НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2019 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Методика аналізу безпеки BLE пристроїв на прикладі фітнес-трекера

Виконав (-ла): студент (-ка) ____ курсу, групи _____
(шифр групи)

Майстренко Олег Миколайович

_____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Коломицев Михайло Володимирович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BLE – Bluetooth Low Energy

LE – Low Energy

GATT – Generic Attribute Profile

ATT – Attribute Protocol

SMP - Security Manager Protocol

HCI – Host Controller Interface

OOB – Out Of Band

LTK - Long Term Key

UUID – Universally Unique Identifier

ВСТУП

Актуальність роботи. З кожним роком на ринку з'являється все більше пристроїв що використовують технологію Bluetooth Low Energy. Ці пристрої все більше стають пов'язаними із нашим повсякденним життям. На базі BLE працюють пристрої екосистеми розумного дому, різноманітні носимі пристрої типу навушників чи фітнес трекерів. BLE навіть використовується в керуванні мобільним електротранспортом (електро самокати та електро скейтборди). Саме тому, перевірка та можливість вдосконалення безпеки пристроїв що нас оточують є, по суті, підвищенням рівня своєї захищеності. Адже завжди існує загроза витоку даних, або ж їх підміна. А якщо зловмисник перехопить контроль над транспортом, то це вже становитиме ще й небезпеку для нашого життя.

Об'єктом дослідження є пристрої Bluetooth Low Energy.

Предметом дослідження є безпека пристроїв Bluetooth Low Energy.

Метою роботи є розробка методики аналізу безпеки пристроїв Bluetooth Low Energy, на основі проведеного дослідження фітнес трекера та опрацьованих теоретичних матеріалів щодо безпеки BLE.

Завдання роботи:

1. Дослідити принципи роботи технології Bluetooth Low Energy.
2. Ознайомитися з існуючими дослідженнями, методами дослідження та рекомендаціями щодо безпеки BLE.
3. Здійснити аналіз безпеки пристрою BLE – фітнес трекера.
4. На основі проаналізованого теоретичного матеріалу та проведеного дослідження розробити та запропонувати методику аналізу безпеки пристроїв BLE.

Методи дослідження - ознайомлення та опрацювання літератури, що представлено монографічними та журнальними матеріалами, електронними ресурсами, які стосуються досліджуваної теми, аналіз існуючих шляхів вирішення проблеми, проведення власного дослідження.

Наукова новизна полягає в тому, що розроблена методика є повним рішенням, в якому викладено основні аспекти перевірки безпеки пристроїв Bluetooth Low Energy, описані важливість кожного з аспектів та методи перевірки.

Результати роботи викладені у третьому розділі, що демонструють практичну роботу нової методики.

Практична значущість результатів. Результати даної роботи можуть бути використані при розробці або ж вдосконаленні пристроїв BLE.

Публікації: результати магістерської дисертації опубліковані у статті «Методика аналізу безпеки BLE пристроїв».

1 ОГЛЯД ТЕХНОЛОГІЇ BLUETOOTH LOW ENERGY

Bluetooth Low Energy (BLE) – дуже поширена технологія бездротового зв'язку, яка широко застосовується в IoT. Наприклад, медичні програми, включаючи моніторинг артеріального тиску та рентгенівські знімки, а також носимі пристрої[1]. Перша специфікація Bluetooth була розроблена групою Bluetooth Special Interest Group (Bluetooth SIG) в 1998 році і опублікована як частина стандарту IEEE 802.15.1 14 червня 2002 року. В даний час існують наступні специфікації:

- 1998-1999: Bluetooth 1.0 and 1.0B – виведена з експлуатації з 2006 року;
- 2001: Bluetooth 1.1 – виведена з експлуатації з 2006 року;
- 2003: Bluetooth 1.2 – виведена з експлуатації з 2009 року;
- 2004: Bluetooth 2.0 + EDR - застаріла в 2014 році, буде виведена з експлуатації в 2019 році;
- 2008: Bluetooth 2.1 + EDR – вважається застарілою, буде виведена з експлуатації в 2020 році;
- 2009: Bluetooth 3.0 + HS – вважається застарілою, буде виведена з експлуатації в 2020 році;
- 2010: Bluetooth 4.0 – вважається застарілою, буде виведена з експлуатації в 2020 році;
- 2013: Bluetooth 4.1 - вважається застарілою, буде виведена з експлуатації в 2020 році;
- 2014: Bluetooth 4.2
- 2016: Bluetooth 5.0

BLE має дві важливі особливості: низьке споживання енергії, що дає змогу збільшити термін експлуатації пристроїв BLE, що працюють від акумуляторів та фреймворк GATT (Generic Attribute Profile), щоб забезпечити програмам для

мобільних пристроїв, планшетів та ПК довільну передачу даних на однорангові пристрої BLE[2].

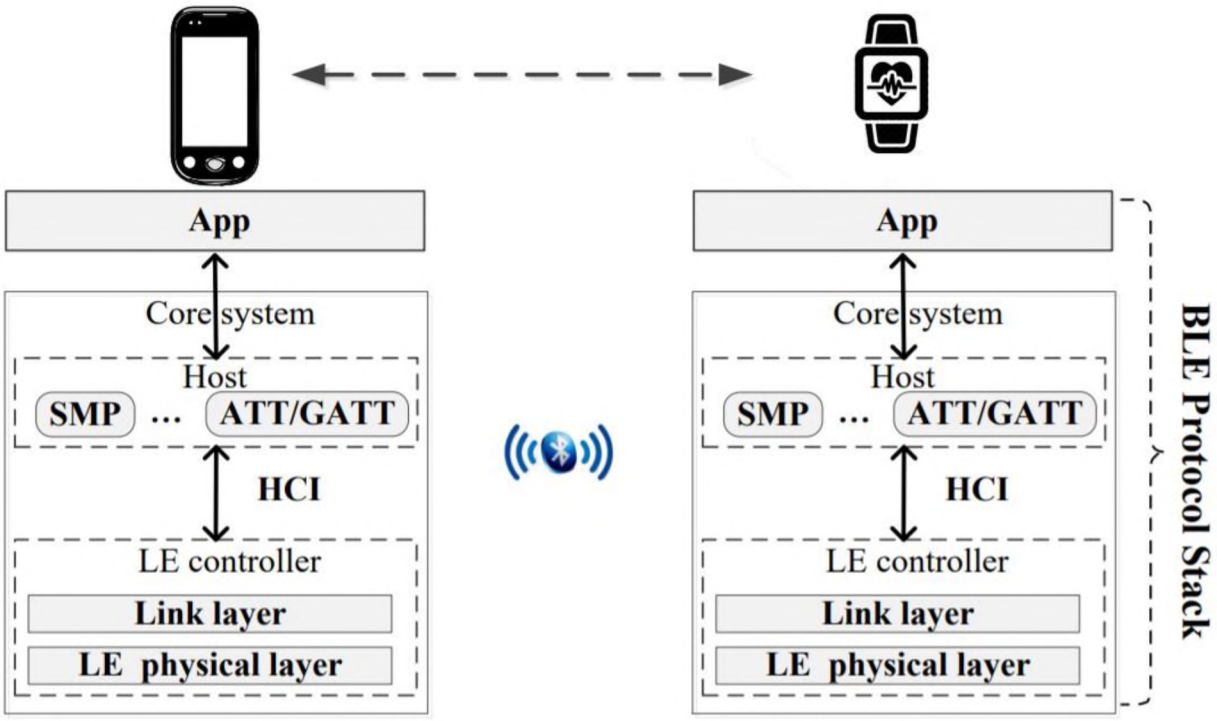

Рисунок 1.1 – Стек протоколу BLE

BLE – технологія зв'язку малої дальності. На Рисунку 1.1 показаний її стек протоколів, де фітнес трекер використовується як зразковий пристрій BLE. У цьому прикладі додаток трекера вимірює артеріальний тиск. Додаток для керування трекером та мобільний додаток використовують основну систему BLE для спілкування. Основна система BLE складається з двох будівельних блоків, контролера LE та хосту. Контролер LE використовує рівень зв'язку та фізичний рівень для створення з'єднання для надсилання/прийому даних. Хост реалізує кілька протоколів, включаючи протокол менеджера безпеки (SMP) та ATT для безпечного зв'язку через з'єднання. ATT використовується для форматування переданих даних. SMP використовує протоколи сполучення для узгодження криптографічних ключів для шифрування даних, цілісність та інші цілі.

Інтерфейс хост-контролера (HCI) – це тонкий шар, який транспортує команди та події між хост-елементами та контролерами стека протоколу Bluetooth.

1.1 Створення з'єднання

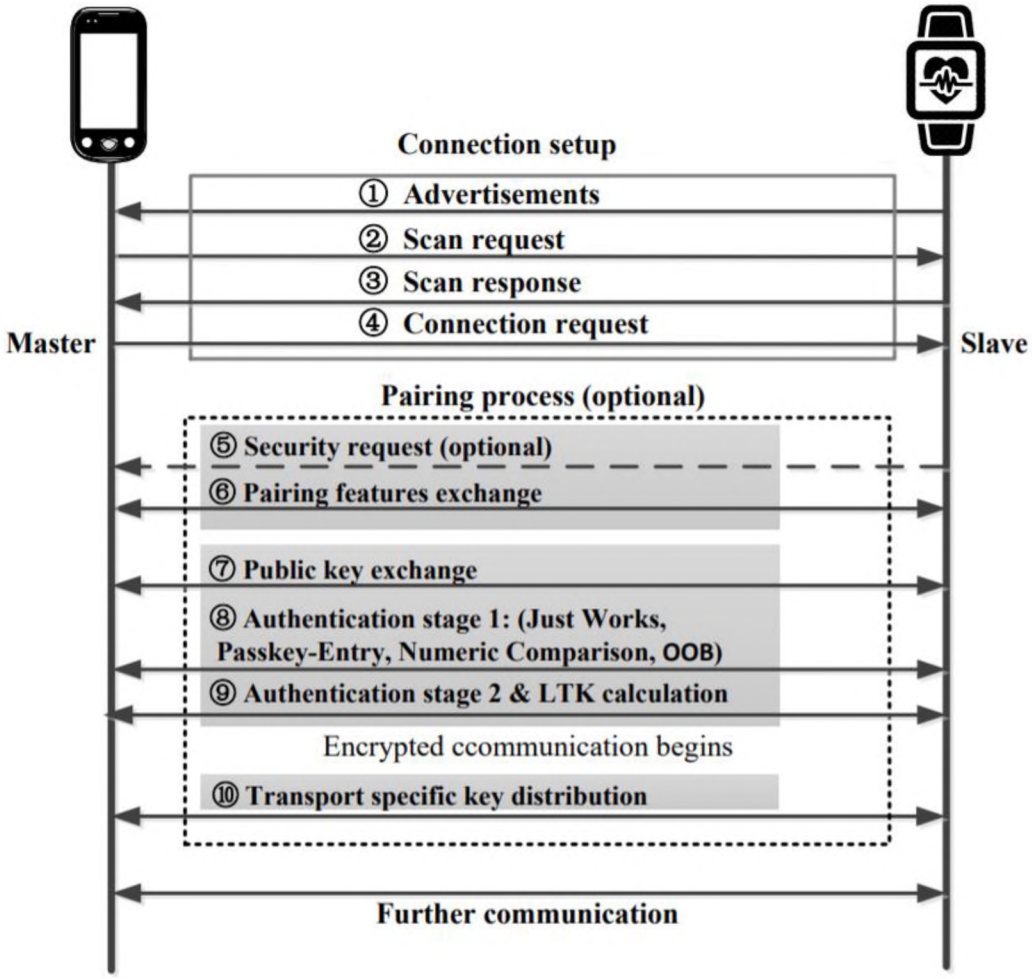

Рисунок 1.2 – Стек протоколу BLE

Кроки 1 - 4 на Рисунку 1.2 ілюструють типовий процес налаштування з'єднання BLE. Точна інформація, якою обмінюються пристрої на кожному кроці, залежить від додатків. На першому кроці фітнес трекер транслює рекламні пакети із зазначенням його доступності. Коли запускається мобільний додаток, програма використовує хост і отримує рекламу. На другому кроці мобільний додаток

надсилає на трекер запит на сканування. Третій крок – фітнес трекер надсилає пакет-відповідь на сканування. Мобільний додаток використовує рекламні пакети та сканування для збору інформації про фітнес трекер, наприклад, ім'я трекера, MAC-адреса та основні сервіси. На четвертому кроці мобільний додаток визначає, чи це саме цей пристрій до якого потрібно підключитись, і надсилає запит на створення з'єднання. Інкремент частотних стрибків включено в запит на з'єднання, який визначає послідовність стрибків, за якою дотримуватимуться мобільний пристрій та фітнес трекер під час зв'язку. В даному випадку мобільний телефон називається мастер/ініціатором за його роль у ініціюванні з'єднання. Пристрій BLE, фітнес трекер, в даному випадку називається слейв/респондентом.

1.2 Процес утворення пари

Після того, як два пристрої BLE встановили з'єднання, та якщо немає пристрою, який явно вимагає створення пари, спілкування продовжується відкритим текстом.

Щоб зашифрувати комунікацію два пристрої повинні запустити процес створення пари та процес узгодження ключів.

Кроки 5 - 9 на Рисунку 1.2 ілюструють типовий процес сполучення. Мобільний додаток може ініціювати процес сполучення через SMP (Рисунок 1.1). Кінцевий користувач також може використовувати системне налаштування додаток для запуску процесу з’єднання.

1.2.1 Фаза 1 - Обмін ознаками створення пари

Крок 5 – запит безпеки (необов'язково). Як пристрій-слейв, фітнес трекер може надіслати запит безпеки та попросити мобільний пристрій (мастер) ініціювати процес створення пари.

Крок 6 - Обмін функціями процесу створення пари. Мобільний додаток надсилає запит на створення пари і фітнес трекер повертає відповідь. Потім два пристрої оголошують свої можливості введення/виводу інформації, такі як клавіатура чи дисплей, вимоги аутентифікації та версія BLE, щоб можна було узгодити відповідний загальний протокол створення пари.

Вимоги до аутентифікації можуть бути зв'язуванням та захистом від MITM. Зв'язування означає, що ключі, згенеровані під час процесу з'єднання, будуть збережені для подальшого використання, щоб зменшити затримку, викликану майбутнім процесом сполучення. Якщо пристрій хоче захищатись від атаки MITM, прапор MITM[3] повинен бути вказаний таким чином, щоб було прийнято протокол введення пароля(Passkey Entry) або протокол порівняння чисел(Numeric Comparison). Отримані пристроями можливості вводу/виводу допоможуть вибрати протокол зв'язку, оскільки різні протоколи сполучення вимагають різних можливостей вводу/виводу. Наприклад, числове порівняння вимагає відображення на обох пристроях.

Якщо є вимоги аутентифікації, але функції вводу/виводу не можуть підтримувати вказане захищене сполучення, згідно зі специфікацією BLE, зв'язок припиняється і користувач буде повідомлений.

