МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Хрищук Олександр Сергійович

УДК 004.89

ДОСЛІДЖЕННЯ ПРОБЛЕМИ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ В БЕЗДРОТОВИХ МЕРЕЖАХ

124 – Системний аналіз

Автореферат
магістерської кваліфікаційної роботи на здобуття освітньої кваліфікації
«Магістр системного аналізу»

Миколаїв – 2021

Магістерська кваліфікаційна робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі інтелектуальних інформаційних систем.

Науковий керівник:	доцент кафедри інтелектуальних інформаційних систем, к. т. н., доцент Кондратенко Галина Володимирівна.
Рецензент:	кандидат технічних наук, доцент Солобуто Лариса Вадимівна.

Захист відбудеться «24» лютого 2021 р. о $9^{\underline{30}}$ год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З магістерською кваліфікаційною роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений «16» лютого 2021 р.

Секретар екзаменаційної комісії, к.пед.н., доцент Н. М. Болюбаш

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми

Актуальність даного дослідження походить від популярності використання бездротових мереж у повсякденному житті. З популярністю приходять загрози. Для бездротових мереж це шанс втратити особисті дані, бути об’єктом шпіонажу або звичайного хуліганства у невчасний момент.

Об’єктом дослідження є бездротові мережі на прикладі мережі Wi-Fi.

Предметом дослідження є існуючі види атак як на мережу, так і на її користувачів.

Мета

Метою дослідження є виявлення, перевірка та оцінка можливої завданої шкоди від основних та найпростіших видів атак. Також, виникає необхідність пошуку та опрацювання наявних методів захисту від проведених атак.

В результаті виконання роботи було проведено аудит тестової Wi-Fi точки за допомогою відкритого програмного забезпечення та відкритих програмних бібліотек. Було написано декілька простих програмних помічників для проведення аудиту, опрацьовано результати аудиту.

Теоретичною основою цієї роботи стали статті та документація до вже готових методів що представлені у мережі Інтернет.

Практичне значення отриманих результатів

Проведене дослідження та аудит тестової точки доступу дають розуміння, на основі практичних досліджень, про загрози, що переслідують користувачів бездротових мереж та показують простоту проведення атак. Також, було надано оцінку та описано можливі методи захисту від описаних атак.

Структура дипломної роботи

Дана робота складається з п’яти розділів. Кожен розділ відповідно присвячений: аналізу предметної області, надання наявної інформації щодо

відомих видів атак, практичне проведення аудиту бездротової мережі, охороні праці і безпеці життєдіяльності, методичній частині магістерської роботи. Загальний обсяг роботи – 65 сторінок. Магістерська робота містить один додаток, 28 рисунків, 6 таблиць і посилання на 27 джерел.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ

Приведено тези щодо актуальності теми даної роботи, наведено можливі варіанті взаємодії із бездротовими мережами, зроблено аналіз загроз.

Розділ 1

Розділ присвячено здобуттю інформації щодо тонкощей реалізації бездротової мережі Wi-Fi: розглянуто історію створення, модель взаємодії, фізичний та протокольний рівні. Також, було визначено найпопулярніші кадри протоколу, що використовуються зловмисниками для втручання або набуття інформації.

Технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11. Під абревіатурою Wi-Fi в даний час розвивається ціле сімейство стандартів передачі цифрових потоків даних по радіоканалах. Основними діапазонами Wi-Fi вважаються 2.4 ГГц (2412 МГц-2472 МГц) і 5 ГГц (5160-5825 МГц). Сигнал Wi-Fi може транслюватися на кілометри навіть при низькій потужності передачі, але для прийому Wi-Fi сигналу зі звичайного Wi-Fi маршрутизатора на далекій відстані потрібна антена з високим коефіцієнтом посилення (наприклад параболічна антена або Wi-Fi гармата).

Wi-Fi був створений в 1998 році в лабораторії радіоастрономії CSIRO[6]. Творцем бездротового протоколу обміну даними є інженер Джон О'Салліван.

Стандарт IEEE 802.11n був затверджений 11 вересня 2009 року. Його застосування дозволяє підвищити швидкість передачі даних практично вчетверо в порівнянні з пристроями стандартів 802.11g (максимальна швидкість яких дорівнює 54 Мбіт/с), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично 802.11n здатний забезпечити швидкість передачі даних до 600 Мбіт/с. З 2011 по 2013 розроблявся стандарт IEEE 802.11ac, стандарт прийнятий в січні 2014 року. Швидкість передачі даних при використанні 802.11ac може досягати декількох 1 Гбіт/с.

