КРИПТОЛОГІЯ/ CRYPTOLOGY

DOI: 10.18372/2225-5036.29.17549

ДОСЛІДЖЕННЯ БЕЗПЕКИ СТАНДАРТУ WI-FI PROTECTED ACCESS 3 (WPA3)

Іван Опірський, Назар Максимів, Марія Женчур

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.

МАКСИМІВ Назар Васильович, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 2002 рік, м. Львів, Львівська область, Україна.
Наукові інтереси: засоби захисту інформації
E-mail: nazarmaxymiv@gmail.com.
ORCID ID: 0009-0009-6496-4056.

ЖЕНЧУР Марія Володимирівна, студентка кафедри захисту інформації Національного університету «Львівська політехніка».
Рік та місце народження: 2002 рік, м. Новояворівськ, Львівська область, Україна.
Наукові інтереси: методи та засоби захисту інформації
E-mail: mariazhenchur@gmail.com.
ORCID ID: 0009-0009-4017-2695.

Анотація. *Wi-Fi технологія є дуже актуальною у наш час, оскільки бездротовий зв'язок став необхідною складовою нашого повсякденного життя. Wi-Fi дозволяє підключатися до Інтернету на різних пристроях, таких як смартфони, планшети, ноутбуки, телевізори та інші Крім того, Wi-Fi технологія постійно розвивається та вдосконалюється. Нові стандарти технології, такі як 802.11ax (Wi-Fi 6), дозволяють покращити швидкість передачі даних та забезпечити більшу стійкість до перешкод та інтерференції. Однак, разом з популярністю Wi-Fi технології з'являється також і більша загроза безпеці мережі. Тому важливо вдосконалювати безпекові методи та алгоритми шифрування Wi-Fi мережі для забезпечення її захищеності та безпеки.*

Дослідження вразливостей протоколів бездротового зв'язку Wi-Fi WPA2 та WPA3 є дуже актуальним у зв'язку з тим, що бездротові мережі є незмінною складовою сучасного світу. Так як, хакерські атаки на бездротові мережі стали розповсюдженими, дослідження вразливостей WPA2 та WPA3 є дуже важливим для забезпечення безпеки мережі Wi-Fi. Адже, вразливості протоколів WPA2 та WPA3 можуть бути використані зловмисниками для отримання несанкціонованого доступу до мережі та отримання конфіденційної інформації, такої як паролі та дані користувачів. В цій статі буде розглянуто такі теми, як вразливості захисту WI-FI мереж за допомогою WPA2 та WPA3, основні засоби захисту від атак та порівняльна характеристика цих двох методів захисту.

Ключові слова: *Wi-Fi, WPA2, WPA3, кіберзлочинність, безпека, шифрування, криптографія, захист.*

Постановка проблеми

Використання бездротових технологій надає користувачам можливість вільного пересування без втрати зв'язку, операторам мережі – більше можливостей для організації з'єднань і доступ у мережу безлічі нових пристроїв [17, 18]. Сьогодні бездротові Wi-Fi мережі використовуються майже всюди завдяки простоті використання мережі, високій мобільності користувачів і простоті встановлення цієї технології. Ця технологія дедалі частіше стає обов'язковим складником не тільки домашніх, але й корпоративних мереж [1]. Wi-Fi можна використовувати в найрізноманітніших умовах, в тому числі:

-вдома: Wi-Fi зазвичай використовується в будинках для підключення смартфонів, ноутбуків, планшетів, ігрових консолей, смарт-телевізорів та інших пристроїв до інтернету;

-офіси: Wi-Fi широко використовується в офісах, щоб дозволити співробітникам підключатися до інтернету, отримувати доступ до електронної пошти і спільно працювати над проектами;

-громадські місця: Wi-Fi часто доступний у громадських місцях, таких як кафе, ресторани, аеропорти, вокзали та готелі, що дозволяє людям виходити в інтернет, перебуваючи в дорозі;

-навчальні заклади: Wi-Fi широко використовується в школах, коледжах та університетах для надання доступу до інтернету учням, викладачам та співробітникам;

-медичні установи: Wi-Fi все частіше використовується в медичних установах, щоб забезпечити віддалений моніторинг пацієнтів і поліпшити комунікацію між медичними працівниками;

-промисловість та виробництво: Wi-Fi використовується в промислових і виробничих умовах для моніторингу та управління обладнанням, а також для збору даних.

Загалом, технологія Wi-Fi стала невід'ємною частиною сучасного життя, дозволяючи людям залишатися на зв'язку і отримувати доступ до інформації практично з будь-якого місця.

Більше того технологія Wi-Fi активно використовується в воєнних розробках. До прикладу можна віднести застосування Wi-Fi у дронах, які активно використовуються в військових діях.

Аналіз останніх досліджень і публікацій

Технологія Wi-Fi дозволяє дронам передавати відеопотоки та інші дані на наземну станцію в режимі реального часу, що дає змогу оператору бачити те, що бачить дрон, і керувати його рухом дистанційно. Wi-Fi з'єднання між дроном і наземною станцією також можна використовувати для надсилання команд і отримання даних з датчиків дрона, таких як GPS-локація, висота і рівень заряду акумулятора. Більше того Wi-Fi також активно використовується на передовій проте, відповідно до чого потрібно однозначно проводити захист та маскування мереж [2].