Якщо два пристрої явно встановили значення прапору MITM false, то вибирається протокол Just Works, який не може захищати від атаки MITM.

1.2.2 Фаза 2 – Обмін ключами та аутентифікація

Крок 7 – обмін відкритими ключами. Рекомендується використовувати протокол обміну ключами Діффі-Хеллмана (ECDH). Так пристрої отримують відкриті ключі один одного і генерують симетричний ключ(DHKey).

Крок 8 – перший етап аутентифікації (критичний крок до безпеки BLE). На цьому етапі інформація, пов'язана з аутентифікацією, обмінюється між двома пристроями. Вводиться PIN-код, якщо використовується ключ доступу. Якщо використовується порівняння чисел, то на двох пристроях відображається 6-значний номер. Також запускається процедура перевірки, щоб переконатися, що відкриті ключі, якими пристрої обмінялися на етапі 7, від призначених пристроїв.

Крок 9 – другий етап аутентифікації та розрахунок LTK. Інформація про автентифікацію, якою пристрої обмінялись раніше, включаючи DHKey, використовується для генерації ключа MacKey та Long Term Key (LTK) на двох пристроях. MacKey використовується для того, щоб гарантувати, що обидва пристрої генерують однаковий LTK. Якщо зв'язування відбувається на етапі 6, LTK зберігається для подальшої генерації ключа та шифрування з'єднання.

BLE визначає два типи ключів, unauthenticated-and-no-MITM-protection ключі для Just Works, та authenticated-and-MITM-protection ключі для введення пароля, числового порівняння та OOB.

Також, для кращого розуміння, варто розглянути вище згадані протоколи асоціації. В Bluetooth 4.2 для BLE доступні чотири протоколи асоціації:

- Numeric Comparison
- Just Works
- Passkey Entry

- Out of Band (OOB)

У Таблиці 1.1 показана модель асоціації, яка може бути використана на основі можливостей вводу/виводу, коли для з'єднання використовується LE Secure Connections. Однак можливості вводу/виводу можна ігнорувати, коли захист MITM не потрібен або дані OOB доступні на будь-якому з пристроїв BLE.

Перш ніж детально обговорити ці моделі асоціацій, нам потрібно визначити пару термінів, які використовуються спільно з моделями:

• Rand / nonce: Rand або nonce являє собою 16-байтові випадкові числа, які обмінюються між пристроями парування під час етапу аутентифікації. Ці випадкові числа використовуються для отримання підтверджуючих значень.

• Підтверджувальне значення: підтверджувальні значення, що мають довжину 16 байт, обмінюються між пристроями парування під час етапу аутентифікації. Підтвердження значень генерується шляхом хешування значень, обмінюваних у пакетах сполучення до цієї точки. Сюди можуть входити об'єкти із запиту на з'єднання, відповіді про парування, випадкових чисел (rand) та відкритих ключів.

Таблиця 1.1 – Відповідність моделі асоціації можливостям вводу/виводу

	ІНІЦІАТОР					
ВІДПОВІДАЧ	вхід/вихід	Лише дисплей	Дисплей, так/ні	Лише клавіатура	Без входу/виходу	Клавіатура, дисплей
Лише дисплей	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry	
Дисплей, так/ні	Just Works	Numeric Comparsion	Passkey Entry	Just Works	Numeric Comparsion	

Кінець таблиці 1.1

	Лише клавіатура	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
	Без входу/виходу	Just Works	Just Works	Just Works	Just Works	Just Works
	Клавіатура, дисплей	Passkey Entry	Numeric Comparsion	Passkey Entry	Just Works	Numeric Comparsion

Порівняння чисел (BLE 4.2 і вище)

Числове порівняння застосовується, коли на обох пристроях є дисплеї та кнопки підтвердження. Після обміну ключами ECDH обидва пристрої BLE обмінюються парою значень (крок 8 на Рисунку 1.2). Потім на пристроях, базуючись на отриманих значеннях перевірки та ключах, генеруються числові значення, які відображаються засобами виводу(дисплеями). Користувач підтверджує, що два відображених числа однакові, натискаючи кнопку «Так» на дисплеї кожного пристрою, щоб продовжити процес з'єднання. Той факт, що два відображених номера однакові, гарантує, що в обміні ключами та значеннями брали участь потрібні пристрої, а не пристрої зловмисника.

Passkey Entry

У моделі асоціації Passkey Entry користувач або вводить ідентичний ключ доступу до обох пристроїв, або один пристрій відображає пароль, і користувач вводить цей пароль на іншому пристрої. Обидва пристрої обчислюють значення підтвердження, використовуючи функцію AES-CMAC з відкритим ключем кожного пристрою, локально генерованим nonce та одним бітом пароля доступу. Потім обидва пристрої обмінюються своїм nonce і підтверджуючим значенням.

Після цього вони обчислюють значення підтвердження, використовуючи відкритий ключ обох пристроїв, невідоме, отримане від однорангового пристрою, і один біт Passkey. Потім пристрої порівнюють обидва підтверджені значення.

У Bluetooth Low Energy 4.2 кроки для підтвердження генерації значення повторюються для загальної кількості бітів ключа (тобто 20 разів для шестизначного десяткового числа). Обмін ключами по одному біту в Bluetooth 4.2 є важливим доповненням до застарілої моделі введення пароля (Bluetooth 4.1 або старішої версії), в якій весь ключ обміну передається в одному блоці даних протоколу підтвердження (PDU).

Out of Band (OOB)

Модель асоціації OOB застосовується незалежно від вимоги до MITM та/або можливостей вводу/виводу, якщо принаймні один пристрій з можливістю OOB вже має криптографічну інформацію, обмінювану поза діапазоном. Під час процесу аутентифікації лише ці значення підтверджуються за допомогою функції AES-CMAC. Тут захист від MITM залежить від опору MITM атакам протоколу OOB, який використовується для обміну інформацією. У BLE 4.1 або старіше обидва пристрої повинні мати можливості OOB, щоб використовувати модель асоціації OOB.

Just Works

Модель Just Works розроблена для пристроїв без можливостей вводу/виводу і піддається атакам MITM. Just Works має майже той самий процес сполучення, що і порівняння чисел, за винятком того, що шестизначне число не генерується і не відображається, а користувач не може впевнитись в тому, що обміняні ключі однакові.

1.2.3 Фаза 3 - Розподіл ключів

Зв'язок після Фази 2 буде зашифрований за допомогою SessionKey, згенерованого з LTK. Шифрування BLE використовує AESCCM (лічильник з CBC-MAC), а один SessionKey забезпечує автентифікацію та конфіденційність.

На Фазі 3 мастер і слейв можуть обмінюватися ключами, включаючи Identity Resolving Key (IRK) для ідентичності пристрою та конфіденційності. Пристрої BLE, такі як мобільні телефони, можна відстежувати, якщо MAC-адреса використовується і в рекламі і в подальшому спілкуванні. В BLE ця проблема конфіденційності вирішується за допомогою IRK та набору протоколів.

IRK дозволяє першому пристрою переводити спеціальні, випадкові MAC адреси, які з'являються в рекламних пакетах з другого пристрою, на реальну MAC-адресу другого пристрою. Ця можливість є лише на пристроях, яким ви явно довіряли.

Взагалі, ці випадкові приватні MAC-адреси змінюються відповідно до таймера, який виробник впроваджує у програмне забезпечення свого продукту. Тому вони точно знають, як часто змінюватиметься MAC-адреса. Але є одна особлива ситуація, створена для того, щоб пристрої, які раніше з'єднувались між собою, дійсно швидко підключалися, в якій цей таймер не використовується.

Пристрої можуть використовувати так звану "спрямовану рекламу". У спрямованій рекламі рекламні пакети вказують як MAC-адресу пристрою, що робить рекламу, так і MAC-адресу пристрою, на який рекламується. Це як надіслати запрошення на певний пристрій, з яким у вас були попередні стосунки, сказавши: "Ей, якщо ви там, будь-ласка, знову підключіться до мене!".

MAC-адреса, яка використовується рекламним пристроєм, є випадковою адресою, якщо LE конфіденційність використовується, але для цієї ситуації це

особливий тип приватної адреси, який називається "адреса повторного з'єднання". Адреси для повторного з'єднання відрізняються від приватних адрес, що використовуються в інших обставинах, оскільки вони змінюються, але не таймером. Натомість дії користувача, як-от увімкнення та вимкнення пристрою або встановлення нового з'єднання, ініціює зміну адреси. Щоб надати виробникам більше можливостей, Bluetooth 4.2 дозволяє приватним адресам повторного з'єднання також змінюватись на нові, випадкові адресі, використовуючи той самий механізм, що базується на таймері, щоб виробники мали повний контроль над тим, як поводиться їх товар щодо конфіденційності та приватних адрес. Перетворення приватних адрес за допомогою криптографічного ключа IRK назад до реальної MAC-адреси пристрою тепер набагато швидше і набагато ефективнішие, оскільки воно відбувається в Контролері, а не в хості в архітектурі Bluetooth Smart[4].

1.3 Режими безпеки BLE

Для підключення BLE, протокол загального доступу (GAP) визначає два режими захисту разом з декількома рівнями безпеки в режимі.

Режим безпеки 1

Режим безпеки 1 забезпечує захист за допомогою шифрування і містить чотири рівні:

- рівень безпеки 1: відсутність безпеки (відсутність автентифікації та без шифрування)
- рівень безпеки 2: несанкціоноване сполучення з шифруванням

- рівень безпеки 3: аутентифіковане парування з шифруванням AES-CCM
- рівень безпеки 4: Автентифіковані захищені з'єднання LE, з'єднання з шифруванням.

Рівень 4 використовує Еліптичну криву Diffie-Hellman P-256 (ECDH) та AES-CCM шифрування.

Режим безпеки 2

Режим безпеки 2 забезпечує захист за допомогою підпису даних і містить два рівні:

- Рівень безпеки 1: Несанкціоноване з'єднання з підписанням даних
- Рівень безпеки 2: Аутентифіковане парування з підписом даних

Змішаний режим безпеки

Змішаний режим безпеки – це коли пристрій потребує підтримки як режим безпеки 1, так і 2, тобто він повинен підтримувати підписані та непідписані дані.

Кожне з'єднання починає своє життя в режимі безпеки 1, рівень 1 і пізніше може бути оновлено до будь-якого рівня безпеки за допомогою процедури аутентифікації, обговореної вище. Під час створення пари обраний метод/алгоритм визначає, чи спарювання виконувало сильну аутентифікацію чи ні. Неаутентифіковані спарювання виникають у ситуаціях, коли пристрій не зміг пройти автентифікацію (наприклад, якщо у нього немає можливостей введення/виводу).

Для підлеглого пристрою, який надає послуги, специфікація BLE визначає режим лише безпечних з'єднань. Цей режим забезпечує найвищий рівень безпеки BLE (Режим 1, рівень 4), в якому можуть використовуватися лише три протоколи безпечного з'єднання, введення пароля, порівняння чисел та захищений OOB, і BLE Legacy заборонено. У цьому режимі, якщо не використовується захищене сполучення, пристрій надсилає пакет провалу створення пари з кодом помилки "Authentication Requirements". Відповідно до специфікації BLE [5], коли пристрій перебуває в режимі Secure Connections Only, "Пристрій може приймати нові вихідні та вхідні з'єднання рівня послуг для служб, для яких потрібен режим безпеки 1, рівень 4, лише в тому випадку, якщо віддалений пристрій підтримує LE Secure з'єднання та автентифіковане з'єднання". Тут підключення на рівні сервісу відноситься до з'єднання рівня додатка. Можна помітити, що BLE вказує використання режиму Secure Connections Only для підлеглого, який надає послуги, наприклад фітнес трекер. Однак специфікація BLE не чітко визначає (або вимагає) режим захищених з'єднань лише для майстра, наприклад мобільний телефон.

1.4 GATT та ATT протокол

Починаючи з версії 4.0, Bluetooth, що включає специфікацію низького рівня споживання енергії, пропонує два основні протоколи: ATT (Attribute Protocol) і GATT (Generic Profile Attribute Profile). Вони в основному орієнтовані на низький рівень споживання енергії, і, як очікується, кожен профіль LE використовуватиме їх. Але їх також можна використовувати через «vanilla» Bluetooth (BR / EDR).

ATT – це протокол провідного додатку, тоді як GATT диктує, як ATT використовується у складі сервісу[6]. Кожен профіль LE повинен базуватися на GATT. Отже, в кінцевому рахунку, кожна послуга LE використовує ATT як протокол програми. Блокування профілів у цих протоколах дає ряд переваг:

- Розробка та реалізація нових LE-профілів набагато простіше, оскільки немає жодного дротового протоколу, який можна зробити з нуля;
- ATT оптимізовано для роботи на пристроях з низьким рівнем споживання енергії: він використовує якомога менше байтів, а реалізація може використовувати структури пам'яті фіксованого розміру для створення пакетів даних (PDU).
- Простота ATT / GATT означає, що прошивка може запропонувати певну ступінь допомоги ATT / GATT, що позбавить програмного забезпечення мікроконтролера від неприємностей.
- Для стеків на основі програмного забезпечення ATT / GATT може бути реалізований лише один раз у самому стеку, що позбавляє програми від неприємностей.
- Менше впроваджень ATT / GATT там означає менше проблем із субоптимальними реалізаціями та супутніми питаннями інтероперабельності (поганий набір програмного забезпечення на сьогоднішній день є проблемою Bluetooth Classic).
- Можуть бути профілі, для яких ATT / GATT не ідеально підходить як протокол програми. Але завжди може бути друге з'єднання L2CAP паралельно з каналом ATT, який, в свою чергу, реалізує протокол, специфічний для профілю.

Тепер розглянемо детальніше кожен протокол.

1.4.1 GATT

Єдиним будівельним блоком ATT є атрибут. Атрибут складається з трьох елементів:

- 16-бітний хендл(handle);
- UUID, який визначає тип атрибута;
- значення певної довжини.

З точки зору ATT, значення є аморфним, це масив байтів будь-якого розміру. Дійсний сенс значення повністю залежить від UUID, і ATT не перевіряє, чи відповідає довжина значення даному UUID тощо.

Хендл – це лише число, яке однозначно ідентифікує атрибут (оскільки може бути багато атрибутів з тим самим UUID всередині пристрою).

Сам ATT не визначає жодного UUID. Ця функція покладається на GATT та профілі вищого рівня. Сервер ATT зберігає атрибути. Клієнт ATT нічого не зберігає; він використовує провідний протокол ATT для читання та запису значень на атрибутах сервера.

В кожного атрибута можуть бути дозволи безпеки. Вони зберігаються десь усередині значення і визначаються профілями вищого рівня. Сам ATT не "знає" їх і не намагається інтерпретувати значення атрибутів для перевірки дозволів. Це задача GATT (і вищого профілю).

Протокол ATT має деякі приємні функції, наприклад пошук атрибутів по UUID, отримання всіх атрибутів із заданим діапазоном оброблюваної інформації тощо, тому клієнту не потрібно заздалегідь знати номери хендлів, а також профілі вищого рівня не повинні їх жорстко кодувати.