27 липня 2011 року IEEE випустив офіційну версію стандарту IEEE 802.22[7]. Системи й пристрої, що підтримують цей стандарт, дозволяють приймати дані на швидкості до 22 Мбіт / с в радіусі 100 км від найближчого передавача.

У жовтні 2018 року «Wi-Fi Alliance» представив нові назви і значки для Wi-Fi:

- 802.11n, Wi-Fi 4;
- 802.11ac, Wi-Fi 5;
- 802.11ax, Wi-Fi 6.

Зазвичай схема мережі Wi-Fi містить не менше однієї точки доступу і не менше одного клієнта. Також можливе підключення двох клієнтів в режимі точка-точка (Ad-hoc), коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережевих адаптерів «безпосередньо». Точка доступу передає свій ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів на швидкості 0,1 Мбіт/с кожні 100 мс. Тому 0,1 Мбіт/с - найменша швидкість передачі даних для Wi-Fi. Знаючи SSID мережі, клієнт може з'ясувати, чи можливе підключення до даної точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на підставі даних про рівень сигналу. Стандарт Wi-Fi дає клієнтові повну свободу при виборі критеріїв для з'єднання.

Прилади Wi-Fi обмінюються даними, передаючи один одному пакети даних: блоки даних, що індивідуально надсилаються та доставляються за допомогою радіо частот. Як і у випадку з усіма радіо пристроями, це робиться шляхом модуляції та демодуляції несучих хвиль. У різних версіях Wi-Fi використовуються різні техніки, 802.11b використовує DSSS на одній несучій, тоді як 802.11a, Wi-Fi 4, 5 і 6 використовують кілька несучих на дещо різних частотах усередині каналу.

Як і в інших локальних мережах IEEE 802, станції запрограмовані з унікальним 48-бітовим MAC-адресом, так що кожна станція Wi-Fi має унікальну адресу. MAC-адреси використовуються для вказівки як пункт призначення та

джерело кожного пакета даних. Wi-Fi встановлює з'єднання на рівні зв'язку, які можна визначити, використовуючи як адреси призначення, так і джерела. Під час прийому передачі приймач використовує адресу призначення, щоб визначити, чи відповідає передача станції, чи її слід ігнорувати. Мережевий інтерфейс зазвичай не приймає пакети, адресовані іншим станціям Wi-Fi.

Канали використовуються в напівдуплексному режимі і можуть розподілятися за часом між різними мережами. Коли зв’язок відбувається за одним і тим же каналом, будь-яка інформація, надіслана одним комп’ютером, приймається локально всіма, навіть якщо ця інформація призначена лише для одного пункту призначення. Мережева карта інтерфейсу перериває центральний процесор лише тоді, коли отримані відповідні пакети: ігнорує інформацію, не адресовану йому. Використання одного і того ж каналу також означає спільну пропускну здатність даних, наприклад, доступна пропускна здатність даних для кожного пристрою зменшується вдвічі, коли дві станції активно передають.

Wi-Fi, як частина сімейства протоколів IEEE 802, організує дані у кадри 802.11, які дуже схожі на кадри Ethernet на рівні каналу передачі даних, але з додатковими полями адрес. MAC-адреси використовуються як мережеві адреси для маршрутизації через локальну мережу.

На додаток до 802.11 сімейство протоколів IEEE 802 має спеціальні положення щодо Wi-Fi. Вони потрібні, оскільки кабельні носії Ethernet, як правило, не використовуються спільно, тоді як при бездротовому зв'язку всі передачі приймаються усіма станціями в межах діапазону, що використовує цей радіоканал. Хоча Ethernet має по суті незначну частоту помилок, носії бездротового зв'язку зазнають значних перешкод. Тому, точна передача не гарантується. Через це для Wi-Fi LLC, визначений IEEE 802.2, використовуються протоколи управління доступом до мультимедіа Wi-Fi для управління спробами передачі, не покладаючись на більш високі рівні стека протоколів.

Бездротові мережі дуже схожі за принципом роботи на звичайні дротові мережі, за виключенням рівня доступу до цифрової інформації мережі: у випадку дротової мережі необхідно мати фізичний контакт з кабелем мережі, що

нівелюється у бездротових мережах, де достатньо знаходитись у радіусі дії випромінювача мережі.