Однією з переваг використання Wi-Fi в дронах є те, що він забезпечує надійний і стабільний зв'язок між дроном і наземною станцією навіть на великих відстанях. Сигнали Wi-Fi також можуть проникати крізь такі перешкоди, як стіни і дерева, що дозволяє керувати дроном зсередини будівлі або за укриттям.

Проте використання мереж Wi-Fi також пов'язане з певними ризиками та вразливостями, які можуть призвести до витоку даних та несанкціонованого доступу. Найпоширеніший протокол безпеки Wi-Fi, WPA2 (Wi-Fi Protected Access II), був розроблений для зменшення цих ризиків і забезпечення безпечного мережевого середовища [3].

WPA2 це більш захищена версія попереднього протоколу WPA і широко використовується для захисту домашніх і корпоративних мереж Wi-Fi. WPA2 забезпечує сильніші алгоритми шифрування, перевірку цілісності повідомлень і протоколи аутентифікації. Що у свою чергу значно ускладнює зловмисникам перехоплення та декодування бездротового мережевого трафіку, а також видачу себе за авторизованих користувачів.

WPA2 важливий ще й тому, що він широко використовується і став стандартом де-факто для захисту мереж Wi-Fi. Більшість сучасних Wi-Fi пристроїв, таких як ноутбуки, смартфони та планшети, підтримують WPA2, що дозволяє користувачам легко підключатися до захищених мереж.

Проте якщо WPA2 не реалізовано належним чином користувач може втратити критично важливі дані, а саме [4]:

1. Імена користувачів та паролі: якщо користувач входить на веб-сайт або інший онлайн-сервіс, підключений до скомпрометованої мережі Wi-Fi, зловмисник може перехопити його облікові дані для входу і використати їх для доступу до облікових записів користувача.

2. Фінансову інформацію: якщо користувач здійснює покупку або виконує фінансову транзакцію

через скомпрометовану мережу Wi-Fi, зловмисник може перехопити інформацію про його кредитну картку, реквізити банківського рахунку або інші конфіденційні фінансові дані.

3. Особисту інформацію: будь-яка особиста інформація, передана через мережу Wi-Fi, наприклад, номери соціального страхування, адреси або номери телефонів, може бути перехоплена і викрадена.

4. Бізнес-дані: якщо скомпрометована мережа Wi-Fi використовується в комерційних цілях, конфіденційні дані компанії, такі як комерційна таємниця, фінансова звітність та інформація про клієнтів, можуть бути викрадені.

Мета та постановка завдання

Метою цього дослідження є порівняння рівня безпеки протоколів WPA3 та WPA2, виявлення можливих вразливостей , що можуть бути використані зловмисниками для злому Wi-Fi.

Завдання, що поставленні до статті:

- ознайомлення з відомими атаками на WPA2 та WPA3 їх основними характеристиками;
- способи захисту від відомих атак;
- опис недоліків WPA2 та WPA3;
- порівняти результати дослідження для WPA2 та WPA3 та зробити висновки про ступінь їх безпеки та захисту від різноманітних атак.

Виклад основного матеріалу

Атаки на WPA2

Проте як і будь яка технологія WPA2 також є вразливою до атак, що може призвести як було наведено в попередньому параграфі до величезних втрат.

Загалом WPA2 є вразливою до таких атак: KRACK, PMKID, Brute Force атак, атак з використанням словників та Атаці злих близнюків. Детальніше зупинемося на кожній з них.

KRACK атака

Атаки на переустановлення ключів (KRACK) – це тип кібератак, які використовують вразливість у WPA2 з метою викрадення даних, що передаються мережею. Ці атаки можуть призвести до викрадення конфіденційної інформації, такої як облікові дані для входу в систему, номери кредитних карток, приватні чати та будь-які інші дані, які жертва передає через мережу.

Принцип роботи KRACK атаки

Зашифроване з'єднання WPA2 ініціюється за допомогою послідовності чотиристоронього рукостискання, хоча для повторного з'єднання не обов'язково виконувати всю послідовність. Для того, щоб уможливити швидке повторне з'єднання, потрібно повторно передавати лише третю частину чотиристоронього рукостискання. Коли користувач повторно підключається до знайомої мережі Wi-Fi, мережа повторно надсилає йому третю частину послідовності рукостискання; це повторне надсилання може відбуватися кілька разів, щоб забезпечити успішне з'єднання. Цей повторюваний крок і є вразливістю, якою можна скористатися (рис. 1).