Але номери хендлів мають бути однаковими для кожного пристрою. Це дозволяє клієнтам кешувати інформацію, використовуючи менше пакетів (і менше енергії) для отримання значень атрибутів після першого виявлення. Профілі вищого рівня визначають, як "натякнути" клієнту, що сервер змінив макет атрибутів (наприклад, після оновлення мікропрограмного забезпечення).

Більшість протоколів ATT – це чистий клієнт-сервер: клієнт бере на себе ініціативу, сервер відповідає. Але ATT має можливості оповіщення та індикації, в яких сервер бере на себе ініціативу сповіщати клієнта про зміну значення атрибуту, рятуючи клієнта від необхідності запитувати атрибут.

Провідний протокол ніколи не надсилає значення довжини; це завжди мається на увазі від розміру PDU, і клієнт повинен "знати" точний макет значення для тих типів UUID, які він розуміє. Якщо не надсилати значення довжини, явно зберігаються байти, що особливо важливі для LE, оскільки MTU (максимальний блок передачі) в LE складає всього 23 байти. Малий LE MTU є проблемою для великих значень атрибутів. Для них ATT має «read long» і «write long» операції, які передають великі атрибути по частинах.

ATT адаптується до зв'язку MTU; він не обмежує розмір пакету найменшим загальним знаменником. Наприклад, 40-байтний атрибут вимагає використання операції «read long» над LE, але він може читатися атомно через транспорт BR/EDR, оскільки мінімальний MTU для останнього становить 48 байт.

ATT дуже, дуже загальний, і залишав би занадто багато, щоб визначати профілі вищого рівня. Окрім зайвої свободи, існують деякі відкриті питання, такі як: що робити, якщо пристрій пропонує декілька послуг? Існує лише один простір для обробки ATT для кожного пристрою, і кілька сервісів повинні спільно використовувати спільний простір. На щастя, у нас є GATT, який формує та обмежує використання атрибутів.

1.4.2 GATT: Generic Attribute Profile

Профіль загальних атрибутів (General Attribute Protocol, GATT) – це обов'язковий профіль із загальними специфікаціями відправки і прийому коротких порцій даних, відомих в Bluetooth Low Link під назвою «атрибути»[7]. Всі нинішні профілі додатків LE засновані на GATT. Інститут стандартизації і розробки протоколу - Bluetooth Special Interest Group вже поставив для пристроїв BLE кілька профілів. Ці профілі це технічні характеристики, що описують спосіб застосування і взаємодії з пристроями.

Наріжним каменем сервісу GATT є атрибут з UUID, рівний 0x2800. Усі атрибути, що слідують за цим, належать цьому сервісу, поки не буде знайдено інший атрибут 0x2800 Наприклад, макет атрибутів пристрою із трьома сервісами наведено в Таблиці 1.2:

Таблиця 1.2 – Макет атрибутів пристрою із трьома сервісами

Хендл	**UUID**	**Опис**
0x0100	0x2800	Сервіс А Визначення
...	...	Інформація про сервіс
0x0150	0x2800	Сервіс В Визначення
...	...	Інформація про сервіс
0x0300	0x2800	Сервіс С Визначення
...	...	Інформація про сервіс

Кожен атрибут сам по собі не «знає», якому сервісу він належить. GATT потрібно визначити це на основі діапазонів хендлів, а діапазони виявляються виключно на основі UUID 0x2800 "наріжних каменів".

Раптом значення хендла стає значним. У прикладі, щоб атрибут належав до служби B, він повинен лежати між 0x0151 та 0x02ff. UUID 0x2800 визначає основні послуги. Існують і вторинні сервіси (UUID 0x2801), які мають бути включені до первинних сервісів.

Отже, як можна знати, чи дана послуга є термометром, брелоком або GPS? Читаючи його значення. Значення атрибуту сервісу містить UUID. Отже, кожен атрибут визначення сервісу має в своєму тілі два UUID: 0x2800 або 0x2801 як атрибут UUID та ще один, що зберігається у значенні, яке визначає послугу. Наприклад, припустимо, що послуга термометра гіпотетичного LE має UUID 0x1816. Повний атрибут сервісу стає таким(Таблиця 1.3):

Таблиця 1.3 – Повний атрибут сервісу

Хендл	**UUID**	**Опис**	**Значення**
0x0100	0x2800	Визначення сервісу термометра	UUID 0x1816
...	...	Інформація про сервіс	...
0x0150	0x2800	Сервіс B Визначення	0x18xx
...	...	Інформація про сервіс	...
0x0300	0x2800	Сервіс C Визначення	0x18xx
...	...	Інформація про сервіс	...

Спочатку це звучить трохи заплутано: два UUID для визначення однієї послуги? Це результат багатошарового підходу GATT/ATT. UUID 0x2800, добре відомий GATT, використовується для пошуку меж обслуговування. Після їх виявлення атрибути зчитуються, а другий UUID (зберігається як значення) вказує послугу. Таким чином, клієнт може знайти всі послуги GATT, не знаючи специфіки, наприклад, послуга термометра.

1.4.3 Характеристики сервісу GATT

Кожен сервіс GATT має ряд характеристик. Характеристики зберігають корисні значення для сервісів, а також їхні дозволи. Наприклад, термометр, ймовірно, повинен мати характеристику температури, яка є лише для читання, і, можливо, дата/час для позначення часу, яка може зчитуватися або записуватися.

Таблиця 1.4 – Демонстрація характеристик сервісу

Хендл	**UUID**	**Опис**	**Значення**
0x0100	0x2800	Визначення сервісу термометра	UUID 0x1816
0x0101	0x2803	Характеристика: температура	UID 0x2A2B Хендл значення: 0x0102
0x0102	0x2A2B	Значення температури	20
0x0104	0x2A1F	Дескриптор: одиниця	Цельсій

Кінець таблиці 1.4

0x0110	0x2803	Характеристика: дата/час	UUID 0x2A08 Хендл значення: 0x0111
0x0111	0x2A08	дата/час	UUID 0x2A08

GATT «знає», що хендл 0x0104 – це дескриптор, який належить до характеристики 0x0101, оскільки

а) це не атрибут значення, оскільки атрибут значення, як відомо, є 0x0102;

б) вона потрапляє в діапазон 0x0103..0x010F, який є між однією характеристикою та наступною.

Значення дескриптора інтерпретується відповідно атрибутом UUID. У прикладі UUID дескриптора є 0x2A1F. Клієнт може безпечно ігнорувати дескриптор, UUID якого невідомий. Це дозволяє легко розширити послугу, не порушуючи старих клієнтів. Кожен сервіс може визначати власні дескриптори, але GATT визначає набір стандартних дескрипторів, які охоплюють більшість випадків, наприклад:

- Числовий формат і презентація;
- Людсько-читабельний опис;
- Дійсний діапазон;
- Розширені властивості;

і так далі. Один особливо важливий дескриптор - це конфігурація, характерна для клієнта.

1.4.4 Дескриптор конфігурації клієнта

Цей дескриптор, UUID якого 0x2902, має 16-бітове значення для читання/запису, яке покликане бути растровим. Це не якийсь дескриптор на стороні клієнта. Це серверний, як і будь-який інший, атрибут. Але сервер зобов'язаний зберігати та представляти окремий екземпляр значення для кожного зв'язаного клієнта, і кожен клієнт може бачити лише власну копію. Звідси і назва.

Перші два біти дескриптора конфігурації клієнта вже взяті за специфікацією GATT. Вони налаштовують характерне сповіщення та індикацію. Інші біти можуть використовуватися для інших функцій, але вони наразі зарезервовані. Слід пам'ятати, що ATT має можливості оповіщення, тому клієнту не потрібно опитуватись щодо оновлень. Встановлюючи дескриптор конфігурації клієнта, клієнт повідомляє серверу, що він хоче отримувати сповіщення, коли характеристика змінюється. Це має сенс, наприклад, для термометра. Розглянемо наступну схему обслуговування термометра з увімкненим дескриптором конфігурації клієнта:

Таблиця 1.5 – Демонстрація дескрипторів характеристик

хендл	**UUID**	**Опис**	**Значення**
0x0100	0x2800	Визначення сервісу термометра	UUID 0x1816
0x0101	0x2803	Характеристика: температура	UID 0x2A2B Хендл значення: 0x0102

Кінець таблиці 1.5

0x0102	0x2A2B	Значення температури	20
0x0104	0x2A1F	Дескриптор: одиниця	Цельсій
0x0105	**0x2902**	Дескриптор конфігурації клієнта	**0x0000**
0x0110	0x2803	Характеристика: дата/час	UUID 0x2A08 Хендл значення: 0x0111
0x0111	0x2A08	дата/час	UUID 0x2A08

Як завжди, GATT знає, що дескриптор конфігурації клієнта належить до температурних характеристик, оскільки хендл потрапляє в діапазон (0x0102..0x010F). І він знає, що це дескриптор конфігурації клієнта через відмінний UUID (0x2902).

1.4.5 Сповіщення та з'єднання

Сповіщення та індикація – це механізми, які дозволяють серверу надсилати повідомлення клієнту. Завдяки їм клієнту не доведеться опитувати сервер для того щоб отримати нові дані. З іншого боку, типовий сервер GATT - це "невеликий" периферійний пристрій, як датчик, який повинен економити енергію. Через це периферійні пристрої LE не можуть брати на себе ініціативу Bluetooth-з'єднання. Але тоді, як сповіщення взагалі можна надіслати? У BLE,

коли сервер має дані для надсилання, він переходить у режим реклами, який надсилає деякий радіосигнал. Кожен профіль вказує часовий проміжок і частоту, яку повинен рекламувати пристрій, врівноважуючи споживання енергії та ймовірність виявлення, враховуючи випадки використання. Пристрій центральної ролі (мобільний телефон, комп'ютер, все, що має більше енергії) має приймач, ввімкнений постійно у режимі прослуховування. Скажімо, це телефон. Коли телефон прослуховує рекламу, і рекламований пристрій "відомий" (він був парним або дозволеним із цим телефоном), телефон повинен з'єднуватися з периферійним пристроєм. Після того, як з'єднання встановлено, зв'язок GATT може протікати і повідомлення може бути доставлено.

Отже, типовою послідовністю є:

1) сервер рекламує;
2) клієнт підключається;
3) сервер повідомляє.

На даний момент будь-яка сторона може встановити тайм-аут для відключення, якщо більше не надходить сповіщення. "Кращий" час очікування залежить від випадку використання; послуга з нечастими сповіщеннями та без будь-яких претензій у режимі реального часу може просто негайно відключитися для економії енергії.

Типовий сервер GATT є периферійним пристроєм, але це не є обов'язковим: у нас може бути периферійний клієнт і центральний сервер, або два центральних пристрої, що спілкуються один з одним. Доречно згадати, що в цьому (досить рідкісному) випадку клієнту доведеться перейти в режим реклами, коли він хоче запитувати сервер, наприклад. прочитати або написати характеристику.

Висновки до розділу 1

В даному розділі було розглянуто технологію Bluetooth Low Energy, принципи за якими пристрої комунікують, процес підключення пристроїв, створення пари та основні режими безпеки.

Також було розглянуто протокол ATT та побудований на ньому профіль, які є найважливішими для розуміння BLE,

2 БЕЗПЕКА BLE ПРИСТРОЇВ, ЗОКРЕМА ФІТНЕС ТРЕКЕРІВ

2.1 Вразливості Bluetooth та види атак

Перш за все, варто ознайомитись із переліком вразливостей та видів атак на Bluetooth. Національний інститут стандартів і технології (NIST) – національний орган зі стандартизації у США – у своїй публікації «Guide to BluetoothSecurity» наводить перелік із двадцяти дев'яти вразливостей, які охоплюють багато версій Bluetooth[8]. У таблиці 2.1, наведеній нижче, описано лише ті, які охоплюють актуальні версії.

Таблиця 2.1 – Вразливості Bluetooth

	Питання безпеки або вразливість	**Примітки**	**Версії**
1	Метод спарювання Just Works не забезпечує захисту від MITM.	Атакуючі MITM можуть захоплювати та маніпулювати даними, переданими між надійними пристроями. Пристрої з низьким рівнем споживання енергії повинні поєднуватися в безпечному середовищі, щоб мінімізувати ризик підслуховування та MITM-атак. Спарювання Just Works не слід використовувати для LE	4.0 4.1 4.2
2	Конфіденційність BLE може бути порушена, якщо адреса Bluetooth буде захоплена і пов'язана з певним користувачем.	Для зниження рівня ризику може бути реалізована конфіденційність адреси.	4.0 4.1 4.2

Кінець таблиці 2.1

3	Спроби аутентифікації можуть повторюватися.	У пристрої Bluetooth повинен бути включений механізм для запобігання необмеженим запитам аутентифікації. Специфікація Bluetooth вимагає експоненціально зростаючого інтервалу очікування між послідовними спробами аутентифікації. Однак для запитів виклику автентифікації не потрібно такого інтервалу очікування, тому зловмисник може зібрати велику кількість відповідей на виклик (які зашифровані секретним ключем посилання), які могли б просочити інформацію про цей секретний ключ.	Всі
4	Не існує автентифікації користувача.	Специфікацією надається тільки автентифікація пристрою. Захист рівня додатків, включаючи автентифікацію користувача, може бути доданий розробником програмного забезпечення.	Всі
5	Служби безпеки обмежені	Аудит, неспростовність та інші послуги не є частиною стандарту. При необхідності розробник програми може впроваджувати ці сервіси додатково.	Всі
6	Пристрої, які можуть бути виявлені та/або підключені схильні до атаки.	Будь-який пристрій який повинен перейти в режим відкриття або підключення для з'єднання, повинен робити це лише протягом мінімальної кількості часу. Пристрій не повинен постійно знаходитись у режимі виявлення або підключення.	Всі

Всі вище згадані вразливості можуть бути використані зловмисниками для проведення атак на пристрої Bluetooth. Загалом можна виділити наступні види атак на пристрої Bluetooth:

- Bluesnarfing
- Bluejacking
- Carwhisperer
- Denial of Service
- Pairing Eavesdropping
- Secure Simple Pairing Attacks

Далі детальніше про кожну з атак.

Bluesnarfing – атака, в результаті якої зловмисник отримує доступ до даних через Bluetooth пристрої, які не тільки включені, але і переведені в режим «доступний всім»[9]. Часто використовувався для отримання доступу до IMEI. IMEI – це унікальний ідентифікатор для кожного пристрою, який зловмисник може потенційно використовувати для маршрутизації всіх вхідних дзвінків з пристрою користувача на пристрій зловмисника. Для реалізації цієї атаки використовуються недоліки в прошивці пристроїв.

Bluejacking – свого роду Bluetooth-спам (іноді фішинг). Атакуючий міг розсилати повідомлення на пристрої, в яких увімкнений Bluetooth[10].

