ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ/ SOFTWARE & HARDWARE ARCHITECTURE SECURITY

DOI: 10.18372/2225-5036.29.17548

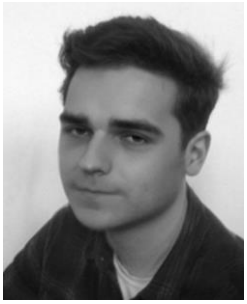
ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ BLUETOOTH-ПРИСТРОЇВ НА ОСНОВІ СМАРТ-ГОДИННИКІВ

Іван Опірський, Анатолій Шевчук, Юрій Сеник, Ольга Михайлова

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
ORCID ID: 0000-0002-8461-8996.

ШЕВЧУК Анатолій Анатолійович, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 2001 рік, м. Скалат, Тернопільська область, Україна.
Наукові інтереси: білий хакінг, методи та засоби захисту IoT-приладів, методи та засоби захисту хмарних технологій, розробка ПЗ в галузі кібербезпеки.
E-mail: tolikshewchuk@gmail.com.
ORCID ID: 0009-0003-5275-1594.



СЕНИК Юрій Андрійович, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 2003 рік, м. Козятин, Вінницька область, Україна.
Наукові інтереси: Розробка ПЗ в галузі кібербезпеки.
E-mail: Senik.yu@gmail.com.
ORCID ID: 0009-0002-2265-6476.

МИХАЙЛОВА Ольга Олександрівна, к.ф-м.н., доцент
Рік та місце народження: 1992 рік, м. Львів, Україна.
Освіта: Львівський національний університет імені Івана Франка, 2014 рік.
Посада: доцент кафедри захисту інформації з 2021 року.
Наукові інтереси: методи і засоби технічного захисту інформації, безпека програмного забезпечення, безпека інфраструктури комп'ютерних мереж, математичні методи та моделі захисту інформації, БПЛА.
Публікації: більше 15 наукових публікацій, серед яких наукові статті, монографії, тези та матеріали доповідей на конференціях.
E-mail: mykhaylovaolga1@gmail.com.
ORCID ID: 0000-0002-3086-3160.

Анотація. *Інтернет речей (IoT) - це мережа фізичних пристроїв, які мають вбудовані датчики та програмне забезпечення для передачі та обміну даними між фізичним світом та комп'ютерними системами, що здатні збирати та обробляти ці дані. Смарт-годинники можна вважати IoT-пристроями, оскільки вони оснащені практично всіма необхідними технологіями. Це носимі комп'ютери з вбудованими датчиками та системами зв'язку. Дослідження захищеності bluetooth в смарт-годинниках є дуже важливим у зв'язку з тим, що сучасний світ тісно пов'язаний з використанням бездротових технологій і Bluetooth є однією з найпоширенішою технологією цього типу. Bluetooth-пристрої містять велику кількість особистої інформації про користувача, такі як: геолокація, контакти, повідомлення та інші дані, що зберігаються на пристрої. Якщо захист від атак не є достатнім, то зловмисники можуть отримати несанкціонований доступ до особистих даних користувачів, що може призвести до серйозних наслідків, включаючи крадіжку ідентифікаційних і фінансових даних та іншу конфіденційну інформацію. У дослідженні описано, як можливі зловмисники можуть використовувати Bluetooth-технологію для злому даних та які кроки можна зробити, щоб захистити свої Bluetooth-пристрої від таких атак. Надані рекомендації щодо налаштування Bluetooth-пристроїв, використання паролів та шифрування, інші способи захисту даних. Наведено приклади зловмисницьких атак на Bluetooth-пристрої на прикладі сніффінг атаки з використанням Ubertooth one. Дослідження може бути корисним для всіх, хто використовує Bluetooth-пристрої, зокрема смарт-годинники, і хоче захистити свої дані від викрадення.*

Ключові слова: *Bluetooth, системи захисту, кібербезпека, Xiaomi Mi Watch, смарт-годинники, Ubertooth.*

Постановка проблеми

На сьогоднішній час Bluetooth-пристрої стали надзвичайно популярними серед користувачів з різних країн світу. Бездротові навушники, зокрема, стали революційним пристроєм, який змінив спосіб прослуховування музики та дзвінків. Bluetooth-годинники стали важливим доповненням до сучасного способу життя, дозволяючи вести облік своїх фізичних показників та отримувати повідомлення без необхідності витягнути телефон з кишені. Протягом останніх років, розробники продовжують вдосконалювати Bluetooth-технологію, додавати нові функції та забезпечувати її більшою швидкістю передачі даних та безпекою. Це дає можливість користувачам насолоджуватися новими функціями та можливостями, які забезпечують їхнє комфортне і зручне використання. У майбутньому Bluetooth-технологія буде продовжувати розвиватися та вдосконалюватися, відкриваючи нові можливості. Щороку, кількість та різноманітність пристроїв збільшується, вже зараз компанії, які раніше спеціалізувалися на виготовленні смартфонів, велику частину своїх ресурсів спрямовують на розробку та покращення своїх Bluetooth-пристроїв [1].

Аналіз останніх досліджень і публікацій

Bluetooth-технологія є однією з найбільш популярних форм бездротового з'єднання в сучасному світі (табл. 1). Вона дозволяє підключати між собою різні електронні пристрої, такі як годинники, телефони, навушники без використання проводів.

Розвиток Bluetooth-пристроїв відбувався протягом десятиліть і почався зі створення першої версії технології у 1994 році (табл. 2). Починаючи зі стандарту Bluetooth 1.0, технологія постійно вдосконалювалася відносно швидкості передачі даних, забезпечення безпеки та додаванням нових функцій [1].