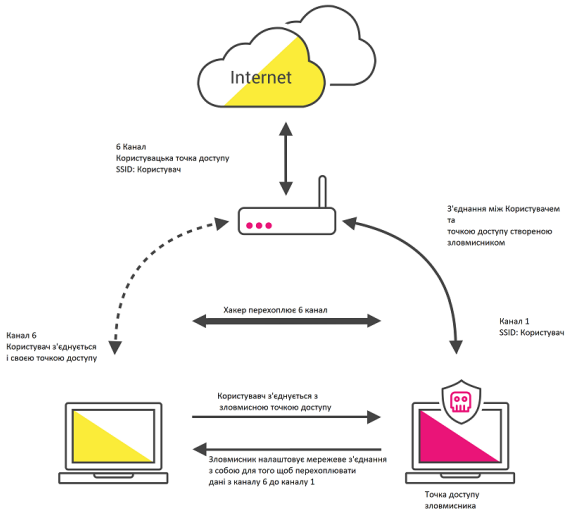

Рис. 1. Методологія здійснення KRACK атаки

Зловмисник може створити клон мережі Wi-Fi, до якої раніше підключалася жертва. Зловмисна мережа-клон може надавати доступ до Інтернету, так що жертва не помітить різниці. Коли жертва намагається знову підключитися до мережі, зловмисник може змусити її приєднатися до мережі-клону, позиціонуючи себе як зловмисника на шляху. Під час процесу з'єднання зловмисник може продовжувати надсилати третю частину рукостискання на пристрій жертви. Щоразу, коли користувач приймає запит на з'єднання, невеликий фрагмент даних розшифровується. Зловмисник може об'єднати цю серію повідомлень, щоб зламати ключ шифрування.

Після того, як шифрування WPA2 зламано, зловмисник може використовувати програмне забезпечення для перехоплення всіх даних, переданих жертвою через мережу Wi-Fi. Це не спрацює для веб-сайтів, які використовують SSL/TLS-шифрування, але зловмисник може використати такий інструмент, як "SSLStrip", щоб змусити жертву відвідувати HTTP-версії веб-сайтів. Жертва може не помітити, що сайт незахищений, і може ввести конфіденційну інформацію, яку зловмисник перехопить.

Слід зазначити, що KRACK-атаки вимагають близькості до роботи. Зловмисник не може атакувати когось на іншому кінці світу або навіть в іншому місті; для здійснення атаки зловмисник і жертва повинні перебувати в зоні дії однієї і тієї ж мережі Wi-Fi.

Як захиститися від KRACK-атак

Найкращий захист від KRACK - переконатися, що на всіх пристроях, підключених до Wi-Fi, встановлені виправлення та найновіша прошивка. Це включає в себе періодичну перевірку виробника вашого роутера, щоб дізнатися, чи доступні патчі.

Найбезпечнішим варіантом підключення є приватна VPN, особливо в громадських місцях. Якщо вам потрібна VPN для особистого користування, уникайте безкоштовних варіантів, оскільки вони мають

власні проблеми з безпекою, а також проблеми з HTTP. Використовуйте платний сервіс, який пропонує надійний постачальник, наприклад, Kaspersky. Крім того, більш сучасні мережі використовують WPA3 для кращої безпеки.

Уникайте використання громадського Wi-Fi, навіть якщо він захищений паролем. Цей пароль доступний майже будь-кому, що значно знижує рівень безпеки.

Атака "Злий близнюк"

Це клас кібератак, до яких користувачі інтернету вразливі, коли підключаються до публічного Wi-Fi. Хакери створюють шкідливі хот-споти в місцях, де користувачі очікують знайти публічний Wi-Fi. Як наслідок, кожен, хто користується публічним Wi-Fi, ризикує наразитися на атаку Evil Twin.

Кіберзлочинці використовують атаки Evil Twin, щоб перехоплювати інтернет-сесії жертв. Якщо ви підключаєтеся до точки доступу Evil Twin, хакери можуть відстежувати ваші веб-відвідування і потенційно викрадати вашу особисту інформацію з метою фішингу, шахрайства та крадіжки персональних даних.

Атака Evil Twin може навіть заразити ваш пристрій шкідливим програмним забезпеченням, надаючи хакерам віддалений доступ до вашого пристрою для доставки вторинного корисного навантаження, такого як шпигунські програми, кейлоггери або трояни, здатні повністю захопити пристрій. Тому надзвичайно важливо знати, що таке атака Evil Twin і що ви можете зробити, щоб захиститися від неї. У цьому посібнику ми озброїмо вас знаннями, необхідними для захисту.

Атака Evil Twin, або хотспот Evil Twin, отримала свою назву від методу, який використовують хакери, щоб заманити своїх жертв.

Хакери зазвичай встановлюють точки доступу Evil Twin в громадських місцях, де ви очікуєте знайти безкоштовний Wi-Fi. Це означає, що ви можете зіткнутися з атакою Evil Twin в кав'ярні, торговому центрі, ресторані, громадському транспорті, аеропорту, публічній бібліотеці - або практично будь-де.

Принцип роботи атаки Evil Twin

Атака Evil Twin ґрунтується на тому, що люди очікують знайти безкоштовний Wi-Fi в громадському місці, де він розгорнутий. Щоб успішно залучити жертв, хакери дають шкідливим точкам доступу непомітну назву (SSID), наприклад, "безкоштовний інтернет Starbucks" або "безкоштовний готельний Wi-Fi". Жертви вважають, що точка доступу є законною і надається місцевим закладом. Підключившись до шкідливої точки доступу, кіберзлочинець може перехоплювати всі дані, які передаються мережею з пристроїв жертви. Це також дозволяє хакеру атакувати пристрій жертви і отримати доступ до його вмісту з метою крадіжки даних або зараження шкідливим програмним забезпеченням. У деяких місцях "Злий двійник" може бути точною копією назви справжньої точки доступу. Це викриває всіх, хто поспішає підключитися.