Carwhisperer – атака на бездротові гарнітури та інші Bluetooth пристрої без дисплея і клавіатури (спочатку – handsfree в автомобілях). Суть атаки полягає в переборі стандартних паролів пристроїв[11]. У разі успішної атаки, зловмисник може не тільки передавати свій аудіосигнал на пристрій, а й підслуховувати.

Denial of Service – як і інші бездротові технології, Bluetooth сприйнятливий до DoS-атак. Результати успішно проведеної атакаи зазвичай включають в себе неможливість використання Bluetooth пристрою і швидкий розряд батареї. Ці

типи атак не критичні через доволі невеликий радіус дії Bluetooth, а також їх можна легко запобігти. Для запобігання подібної атаки на пристрої Bluetooth, достатньо просто вийти з радіусу дії атакуючого передавача.

Pairing Eavesdropping - сніффінг Bluetooth ефіру з метою перехоплення фреймів, що посилаються під час спарювання пристроїв[12]. Атакуючий, маючи дані фрейми, може досить швидко вирахувати секретний ключ. Схильні тільки Bluetooth версії 2.0 і нижче в режимі спарювання PIN / Legacy і Low Energy Bluetooth в режимі спарювання Legacy.

Secure Simple Pairing Attacks - ряд методик, що може змусити віддалений пристрій використовувати Just Works SSP, а потім використати його відсутність захисту від MITM (наприклад, пристрій атаки стверджує, що він не має можливості введення/виводу). Крім того, фіксовані ключі також можуть дозволити зловмиснику здійснювати MITM-атаки.

2.2 Методи запобігання атак на Bluetooth пристрої

Для запобігання атакам на пристрої Bluetooth та зменшення ризиків, Національний інститут стандартів і технології пробонує збір вказівок та рекомендацій щодо створення та підтримки захищених Bluetooth пристроїв. Це є певний контрольний список(чеклист), в якому для кожної рекомендації чи настанови стовпець обґрунтування перераховує області, що стосуються пристров Bluetooth, загрози безпеці та вразливостей, пов’язаних з цими областями, пом'якшення ризику для захисту пристроїв від цих загроз та вразливостей. Крім того, для кожної рекомендації передбачено три колонки контрольного списку.

Перша колонка – Рекомендується до виконання. Якщо в цій колонці є відмітка, то це означає, що цей запис є рекомендацією для всіх організацій.

Друга колонка – Потрібно враховувати. Якщо в цій колонці є відмітка, то це означає, що організація повинна ретельно розглянути дану рекомендацію з однієї або декількох наступних причин:

- По-перше, реалізація рекомендації може забезпечити більш високий рівень безпеки для бездротового оточення, пропонуючи додатковий захист.
- По-друге, рекомендація підтримує глибоку стратегію оборони.
- По-третє, це може мати суттєвий вплив на ефективність, експлуатацію чи витрати.

Підсумовуючи це, якщо встановлено відмітку «Потрібно враховувати» – організації повинні ретельно розглянути варіант і зважити витрати в порівнянні з вигодами.

Остання колонка – Статус. Вона навмисно залишається порожньою, щоб дозволити представникам організації використовувати цю таблицю як справжній контрольний список. Наприклад, особа, яка здійснює аудит безпеки бездротового зв'язку в середовищі Bluetooth, може швидко перевірити кожну рекомендацію організації, перевіряючи чи вона виконана.

За NIST збір вказівок та рекомендацій щодо створення та підтримки захищених Bluetooth пристроїв складається з трьох категорій та є наступним:

Організаційні рекомендації

1. Розробіть організаційну політику безпеки бездротової мережі Bluetooth. Політика безпеки є основою для всіх інших контрзаходів.
2. Переконайтеся, що всі користувачі Bluetooth ознайомлені з правилами безпеки по використанню Bluetooth. Програма інформування про безпеку допомагає користувачам брати до уваги практику, яка допомагає запобігти інциденти безпеки.

3. Регулярно проводьте комплексні оцінки безпеки Bluetooth. Оцінки безпеки допомагають ідентифікувати пристрої Bluetooth, які використовуються в організації, а також допомагають забезпечити дотримання політики безпеки бездротової мережі.
4. Переконайтеся, що пристрої Bluetooth, які використовуються повністю зрозумілі з точки зору архітектури та задокументовані відповідно. Пристрої з підтримкою Bluetooth можуть містити різні мережеві технології і інтерфейси, що дозволяють підключатися до локальних і глобальних мереж. Організація повинна розуміти загальну зв'язність кожного пристрою для виявлення можливих ризиків і вразливостей. Ці ризики і уразливості можуть бути потім нівельовані в політиці безпеки бездротової мережі.
5. Надайте користувачам список запобіжних заходів, які вони повинні зробити, щоб краще захистити кишенькові пристрої з підтримкою Bluetooth від крадіжки. нізація і її співробітники несуть відповідальність за свої пристрої з підтримкою Bluetooth, тому що крадіжка цих пристроїв може призвести до інцидентів інформаційної безпеки.
6. Ведіть повну інвентаризацію всіх бездротових пристроїв і адрес Bluetooth (BD_ADDRs). Повний інвентаризаційний список Bluetooth пристроїв можна надати в рамках проведення аудиту з метою виявлення несанкціонованих пристроїв.

Технічні рекомендації

7. Змініть настройки Bluetooth за умовчанням, щоб вони відповідали політиці безпеки організації. Оскільки стандартні параметри, як правило, небезпечні, необхідно уважно вивчити ці параметри, щоб переконатися, що вони відповідають політиці безпеки організації.

Наприклад, зазвичай необхідно змінити ім'я пристрою (тобто так, щоб воно не відображало тип платформи).

8. Встановіть пристрої Bluetooth на найнижчий необхідний і достатній рівень потужності, щоб радіус сигналу залишався в захищеному периметрі організації. Установка пристроїв Bluetooth з мінімальним необхідним і достатнім рівнем потужності забезпечує безпечний доступ авторизованим користувачам. Слід уникати використання пристроїв класу 1, а також зовнішніх підсилювачів або антен з високим коефіцієнтом посилення через їх розширеного діапазону.
9. Виберіть PIN-коди, які є досить випадковими, довгими і приватними. Уникайте статичних і слабких PIN-кодів, наприклад, 000000. PIN-коди повинні бути випадковими, щоб зловмисники не могли легко їх вгадати. Довші PIN-коди більш стійкі до атак типу brute-force. Для пристроїв Bluetooth 2.0 (або більш ранніх версій) слід використовувати восьмисимвольний буквено-цифровий PIN-код, якщо це можливо. Використання єдиного PIN-коду неприйнятно.
10. Переконайтеся, що ключі з'єднання (сесійні ключі/link keys) не засновані на ключах пристрою. Використання "shared link keys" визнано застарілим, починаючи з версії Bluetooth 1.2.
11. Не використовуйте режим спарювання «Just Works» для пристроїв Bluetooth 2.1 і вище, що використовують SSP. Режим спарювання «Just Works» не забезпечує захист від MITM.
12. Для пристроїв з Bluetooth 2.1 і більш пізніми версіями, які використовують SSP, для кожного спарювання повинні використовуватися випадкові і унікальні ключі доступу на основі моделі асоціації «Passkey Entry». Якщо при декількох спарювання використовується один і той же ключ доступу, то захист від MITM атак, передбачена в моделі спарювання «Passkey Entry», значно зменшується.

13. Якщо пристрою з Bluetooth версій 2.1 і пізніше, котрі використовують Security Mode 4, необхідно з'єднатися з більш старими версіями Bluetooth, які не підтримують Security Mode 4, то даний пристрій бажано відкотити до Security Mode 3. Специфікації Bluetooth дозволяють пристрою 2.1 повернутися в будь-який режим безпеки (Security Mode) для забезпечення сумісності. Це дозволяє повернутися до режимам захисту 1-3. Як обговорювалося раніше, режим безпеки 3 забезпечує кращу безпеку.
14. Low energy Bluetooth пристрою з версіями 4.0 і 4.1 повинні використовувати Security Mode 1 Level 3, коли це можливо. Інші режими небезпечні.
15. Low energy Bluetooth пристрою з версією 4.2 і вище повинні використовувати Security Mode 1 Level 4, якщо це можливо. Даний режим дозволяє забезпечити максимальний рівень безпеки для таких пристроїв.
16. Bluetooth пристрої BR / EDR з версіями 4.0 і 4.1 повинні використовувати Security Mode 4 Level 4, якщо це можливо. Якщо Security Mode 4 Level 4 не підтримується, то замість нього варто використовувати Security Mode 4 Level 3.
17. Незатверджені служби та профілі повинні бути відключені. Більшість реалізацій стека Bluetooth підтримують кілька профілів і пов'язаних з ними сервісів. Рекомендується дозволити тільки попередньо визначені профілі і сервіси.
18. Пристрої Bluetooth повинні бути налаштовані за замовчуванням як «приховані», за винятком випадків, коли це необхідно для спарювання. Дане налаштування дозволить приховати пристрій Bluetooth від інших пристроїв.

19. Необхідно використовувати шифрування з'єднання. Без використання шифрування з'єднання передача даних вразлива до прослуховування ефіру.
20. Якщо використовується багатоканальний бездротовий зв'язок, переконайтеся, що шифрування увімкнено на кожній ланці ланцюга зв'язку. Один небезпечний зв'язок призводить до компрометації всього ланцюга зв'язку.
21. Переконайтеся, що для всіх підключень виконується взаємна аутентифікація пристрою. Для забезпечення перевірки автентичності всіх пристроїв в мережі потрібна взаємна аутентифікація.
22. Включити шифрування для всіх широкомовних передач (режим шифрування 3). Широкомовні передачі, захищені за допомогою шифрування з'єднань, забезпечують рівень безпеки, який захищає ці передачі від перехоплення.
23. Налаштуйте розміри ключів шифрування максимально довгими, які дозволяє пристрій. Використання максимально допустимих розмірів ключів забезпечує захист від атак перебору.
24. Використовуйте перевірку справжності на рівні додатку та шифрування поверх стека Bluetooth для конфіденційної передачі даних. Оскільки пристрої можуть автоматично підключатися до раніше пов'язаним пристроїв, то бажано використовувати додатки, які додатково реалізують функції шифрування і аутентифікації.
25. Використовуйте перевірку справжності на рівні додатку та шифрування поверх стека Bluetooth для конфіденційної передачі даних. Оскільки пристрої можуть автоматично підключатися до раніше пов'язаних пристроїв, то бажано використовувати додатки, які додатково реалізують функції шифрування і аутентифікації.

26. Додайте шари для перевірки автентичності користувачів, такі як: біометрія, смарт-карти, двофакторна аутентифікація Впровадження потужних механізмів аутентифікації може мінімізувати уразливості, пов'язані з паролями і PIN-кодами.
27. Якщо ви використовуєте рішення Mobile Device Management (MDM), переконайтеся, що політика безпеки Bluetooth в організації забезпечується належним чином за допомогою технічних засобів. Політики безпеки можуть бути застосовані рішеннями MDM. Налаштування за замовчуванням, як правило, небезпечні. Необхідно уважно вивчити ці параметри, щоб переконатися, що вони відповідають політиці безпеки організації.

Експлуатаційні вимоги

28. Переконайтеся, що функцію Bluetooth відключені, коли вони не використовуються. Bluetooth повинен бути відключений на всіх пристроях, за винятком випадків, коли користувач явно дозволяє Bluetooth встановлювати з'єднання. Це мінімізує вплив потенційних зловмисних дій. Для пристроїв, які не підтримують відключення Bluetooth (наприклад, гарнітури), все пристрій повинен бути відключено, якщо воно не використовується.
29. Виконуйте зпарювання пристроїв якомога рідше, в ідеальному випадку в безпечній зоні, де зловмисники не можуть перехопити фрейми з обміном ключами доступу при сполученні. (Примітка: «безпечна область» визначається як непублічна зона, що знаходиться в приміщенні далеко від вікон в місцях з обмеженими фізичними засобами контролю доступу.) Користувачі не повинні відповідати на будь-які повідомлення, що запитують PIN-код, якщо користувач не ініціював створення пари і

не впевнений, що запит PIN-коду відправляється одним з пристроїв користувача. Сполучення є важливою функцією безпеки і вимагає, щоб користувачі пам'ятали про можливі підслуховуючі пристрої. Якщо зловмисник може захопити передані фрейми, пов'язані зі сполученням, визначення ключа посилання є простим для пристроїв з Bluetooth всі версії до 2.1 і ще 4.0, оскільки безпека залежить виключно від ентропії і довжини PIN-коду.

30. Bluetooth BR / EDR в режимах Security Mode 2 або 4 повинен використовуватися в контрольованій зоні. NIST настоятельно рекомендует, чтобы устройства Bluetooth BR/EDR использовали режим безопасности 3.
31. Переконайтеся, що портативні пристрої з інтерфейсами Bluetooth налаштовані на використання пароля. Це допомагає запобігти несанкціонованому доступу, якщо пристрій втрачено або вкрадено.
32. У разі втрати або крадіжки пристрою Bluetooth користувачі повинні негайно видалити відсутній пристрій зі списку парних пристроїв у всіх інших пристроях Bluetooth. Ця політика запобігатиме використання зловмисником втраченого або вкраденого пристрою для доступу до іншого пристрою Bluetooth, який належить користувачеві.
33. Встановіть антивірусне програмне забезпечення на хостах з підтримкою Bluetooth, які підтримують таке програмне забезпечення. Антивірусне програмне забезпечення допоможе запобігти появі шкідливого ПО в мережі Bluetooth.
34. Повністю тестуйте та регулярно розгортайте патчі та оновлення програмного забезпечення та мікропрограмного забезпечення Bluetooth. Патчі повинні бути повністю протестовані перед розгортанням, щоб підтвердити, що вони ефективні.

35. Користувачі не повинні приймати передачі повідомлень, файлів і зображень з невідомих чи підозрілих пристроїв. Зі збільшенням числа пристроїв з підтримкою Bluetooth важливо, щоб користувачі встановлювали з'єднання тільки з іншими довіреними пристроями і брали контент тільки з цих довірених пристроїв.
36. Необхідно повністю проаналізувати наслідки розгортання будь-яких функцій безпеки або продукту до розгортання. Щоб забезпечити успішне розгортання, організація повинна повністю зрозуміти технічні, захисні, експлуатаційні та кадрові вимоги до впровадження.
37. Слід наголосити людини для відстеження випуску нових версій Bluetooth, а також стандартів безпеки (наприклад, через Bluetooth SIG), появи нових вразливостей і атак. Особа, призначена для відстеження новітніх технологій, стандартів і ризиків, допоможе забезпечити безперервне безпечне використання Bluetooth.

На жаль, NIST дає тільки рекомендації, але не розповідає, як їх виконувати. І якщо деякі рекомендації цілком реально виконати на смартфонах (наприклад, переклад пристрою в режим «невидимки» - №18), то на інших пристроях їх виконання може бути і не передбачено в принципі. Таким чином, єдиним способом є правильний підбір пристроїв на основі специфікації і подальша перевірка пристрою на відповідність їй.