Таблиця 1

Розвиток технології Bluetooth

Рік створення	Версія	Швидкість передачі даних	Моделі Bluetooth-годинників
1994	Bluetooth 1.0	1 Мбіт/с	Перша версія Bluetooth
2001	Bluetooth 1.2	1 Мбіт/с	Підтримка передачі голосу та даних одночасно
2004	Bluetooth 2.0	3 Мбіт/с	Підвищена швидкість передачі даних та покращена безпека
2007	Bluetooth 2.1	3 Мбіт/с	Автоматичне управління вимкненням Bluetooth
2009	Bluetooth 3.0	24 Мбіт/с	Підтримка високошвидкісної передачі даних
2010	Bluetooth 4.0	25 Мбіт/с	Нові можливості, такі як BLE (Bluetooth Low Energy) та NFC (Near Field Communication)
2013	Bluetooth 4.1	25 Мбіт/с	Покращене управління енергоспоживанням
2014	Bluetooth 4.2	25 Мбіт/с	Підвищена безпека та швидкість передачі даних
2016	Bluetooth 5.0	50 Мбіт/с	Підвищена швидкість передачі даних та дальність
2020	Bluetooth 5.2	78 Мбіт/с	Покращена безпека та підтримка нових функцій, таких як Audio Sharing та LE Audio

Таблиця 2

Продажі Bluetooth-пристроїв за 2022 рік

Пристрої	Кількість	Компанії–виробники	Поширеність пристроїв по країнах.
Навушники	220 млн.	Apple, Samsung, Xiaomi, Huawei, Sony та інші	США, Китай, Європа, Індія, Японія, Бразилія та інші
Годинники	140 млн.	Apple, Samsung, Xiaomi, Huawei, Garmin та інші	США, Китай, Великобританія Японія, Німеччина та інші
Колонки	110 млн.	JBL, Bose, Sony, Ultimate Ears та інші	США, Китай, Європа, Індія, Японія, Бразилія та інші
Автомобільні системи	50 млн.	Pioneer, Sony, Kenwood, Alpine, JVC та інші	США, Китай, Європа, Японія, Індія, Австралія та інші

Розвиток технологій не оминає й галузі годинників (табл. 3). Однією з новинок є смарт-годинник - пристрій, який не лише показує час, але й взаємодіє з користувачем та надає можливість користуватися різними функціями. Смарт-годинники, на відміну від звичайних годинників, можуть виконувати різноманітні завдання, такі як моніторинг здоров'я, отримання повідомлень, контроль за фізичною активністю та багато іншого. Також, вони можуть бути синхронізовані з іншими пристроями, такими як телефони та комп'ютери, що дає можливість виконувати більш складні завдання (рис. 1).

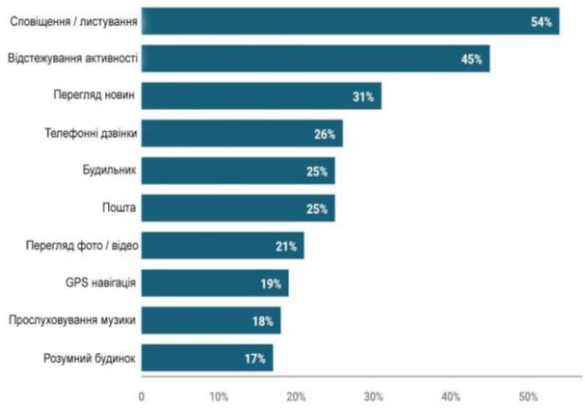


Рис. 1. Функції, які використовують користувачі смарт-годинників щоденно [4]

За останні роки смарт-годинники стали дедалі більш популярними серед споживачів, які шукають нові технології, що полегшують їхні повсякденні справи. Тільки в 2022 році, було продано понад 140 мільйонів різних розумних-годинників (рис.2).

Це змушує виробників постійно розвиватися та вдосконалювати свої пристрої, додавати нові функції та поліпшувати вже існуючі. Але разом з розвитком смарт-годинників з'являється й питання їхньої безпеки та захисту від зловмисників, оскільки вони містять велику кількість особистої інформації користувача.

Тому виробники та дослідники продовжують займатися розробкою нових методів захисту від зломів та крадіжок даних з смарт-годинників.

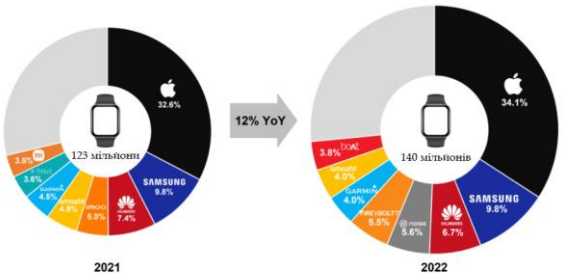


Рис. 2. Збільшення кількості проданих годинників

Таблиця 3

Кількість власників Bluetooth-годинників

Пристрої	Кількість	Найбільше користувачів	Моделі Bluetooth-годинників
Apple Watch	100 млн.	США, Канада, Великобританія, Франція, Японія та інші	Apple Watch Series 4, Apple Watch Series 5, Apple Watch Series 6, Apple Watch Series 7
Samsung Galaxy Watch	50 млн.	США, Південна Корея, Великобританія, Німеччина, Франція та інші	Samsung Galaxy Watch 4, Samsung Galaxy Watch 3, Samsung Galaxy Watch Active 2, Samsung Galaxy Watch Active, Samsung Galaxy Watch