Виконання поставленої задачі дасть розуміння найпопулярніших ризиків при використанні бездротових мереж Wi-Fi.

Розділ 2

В цьому розділі було ознайомлено з інструментарієм дипломної роботи: описано вже існуюче програмне забезпечення та визначено бібліотеки для легкої розробки власного.

На другому етапі було розібрано найпопулярніші атаки на бездротову мережу Wi-Fi:

- блокування роботи мережі;
- ідентифікація користувача мережі за IMSI;
- детектування можливих місць перебування користувача;
- пошук користувача\точки доступу у радіусі дії мережі;
- збір наявної інформації в мережі.

Більшість атак на мережі типу Wi-Fi використовують протокольний рівень та маніпулюють пакетами даних відносно жертви або точки доступу. Також, при атаках враховуються оточуючі властивості (якість та спроможність сигналу дійти до жертви) для найбільш вигідного результату.

Для проведення аудиту буде використано вже існуюче спеціальне програмне забезпечення. Для деяких випадків буде розроблено на мові програмування C++ з використанням бібліотек та фреймворку Qt для спрощення реалізації:

- Qt – мультиплатформний фреймворк для розробки програмного забезпечення на мові програмування C ++. Qt дозволяє запускати написане з його допомогою програмне забезпечення в більшості сучасних операційних систем шляхом простої компіляції програми для кожної системи без зміни коду. Включає в себе всі основні класи, які можуть знадобитися при розробці прикладного програмного забезпечення, починаючи від елементів графічного інтерфейсу і

закінчуючи класами для роботи з мережею, базами даних та XML. Є повністю об'єктно-орієнтованим, розширюваним і підтримує техніку компонентного програмування.

- libpcap – служить для створення програм аналізу мережевих даних, що надходять на мережеву карту пристрою. Програмне забезпечення мережевого моніторингу може захопити пакети, які подорожують по мережі, а також передати пакети в мережі. Libpcap також підтримує збереження захоплених пакетів в файл і читання файлів, що містять збережені пакети. Файл захопленого трафіку зберігається в форматі, зрозумілому для додатків, що використовують pcap.

- libnl – це колекція бібліотек, що надають API для інтерфейсів ядра Linux на основі протоколу netlink. Netlink - це механізм IPC, головним чином якого є налагодження взаємодії між процесами ядра та простору користувача. Він був розроблений, щоб бути більш гнучким наступником ioctl, забезпечуючи в основному мережеву конфігурацію ядра та інтерфейси моніторингу.

- Авжеж, існують готові програмні застосунки для проведення аудиту бездротової мережі Wi-Fi:

- Aircrack-ng – набір програм, призначених для виявлення бездротових мереж, перехоплення переданого через бездротові мережі трафіку, аудиту WEP і WPA/WPA2-PSK ключів шифрування, в тому числі пентесту бездротових мереж. Програма працює з будь-якими бездротовими мережевими адаптерами, драйвер яких підтримує режим моніторингу.

- tcpdump – утиліта, що дозволяє перехоплювати і аналізувати мережевий трафік, що проходить через комп'ютер, на якому запущена дана програма. Для виконання програми потрібна наявність прав супер-користувача і прямий доступ до пристрою.

- Wireshark – програма-аналізатор трафіку для комп'ютерних мереж Ethernet та інших. Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, однак Wireshark має графічний користувальницький інтерфейс і набагато більше можливостей із сортування та фільтрації інформації. Програма дозволяє користувачеві переглядати весь

мережевий трафік в режимі реального часу, переводячи мережеву карту в нерозбірливий режим.

- hostapd – демон точки доступу – це програмне додаток для користувальницького простору, що дозволяє мережевій картці інтерфейсу виступати в якості точки доступу та сервера аутентифікації. Даний програмний надає багату варіативність налаштувань точки доступу та простоту використання.

- dnsmasq – легкий DNS та DHCP сервер, призначений для забезпечення доменними іменами і пов'язаними з ними сервісами невеликі мережі. Може забезпечувати іменами локальні машини, які не мають глобальних DNS-записів.

- iptable – програмний додаток командного рядка, є стандартним інтерфейсом управління роботою брандмауера netfilter для ядра Linux, починаючи з версії 2.4. З її допомогою створюють та змінюють правила, що керують фільтрацією і перенаправленням пакетів трафіку мережі.