2.3 Безпека фітнес трекерів

Фітнес-браслети і смарт годинники стали дуже популярним пристроями не тільки серед любителів спорту. Зарубіжні медичні страхові компанії субсидують покупку фітнес-трекерів або винагороджують за їх використання, тому що

клієнти, які займаються фізичною активністю, обходиться страховим компаніям дешевше. Ось чому дослідники AV-Test провели комплексне тестування безпеки 7 сучасних фітнес-браслетів для ОС Android. Також була досліджена безпека смарт годинника Apple Watch[13].

Виконання тесту поділялося на три етапи, які в кінцевому рахунку дали сукупні результати тесту. Ці три етапи:

- Аналіз оригінальної програми
- Аналіз зв'язку Bluetooth між трекером та смартфоном (із встановленим оригінальним та/або тестовим додатком)
- Аналіз онлайн-спілкування оригінального додатка

Перший крок включає аналіз оригінального додатка на предмет можливих уразливих місць. Таким чоном здійснюється перевірка цілісних заходів безпеки, таких як придушення коду та захист даних користувачів, що зберігаються додатком.

Другий крок – це спостереження та аналіз зв’язоку Bluetooth, тобто відстежування трафіку даних між трекером та додатком і, врешті, спроба імітувати зв’язок (наприклад, шляхом повторної передачі зв'язку з другого смартфона), щоб перевірити надійність аутентифікації та можливість зловмиснику отримати доступ до функцій відстеження або збережених даних.

На останньому з трьох етапів аналізується повне спілкування в Інтернеті з початковою програмою та з неї.

У тесті дослідників з AV-Test були розглянуті наступні пристрої:

- Basis Peak
- Microsoft Band 2
- Mobile Action Q-Band

- Pebble Time
- Runtastic Moment Elite
- Striiv Fusion
- Xiaomi MiBand
- Apple Watch

В таблиці 2.2 відображено особливості кожного з протестованих пристроїв.

Таблиця 2.2 – Особливості трекерів, що брали участь в тестуванні

	Apple Watch	Basis Peak	Microsoft Band 2	Mobile Action Q-Band	Pebble Time	Runtastic Moment Elite	Striiv Fusion	Xiaomi MiBand
Bluetooth 4.0 (Low Energy)	+	+	+	+	+	+	+	+
Wi-Fi	+	-	-	-	-	-	-	-
Мікрофон	+	-	+	-	+	-	-	-
Дисплей	+	+	+	+	+	-	+	-
Пульсометр	+	+	+	-	-	-	-	-
Крокомір	+	+	+	+	+	+	+	+
Моніторинг сну	-	+	+	+	+	+	+	+
Вбудований GPS	-	-	+	-	-	-	-	-
Магнітометр	-	-	-	-	+	-	-	-
Барометр	-	-	+	-	-	-	-	-
УФ-датчик	-	-	+	+	-	-	-	-
Датчик навколишнього світла	+	-	+	+	+	-	-	-
Ємнісні/гальванічні датчики	-	+	+	-	-	-	-	-
Температура тіла	-	+	+	-	-	-	-	-

Дослідники зосередили свою увагу на двох основних проблемах:

1. З точки зору кінцевого користувача, чи захищені дані, що записуються трекером або додатком, від шпигунства і злому третіми особами?
2. З точки зору страхових компаній та інших організацій, чи захищені дані в трекері від підробки?

Перше питання передбачає розгляд ситуації, коли зловмисники можуть використовувати дані, що поставити користувача в невигідне становище. Друге питання стосується страхових компаній, які заохочують своїх клієнтів за досягнення фітнес-цілей. Якщо сам пристрій або його додаток може бути зламано з метою модифікації даних, дана уразливість може широко експлуатуватися.

Дослідники перевірили кожен трекер по 10 тестових критеріям, розділених на 3 області: трекер, додаток і передача даних по мережі. Підсумкова таблиця ризиків показує області, в яких у учасників тестування виникли проблеми(таблиця 2.3). Терміни «помилка» або «пролом в безпеці» навмисно не застосовувалися, тому що в тестових зонах фіксувався підвищений або високий ризик проникнення, а не 100-відсотковий ризик. Дослідники не робили спроб подальшого злому потенційно вразливою зони. Вони просто проаналізували потенційні дії зловмисника у цій галузі та можливі наслідки.

Таблиця 2.3 – Результати для перевірених продуктів у трьох категоріях: трекер, додаток та інтернет-комунікації.

	Basis Peak	Microsoft Band 2	Mobile Action Q-Band	Pebble Time	Runtastic Moment Elite	Striiv Fusion	Xiaomi MiBand
Трекер							
Контрольована видимість	-	+	+-	+	-	-	+-
Конфіденційність Bluetooth LE	-	+	-	-	-	-	-
Контрольоване підключення	+	+	-	+	-	-	+
Адекватна автентифікація	+	+	-	+	-	-	+-
Захист від зміни даних	+	+	-	+	-	-	+-
Додаток							
Відсутнє незахищене локальне сховище	+	+	+	+	+	+	-
Обфускація коду	+-	-	+	+	+-	-	+
Відсутній вихід журналу / налагодження	-	-	+	-	-	-	-
Онлайн комунікація							
Шифрування	+	+	+-	+	+-	+-	+-
Захист від підроблення	+	+-	+-	+	+-	+-	+-

Далі варто пояснити критерії оцінки фітнес трекерів.

Видимість: всі фітнес-трекери використовують Bluetooth для підключення до смартфону. Отже, в першу чергу були розглянуті традиційні проблеми бездротових підключень за даною технологією. Перший аспект безпеки –

видимість для інших пристроїв Bluetooth. Пристрої повинні бути видимими для інших пристроїв лише під час сполучення на деякий проміжок часу. Дана міра безпеки пропонується тільки браслетами від Microsoft і Pebble. Mobile Action анонсує дану можливість, але на ділі залишається видимим. Також, трекер Xiaomi MiBand, за дослідженнями AV-Test, частково відповідав цьому критерію. За їхніми словами він був завжди невидимий для інших пристроїв після створення пари. Але, на мою думку це є не зовсім так. Фітнес трекер Xiaomi MiBand і справді невидимий для інших пристроїв після спарювання, але не для утиліти hcitool. Про це детальніше в 3 розділі.

BLE конфіденційність: Другий важливий аспект безпеки Bluetooth-підключення – функція BLE Privacy, яка з'явилася, починаючи з Android 5.0. Завдяки даній функції, пристрій повторно генерує нову MAC-адресу для бездротового підключення Bluetooth. Фактична адреса ніколи не розкривається і не відстежується. Дана технологія використовується тільки в Microsoft Band 2. В інших пристроях технологія не реалізована.

Контрольоване підключення: коли пристрій підключаэться, з технічної точки зору існує кілька можливих варіантів. Одним з найбільш безпечних рішень є ексклюзивне поєднання Bluetooth (трекер дозволяє підключення лише до одного довіреного смартфону), яке реалізовано в Basis Peak та Microsoft Band 2. Pebble Time дозволяє підключення з декількома пристроями, але користувачеві потрібно вручну їх підтверджувати, що також є безпечним сценарієм . Xiaomi MiBand використовує простий, але безпечний метод – після успішного сполучення, він припиняє рекламувати свою присутність і не дозволяє інші підключення. Фітнес-браслети від Striiv, Runtastic і Mobile Action не використовують технології захисту підключень до невідомих пристроїв.

Аутентифікація: для того щоб сторонній смартфон не створив успішно пару з трекером, деякі фітнес-пристрої пропонують додаткову функцію безпеки

– аутентифікацію, а саме Basis Peak, Microsoft Band 2 і Pebble Time. Хоча Xiaomi теж використовує дану технологію, її дуже просто обійти, а значить при певних обставинах вона буде марною. Решта три продукти або не пропонують подібну додаткову безпеку, або реалізують в недостатній мірі.

Захист від зміни даних: Цей аспект цікавий не тільки користувачам, але і страховим компаніям і судовим органам, які покладаються на достовірність даних трекера. Лабораторія протестувала наявність захисту цілісності даних і захисту від запису або модифікації даних трекера. Захист повинен бути налаштований таким чином, щоб запобігати будь-яким спробам несанкціонованої зміни і підробки даних браслета з боку користувача смартфона. Тільки продукти від Basis, Microsoft, Pebble і Xiaomi пропонують базовий захист в даній області. Проте, пристрої від Xiaomi можуть бути введені в оману через слабку аутентифікацію. В результаті треті особи можуть запустити вібрацію, змінити налаштування будильника або скинути пристрій до заводських налаштувань. Фітнес-трекери від Striiv і Mobile Action не використовують будь-яких адекватних методів аутентифікації або інших механізмів захисту, а значить є уразливими для модифікації даних. На Striiv Fusion значення вимірювань тіла можна змінити до нереальних значень. Ці дані згодом використовуються для розрахунку пройденої відстані і спалених калорій. У трекері Mobile Action також можна змінити параметри ваги, зросту, довжини кроку користувача. Ці значення були також використані безпосередньо для розрахунку спожитих калорій і пройденої відстані.

Локальна пам'ять: навіть якщо технології трекера безпечні, відповідний додаток на смартфоні може бути слабкою ланкою. Ось чому під час тестування перевірялося, чи доступні дані фітнес-додатки іншим встановленим на Вашому пристрої. Функції безпеки для смартфонів Android без root-доступу є достатніми для запобігання несанкціонованому доступу. Проте, якщо дані зберігаються в

неправильному місці, вони доступні кожному. Xiaomi MiBand - єдиний браслет, який допустив подібну помилку. Додаток зберігає файл журналу активності у відкритій області сховища. Журнал включає дані, що передаються, інформацію про користувача, зокрема ім'я користувача, дані тіла і т.п.

Обфускація коду: під час другого випробування, об'єктом дослідження служив код програми. Зокрема, перевірялося, чи використовує додаток технології обфускації коду. Дані технології запобігають реверс-інжинірингу та приховують корисну інформацію від хакерів. Додатки від Mobile Action, Pebble і Xiaomi використовують обфускацію в повному обсязі. Basis і Runtastic використовують технологію лише частково, що може становити небезпеку. Продукти від Microsoft і Striiv зовсім не застосовують обфускація, а значить відповідні компетентні фахівці можуть провести інспекцію коду.

Журнали та налагоджувальна інформація: додаткові помилки програмування можуть розкриватися на етапі реєстрації подій і виведення налагоджувальної інформації. Іноді в цих вихідних даних відсутні важливі дані, тому розробники нехтують механізмами безпеки. Тільки додаток від Mobile Action повністю безпечно в цьому відношенні. Решта програм виводять інформацію таким чином, що вона може бути перехоплена зловмисниками.

Безпечна передача даних по мережі: в підсумковій перевірці брали участь всі з'єднання програми. Чи можна відстежити підключення? Чи є воно незашифрованим? Які саме дані передаються? Примітно, що всі підключення, які повинні бути зашифровані, дійсно були зашифровані. Відкриті HTTP підключення дуже легко перехопити, тому, ймовірно, вони виконувалися в незашифрованому вигляді.

Крім того, лабораторія перевіряла, чи є вміст захищеного підключення придатним для читання після установки кореневого сертифіката. Ця оцінка має важливе значення, тому що сигналізує про те, чи може користувач управляти

переданими даними. Продукти від Basis і Pebble показали, що безпека в даній області можлива – вони досить захищені від несанкціонованого доступу. У разі інших продуктів, залишалася можливість моніторингу захищених підключень і часткової модифікації. Таким чином, дані аутентифікації і синхронізації можуть бути прочитаними.

Отже, можна зробити висновок, що розробники не приділяють належної уваги аспекту безпеки своїх фітнес трекерів. Оцінка ризиків показує, що більшість Android трекерів є незахищеними.

Тест Apple Watch був підготовлений таким же чином, як і випробування пристроїв для платформи Android. Проте, Android і iOS є різними операційними системами, тому перевірка певних критеріїв ризику не може бути проведена в системі від Apple.

В області мережевих з'єднань перевірялося шифрування каналів передачі даних і здатність зміни даних при наявності кореневих сертифікатів. Bluetooth-видимість може контролюватися користувачем. Це означає, що годинник не може постійно відслідковуватися. У тесті BLE privacy Apple Watch призначав нову MAC-адресу щоразу, коли активувався Bluetooth. Таким чином, пристрій практично неможливо відстежити. У тесті дана функція працювала неодноразово. При івумкненні і вимкненні авіа-режиму Apple Watch завжди показує свою істинну MAC-адресу для компонентів Bluetooth.

З точки зору контрольованих підключень Apple використовує спеціальну техніку запобігання крадіжки даних: якщо пристрій пов'язаний з обліковим записом, то відв'язати його без труднощів не вийде. Скидання до заводських налаштувань тут не допоможе. Якщо злочинець продасть крадений Apple Watch, новий користувач не зможе з'єднати гаджет зі своїм iPhone.

Apple Watch використовує переважно зашифровані підключення, які додатково захищаються. Оновлення передаються в незашифрованому вигляді по протоколу HTTP.

В цілому, Apple Watch отримав високий рейтинг безпеки. Хоча дослідники й ідентифікували потенційно вразливі місця, та їх експлуатація потребує від зловмисників дуже багато часу і сил.

Висновки до розділу 2

В даному розділі було детально розглянуто безпеку Bluetooth Low Energy. Розглянуто та проаналізовано існуючі рекомендації для покращення рівня безпеки BLE, а саме, запропонований NIST контрольний список рекомендацій. На жаль, основним недоліком рекомендацій за NIST є відсутність шляхів та методів їх впроваджень.

Також було розглянуто дослідження безпеки фітнес трекерів групою тестувальників з AV-Test. В їхньому дослідженні також фігурував фітнес трекер від Xiaomi, але попередньої моделі. Загалом тестування виявилося вдалим та результативним, але недолік в ньому це не до кінця проведене дослідження безпеки. Неповнота дослідження полягає в тому, що дослідники не перевіряли чи загрози можна реалізувати. Йшлося лише про значну ймовірність реалізації загрози.

3 РОЗРОБКА МЕТОДИКИ АНАЛІЗУ БЕЗПЕКИ BLE ПРИСТРОЇВ

Зразковим пристроєм для тестування безпеки Bluetooth Low Energy мною був обраний фітнес трекер Xiaomi MiBand 3. Xiaomi – світовий лідер з продажу фітнес-трекерів. За офіційними даними компанії, на старті продажів трекера MiBand 3, перший мільйон пристроїв було продано всього за 17 днів. Це свідчить про високий рівень популярності даного продукту.

Також, за результатами тестування, проведеного групою дослідників AV-Test, результати якого описані в попередньому розділі, фітнес трекер MiBand 3 є не найгіршим пристроєм серед аналогів на ринку в плані безпеки.

3.1 Дослідження безпеки фітнес трекера Xiaomi MiBand 3

Першим кроком в дослідженні безпеки фітнес трекера є збір даних про його роботу. Базуючись на результатах дослідження лабораторії AV-Test та рекомендаціях щодо безпеки Bluetooth, створених NIST(пункт 18 контрольного списку безпеки Bluetooth – пристрої Bluetooth повинні бути налаштовані за замовчуванням як «приховані», за винятком випадків, коли це необхідно для спарювання.), було вирішено перевірити чи є трекер доступним для інших пристроїв.