Приклади атак Evil Twin

Атака "злий двійник" може призвести до низки інших атак на кібербезпеку. Нижче ми зібрали інформацію про види атак, які можуть здійснити хакери, якщо ви випадково підключилися до хот-споту Evil Twin.

- *Людина посередині*

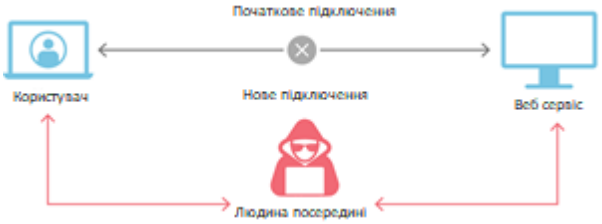

Рис. 2. Методологія здійснення MITM атаки

Якщо ви підключаєтеся до точки доступу Evil Twin, хакер може перехопити ваші дані, коли вони проходять через їхню фальшиву мережу (рис. 2). Цей клас кібератак називається атакою "Людина посередині" (MitM). Під час MitM-атаки хакер, який перехоплює ваш сеанс, отримує можливість робити різні мерзенні речі.

Однією з таких є перехоплення сеансу, де хакер перехоплює ключ автентифікації, що дає йому можливість отримати доступ до вашої електронної пошти або іншого особистого облікового запису (рис. 3).

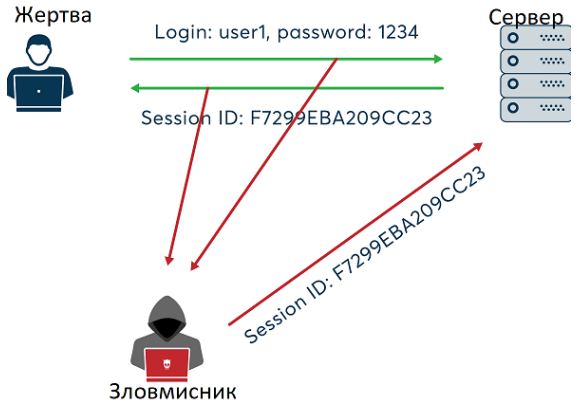

Рис. 3. Методологія здійснення перехоплення сеансу

Атака з відтворенням (хакер записує вашу активність і повторює дію, яку ви щойно виконали, наприклад, вхід в обліковий запис). Хакер змінює ваш контент так, що одержувач отримує щось відмінне від того, що ви мали намір надіслати (змінені повідомлення тощо). Хакер видаляє ваш вміст, щоб він ніколи не потрапив до адресата.

Ще одна можливість, коли ви підключаєтеся до точки доступу Evil Twin, полягає в тому, що хакер може здійснити DNS-атаку. Наприклад, хакери можуть використовувати цей тип атаки для перенаправлення користувачів на іншу веб-сторінку, ніж та, яку

вони мали намір відвідати, що називається перехопленням DNS (рис. 4).

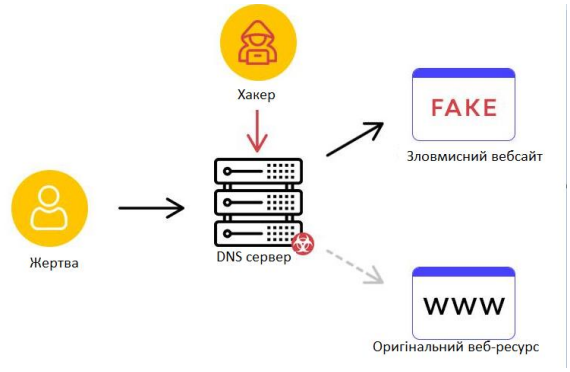

Рис. 4. Методологія здійснення DNS перехоплення

Проблема цього виду перехоплення DNS полягає в тому, що жертва навряд чи зрозуміє, що хакер перенаправив її на шкідливий веб-сайт. Сайт може бути заражений шкідливим програмним забезпеченням або фальшивим порталом для входу, призначеним для "фішингу" їхніх даних.

Це означає, що хакер міг успішно заразити користувача шкідливим програмним забезпеченням, яке закріплюється на зараженому пристрої, дозволяючи йому завантажувати вторинні пакети з командно-контрольного сервера (CnC).

За найгірших обставин це може призвести до зараження жертви серйозним трояном для віддаленого доступу, який дозволяє хакеру отримати повний контроль над пристроєм і викрасти дані, цінні для шахрайства та крадіжки особистих даних.

Як захиститися від атаки Evil Twin

Найпростіший спосіб не стати жертвою атаки Evil Twin – повністю уникати публічних точок доступу до бездротової мережі. Однак на практиці більшість людей покладаються на безкоштовний інтернет, щоб заощадити на своїх мобільних тарифних планах. Як наслідок, повне утримання від громадського Wi-Fi не буде практичним. Хороша новина полягає в тому, що є різні способи захистити себе.

