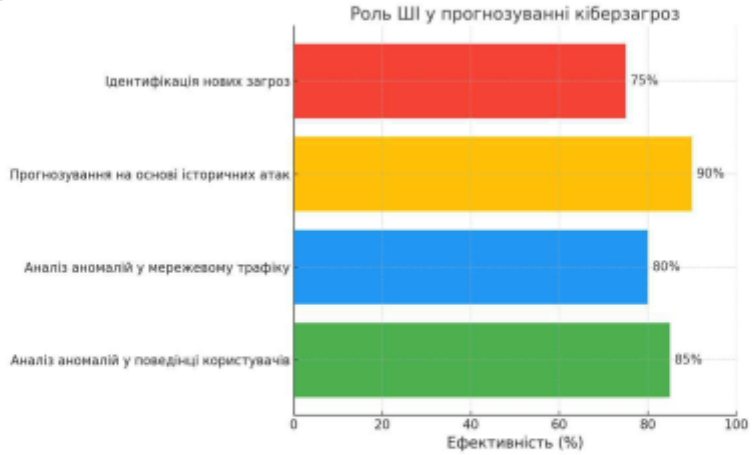

Рисунок 1 - Роль ШІ у прогнозуванні кіберзагроз

Оскільки атаки на мобільні додатки постійно змінюються і адаптуються до нових умов, прогнозування і проактивний підхід дозволяють швидко реагувати на нові види кіберзагроз, до того як вони завдадуть шкоди [1].

2. Машинне навчання для посилення шифрування і захисту даних мобільних додатків

ШІ та машинне навчання активно використовуються для вдосконалення методів шифрування і захисту даних у мобільних додатках, що є критично важливим для безпеки користувачів. Сучасні мобільні додатки зберігають величезні обсяги особистих даних, включаючи фінансову інформацію, особисті документи та конфіденційну переписку, що робить їх привабливою ціллю для кіберзлочинців. Машинне навчання дозволяє створювати більш складні і адаптивні методи шифрування, що можуть швидко реагувати на нові загрози та вдосконалюватися з часом, вивчаючи поведінку кіберзлочинців і виявляючи їхні нові стратегії.

Однією з важливих переваг використання машинного навчання для шифрування є здатність адаптувати системи шифрування до нових типів атак, таких як атаки через квантові обчислення або спроби злому через слабкі паролі. Наприклад, алгоритми ШІ можуть бути використані для виявлення та посилення вразливостей в алгоритмах шифрування на основі змінних умов, таких як місце розташування користувача або поведінка його пристрою. Це дозволяє значно підвищити рівень захисту даних, роблячи їх менш вразливими до атак.

Дослідження, проведене командою фахівців з Університету Каліфорнії в Лос-Анджелесі (UCLA), показало, що застосування машинного навчання для криптографії значно збільшує ефективність шифрування. Вони використовували методи глибокого навчання для автоматичного виявлення нових слабких місць у алгоритмах шифрування і створення адаптивних захисних механізмів, здатних швидко реагувати на зміни в атаках.

За словами авторів, такі підходи значно покращують безпеку мобільних додатків, роблячи їх більш стійкими до нових загроз і знижуючи ймовірність

витоку конфіденційної інформації [2].

Машинне навчання також допомагає у вдосконаленні методів генерації паролів і аутентифікації, що є критичними для захисту користувачів. Алгоритми можуть аналізувати патерни поведінки користувачів і створювати більш складні, але при цьому зручні для запам'ятовування паролі.

Крім того, система машинного навчання може автоматично виявляти слабкі паролі і пропонувати користувачам замінити їх на більш безпечні варіанти, що значно знижує ризик злому акаунтів.

Інші дослідження підтверджують, що використання методів машинного навчання в комбінації з багатофакторною аутентифікацією дозволяє значно посилити захист даних. У дослідженні, опублікованому в журналі Computers Security, зазначено, що системи з використанням машинного навчання і біометрії для аутентифікації користувачів забезпечують більш високий рівень безпеки, ніж традиційні методи паролів [3].

Це важливо, оскільки з кожним роком збільшується кількість інцидентів, пов'язаних із крадіжкою паролів та іншими формами несанкціонованого доступу до особистих даних користувачів мобільних додатків .