Як і очікувалось, трекер, що не був зпарений з телефоном, був видимий постійно. Після підключення трекера до телефону за допомогою фірмового ПЗ, трекер став недоступним для інших телефонів. Проте, використавши утиліту hcitool, пристрій був виявлений. Використавши, офіційний додаток від Xiaomi,

можемо в цьому впевнитись. В розділі налаштувань трекера можна побачити його MAC-адресу(рисунок 3.1).

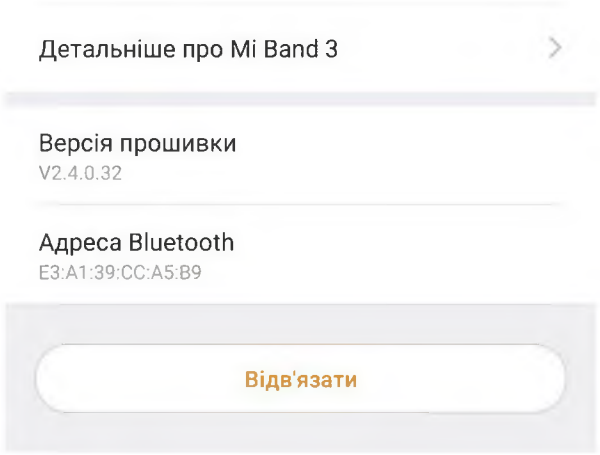

Рисунок 3.1 – Демонстрація MAC-адреси досліджуваного пристрою

Також після повторних підключеннь трекера до телефону та повторних сканувань, MAC-адреса пристрою залишалась незмінною. Це свідчить про те що MiBand не використовує генерацію випадкових MAC-адрес і може бути відстежений. Результати сканування та пошуку підключеного до телефону фітнес трекера показано на рисунку 3.2.

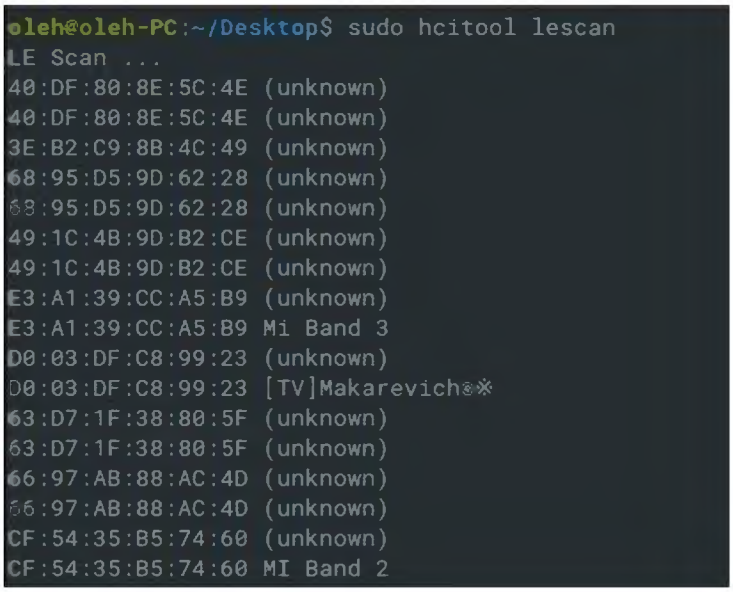

Рисунок 3.2 – Результати сканування BLE пристроїв утилітою hcitool.

Після виявлення пристрою та його MAC-адреси, була здійснена спроба підключитись до трекера. Для підключення було використано утиліту gatttool. Командою `sudo gatttool -b E3:A1:39:CC:A5:B9 -I -t random` можна ініціювати підключення до BLE пристрою. Параметри, з якими запускається утиліта: -b – MAC-адреса пристрою, -I інтерактивний режим, -t тип адреси.При спробі підключення до вже підключеного пристрою отримуємо помилку рисунок 3.3.

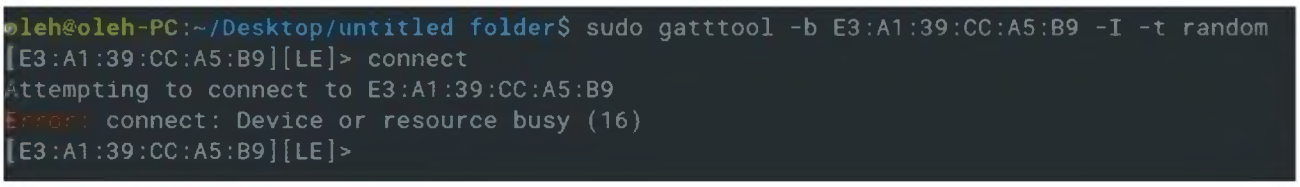

Рисунок 3.3 – Результат спроби підключення до вже підключеного пристрою

Вимкнувши на телефоні Bluetooth, таки вдалося підключитися до фітнес трекера. Отже, вже можна сказати, що певна загроза вже існує. Передумовою успішного проведення атаки може стати цілком реальний сценарій – ваш телефон розрядився, або ж ви вимикали на ньому Bluetooth та забули його знову увімкнути. Про це також було сказано командою AV-Test що тестувала фітнес трекери, але в своєму дослідженні вони лише показали вразливість і не довели, що атака із використанням цієї вразливості може бути успішно проведена.

Підключившись до фітнес трекера маємо змогу спробувати комунікувати з ним. Використовуючи все ту ж gatttool, командами primary та characteristic отримуємо перелік основних сервісів та характеритик пристрою рисунок 3.4, 3.5.

```
^Coleh@oleh-PC:~/Desktop$ sudo gatttool -b E3:A1:39:CC:A5:B9 -I -t random
[E3:A1:39:CC:A5:B9][LE]> connect
Attempting to connect to E3:A1:39:CC:A5:B9
Connection successful
[E3:A1:39:CC:A5:B9][LE]> primary
attr handle: 0x0001, end grp handle: 0x0007 uuid: 00001800-0000-1000-8000-00805f9b34fb
attr handle: 0x0008, end grp handle: 0x000b uuid: 00001801-0000-1000-8000-00805f9b34fb
attr handle: 0x000c, end grp handle: 0x0016 uuid: 0000180a-0000-1000-8000-00805f9b34fb
attr handle: 0x0017, end grp handle: 0x001c uuid: 00001530-0000-3512-2118-0009af100700
attr handle: 0x001d, end grp handle: 0x0023 uuid: 00001811-0000-1000-8000-00805f9b34fb
attr handle: 0x0024, end grp handle: 0x0026 uuid: 00001802-0000-1000-8000-00805f9b34fb
attr handle: 0x0027, end grp handle: 0x002c uuid: 0000180d-0000-1000-8000-00805f9b34fb
attr handle: 0x002d, end grp handle: 0x0057 uuid: 0000fee0-0000-1000-8000-00805f9b34fb
attr handle: 0x0058, end grp handle: 0x006c uuid: 0000fee1-0000-1000-8000-00805f9b34fb
[E3:A1:39:CC:A5:B9][LE]>
```

Рисунок 3.4 – Перелік отриманих основних сервісів пристрою

```
[E3:A1:39:CC:A5:B9][LE]> characteristics
handle: 0x0002, char properties: 0x02, char value handle: 0x0003, uuid: 00002a00-0000-1000-8000-00805f9b34fb
handle: 0x0004, char properties: 0x02, char value handle: 0x0005, uuid: 00002a01-0000-1000-8000-00805f9b34fb
handle: 0x0006, char properties: 0x02, char value handle: 0x0007, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x0009, char properties: 0x22, char value handle: 0x000a, uuid: 00002a05-0000-1000-8000-00805f9b34fb
handle: 0x000d, char properties: 0x02, char value handle: 0x000e, uuid: 00002a25-0000-1000-8000-00805f9b34fb
handle: 0x000f, char properties: 0x02, char value handle: 0x0010, uuid: 00002a27-0000-1000-8000-00805f9b34fb
handle: 0x0011, char properties: 0x02, char value handle: 0x0012, uuid: 00002a28-0000-1000-8000-00805f9b34fb
handle: 0x0013, char properties: 0x02, char value handle: 0x0014, uuid: 00002a23-0000-1000-8000-00805f9b34fb
handle: 0x0015, char properties: 0x02, char value handle: 0x0016, uuid: 00002a50-0000-1000-8000-00805f9b34fb
handle: 0x0018, char properties: 0x18, char value handle: 0x0019, uuid: 00001531-0000-3512-2118-0009af100700
handle: 0x001b, char properties: 0x04, char value handle: 0x001c, uuid: 00001532-0000-3512-2118-0009af100700
handle: 0x001e, char properties: 0x08, char value handle: 0x001f, uuid: 00002a46-0000-1000-8000-00805f9b34fb
handle: 0x0021, char properties: 0x1a, char value handle: 0x0022, uuid: 00002a44-0000-1000-8000-00805f9b34fb
handle: 0x0025, char properties: 0x04, char value handle: 0x0026, uuid: 00002a06-0000-1000-8000-00805f9b34fb
handle: 0x0028, char properties: 0x10, char value handle: 0x0029, uuid: 00002a37-0000-1000-8000-00805f9b34fb
handle: 0x002b, char properties: 0x0a, char value handle: 0x002c, uuid: 00002a39-0000-1000-8000-00805f9b34fb
handle: 0x002e, char properties: 0x1a, char value handle: 0x002f, uuid: 00002a2b-0000-1000-8000-00805f9b34fb
handle: 0x0031, char properties: 0x14, char value handle: 0x0032, uuid: 00000001-0000-3512-2118-0009af100700
handle: 0x0034, char properties: 0x10, char value handle: 0x0035, uuid: 00000002-0000-3512-2118-0009af100700
handle: 0x0037, char properties: 0x14, char value handle: 0x0038, uuid: 00000003-0000-3512-2118-0009af100700
handle: 0x003a, char properties: 0x16, char value handle: 0x003b, uuid: 00002a04-0000-1000-8000-00805f9b34fb
handle: 0x003d, char properties: 0x14, char value handle: 0x003e, uuid: 00000004-0000-3512-2118-0009af100700
handle: 0x0040, char properties: 0x10, char value handle: 0x0041, uuid: 00000005-0000-3512-2118-0009af100700
handle: 0x0043, char properties: 0x12, char value handle: 0x0044, uuid: 00000006-0000-3512-2118-0009af100700
handle: 0x0046, char properties: 0x12, char value handle: 0x0047, uuid: 00000007-0000-3512-2118-0009af100700
handle: 0x0049, char properties: 0x18, char value handle: 0x004a, uuid: 00000008-0000-3512-2118-0009af100700
handle: 0x004c, char properties: 0x10, char value handle: 0x004d, uuid: 00000010-0000-3512-2118-0009af100700
handle: 0x004f, char properties: 0x16, char value handle: 0x0050, uuid: 00000020-0000-3512-2118-0009af100700
handle: 0x0052, char properties: 0x08, char value handle: 0x0053, uuid: 0000000e-0000-3512-2118-0009af100700
handle: 0x0055, char properties: 0x14, char value handle: 0x0056, uuid: 0000000f-0000-3512-2118-0009af100700
handle: 0x0059, char properties: 0x16, char value handle: 0x005a, uuid: 00000009-0000-3512-2118-0009af100700
handle: 0x005c, char properties: 0x08, char value handle: 0x005d, uuid: 0000fedd-0000-1000-8000-00805f9b34fb
handle: 0x005e, char properties: 0x02, char value handle: 0x005f, uuid: 0000fede-0000-1000-8000-00805f9b34fb
handle: 0x0060, char properties: 0x02, char value handle: 0x0061, uuid: 0000fedf-0000-1000-8000-00805f9b34fb
handle: 0x0062, char properties: 0x0a, char value handle: 0x0063, uuid: 0000fed0-0000-1000-8000-00805f9b34fb
handle: 0x0064, char properties: 0x0a, char value handle: 0x0065, uuid: 0000fed1-0000-1000-8000-00805f9b34fb
handle: 0x0066, char properties: 0x02, char value handle: 0x0067, uuid: 0000fed2-0000-1000-8000-00805f9b34fb
handle: 0x0068, char properties: 0x0a, char value handle: 0x0069, uuid: 0000fed3-0000-1000-8000-00805f9b34fb
handle: 0x006a, char properties: 0x1a, char value handle: 0x006b, uuid: 0000fec1-0000-3512-2118-0009af100700
```

Рисунок 3.5 – Перелік отриманих характеристик пристрою

Далі, отримавши MAC-адресу пристрою, та здійснивши успішне підключення, варто розібратися як комунікує телефон з пристроєм Xiaomi. В ОС Android передбачена можливість логування комунікації з Bluetooth пристроями. Для цього потрібно зробити певні налаштування в панелі розробника.

Провівши всі необхідні налаштування, очищуємо логи Bluetooth та здійснюємо зпарювання фітнес трекера та телефона, цим самим отримуємо пакети комунікації пристроїв. По суті це є аналогом MITM атаки, адже в логах зберігаються ті ж самі пакети що і передаються. Єдиною відмінністю є те, що немає зайвих даних, і це не аби як спрощує процес аналізу комунікації BLE пристроїв.

Отриманий лог файл для подальшого дослідження відкриваємо в програмі Wireshark. Аналізуючи пакети «перехопленого» трафіку, особливу увагу слід звертати на пакети протоколу ATT, так як він в даному випадку є основним. Тому, відсортувавши пакети за протоколом шукаємо початок комунікації телефона та фітнес трекера. Комунікація починається з «Read By Group Type» запиту. Суть даного запиту в отриманні всіх основних сервісів пристрою BLE в діапазоні від 0x0001 (мінімальне значення хендлу атрибута) до 0xFFFF (максимальне значення хендлу атрибута). Наступний етап в комунікації пристроїв – аналогічний попередньому. Використовуючи «Read By Type» запити телефон отримує всі характеристики кожного сервісу. Відповідні пакети комунікації пристроїв зображено на рисунку 3.6.Загалом ці кроки є спільні для всіх пристроїв BLE.

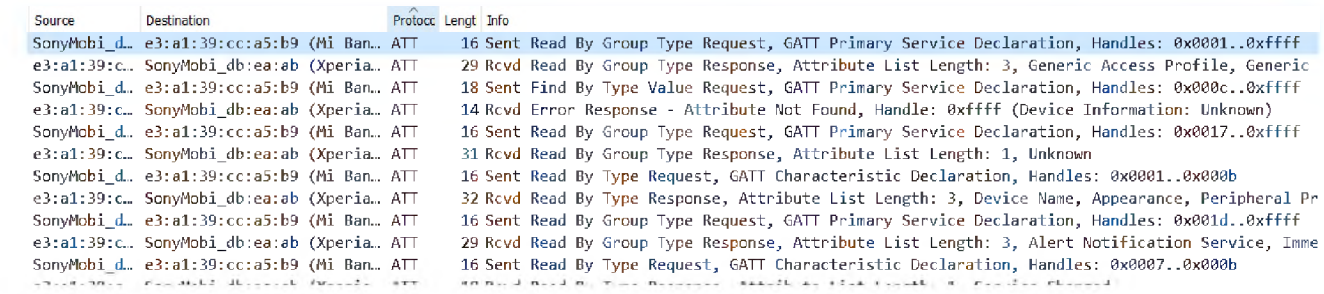

Рисунок 3.6 – Пакети комунікації BLE пристроїв, обмін характеристик та сервісів

Наступні пакети, які відрізнялись від пакетів обміну інформацією були пакети, починаючи з №607. В цьому пакеті телефон звертається до характеристики з UUID 00000009000035122118000 9af100700, яка відповідає за аутентифікацію(рисунок 3.7).