Xiaomi Mi Watch	30 млн.	Китай, Індія, росія, Південна Корея, Польща та інші	Xiaomi Mi Watch, Xiaomi Mi Watch Lite, Xiaomi Mi Watch Color, Xiaomi Mi Watch Revolve, Xiaomi Mi Watch Lite 2
Huawei Watch	20 млн.	Китай, Європа, росія, Канада, Мексика та інші	Huawei Watch GT 2 Pro, Huawei Watch GT 2, Huawei Watch GT, Huawei Watch 3, Huawei Watch Fit
Garmin Forerunner	10 млн.	США, Канада, Австралія, Великобританія, Німеччина та інші	Garmin Forerunner 945, Garmin Forerunner 945 LTE, Garmin Forerunner 745, Garmin Forerunner 945 Music, Garmin Forerunner 245

Мета та постановка завдання

Метою даної роботи є дослідження захищеності Bluetooth-пристроїв на основі смарт-годинників з використанням Ubertooth One. У цій публікації будуть розглянуті основні проблеми, пов'язані з безпекою Bluetooth-з'єднань, та методи їх вирішення з використанням Ubertooth One. Дослідження проводиться з метою підвищення рівня безпеки Bluetooth-пристроїв та забезпечення конфіденційності та цілісності даних користувачів.

Виклад основного матеріалу

Персональні дані та їх обробка

В сучасному світі наша життєва активність досить часто відображається в цифровому вигляді. Персональні дані, які ми залишаємо в Інтернеті, на комп'ютерах та мобільних пристроях, стають все більшою складовою нашого життя. А з розвитком технологій виникають нові засоби збору та обробки цих даних. Одним з таких пристроїв є розумний годинник. Їхні функції та можливості, які забезпечують більш зручний та інформативний спосіб життя (рис. 3)

Основні причини популярності розумних годинників:

- фітнес-функції: розумні годинники забезпечують розширені можливості для відстеження фізичної активності та здоров'я, такі як підрахунок кількості кроків, відстеження пульсу, моніторинг сну та інше;
- сповіщення: розумні годинники дозволяють отримувати повідомлення, дзвінки, електронну пошту та інші сповіщення без потреби перевіряти телефон кожен раз;
- управління музикою: розумні годинники дозволяють керувати музикою на телефоні безпосередньо з годинника;
- голосові помічники: розумні годинники підтримують голосові помічники, такі як Siri або Google Assistant, що дозволяє користувачам задавати питання, давати команди та отримувати відповіді безпосередньо з годинника;
- стиль та мода: розумні годинники можуть бути стильними та модними аксесуарами, які доповнюють образ та підкреслюють індивідуальність користувача [3].

Розумні годинники здатні збирати різні дані про користувача, включаючи кількість кроків, які він зробив, кількість сну, якість сну, серцевий ритм, калорії, споживані напої та багато іншого. Ці дані збираються за допомогою різних датчиків, включаючи акселерометр, гіроскоп та датчик серцевого ритму.

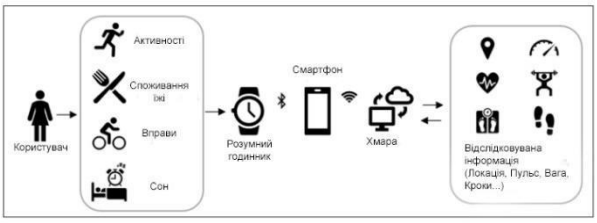


Рис. 3. Схема використання Смарт-годинника

Ці дані можуть бути корисними для користувача, оскільки вони можуть допомогти йому зрозуміти, як його здоров'я та активність змінюється з часом. Але ці дані можуть бути також використані іншими особами, наприклад, страховими компаніями або рекламодавцями. Тому важливо, щоб ці дані були оброблені та збережені з високим рівнем безпеки.

Фітнес-трекери та розумні годинники, можуть збирати різноманітні дані про користувача. Ці дані можуть включати:

1. пульс;
2. кров'яний тиск;
3. рівень активності;
4. режими сну;
5. місцезнаходження.

Все це дає можливість використовувати годинники також для медичних цілей. Одним із способів є використання даних для відстеження стану здоров'я пацієнта протягом тривалого часу. Це може бути корисним для виявлення тенденцій або змін у стані здоров'я. Іншим способом є використання даних для діагностики та лікування пацієнтів. Наприклад, якщо дані розумного годинника пацієнта показують нерегулярний пульс, лікар може використовувати цю інформацію для діагностики та лікування основного захворювання [14].

Процес збору даних в Bluetooth годинниках відбувається наступним чином:

1. датчики в годиннику: годинники можуть мати вбудовані датчики, такі як акселерометр, гіроскоп, пульсометр та GPS, які дозволяють збирати різні дані про користувача;
2. передача даних через Bluetooth: дозволяє годиннику надсилати зібрані дані на сумісний з ним смартфон чи інший пристрій;
3. збір та аналіз даних: після передачі даних на сумісний пристрій, можна використовувати спеціальні додатки для збору та аналізу цих даних. Наприклад, додаток для фітнесу може зібрати дані про кількість кроків, відстань та кількість спалених калорій, щоб допомогти користувачу контролювати свої фітнес-цілі;

4. зберігання даних: після збору та аналізу даних, вони можуть бути збережені на пристрої користувача чи у хмарному сховищі; це дозволяє зберігати дані та порівнювати їх з часом, щоб визначити покращення у своїх цілях та досягненнях.