ШІ також допомагає у постійному оновленні алгоритмів шифрування, що дозволяє створювати системи, які адаптуються до нових атак в реальному часі. Завдяки таким підходам мобільні додатки можуть не тільки захищати дані, але й забезпечувати найвищий рівень конфіденційності для своїх користувачів, що є важливим фактором для збереження їх довіри та безпеки в цифровому середовищі.

Висновок. У роботі проаналізовано застосування штучного інтелекту для підвищення безпеки мобільних додатків. Зокрема, розглянуто можливості прогнозування кіберзагроз за допомогою машинного навчання, яке дозволяє своєчасно виявляти аномалії і знижувати ризик атак.

Крім того, приділено увагу використанню ШІ для вдосконалення методів шифрування даних та аутентифікації, що забезпечує більш високий рівень захисту персональної інформації користувачів.

Перелік використаних джерел.

1. Samar, S. (2022). AI-based threat prediction models for mobile application security. Journal of Cyber Security and Technology.

2. Chen, Z., Zhou, X. (2022). Machine learning-based cryptographic systems for mobile application security. Computers Security.

3. Ruan, K., Liu, T. (2023). Adaptive encryption methods for mobile app data protection using AI. Journal of Artificial Intelligence and Security.

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2024
Тернопіль

У збірнику опубліковано матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. - 130с.

Технічний редактор: Давлетова А.Я.

Адреса редакції:
Громадська організація «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: conferencekb@gmail.com

УДК 004.056.2

Марія МИКОЛИШИН

Західноукраїнський національний університет

РОЗВИТОК СТАНДАРТІВ БЕЗПЕКИ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Вступ. Сьогодні мобільні пристрої є невід'ємною частиною нашого повсякденного життя. Вони містять багато конфіденційної інформації, як-от особисті дані та робочі документи, що робить їх привабливою ціллю для кіберзлочинців. З кожним роком загроза витоку даних зростає, тому потреба у стандартах безпеки для мобільних пристроїв стає критичною. Основна мета таких стандартів - забезпечення захисту даних та зниження ризиків, пов'язаних з кіберзагрозами. Тому тема роботи є актуальною.

Мета: аналіз розвитку стандартів безпеки мобільних пристроїв, характеристика їхніх основних принципів, а також розкриття їхньої ролі у захисті інформації користувачів.

1. Аналіз розвитку стандартів безпеки мобільних пристроїв

Розвиток стандартів безпеки мобільних пристроїв є реакцією на зростаючі загрози інформаційної безпеки, пов’язані з використанням мобільних технологій. Ранні моделі мобільних пристроїв не передбачали значного рівня захисту, адже їх функції були обмежені телефонними дзвінками та текстовими повідомленнями. Проте з появою смартфонів, які зберігають персональні та робочі дані користувачів, потреба у стандартах для забезпечення конфіденційності, цілісності та доступності інформації стала очевидною.

Міжнародна організація зі стандартизації (ISO) та Інститут стандартів і технологій США (NIST) були одними з перших організацій, які почали розробку стандартів безпеки для мобільних пристроїв. Наприклад, ISO/IEC 27001 визначає вимоги до систем управління інформаційною безпекою, що використовуються для захисту корпоративних мобільних пристроїв [1].

У той же час, стандарт NIST SP 800-124 охоплює рекомендації щодо управління мобільними додатками та операційними системами, зокрема в корпоративних середовищах, де ризики можуть бути значно вищими [2].

З розвитком технологій стандарти також еволюціонували. Наразі активно використовуються підходи до управління ризиками, що враховують новітні загрози, такі як соціальна інженерія, зловмисні мобільні додатки та фішинг. Графік на рисунку 1 ілюструє серйозність загроз для мобільних пристроїв: у 2023 році було зафіксовано та заблоковано понад 33 мільйони атак, спрямованих на мобільні пристрої, що на приблизно 52% більше, ніж у попередньому році [3].

Крім того, важливу роль почали відігравати стандарти, пов'язані з управлінням мобільними пристроями в корпоративному середовищі (MDM) та їх захистом через багатофакторну автентифікацію, шифрування даних, моніторинг та аналіз поведінки користувачів.