А саме:

1. Вимкнути автопідключення;
2. Уникайте підключення до незахищених Wi-Fi мереж;
3. Ставтеся з підозрою, якщо вас відключають від публічного Wi-Fi;
4. Не входьте в особисті акаунти;
5. Переходьте на HTTPS-сайти;
6. Використовуйте двофакторну автентифікацію;
7. Використовуйте VPN;
8. Увімкніть брандмауер та використовуйте антивірус.

PKMID

Основна відмінність від існуючих атак полягає в тому, що в цій атаці не потрібне повне 4-стороннє рукостискання EAPOL. Нова атака виконується в RSN IE (Robust Security Network Information Element), і для її успішного відтворення достатньо одного кадру EAPOL. Наразі невідомо, для якої кількості маршрутизаторів цей метод буде працювати - швидше за все, для всіх існуючих мереж 802.11i / p / q / r з увімкненими функціями роумінгу, а це більшість сучасних маршрутизаторів.

Основні особливості pmkid-атаки:

- не потрібно чекати клієнтів – атакується безпосередньо точка доступу;
- не потрібно чекати повного 4-стороннього рукостискання між клієнтом і точкою доступу;
- відсутність ретрансляції EAPOL кадрів;
- виключається можливість перехоплення некоректних паролів від клієнта;
- втрата EAPOL кадрів у разі віддалення/втрати зв'язку з клієнтом;
- висока швидкість завдяки відсутності необхідності фіксувати значення nonce та replaycounter;
- немає потреби в спеціалізованому форматі вихідних даних (pcap, hccapx тощо) - перехоплені дані зберігаються у вигляді шістнадцяткових рядків.

Принцип роботи PMKID атаки

Спочатку зловмисник перехоплює чотиристороннє рукостискання, яке відбувається між клієнтським пристроєм і точкою доступу, коли клієнт підключається до мережі.

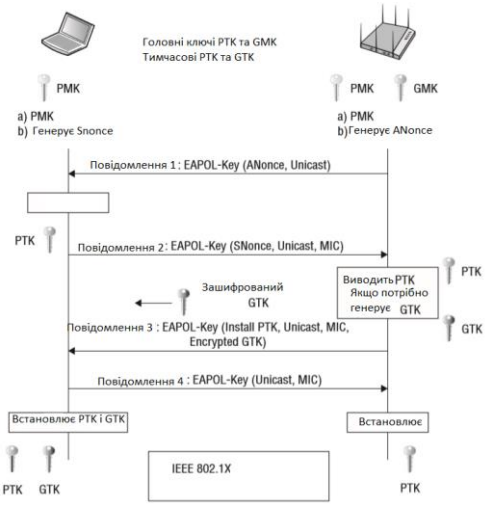

Рис. 5. Методологія здійснення PMKID атаки

Рукостискання містить необхідну інформацію для отримання PMKID (рис. 5). Потім зловмисник використовує такий інструмент, як Hashcat, для вилучення PMKID з перехоплених пакетів даних.

Отримавши PMKID, зловмисник може використовувати словник або атаку грубої сили, щоб зламати PSK і отримати доступ до мережі Wi-Fi.

Атака може бути проведена швидко і ефективно, оскільки PMKID може бути отриманий за лічені секунди, і атака може бути проведена в автономному

режимі, що означає, що зловмиснику не потрібно бути фізично присутнім в мережі для проведення атаки.

Як захиститися від атаки PMKID

1. Використовуйте надійний та унікальний пароль.
2. Оновлюйте прошивку вашого Wi-Fi маршрутизатора.
3. Вимкніть WPS.
4. Використовуйте віртуальну приватну мережу (VPN).
5. Проводьте моніторинг своєї мережі.

Атака грубою силою (Brute force attack)

Популярний метод злому: за деякими даними, на частку атак грубою силою припадає п'ять відсотків підтверджених порушень безпеки. Атака грубою силою передбачає "вгадування" імені користувача та паролів для отримання несанкціонованого доступу до системи. Це простий метод атаки, який має високий відсоток успіху.

Деякі зловмисники використовують додатки та скрипти як інструменти грубого перебору. Ці інструменти перебирають численні комбінації паролів, щоб обійти процеси автентифікації. В інших випадках зловмисники намагаються отримати доступ до вебдодатків шляхом пошуку правильного ідентифікатора сеансу.

Хоча деякі зловмисники все ще виконують атаки грубої сили вручну, сьогодні майже всі атаки грубої сили виконуються ботами. Зловмисники мають списки загальновживаних облікових даних або реальні облікові дані користувачів, отримані через проломи в системі безпеки або з темного інтернету.

Атаки грубої сили - це тип злому паролів, коли зловмисник перебирає всі можливі комбінації символів, поки не знайде правильний пароль.

Принцип роботи атаки грубої сили

Зловмисник спочатку вибирає ціль, зазвичай обліковий запис користувача або зашифрований файл, до якого він хоче отримати доступ.

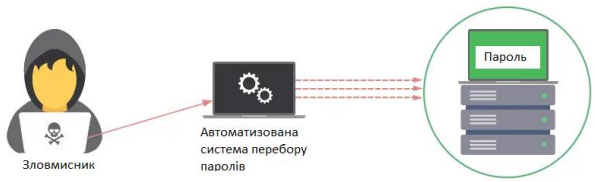

Рис. 6. Здійснення брут форс атаки

Потім він створює програму або використовує інструмент, який може автоматично генерувати паролі, і пробує їх один за одним, поки не знайде правильний пароль (рис. 6).