Проблеми захищеності Bluetooth годинників

Існують три основні причини, через які розумний годинник може становити загрозу безпеці та конфіденційності.

1. Збір даних

Годинник постійно відстежує склад вашого тіла і діяльність. Потім ці дані синхронізуються пристроями та серверами компанії. Зараз, дані можуть потрапити в чужі руки двома шляхами (рис. 4).

Перший – якщо зловмисник заволодіє вашим телефоном і всіма даними, що містяться на ньому. Управління цим ризиком знаходиться під контролем користувача.

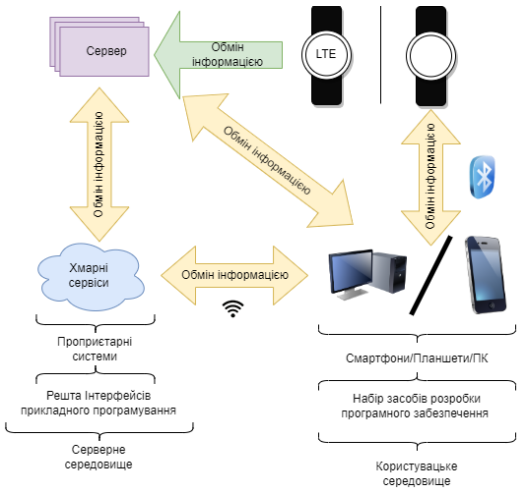


Рис. 4. Процес збору даних з Bluetooth-годинників

Іншим способом компрометації даних є витік даних або кібератака на компанію, яка розробляє розумні годинники. Управління цим ризиком не залежить безпосередньо від користувача, тому вибір компанії, яка надає пріоритет конфіденційності, є важливим фактором, який слід враховувати перед покупкою розумного годинника [16].

Крім ризику кібератак і витоку даних, сторонні програми також мають доступ до конфіденційних даних користувача, які збирає смарт-годинник.

2. Передача даних між годинником і телефоном

Безпека Wi-Fi і Bluetooth з кожним роком покращується. Однак ці технології бездротового підключення залишаються вразливими до витоку даних [13].

Розумні годинники мають три способи підключення: Bluetooth, Wi-Fi або LTE. Більшість моделей оснащені Bluetooth і Wi-Fi, а дорожчі моделі мають LTE. Для передачі даних із годинника на телефон (і сервери компанії) моделі Bluetooth/Wi-Fi мають синхронізуватися з програмою. Однак моделі LTE можуть підключатися до Інтернету напряму та синхронізувати дані в режимі реального часу. Однак моделі LTE зазвичай споживають більше енергії, і більшість людей віддають перевагу Bluetooth або Wi-Fi. Неважливо, яку модель вибирати, завжди існує ризик того, що хтось із відповідними інструментами, навичками та мотивацією може зламати ваш пристрій і викрасти дані.

3. Годинник завжди можна відстежити

Годинник може використовувати дані GPS для створення карти маршруту вашого тренування на відкритому повітрі або поїздки на роботу. Завдяки цьому вас постійно можна відстежувати, тому що, якщо у вас є годинник, то здебільшого він буде у вас на руці практично завжди.

Таблиця 4

Порівняння вбудованих видів безпек в різних моделях розумних годинників

Вид безпеки	Apple Watch Series 7	Mi Band 6	Amazfit GTS 2	Samsung Galaxy Watch 4
Шифрування	AES-256	AES-128	AES-128	AES-256
Захист пароля	Так	Так	Так	Так
Захист від підробки даних	Так	Так/Ні	Так/Ні	Так
Вбудований VPN	Ні	Ні	Ні	Ні
Антивірусний захист	Ні	Ні	Ні	Ні
Visibility Control	Так	Так	Так	Так
Конфіденційність Bluetooth LE	Так	Так	Ні	Так
Контрольоване підключення	Так	Так	Так	Так
Захист від зміни даних	Так	Так	Ні	Так
Незахищене локальне сховище	Ні	Так	Ні	Ні
Обфускація коду	Так	Так	Так	Так

Способи захисту Bluetooth годинників

Безпека розумних годинників не є ідеальною, але можна зробити декілька простих речей, щоб зробити їх безпечнішими у використанні.

1. Видалити непотрібні програми сторонніх розробників ПЗ.

Розумний годинник постачається з програмами за замовчуванням. Ці програми не займають багато пам'яті, але вони точно можуть збирати дані. Потрібно переглянути програми на розумному годиннику та подумати про видалення непотрібних. Також потрібно перевірити, чи існуюча програма відповідає потребам, перш ніж встановлювати нову. Можна не тільки зменшити кількість додатків, які мають доступ до ваших даних, але й збільшити час роботи акумулятора годинника.

2. Вимикати розумний годинник, коли він вам не потрібен.

Потрібно подумати про те, щоб вимкнути розумний годинник, коли він не використовується, особливо якщо ви турбуєтеся про моніторинг місцезнаходження. Він все одно збиратиме дані про тіло та активність, але шанси прив'язати ці дії до вашого дому нижчі. Недоліком є те, що можуть не подобатися нагадування на основі місцезнаходження.

3. Уникати громадського Wi-Fi , підключення може зробити вас вразливим до злому.

4. Постійно оновлювати ОС свого смарт-годинника, щоб хакери не могли скористатися недоліками безпеки.

5. Зробити свій бездротовий маршрутизатор більш безпечним , щоб захистити його від хакерів.

6. Регулярно оновлювати телефон і комп'ютер, який використовується для обміну даних із годинником.