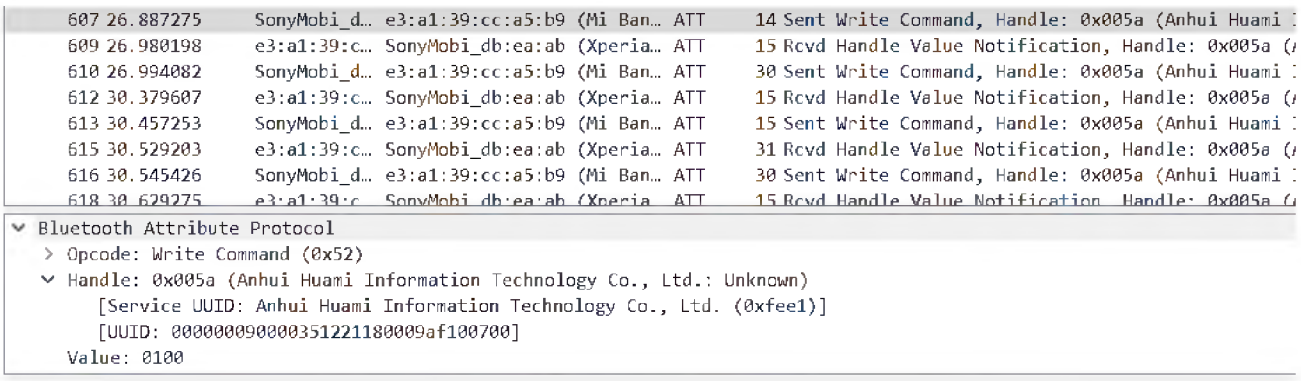

Рисунок 3.7 – Пакет ініціації з’єднання

Проаналізувавши наступні пакети, пов’язані з даною характеристикою, було виявлено наступний алгоритм проведення аутентифікації:

1. Налаштування auth-повідомлень (для отримання відповіді) за допомогою відправки двухбайтового запиту \x01\ x00 до дескриптора сповіщень.
2. Відправлення 16-байтового ключа шифрування до характеристики з командою і додавання двох байт \x01\x00 + KEY.
3. Запит випадкового ключа з пристрою з командою за допомогою відправки двох байт \x02\x00 до характеристики аутентифікації.
4. Отримання випадкового ключа від пристрою (останні 16 байт).

5. Шифрування цього випадкового ключа за допомогою 16-байтового ключа, використовуючи алгоритм шифрування AES / ECB / і зворотна відправка в Char (\x03 \x00 + закодована інформація).

Про успішну аутентифікацію свідчитиме останній пакет відповідь від тієї ж характеристики з UUID 00000009000035122118000 9af100700 із відповіддю \x10\x03\x01.

Одразу ж після аутентифікації, в логах бачимо запит на читання характеристики з хендлом 0x002f та UUID 0x2a2b. У відповідь отримуємо дату та час (рисунок 3.8). За цими двома пакетами слідують запит запису даних до цієї ж характеристики та відповідь фітнес трекера. Таким чиом синхронізується дата та час пристроїв після аутентифікації.

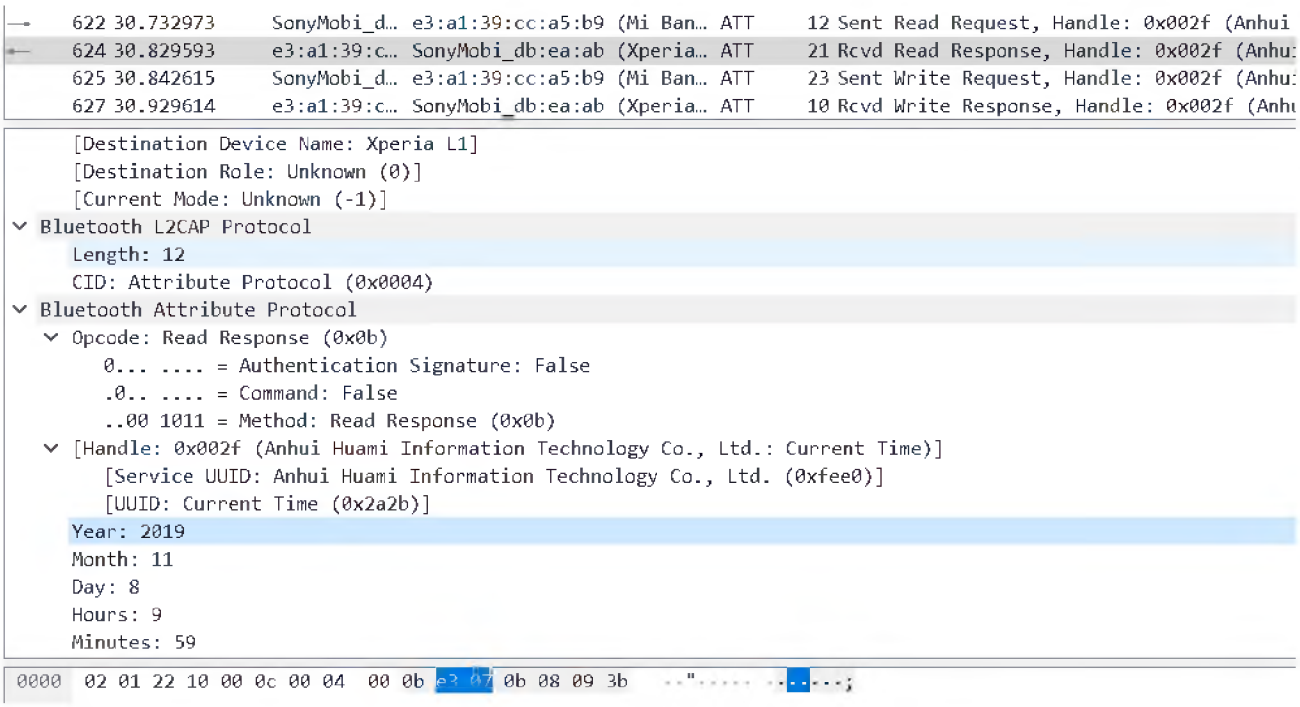

Рисунок 3.8 – Пакети синхронізації дати та часу пристроїв

Аналогічним способом та методом спроб отримуємо інші, потрібні нам характеристики та сервіси.

Сервіс моніторингу серцебиття UUID = 0000180d-0000-1000-8000-00805f9b34fb та характеристика з UUID = 00002a37-0000-1000-8000-00805f9b34fb, яка відповідає за виміри серцебиття.

Сервіс сповіщень UUID = 00001811-0000-1000-8000-00805f9b34fb та характеристика з UUID = 00002a46-0000-1000-8000-00805f9b34fb, яка відповідає за створення нового сповіщення. Для створення сповіщення потрібно здійснити запит запису до даної характеристики. В значенні, яке передається до характеристики перші два байти відповідають за тип сповіщення.

- 01 – електронна пошта
- 03 – дзвінок
- 04 – пропущений дзвінок
- 05 – текстове повідомлення

Два наступні байти відповідають за номер сповіщення. Все інше – тіло сповіщення.

Дослідивши принцип взаємодії трекера з телефоном варто перевірити чи реально здійснити підключення до зпареного пристрою та взаємодіяти з ним. Для перевірки була використана програма, написана на мові програмування Node.js. Програма працює на базі бібліотеки WebBluetooth.

Підключення до трекера відбувається наступним чином: за допомогою бібліотеки WebBluetooth, знаходимо видимі пристрої та відфільтровуємо за сервісами. А саме за основним сервісом реклами з хендлом 0xFEE0 та опційними сервісом якому належить характеристика аутентифікації та сервісом сповіщень. Далі визначаємо підключення пристрою за допомогою *gatt.connect()*

```
    log('Searching Bluetooth Device...');
const device = await bluetooth.requestDevice({
 filters: [
```

```
    { services: [ 0xFEE0 ] }
  ],
  optionalServices:[SERVICE_MIBAND_2,
SERVICE_IMMEDIATE_ALERT]
});
device.addEventListener('gattserverdisconnected', () => {
  log('Device disconnected');
});
log('Connecting to the device...');
const server = await device.gatt.connect();
log('Connected');
```

Після підключення до трекера перший крок аутентифікації було замінено на виклик метод бібліотеки WebBluetooth *startNotifications()* до характеристики аутентифікації та створення обробника відповідей від даної характеристики:

```
let auth = await
miband2.getCharacteristic(UUID_BASE('0009'))
auth.startNotifications()
auth.addEventListener('characteristicvaluechanged', (event)=>{
```

Далі аутентифікація здійснюється за вище описаним алгоритмом та за допомогою методу *writeValue()* – запис значення до характеристики та методів бібліотеки browserify-aes для шифрування ключа.

Здійснивши успішне підключення до пристрою та аутентифікацію робимо спробу вивести сповіщення дзвінка на фітнес трекері:

```
alert.writeValue(AB([0x02]))
```

Результат виконання програми зображено на рисунку 3.9

Рисунок 3.9 – Результат виконання програми взаємодії з трекером при успішному підключенні, аутентифікації та надсиланні сповіщення

Повний код програми наведено в додатку А.

Отже, підсумовуючи результати тестування, можна зробити певні висновки про рівень безпеки даного трекера (Xiaomi MiBand 3). На жаль, результати дослідження групи тестувальників з AV-Test підтвердились. Хоча в їхньому дослідженні фігурувала попередня версія фітнес трекера, захист від перехоплення контролю над пристроєм залишився на тому ж самому рівні, що не є добре.

3.2 Розробка методики аналізу безпеки BLE пристроїв

Базуючись на проведеному дослідженні безпеки фітнес трекера Xiaomi MiBand 3, теоретичних відомостях про Bluetooth Low Energy та дослідженні безпеки найпопулярніших фітнес трекерів групою AV-Test, було розроблено методику аналізу безпеки BLE пристроїв. Технологія Bluetooth LE має протокол ATT та побудований поверх нього профіль GATT. Вони чітко визначають як мають комунікувати BLE пристрої. Саме тому, зібраних даних у попередньому дослідженні було цілком достатньо.

За основу методики тестування BLE пристроїв було взято перевірку пристрою за наступними критеріями:

- Контрольована видимість
- Безпека передачі даних
- Контрольоване підключення
- Аутентифікація

Контрольована видимість

Кожен пристрій Bluetooth Low Energy має бути невидимий для інших за замовчуванням. Пристрій може надсилати рекламні пакети(тобто ставати видимим) лише безпосередньо перед підключенням або створенням пари. При цьому додатковою мірою захисту буде генерація MAC-адрес.

Даний аспект безпеки є важливим, адже він пов'язаний із конфіденційністю користувача. Дізнавшись реальну MAC-адресу пристрою, ми вже можемо пов'язувати її з конкретною людиною.

Отже, для перевірки пристрою на відповідність даному критерію необхідно дослідити чи є досліджуваний пристрій видимий на різних етапах його роботи. Тобто чи є пристрій видимий коли від не прив'язаний до жодного пристрою, коли пристрій прив'язаний, але не підключений, коли пристрій підключений, в момент підключення або ж створення пари.

У випадку коли пристрій є видимим, слід перевірити чи його MAC-адреса є незмінною.

Безпека передачі даних

Безпека передачі даних також є дуже важливим аспектом безпеки пристрою BLE. Дані, що передаються небезпечним шляхом, можуть бути перехоплені та розкриті.

Для перевірки безпеки пристрою за даним критерієм важливо знати чи можна відстежити підключення? Чи є воно незашифрованим? Які саме дані передаються?

Безпека передачі даних визначається шляхом спроби перехвату BLE трафіку та його аналізу. Даний крок перевірки можливий лише після виявлення та ідентифікації потрібного пристрою. Або ж, якщо є доступ до пристрою, і є можливість отримати log файл – проаналізувати залогований трафік.

Контрольоване підключення

Пристрій має дозволяти одночасне підключення лише одного пристрою. Також створення пари з іншим пристроєм має бути ексклюзивним. Тобто, після створення пари, підключення дозволяється лише для одного довіреного пристрою. В разі потреби підключити кілька довірених пристроїв необхідна наявність механізму підтвердження створення пари.

Для перевірки безпеки пристрою за даним критерієм необхідно проаналізувати як відбувається створення пари пристроями. В першу чергу як створюється пара з точки зору користувача. Тобто, чи бере участь користувач у створенні пари, чи вимагається від нього якісь додаткові дії. Далі необхідно проаналізувати як працює механізм створення пари, які протоколи асоціації при цьому використовуються.

Аутентифікація

Аутентифікація є чи не найважливішим критерієм безпеки пристроїв Bluetooth Low Energy. При правильно побудованому механізмі аутентифікації стронні пристрої не зможуть підключитися до пристроя. На прикладі раніше досліджуваного трекера Xiaomi MiBand 3 видно, що навіть проста та далеко не досконала система аутентифікації ускладнює перехоплення контролю над пристроєм(без аутентифікації підключення до пристрою переривалось через кілька секунд та було неможливо взаємодіяти з ним).

Для перевірки методу аутентифікації пристрою, для початку, необхідно перевірити чи присутня взагалі аутентифікація. При підключенні до пристрою необхідно спробувати з ним взаємодіяти. Надіслати команди на запити чиання, записування, які явно дадуть зрозуміти що пристрій доступний або ж навпаки.

Якщо було виявлено що при підключенні пристрій ніяк не реагує на команди, або ж перериває з'єднання – скоріше за все аутентифікація присутня. Найкращим способом для виявлення схеми/методу аутентифікації є аналіз пакетів BLE трафіку пристроя. Зазвичай орієнтирами для пошуку пакетів аутентифікації є UUID характеристик. Для прикладу, для характеристики Current Time, є нормативний UUID, вказаний на www.bluetooth.com. ЇЇ хендл – 0x2A2B. Є очевидним, що датою та часом пристрої обмінюються лише після успішного підключення, і скоріш за все дата та час буде однією з перших задіяних характеристик.

Що стосується відправних точок пошуку початку аутентифікації, то такими скоріш за все будуть пакети Find Information Request та Find Information Response, в яких пристрої обмінюються інформацією, необхідною для початку нормальної комунікаціїї.

Висновки до розділу 3

В даному розділі було проведено дослідження безпеки фітнес трекера Xiaomi MiBand 3, і на основі цього дослідженна та зібраної вище інформації було розроблено методику аналізу безпеки BLE пристроїв.