Розділ 3

Третій розділ присвячено практичній реалізації аудиту щодо тестової точки доступу: було зібрано тестовий стенд, виконано та задокументовано використання вже описаних атак на бездротову мережу. В ході виконання було виявлено особливості проведення деяких атак, що було відображено у розділі пояснювальної записки.

Розділ 4

Цей розділ є спеціальною частиною для дипломної роботи, що піклується про охорону праці розробника даного програмного застосунку. Було проаналізовано можливий вплив шкідливих та небезпечних факторів, що супроводжують діяльність програміста: допустимий рівень звуку, електромагнітних випромінювань, якість освітлення, ергономіку робочого місця та протипожежну безпеку. Для кращого результату на кадрах у програмному застосунку та комфортної розробки було розраховано кількість світла, що є у приміщенні де ведеться розробка. Отримані данні було порівняно з необхідною за

стандартами праці кількістю світла. В результаті, було вжито заходів щодо додаткового освітлення приміщення.

ВИСНОВКИ

Було проведено низку роботи щодо дослідження проблем безпеки даних у бездротових мережах на прикладі Wi-Fi мереж: аудит тестової мережі та аналіз отриманих даних.

В трьох розділах роботи було висвітлено такі аспекти: принцип роботи бездротових мереж на прикладі Wi-Fi мереж, розібрано фізичний та пакетний рівні взаємодії випромінювача, описано найпопулярніші існуючі види атак на бездротову мережу Wi-Fi. Описаний теоретичний матеріал було підкріплено практичним виконанням та документуванням аудиту тестової точки доступу бездротової мережі Wi-Fi.

АНОТАЦІЯ

до магістерської кваліфікаційної роботи
студента групи 607 ЧНУ ім. Петра Могили
Хрищука Олександра Сергійовича
на тему: «Дослідження проблеми безпеки передачі даних бездротових мережах»

Актуальність даного дослідження походить від популярності використання бездротових мереж у повсякденному житті. З популярністю приходять загрози. Для бездротових мереж це шанс втратити особисті дані, бути об’єктом шпіонажу або звичайного хуліганства у невчасний момент.

Об’єктом дослідження є бездротові мережі на прикладі мережі Wi-Fi.

Предметом дослідження є існуючі види атак як на мережу, так і на її користувачів.

Метою дослідження є виявлення, перевірка та оцінка можливої завданої шкоди від основних та найпростіших видів атак. Також, виникає необхідність пошуку та опрацювання наявних методів захисту від проведених атак.

В результаті виконання роботи було проведено аудит тестової Wi-Fi точки за допомогою відкритого програмного забезпечення та відкритих програмних бібліотек. Було написано декілька простих програмних помічників для проведення аудиту, опрацьовано результати аудиту.

Дана робота складається з п’яти розділів. Кожен розділ відповідно присвячений: аналізу предметної області, надання наявної інформації щодо відомих видів атак, практичне проведення аудиту бездротової мережі, охороні праці і безпеці життєдіяльності, методичній частині магістерської роботи. Загальний обсяг роботи – 65 сторінок. Магістерська робота містить один додаток, 28 рисунків, 6 таблиць і посилання на 27 джерел.

Ключові слова: бездротові мережі, Wi-Fi, аудит, безпека даних, анонімність користувачів.

ABSTRACT

to the master's qualification work by the student of the group 607
of Petro Mohyla Black Sea National University
Khryshchuk Oleksandr Serhiyovych
«Diving into the problem of data transmission security in wireless networks»

The relevance of this study stems from the popularity of using wireless networks in everyday life. With popularity come threats. For wireless networks, this is a chance to lose personal information, be the object of espionage or ordinary hooliganism at the wrong time.

The object of the study is wireless networks on the example of Wi-Fi.

The subject of the study is the existing types of attacks on both the network and its users.

The purpose of the study is to identify, verify and assess the possible damage caused by the basic and simplest types of attacks. Also, there is a need to find and develop existing methods of protection against attacks.

As a result, the test Wi-Fi hotspot was audited using open source software and open source software libraries. Several simple software assistants were written for the audit, and the results of the audit were processed.

This work consists of five sections. Each section is devoted to: analysis of the subject area, providing available information on known types of attacks, the practical audit of the wireless network, occupational safety and health, the methodological part of the master's thesis. The total volume of the work is 65 pages. The master's thesis contains one appendix, 28 figures, 6 tables and references to 27 sources.

Keywords: wireless networks, Wi-Fi, audit, data security, user anonymity.