7. Регулярно видаляйте непотрібні дані смарт-годинника.

8. Вимкнути в налаштування годинника GPS-трекінг.

9. Встановити додатки, які орієнтовані на конфіденційність [17].

Атаки на Bluetooth годинники

Smart-годинники, як і будь-який інший пристрій, що підключається до мережі Інтернет, можуть бути піддаються різним видам кібератак. Ось деякі типові атаки на smart-годинники, на які можуть бути вразливі ці пристрої:

1. Фішингові атаки: ці атаки полягають у відправленні користувачеві підробленого повідомлення або електронної пошти, яке намагається переконати користувача надати свої облікові дані, такі як ім'я користувача і пароль;

2. Вірусні атаки: smart-годинники можуть стати жертвами вірусів, які можуть пошкодити або скомпрометувати пристрій. Наприклад, зловмисники можуть розсилати відправки, що містять вірусні додатки, які дозволяють зловмисникам отримувати доступ до особистих даних користувача;

3. Атаки на Bluetooth: smart-годинники використовують Bluetooth для підключення до інших пристроїв, таких як смартфони і ноутбуки. Зловмисники можуть використовувати; Bluetooth-атаки для отримання доступу до пристрою та його даних, або для відправки шкідливих команд на пристрій;

4. Соціальна інженерія: ці атаки полягають у використанні соціальної інженерії для отримання доступу до пристрою, наприклад, зловмисники можуть намагатися отримати фізичний доступ до пристрою, зламати пароль або використати зламану інформацію з облікового запису користувача;

5. Атаки на додатки: smart-годинники мають різноманітні додатки, які можуть бути піддаються атакам; зловмисник може створити фальшивий додаток, який схожий на оригінальний додаток, та використовувати його для збору;

6. Фізичні атаки: smart-годинники можуть бути скомпрометовані, якщо їх вкрасти або загубити; хакери можуть використовувати викрадений пристрій, щоб отримати доступ до особистих даних користувача.

Далі, розглянемо декілька атак більш детально. Атака сторонніми каналами – це методи злому, коли зловмисники використовують розумні годинники, щоб отримати доступ до введеного користувачем тексту на мобільному пристрої (рис. 5). Такі атаки використовують можливість бездротового з'єднання між розумним годинником і мобільним телефоном, щоб перехоплювати і аналізувати дані, що передаються між ними. Коли користувач вводить пароль або іншу конфіденційну інформацію на мобільному телефоні за допомогою клавіатури, розумний годинник може відслідковувати його рухи і отримувати доступ до введеного тексту [5].

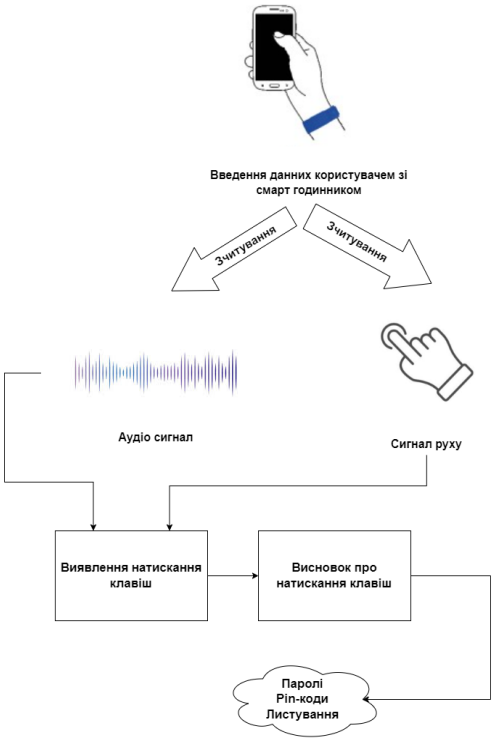


Рис. 5. Схема процесу проведення атаки сторонніми каналами

Існує кілька видів атак сторонніми каналами, таких як акустична атака, інфрачервона атака та електромагнітна атака. В кожному з цих випадків зловмисники використовують різні методи, щоб отримати доступ до конфіденційної інформації користувача.

Щоб захиститися від даного типу атак з, користувачі можуть використовувати захисні механізми,

такі як шифрування даних та використання безпечних протоколів з'єднання. Також рекомендується використовувати клавіатуру з віртуальною розкладкою, яка випадковим чином переміщує кнопки на клавіатурі, щоб ускладнити використання прослуховування клавіатури [6].

Атаки автентифікації з бічного каналу за допомогою розумних годинників - це методи злому, коли зловмисники використовують розумні годинники, щоб отримати доступ до конфіденційної інформації, такої як паролі і коди доступу, які використовуються для автентифікації користувача в системі [15].

Ці атаки використовують можливість бездротового з'єднання між розумним годинником і мобільним пристроєм, який зазвичай використовується для автентифікації користувача. Зловмисники можуть перехоплювати дані, що передаються між розумним годинником і мобільним телефоном, щоб отримати доступ до конфіденційної інформації [8].

Наприклад, коли користувач використовує розумний годинник для автентифікації в системі, зловмисник може перехопити дані, що передаються між годинником і мобільним телефоном, і використовувати їх для створення фальшивого з'єднання з системою. Це може дозволити зловмиснику отримати доступ до захищеної інформації, такої як фінансові дані, електронна пошта або особиста інформація [11].

Існує кілька методів для захисту від атак автентифікації з бічного каналу за допомогою розумних годинників [7].