Програма генерує паролі на основі набору правил, таких як довжина, тип символів та інші параметри, і перебирає всі можливі комбінації, поки не знайде правильний пароль.

Атаки грубої сили можуть бути виконані офлайн або онлайн. При офлайн-атаці зловмисник має доступ до зашифрованих даних і може спробувати різні паролі, не будучи виявленим. Під час онлайн-атаки зловмисник намагається вгадати пароль через веб-інтерфейс, наприклад, через форму входу в систему.

Атаки грубої сили можуть займати багато часу і вимагати великих обчислювальних потужностей, особливо якщо пароль довгий і складний.

Типи атак грубої сили

Проста атака грубої сили - використовує систематичний підхід до "вгадування", який не покладається на зовнішню логіку.

Гібридні атаки грубого перебору - починаються з зовнішньої логіки, щоб визначити, яка варіація пароля може бути найбільш вірогідною, а потім продовжуються простим підходом, щоб спробувати багато можливих варіацій. Словникові атаки – вгадують імена користувачів або паролі за допомогою словника можливих рядків або фраз.

Атаки веселковими таблицями – веселкова таблиця - це заздалегідь обчислена таблиця для реверсування криптографічних хеш-функцій. Її можна використовувати для вгадування функції певної довжини, що складається з обмеженого набору символів.

Зворотна атака грубої сили – використовує загальний пароль або набір паролів проти багатьох можливих імен користувачів. Націлена на мережу користувачів, про яких зловмисники раніше отримали дані.

Підбір облікових даних – використовує раніше відомі пари пароль-ім'я користувача, перевіряючи їх на різних веб-сайтах. Використовує той факт, що багато користувачів мають однакові імена користувачів і паролі в різних системах.

Як запобігти злому паролів грубою силою

-ніколи не використовувати інформацію, яку можна знайти в Інтернеті (наприклад, імена членів сім'ї);

-містити якомога більше символів;

-поєднувати літери, цифри та символи;

-бути різними для кожного облікового запису користувача.

Як адміністратор, ви можете застосувати певні методи, щоб захистити користувачів від злому паролів грубою силою:

Інструменти captcha, такі як reCAPTCHA, вимагають від користувачів виконання простих завдань для входу в систему. Користувачі можуть легко вико-

нати ці завдання, в той час як інструменти грубої сили не можуть.

Вимога надійних паролів – ви можете змусити користувачів створювати довгі та складні паролі. Ви також повинні забезпечити періодичну зміну паролів. Двофакторна автентифікація - ви можете використовувати кілька факторів для підтвердження особи та надання доступу до облікових записів.

Якщо підсумувати, будь яка з цих атак дозволить зловмиснику викрасти конфіденційні дані користувача та скористатися ними у власних цілях. В таблиці наведено критичність кожного виду атак та дані які буде скомпрометовано під час їх виконання (табл. 1).

Таблиця 1

Типи атак та їх критичність для користувача

Атака	Критичність	Втрачені дані
KRACK Attack	Висока	Будь-який трафік, включаючи паролі та конфіденційні дані
Rogue Access Point	Висока	Будь-який трафік, включаючи паролі та конфіденційні дані
Evil Twin Attack	Висока	Будь-який трафік, що проходить через фальшиву точку доступу, включаючи паролі та конфіденційні дані
PMKID Attack	Середня	Ім'я та пароль до межі
Brute Force Attack	Середня	Пароль до мережі
Dictionary Attack	Низька	Пароль до мережі

Порівняння WPA2 та WPA3

Протягом довгого часу основними методами зламу маршрутизаторів, які працювали по WPA2, були злам PIN-коду під час підключення через WPS або перехоплення рукостискання і підбір ключа методом підбору. Для забезпечення безпеки можна було відключити WPS і встановити складний пароль.

Тому WPA2 вважався надійним доти, доки не була опублікована атака KRACK (Key Reinstallation Attack) у жовтні 2017 року. В основі цієї атаки лежить уразливість чотирьохелементного рукостискання WPA2. Проблему було знайдено безпосередньо у протоколі. Під час розробки нового стандарту безпеки метою було усунення проблем, які з'явились з появою KRACK. У WPA3 появилась підтримка методу з'єднання SEA (Simultaneous Authentication of Equals), який вважається більш надійним.

Технологія SEA заснована на протоколі обміну ключами Діффі-Хеллмана з використанням кінцевих циклічних груп. SEA відноситься до протоколу типу PAKE (Password-authenticated key agreement) і надає інтерактивний метод, згідно з яким дві і більше сторін встановлюють криптографічні ключі, які засновані на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який отримує кожна зі сторін для аутентифікації з'єднання, вибирається на основі інформації з пароля, ключів і MAC-адрес обох сторін. Якщо ключ однією зі сторін виявиться скомпрометованим, це не спричинить компрометації ключа сесії. Навіть дізнавшись пароль, зловмисник не зможе розшифрувати пакети. Також у WPA3 з'явилась підтримка PMF (Protected Management Frames), що контролює цілісність трафіку.