В результаті проведеного дослідження безпеки фітнес трекера, було виявлено ряд вразливостей, які в сукупності дозволяють перехопити контроль над пристроєм, а саме:

1. Пристрій завжди видимий при скануванні. Хоча після створення пари і стає невидимим для інших телефонів, та цього замало.
2. При комунікації трекера з іншими пристроями дані, якими вони обмінюються не підлягають шифруванню, що дає можливість перехопити пакети комунікації та отримати з них дані користувача, або ж використати їх для подальшого пошуку вразливостей
3. При перевірці безпеки підклчення було виявлено що трекер не дозволяє паралельного підключення кількох пристроїв. Також при зв'язуванні з новим пристроєм пристрій вимагав натиснути кнопку. Ці механізми роботи трекера виявились найкращими методами захисту від перехоплення контролю, що були в даному пристрої, але не найкращими з тих, які можна було б впровадити. По-перше пристрій не завжди може бути підключений до телефону. Наприклад телефон знаходиться поза радіусом дії Bluetooth, або ж найпростіше – телефон розряджений. По-друге, навіть із наявною вимогою підтвердити створення пари із новим пристроєм, це можна зробити випадково зачепивши трекер пальцем, або ж натиснути на нього за звичкою.
4. Аутентифікація також не є сильною стороною досліджуваного пристрою. Хоча певний механізм аутентифікації й існує, та це майже

нівелюється його простотою та відсутністю шифрування трафіку що передається.

4 РОЗРОБКА СТАРТАП ПРОЕКТУ

4.1 Опис ідеї проекту

Першим етапом є аліз змісту ідеї, можливих напрямків застосування, основних вигод, що може отримати користувач товару (Таблиця 4.1) і виокремлення основних відмінностей від існуючих аналогів та замінників.

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Аналіз безпеки пристроїв Bluetooth Low Energy	Захист інформації	Безпека інформації
	Виявлення недоліків в захищеності пристрою	Виявлення дедоліків для подальшого вдосконалення пристрою

Конкурентами є компанії, що надають аналогічні послуги, але перевагою мого проекту є вузька спеціалізація на дослідженні саме BLE пристроїв та надання рекомендацій щодо шляхів усунення виявленх вразливостей.

4.2 Технологічний аудит ідеї проекту

Таблиця 4.2 - Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Аналіз безпеки пристроїв Bluetooth Low Energy	Технологія 1 (реалізована методика)	наявні	доступні
2		Технологія 2 (наявність бази досліджень)	Потрібно розробити	доступні
3		Технологія 3 (оформлення результатів дослідження)	наявні	доступні

В таблиці 4.2 наведено основні технології, необхідні для створення кінцевого продукту. Оскільки обрані технології реалізації є досупними, то проект може бути реалізовано.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Для врахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів варто проаналізувати наявність попиту, обсяг, динаміку розвитку ринку (Таблиця 4.3).

Таблиця 4.3 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	3
2	Загальний обсяг продаж, грн/ум.од	30000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	відсутні
5	Специфічні вимоги до стандартизації та сертифікації	відсутні
6	Середня норма рентабельності в галузі (або по ринку), %	30

На основі проведеного дослідження є можливість стверджувати про привабливість проекту для входження на ринок за попереднім оцінюванням.

Таблиця 4.4 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Дослідження безпеки пристрою BLE для його подальшого вдосконалення	Компанії виробники пристроїв BLE, що не мають власного підрозділу аналізу безпеки, або ж мають потребу в додатковій перевірці	відсутні	Виявлення вразливостей, або визнання їх відсутності, пропозиції шляхів вирішення виявлених проблем

Далі варто провести аналіз ринкового середовища: скласти таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (Таблиця №4.5 - 4.6). Фактори в таблиці подано в порядку зменшення значущості. Також проведено визначення загальних рис конкуренції на ринку (Таблиця 5.8).

Таблиця 4.5 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Агресивність конкурентів	Вплив на систему	може порушити налагоджену систему розповсюдження
2	Економічні складності порушили фінансове забезпечення компанії	відсутність фінансування	Порушення фінансового забезпечення компанії

Таблиця 4.6 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Тривале існування на ринку	тривале існування на ринку	дає можливість виходу на нові ринки
2	Стабілізація бізнес-середовища	формування стабільного середовища	за рахунок стабілізації бізнес-середовища можна поліпшити фінансове забезпечення компанії
3	Трудова міграція фахівців	Підвищення кваліфікованості спеціалістів	Розширення штату

Таблиця 4.7 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Тип конкуренції - олігополія	На ринку присутні компанії, які зарекомендували себе так, що клієнти націлені на користування лише їх послугами через розрекламованість	Збільшення інформованості потенційних клієнтів про якість послуг, що надаються, та донесення усіх переваг у співпраці з клієнтами-підприємствами
2. За рівнем конкурентної боротьби - інтернаціональний	Планується надання послуг за межами країни	Реклама на іноземних ринках
3. За галузевою ознакою - внутрішньогалузева	Внутрішньогалузева. Усі методики та технології, що застосовуються у аналізах, є вузькоспеціалізованими та вузько направленими	Необхідно добре зарекомендувати компанію та підвищити авторитет у даній галузі
4. Конкуренція за видами товарів: - товарно-видова	Кінцевий результат – аналіз безпеки	
5. За характером конкурентних переваг - цінова	За умови надання послуг з однаковим переліком пунктів і однаковою якістю, перевага надається більш бюджетним пропозиціям	Поєднання бюджетності та доступності з підтриманням високого рівня якості надання послуг
6. За інтенсивністю - марочна	Для успішної конкуренції потрібна гарна впізнаваність	Запровадження власної марки, яка буде впізнаватися

Більш детальний аналіз умов конкуренції в галузі можна провести за моделлю п'яти сил М. Портера, що наведений нижче в таблиці 4.8.

Таблиця 4.8 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Клієнти
	Компанії що пропонують ті ж самі послуги	Компанії що пропонують аналогічні послуги	Розробники пристроїв BLE, незалежно від масштабів виробництва
Висновки:	Присутня значна конкуренція	Існує невелика ймовірність появи нових кнкурентів	Клієнти рано чи пізно будуть використовувати схожі засоби. Потрібно вчасно зайти на ринок.

На основі ринкових загроз та можливостей, та сильних і слабких сторін, виділених у попередній таблиці, можна скласти SWOT-аналіз. Це матриця аналізу аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities). Це фінальний етап ринкового аналізу можливостей впровадження проекту (Таблиця 4.9).

Таблиця 4.9 - SWOT-аналіз стартап-проекту

Сильні сторони: 1. Вузька спеціалізація 2. Низька ціна 3. Високий попит	Слабкі сторони: 1. Інформованість клієнтів 2. Слабке самозабезпечення фінансовими ресурсами
Можливості: 1. Можливість зміцнення іміджу 2. Можливість збільшення обсягів надання послуги	Загрози: 1. Збільшення конкуренції 2. Загроза праці без прибутку

З результатів SWOT-аналізу видно, що найбільші проблеми запуску стартапу – це проблеми, що пов’язані із входженням на ринок даних послуг. Але ця проблема вирішується за допомогою гарно розробленої методики маркетингу та просування продукту.

4.4 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції продукту, який отримає споживач. Для цього у таблиці 4.10 підсумовано результати попереднього аналізу конкурентоспроможності продукту.

Таблиця 4.10 – Визначення ключових переваг концепції потенційного продукту

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Аналіз безпеки BLE пристрою	Аналіз безпеки BLE пристрою	Вузька спеціалізація, в подальшому репутація
2	Шляхи вирішення виявлених проблем	Шляхи вирішення виявлених проблем	Конкуренти не пропонують

З таблиці 4.10 видно, що основними перевагами послуги є вузька спеціалізація, що може використовуватись при рекламуванні, та пропонування шляхів вирішення проблем, які були виявлені в ході аналізу безпеки.

З урахуванням вище сказаного можна визначити наступні пункти концепції маркетингових комунікацій:

1. Використання сильних сторін продукту і надання широкого спектру послуг для потенційного клієнта.
2. Використання соціальних і медіа можливостей.

Висновки до розділу 4

Після проведення даного маркетингового аналізу можна зробити висновок, що є висока можливість ринкової комерціалізації проекту. Обґрунтуваннями для такого рішення є високий попит, зростаюча динаміка ринку, задовільна рентабельність роботи на рику. Не зважаючи на існуючі незначні бар'єри входження та конкуренцію, з огляду на потенційні групи клієнтів і високу конкурентоспроможність, проект є високоперспективним. Для ринкової реалізації проекту доцільними є проведення додаткових рекламних компаній та пошук безкоштовних рекламних майданчиків або цільового персонального розповсюдження інформації для потенційних клієнтів.

ВИСНОВКИ

В даній роботі було розглянуто технологію Bluetooth Low Energy, її основні принципи та безпеку. Було вивчено праці про безпеку BLE пристроїв, зокрема контрольний лист рекомендіцій від NIST та оцінка безпеки фітнес трекерів групою дослідників з AV-Test.

Також було проведено власне дослідження безпеки BLE пристрою, а саме фітнес трекера Xiaomi MIBand 3, в результаті якого було виявлено ряд певних вразливостей.

На основі зібраних даних та з урахуванням недоліків розглянутих робіт було розроблено методику аналізу безпеки BLE пристроїв. Суть цієї методики полягає у перевірці відповідності пристроїів наступним критеріям:

1. Контрольована видимість
2. Безпека передачі даних
3. Контрольоване підключення
4. Аутентифікація

Також в методиці даються чіткі вказівки для перевірки кожного з критеріїв.

Теоретично, ця методика може застосовуватись до більшості BLE пристроїв, адже технологія BLE передбачає певні нормативні аспекти, які є спільними для багатьох пристроїв і ключовими при перевірці безпеки.

В четвертому розділі представлено стартап проект надання послуги аналізу безпеки BLE пристроїв. Згідно з проведеними дослідженнями стартап-проект є потенційно успішним.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. 2018 Bluetooth Market Update | Bluetooth Technology Website [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.bluetooth.com/bluetooth-resources/2018-bluetooth-market-update/
2. GATT Specifications | Bluetooth Technology Website [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.bluetooth.com/specifications/gatt/
3. BLE v4.2: Creating Faster, More Secure, Power-Efficient Design—Part 3 (.PDF Download) | Electronic Design [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.electronicdesign.com/datasheet/ble-v42-creating-faster-more-secure-power-efficient-design-part-3-pdf-download
4. BLE v4.2: Creating Faster, More Secure, Power-Efficient Designs—Part 2 | Electronic Design [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.electronicdesign.com/technologies/communications/article/21801870/ble-v42-creating-faster-more-secure-powerefficient-designspart-2
5. Core Specifications | Bluetooth Technology Website [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.bluetooth.com/specifications/bluetooth-core-specification/
6. Generic Attribute Profile (GATT) — BLE-Stack User's Guide for Bluetooth 4.2 3.01.00.05 documentation [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://dev.ti.com/tirex/content/simplelink_cc2640r2_sdk_1_40_00_45/docs/blestack/ble_user_guide/html/ble-stack-3.x/gatt.html
7. Attribute Protocol (ATT) and Generic Attribute Profile (GATT) - Building Bluetooth Low Energy Systems [Book] – 2017. – Режим доступу до ресурсу: https://www.oreilly.com/library/view/building-bluetooth-low/9781786461087/3323a094-8c3b-4c99-b28a-b284745a61b5.xhtml

8. Guide to Bluetooth Security | NIST [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.nist.gov/publications/guide-bluetooth-security-1
9. What is Bluesnarfing? A Closer Look at the Vulnerabilities of Bluetooth. [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.finjanmobile.com/what-is-bluesnarfing/
10. What is Bluejacking? - Definition from Techopedia [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.techopedia.com/definition/5045/bluejacking
11. Amrita Mitra, What is Car Whisperer? [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.thesecuritybuddy.com/bluetooth-security/what-is-car-whisperer/
12. Attack on the Bluetooth Pairing Process - Schneier on Security [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: https://www.schneier.com/blog/archives/2005/06/attack_on_the_b_1.html
13. Seven Fitness Wristbands and the Apple Watch in a Security Check 2016 | AV-TEST [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.av-test.org/en/news/seven-fitness-wristbands-and-the-apple-watch-in-a-security-check-2016/

ДОДАТОК А

Програмна реалізація підключення до фітнес трекера та ініціювання сповіщення дзвінка

```
const bluetooth = require('webbluetooth').bluetooth;
const crypto = require('browserify-aes');

const UUID_BASE = (x) => `0000${x}-0000-3512-2118-0009af100700`

const SERVICE_ALERT_NOTIFICATION = 0x1811
const SERVICE_IMMEDIATE_ALERT =    0x1802
const SERVICE_HEART_RATE =         0x180d
const SERVICE_MIBAND_1 =           0xfee0
const SERVICE_MIBAND_2 =           0xfee1
const key = new Buffer('30313233343536373839404142434445', 'hex');

const AB = function() {
  let args = [...arguments];
  args = args.map(function(i) {
    if (i instanceof Array) {
      return Buffer.from(i);
    }
```

```
    return i;
  })
  let buf = Buffer.concat(args);
  let ab = new ArrayBuffer(buf.length);
  let view = new Uint8Array(ab);
  for (let i = 0; i < buf.length; ++i) {
    view[i] = buf[i];
  }
  return ab;
}

const log = console.log;

async function test() {
  try {
    log('Searching Bluetooth Device...');
    const device = await bluetooth.requestDevice({
      filters: [
        { services: [ 0xFEE0 ] }
      ],
      optionalServices: [SERVICE_MIBAND_2, SERVICE_IMMEDIATE_ALERT]
```

```
});

device.addEventListener('gattserverdisconnected', () => {
  log('Device disconnected');
});

log('Connecting to the device...');
const server = await device.gatt.connect();
log('Connected');
let miband2 = await server.getPrimaryService(SERVICE_MIBAND_2);

let auth = await miband2.getCharacteristic(UUID_BASE('0009'))
let srvc_alert = await server.getPrimaryService(SERVICE_IMMEDIATE_ALERT)
let alert = await srvc_alert.getCharacteristic(0x2a06)

auth.startNotifications()
auth.addEventListener('characteristicvaluechanged', (event)=>{
  const value = Buffer.from(event.target.value.buffer);
  const cmd = value.slice(0,3).toString('hex');
  log(cmd);
  switch(cmd){
```

```
        case '100201':
          let rdn = value.slice(3)
          let cipher = crypto.createCipheriv('aes-128-ecb', key, '').setAutoPadding(false)
          let encrypted = Buffer.concat([cipher.update(rdn), cipher.final()])
          auth.writeValue(AB([0x03, 0x08], encrypted))
          break;
        case '100301':
          log('Success')
          alert.writeValue(AB([0x02]));
      }
    });
    auth.writeValue(AB([0x02, 0x08]));
  } catch(error) {
    log('ERROR!', error);
  }
}
test();
```