Один з найефективніших методів полягає у використанні двофакторної аутентифікації, що передбачає використання двох різних методів автентифікації для підтвердження ідентифікації користувача [10].

Наприклад, користувач може використовувати пароль та зовнішній токен для автентифікації в системі.

Bluetooth Sniffing - це процес перехоплення бездротового зв'язку між Bluetooth-пристроями для збору і аналізу даних. Одним з інструментів, які бути використані для Bluetooth Sniffing, є Ubertooth (рис. 6).

Ubertooth - це засіб збору та аналізу Bluetooth-трафіку, який може використовуватися для здійснення атак, таких як аналіз шифрування, перехоплення даних, а також для виявлення безпекових вразливостей в Bluetooth-протоколі.

Для використання Ubertooth для Bluetooth Sniffing необхідно встановити програмне забезпечення на комп'ютер та підключити Ubertooth до USB-порту. Далі, з використанням програмного забезпечення, можна розпочати перехоплення Bluetooth-трафіку. [9]

Ubertooth може бути використаний для перехоплення трафіку між Bluetooth-пристроями, такими як мобільні телефони, ноутбуки, навушники або інші пристрої з Bluetooth-інтерфейсом. Для цього Ubertooth може сканувати Bluetooth-діапазон для пошуку доступних пристроїв та слідкувати за передачею даних між ними.

Після перехоплення трафіку Ubertooth може допомогти в аналізі та інтерпретації даних. Наприклад, можна використовувати Ubertooth для аналізу шифрування Bluetooth-трафіку та для здійснення атак на з'єднання, що засновані на виявлених вразливостях. Також можна використовувати Ubertooth для влагодження та тестування Bluetooth-протоколів.

Рис. 6. Інструмент для сніфінгу – Ubertooth one

З метою захисту від Bluetooth Sniffing можна використовувати криптографічні протоколи, такі як AES-256, для шифрування переданих даних між Bluetooth-пристроями [2].

Bluetooth Sniffing за допомогою Ubertooth

Далі, розглянемо на прикладі реалізацію Bluetooth Sniffing.

Крок №1

Для виконання даної атаки нам знадобиться Ubertooth One, середовище для проведення атаки(Kali linux), ПЗ(Wireshark), Smart-годинник (Amazfit Bip Watch).

Встановлюємо компоненти для Ubertooth One Встановлюємо бібліотеку libbtbb, щоб Ubertooth мав змогу декодувати пакети Bluetooth Завантажуємо Ubertooth з гіт репозиторію Встановлюємо модулі для роботи з Wireshark, що дозволяють використовувати графічний інтерфейс.

Крок №2

Після налаштування попередніх плагінів, ми приєднуємо пристрій Ubertooth One через порт USB (рис. 7).

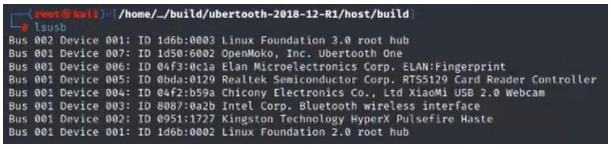


Рис. 7. Перегляд підключених пристроїв

Після першого запуску Ubertooth One необхідно оновити його мікропрограму. Інструменти, які були завантажені раніше, полегшують спрощений спосіб досягнення цього завдання.

Крок №3

Перевіряємо функціональність пристрою Ubertooth за допомогою аналізатора спектру, який є інструментом для аналізу діапазону 2,4 ГГц (рис. 8).

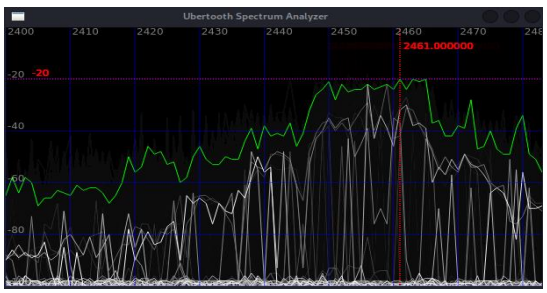


Рис. 8. Перевірка функціональності Ubertooth one, за допомогою аналізатора спектру

Зокрема, він надає інструмент графічного інтерфейсу користувача (GUI) під назвою ubertooth-specan-ui, який візуально контролює частоти.

Крок №4

BD_ADDR робить можливим *розподіл* прослуханих пакетів Bluetooth. Ubertooth One може почати сканування LAP (рис. 9).

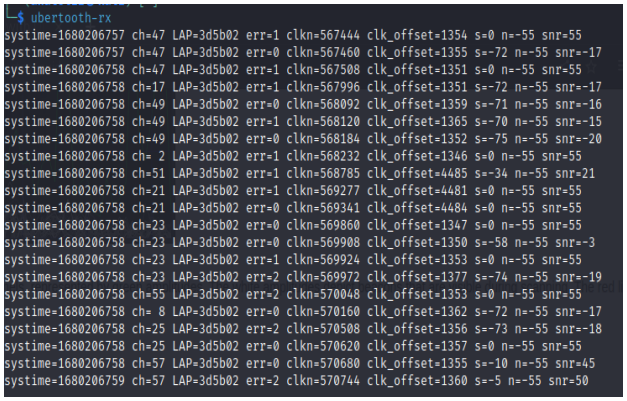


Рис. 9. Активація розподілу прослуханих пакетів Bluetooth

BD_ADDR — це 48-бітна MAC-адреса. LAP складається з молодших 24 бітів BD_ADDR і є єдиною частиною адреси, яка передається з кожним пакетом. тим самим, можна визначити, частину Mac-адреси годинника-жертви.