Незмінним залишилась кількість режимів роботи. Як і у попередній версії, у WPA3 існує 2 режими: WPA3-personal та WPA3-Enterprise.

WPA3-Personal забезпечує надійний захист, особливо в поєднанні з використанням складного паролю.

Якщо обраний пароль не є складним, для цього встановили нове обмеження на число спроб аутентифікації в межах одного рукостискання. Тому метод підбирання паролю у режимі поза мережею стає неможливим. WPA3-Enterprise виконує шифрування на основі мінімум 192-розрядних ключів.

Покращення безпеки, яке було зроблено в WP3, зменшує ймовірність атак злому паролів, таких як атака WPA2 KRACK. WPA2 вразлива до атак грубої сили та словникових атак. Це пов'язано з тим, що безпека залежить від встановлення надійного пароля постачальником точки доступу, а багато закладів цього не роблять (табл. 2).

У WPA3 протокол обміну попереднім спільним ключем (PSK) замінено на одночасну автентифікацію рівняння (SAE) або обмін ключами Dragonfly, що покращує безпеку початкового обміну ключами та пропонує кращий захист від атак на основі офлайн-словника.

Таблиця 2

Порівняльна характеристика WPA2 та WPA3

Характеристика	WPA2	WPA3
Рік випуску	2004	2018
Ключ шифрування	128 біт	192 або 256 біт
Протокол аутентифікації	802.1X / EAP	SAE
Захист від атак розподіленого відмову в обслуговуванні (DDoS)	Відсутній	Захист від DDoS атак
Захист від атак перехоплення (Man-in-the-middle)	Відсутній	Захист за допомогою аутентифікації на основі обміну пакетами
Підтримка застосування WPA3 на старих пристроях	Відсутня	Можливість роботи в режимі "WPA3-перехід" для підтримки старих пристроїв

Недоліки безпеки WPA3.

Уразливості протоколу Dragonfly отримали назву Dragonblood. Виявлені недоліки можна розділити на дві категорії. Перша категорія складається з атак на зниження рівня пристроїв, що підтримують WPA3, а друга категорія складається зі слабких місць у рукостисканні WPA3 Dragonfly, яке в стандарті Wi-Fi більш відомо як рукостискання Simultaneous Authentication of Equals (SAE). Ці недоліки можна використати для відновлення пароля мережі Wi-Fi, запуску атак на споживання ресурсів і примусового використання пристроїв слабкіших груп безпеки. Усі атаки спрямовані на домашні мережі (тобто WPA3-Personal), де один пароль використовується для всіх користувачів.

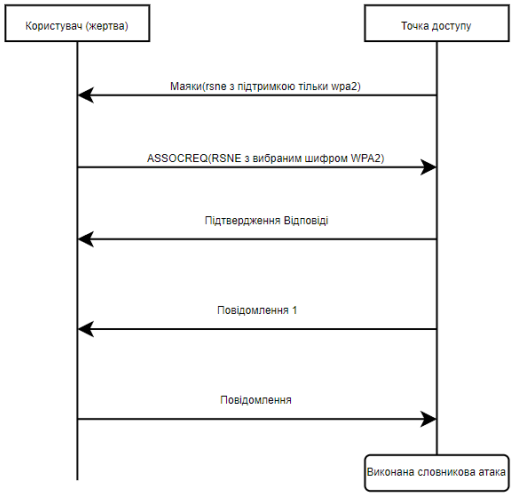

Рис. 7. Методологія здійснення словникової атаки

Атаки на WPA3

Downgrade & Dictionary атака проти WPA3-Transition.

Ця атака використовує зворотну сумісність WPA3. Щоб задовольнити старіші клієнти, які підтримують лише WPA2, і мотивувати перехід до WPA3, у специфікації WPA3 було визначено режим переходу. У цьому режимі мережа Wi-Fi підтримує використання WPA3 і WPA2 з ідентичним паролем.

Рис. 8. Створення шахрайської мережі.

Така мережа показує лише підтримку WPA2

Принцип роботи атаки Downgrade & Dictionary

Зловмисник може створити шахрайську мережу та змусити клієнтів, які підтримують WPA3, підключатися до шахрайської мережі, яка підтримує лише WPA2 (рис. 7). Зафіксоване часткове рукостискання WPA2 можна використати для відновлення пароля мережі (за допомогою атак грубої сили або словника). Для виконання цієї атаки не потрібне використання атаки «людина посередині» (рис. 8).

Приклад здійснення атаки Downgrade & Dictionary

Спочатку зловмисник глушить оригінальну точку доступу та створює шахрайську мережу WPA3-Transition (рис. 9).

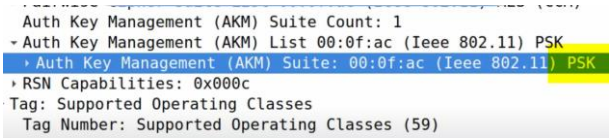

Рис. 9. Інформація про підтримку WPA2

Жертва виконує підключення без використання SAE рукостискання (рис. 10).