Розробка стандартів для новітніх технологій, таких як Інтернет речей (IoT) та мережі 5G, стала важливим пріоритетом у сфері інформаційної безпеки. Ці інновації не лише значно розширюють функціональні можливості мобільних пристроїв, але й відкривають нові

потенційні шляхи для атак, оскільки підключені пристрої взаємодіють через численні мережі та обмінюються великими обсягами даних. Відтак, сучасні стандарти безпеки повинні охоплювати не лише захист окремих пристроїв, а й передбачати комплексний захист інформації на всіх рівнях взаємодії між пристроями, мережами та хмарними сервісами.

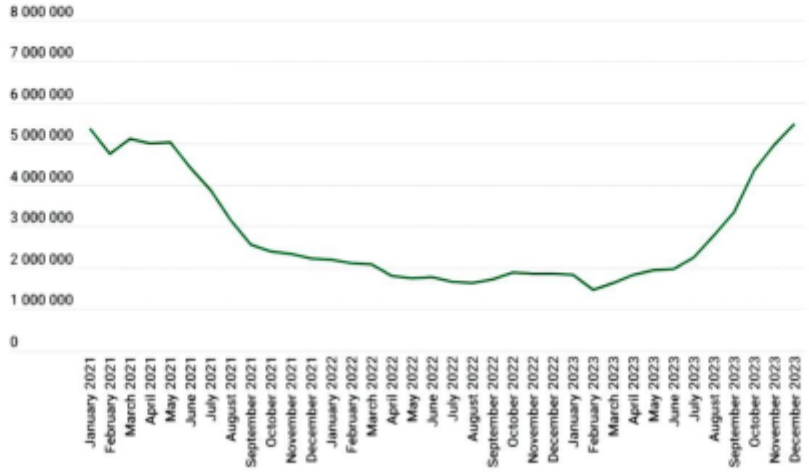

Рисунок 1 - Динаміка атак на мобільні пристрої, 2023 рік

Зокрема, для IoT важливо враховувати захист кожного елемента в розподілених мережах, включаючи датчики, контролери та кінцеві пристрої, оскільки кожен з них може стати вразливим для зовнішнього втручання. Мережі 5G, зі свого боку, забезпечують високу швидкість передачі даних, але також ускладнюють контроль безпеки через зростаючу кількість підключень та розширену архітектуру. Це ставить додаткові вимоги до стандартів безпеки, що мають враховувати безпеку як на рівні апаратного забезпечення, так і на рівні програмного забезпечення.

Таким чином, сучасні стандарти повинні бути адаптивними та забезпечувати багаторівневий захист, щоб гарантувати безпеку як традиційних мобільних пристроїв, так і нових інтегрованих систем, що використовують IoT та 5G.

2. Характеристика основних принципів стандартів безпеки мобільних пристроїв

Основні принципи стандартів безпеки мобільних пристроїв спрямовані на забезпечення захисту даних, конфіденційності користувачів і цілісності інформації. Ці принципи включають:

1. Конфіденційність: стандарти повинні гарантувати, що лише уповноважені користувачі мають доступ до чутливої інформації. Це досягається через використання методів аутентифікації, таких як паролі, біометричні дані або багатофакторна автентифікація, що допомагають у запобіганні несанкціонованому доступу.

2. Цілісність: датчики та програмне забезпечення мобільних пристроїв повинні захищати дані від несанкціонованих змін. Це означає, що будь-яка інформація, що передається або зберігається, повинна бути перевірена на достовірність, щоб уникнути підробки або втрати даних.

3. Доступність: мобільні пристрої повинні забезпечувати постійний доступ до даних для авторизованих користувачів, уникаючи збоїв у роботі системи. Це включає в себе надійні механізми резервного копіювання та відновлення, які можуть відновити дані у випадку втрати або атаки.

4. Управління ризиками: стандарти повинні включати систематичний підхід до управління ризиками, що передбачає ідентифікацію, аналіз та оцінку ризиків, пов'язаних із використанням мобільних пристроїв. Це дозволяє підприємствам вчасно вживати заходів для захисту інформації.

5. Прозорість: важливо, щоб користувачі були інформовані про політики безпеки, методи захисту та можливі ризики, пов'язані з використанням мобільних пристроїв. Прозорість у комунікаціях підвищує довіру до технологій та забезпечує більш відповідальне використання.