Крок №5

Одним із найпотужніших інструментів, які надає Ubertooth One, є режим аналізу з низьким енергоспоживанням Bluetooth.

Крім усього іншого, він може сніфити і стежити за з'єднаннями і навіть втручатися в нього. У режимі «підписка» Ubertooth слухає один із трьох рекламних каналів. Після встановлення BLE-з'єднання, Ubertooth стежитиме за переходами вздовж каналів даних, фіксуючи передачу між пристроями.

За замовчуванням Ubertooth можна використовувати для відстеження будь-якого з'єднання, яке він спостерігає випадковим чином. Далі, можна спробувати перехопити певні пакети, надіслані годинником, визначивши тим самим, наприклад його Mac-адресу, чи назву пристрою, тоді з цією інформацію можна проводити інші атаки.

Загалом, Ubertooth – це багатофункціональний пристрій для здійснення різних типів атак на Bluetooth-пристрої.

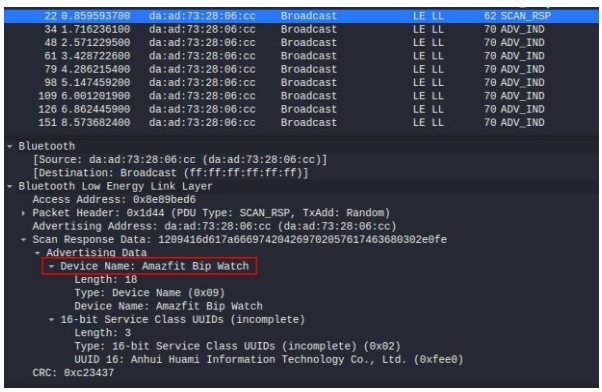


Рис. 10. Успішно перехоплені пакети з розумного годинника – Amazfit Bip Watch

Таблиця 5

Можливі атаки з допомогою Ubertooth-one

Тип атаки	Опис
Атака на протокол шифрування	За допомогою Ubertooth One можна вивчити протоколи шифрування, використовувані в Bluetooth-з'єднаннях, та виявити можливі вразливості в цих протоколах.
Атака на ідентифікатор пристрою	За допомогою Ubertooth One можна виявити можливі вразливості в ідентифікаторах Bluetooth-пристроїв та підробити їх, що дозволяє зловмисникам відправляти шкідливі пакети даних на пристрої.
Атака на перехоплення даних	За допомогою Ubertooth One можна вивчити протоколи, використовувані для передачі даних в Bluetooth-з'єднаннях, та перехоплювати ці дані. Це може призвести до витоку конфіденційної інформації.
Атака на дозвіл доступу	За допомогою Ubertooth One можна вивчити протоколи, використовувані для авторизації користувачів на Bluetooth-пристроях, та виконувати атаки на дозвіл доступу, що дозволяє зловмисникам отримувати несанкціонований доступ до пристрою.

Висновки. В статті було досліджено основні проблеми, пов'язані з безпекою Bluetooth-з'єднань, такі як перехоплення даних, атаки на протоколи шифрування та підроблення ідентифікаторів пристроїв.

Безпека Bluetooth-пристроїв є досить складною та багатогранною проблемою, яка стає все більш актуальною в світі швидко зростаючої кількості бездротових пристроїв, що використовують технологію Bluetooth. Основні проблеми безпеки пов'язані з можливістю зламування паролів, перехопленням та підробкою сигналів, а також з вразливостями, що виникають в процесі обміну даними між пристроями. Однією з основних рекомендацій для забезпечення безпеки Bluetooth-пристроїв є використання надійних паролів та шифрування даних. Також варто звернути увагу на те, яку версію Bluetooth використовує пристрій, оскільки пізніші версії мають покращену захист від атак. Для забезпечення безпеки Bluetooth-пристроїв також важливо оновлювати програмне забезпечення на пристроях, що використовують технологію Bluetooth, оскільки вразливості можуть бути виправлені за допомогою оновлень. В цілому, безпека Bluetooth-пристроїв залежить від багатьох факторів, таких як використання надійних паролів та шифрування даних, версії Bluetooth, оновлення програмного забезпечення, та багатьох інших. При правильному використанні технології Bluetooth та дотриманні рекомендацій безпеки, ризик порушення безпеки Bluetooth-пристроїв може бути значно зменшений. Для розв'язання проблем безпеки було використано

Одним з найбільш цінних аспектів використання Ubertooth One є можливість аналізувати трафік Bluetooth з високою точністю і швидкістю. Інструмент

має високу чутливість, що дозволяє виявляти й аналізувати сигнали, які інші пристрої можуть пропустити. Також важливим аспектом є те, що Ubertooth One є дуже гнучким та легко настроюється під потреби користувача. Він має відкритий код, що дозволяє змінювати та покращувати його функціональність. Більш того, додаткові функції можуть бути додані до інструменту за допомогою різних плагінів, що значно розширює можливості Ubertooth One.

Стаття показує, що дослідження захищеності Bluetooth-пристроїв на основі смарт-годинників з використанням Ubertooth One є ефективним методом забезпечення безпеки та захисту даних користувачів. Такий аудит безпеки може бути проведений будь-яким користувачем, хто має Ubertooth One та базові знання про Bluetooth-технології. Застосування Ubertooth One є корисним не лише для фахівців з безпеки, а й для будь-якого користувача, який хоче захистити свої дані та пристрої від зловмисних атак.