6. Сумісність і стандартизація: для забезпечення ефективності захисту інформації мобільних пристроїв необхідно дотримуватися загальноприйнятих стандартів і протоколів. Це забезпечує не лише взаємодію між різними системами, але й узгодженість у реалізації заходів безпеки.

Ці принципи формують основи для розробки ефективних стандартів безпеки інформації, які адаптуються до постійно змінюваного технологічного середовища. Вони допомагають організаціям забезпечити безпеку своїх мобільних пристроїв і захистити дані своїх користувачів від загроз, кількість яких зростає [4].

3. Роль стандартів безпеки мобільних пристроїв у захисті інформації користувачів

Стандарти безпеки мобільних пристроїв відіграють ключову роль у захисті інформації користувачів, оскільки зростаюча залежність від мобільних технологій супроводжується зростанням загроз інформаційній безпеці. У світі, де особисті дані, фінансова інформація та конфіденційні комунікації зберігаються та передаються через мобільні пристрої, надійний захист інформації стає критично важливим.

По-перше, стандарти безпеки надають основу для розробки ефективних механізмів захисту, які використовуються виробниками мобільних пристроїв та розробниками програмного забезпечення. Сучасні рішення включають комплексний підхід до безпеки інформації, де основними складовими є шифрування даних, аутентифікація користувачів, контроль доступу, а також регулярні оновлення безпеки. Це дозволяє оперативно усувати вразливості, адаптуючись до нових викликів і забезпечуючи постійний захист від змінних загроз.

По-друге, дотримання стандартів суттєво підвищує рівень довіри споживачів до мобільних технологій. Користувачі, впевнені в надійному захисті своїх даних, частіше готові використовувати мобільні пристрої для зберігання чутливої інформації та здійснення

фінансових операцій. Це також стимулює розробників та виробників технологій до інновацій, оскільки вони прагнуть відповідати зростаючим вимогам та очікуванням користувачів, створюючи нові безпечні рішення.

Крім того, стандарти безпеки сприяють зменшенню ризиків, пов'язаних із мобільними атаками, шляхом надання чітких рекомендацій щодо розпізнавання та реагування на різноманітні загрози. Це дозволяє як організаціям, так і звичайним користувачам своєчасно вживати заходів для захисту пристроїв. Наприклад, підвищення обізнаності про ризики, такі як фішинг, шкідливі програми або інші види атак, допомагає користувачам уникати небезпечних ситуацій та значно знижує ймовірність компрометації їхніх даних.

Нарешті, стандарти безпеки мобільних пристроїв мають широку роль у формуванні загальної екосистеми безпеки, що об'єднує постачальників послуг, розробників програмного забезпечення та користувачів у єдине середовище з чіткими правилами. Це дозволяє усім учасникам діяти з упевненістю, знаючи, що їхня інформація надійно захищена, а приватність збережена.

Таким чином, стандарти безпеки мобільних пристроїв є невід'ємним елементом забезпечення інформаційної безпеки користувачів, оскільки вони захищають особисті дані, сприяють довірі до нових технологій, знижують ризики кібератак і створюють умови для безпечного використання мобільних пристроїв у сучасному цифровому світі.

Висновок. У роботі проаналізовано розвиток стандартів безпеки мобільних пристроїв, охарактеризовано їх основні принципи та розглянуто їхню важливу роль у забезпеченні захисту інформації користувачів. Встановлено, що ці стандарти допомагають запобігати кіберзагрозам та формують довіру до новітніх технологій, підкреслюючи необхідність їх дотримання для створення безпечного цифрового середовища.

Перелік використаних джерел.

1. ISO Standard: International Organization for Standardization. A critical review of practices and challenges in intrusion detection systems for iot: toward universal and resilient systems. IEEE Commun. Surv. Tutorials, 20 (4) (2018), pp. 3496-3509.

2. NIST Publication: National Institute of Standards and Technology. NIST Special Publication 800-124 Revision 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise. (2013).

3. Kivva, Anton. «The Mobile Malware Threat Landscape in 2023.»

4. K. R. Choo, C. H. Lee. The importance of information security in mobile devices: A perspective from users' and organizations' security. IEEE Commun. Surv. Tutorials, 20 (3) (2018), pp. 2678-2690.