Список літератури

[1] Специфікація Bluetooth [Електронний ресурс] – https: // www. bluetooth. com / specifications / bluetooth-core-specification/.

[2] Опис технічних характеристики Ubertooth One [Електронний ресурс] – https: // github. com/ greatscottgadgets/ubertooth/wiki.

[3] І.Р. Опірський, І.С. Р.В. Головчак, І.Р. Мойсійчук, Т. Балянда, і С. Гаранюк, «Проблеми та загрози безпеці іот пристроїв»// Кібербезпека: освіта, наука, техніка, вип. 3, вип. 11, С. 31-42, 2021.

[4] Опірський І.Р., Тютіков О.Ю. Проблематика побудови концепції «Розумного міста» // НАУ: «Захист інформації». – Том 2, Випуск №22. – Київ, 2020р. С.114-119.

[5] Asonov, D., and Agrawal, R. Keyboard acoustic emanations. In IEEE S & P (2004).

[6] Cai, L., and Chen, H. Touchlogger: Inferring keystrokes on touch screen from smartphone motion. In HotSec (2011).

[7] Owusu, E., Han, J., Das, S., Perrig, A., and Zhang, J. ACCessory: Password Inference Using Accelerometers on Smartphones. In ACM HotMobile (2012).

[8] Vuagnoux, M., and Pasini, S. Compromising electromagnetic emanations of wired and wireless keyboards. In USENIX Security (2009).

[9] Xu, Z., Bai, K., and Zhu, S. Taplogger: Inferring user inputs on smartphone touchscreens using on

[10] P. C. van Oorschot, A. Somayaji, and G. Wurster, "Hardware-assisted circumvention of self-hashing software tamper resistance," IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 2, pp. 82–92, April 2005.

[11] A. Lewis, Y. Li, and M. Xie, "Real time motion-based authentication for smartwatch," in 2016 IEEE Conference on Communications and NetworkSecurity (CNS), Oct 2016, pp. 380–381.

[12] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," in 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Sept 2015, pp. 1–6.

[13] M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, and B. Messabih, "A completely automatic public physical test to tell computers and humans apart: A way to enhance authentication schemes in mobile devices," in 2015 International Conference on High Performance Computing Simulation (HPCS), July 2015, pp. 203–210.

[14] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA:ACM, 2011, pp. 197–200.

[15] D. Nyang, A. Mohaisen, and J. Kang, "Keylogging-resistant visual authentication protocols," IEEE Transactions on Mobile Computing, vol. 13, no. 11, pp. 2566–2579, Nov 2014.

[16] I. Oakley, J. H. Huh, J. Cho, G. Cho, R. Islam, and H. Kim, "The personal identification chord: A four button authentication system for smartwatches," in Proceedings of the 2018 on Asia Conference on Computer and Communications Security, ser. ASIACCS '18. New York, NY, USA: ACM, 2018, pp. 75–87.

[17] A. Merlo, M. Migliardi, and P. Fontanelli, "Measuring and estimating power consumption in android to support energy-based intrusion detection," vol. 23, no. 5, pp. 611–613.

УДК 004.056.5

Opirskyy I., Shevchyk A., Senyk Yu., Mykhaylova O. Security research of bluetooth devices based on smart watches

Abstract. *The Internet of Things (IoT) is a network of physical devices that have built-in sensors and software to transmit and exchange data between the physical world and computer systems capable of collecting and processing that data. Smart watches can be considered as IoT devices because they are equipped with almost all necessary technologies. These are wearable computers with built-in sensors and communication systems. Studying the security of bluetooth in smart watches is very important due to the fact that the modern world is closely related to the use of wireless technologies and Bluetooth is one of the most common technologies of this type. Bluetooth devices contain a large amount of personal information about the user, such as: geolocation, contacts, messages and other data stored on the device. If protection against attacks is not sufficient, attackers can gain unauthorized access to users' personal data, which can lead to serious consequences, including the theft of identity and financial data and other sensitive information. The study describes how potential attackers can use Bluetooth technology to compromise data and what steps you can take to protect your Bluetooth devices from such attacks. Recommendations for setting up Bluetooth devices, using passwords and encryption, and other data protection methods are provided. Examples of malicious attacks on Bluetooth devices are given using the example of a sniffing attack using the Ubertooth one. The research can be useful for anyone who uses Bluetooth devices, especially smartwatches, and wants to protect their data from being stolen.*

Key words: *Bluetooth, security systems, cyber security, Xiaomi Mi Watch, smart watches, Ubertooth.*

Опірський Іван Романович, доктор технічних наук, професор, кафедра захисту інформації, Національного університету «Львівська політехніка».
Ivan Opirskyy, doctor of Technical Sciences, professor, Department of Information Security, Lviv Polytechnic National University.

Шевчук Анатолій Анатолійович, студент, кафедра захисту інформації, Національного університету «Львівська політехніка».
Anatolii Shevchyk, student, Department of Information Security, Lviv Polytechnic National University.

Сеник Юрій Андрійович, студент, кафедра захисту інформації, Національного університету «Львівська політехніка».
Yurii Senyk, student, Department of Information Security, Lviv Polytechnic National University.

Михайлова Ольга Олександрівна, кандидат фіз.-мат. наук, доцент, кафедра захисту інформації, Національного університету «Львівська політехніка».
Olga Mykhaylova, candidate of physics and mathematics Sciences, Associate Professor, Department of Information Protection, Lviv Polytechnic National University.

Отримано 1*3 лютого 2023 року,* затверджено редколегією *27 березня 2023 року*