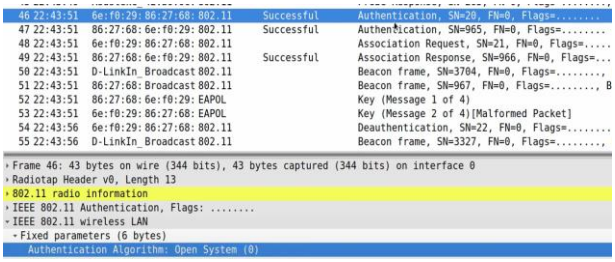

Рис. 10. Підключення без SAE рукостискання

Зловмисник тепер захоплює перші два повідомлення 4-стороннього рукостискання (рис. 11).

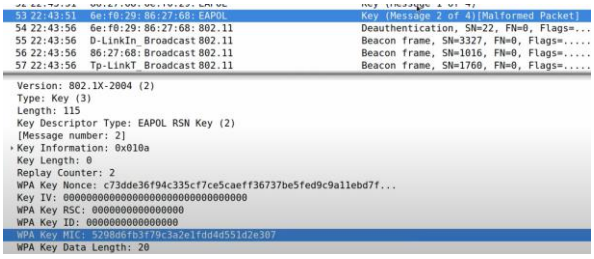

Рис. 11. Захоплення повідомлень

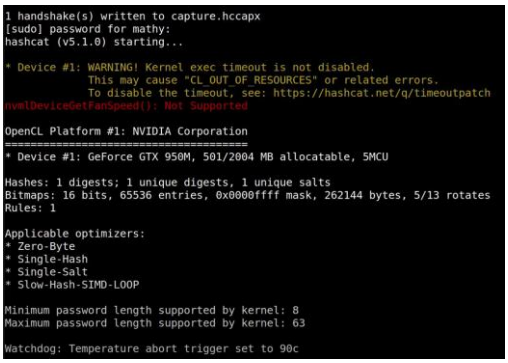

Рис. 12. Здійснення словникової атаки

Після цього зловмисник виконує атаку за словником (рис. 12, 13)

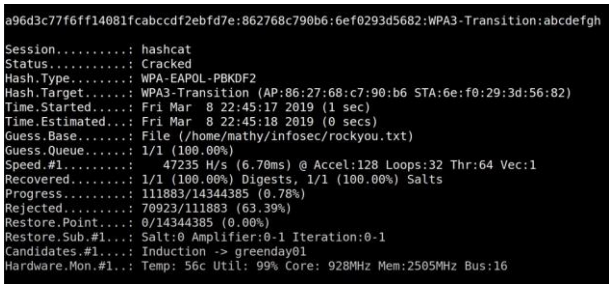

Рис. 13. Успішне виконання атаки

Як захиститись від атаки Downgrade & Dictionary

Загалом, захист від атак downgrade & dictionary включає в себе використання сильних та унікальних паролів, вимагання підтвердження від пристроїв, перевірку оновлень програмного забезпечення та, якщо можливо, використання більш безпечної версії WPA3.

Атака Security Group Downgrade

Ця атака може бути виконана зловмисником, який знаходиться на маршруті між клієнтом і сервером, і вона може бути успішною, якщо веб-браузер і веб-сервер не встановлюють належних заходів безпеки. Якщо SGDA успішно впроваджується, він може змусити веб-браузер і веб-сервер використовувати менш безпечний протокол замість більш безпечного.

SGDA може бути використана для виконання різних типів атак, таких як витік інформації, підробка сертифікатів, викрадення ідентифікаторів користувачів і паролів, а також внесення змін в передачу даних.

Принцип роботи Security Group Downgrade атаки

Пристрій, який ініціює рукостискання (зазвичай клієнт), надсилає кадр фіксації, який містить групу безпеки, яку він бажає використовувати. Якщо точка доступу не підтримує цю групу, вона відповідає повідомленням про відхилення, змушуючи клієнта надіслати кадр фіксації за допомогою іншої групи. Цей процес триває, доки не буде знайдено групу безпеки, яка підтримується обома сторонами. Зловмисник може видати себе за точку доступу та підробити повідомлення про відхилення, щоб змусити клієнтів вибрати слабку групу безпеки (рис. 14).

Як захиститись від атаки SGD

Для захисту від атаки Security Group Downgrade на WPA3 можна використовувати наступні підходи: відключити режим перехідного режиму, якщо можливо; використовувати складні паролі для мережі Wi-Fi; налаштувати мережу Wi-Fi з відповідними налаштуваннями захисту, які використовують WPA3, такі як SAE або Dragonfly; перевірити наявність оновлення прошивки для маршрутизатора або точки доступу Wi-Fi і встановити їх; налаштувати мережу Wi-Fi з відповідними налаштуваннями, які виключають підтримку застарілих захисту і протоколів, таких як WPA2 або TKIP; перевірити наявність інших вразливостей, таких як KRACK, і вжити відповідні заходи безпеки для їх запобігання.

Рис. 14. Методологія здійснення SGD атаки

Атака Cache-Based Side-Channel

Цей тип атаки на комп'ютерні системи використовує недоліки в кеш-пам'яті комп'ютера для отримання конфіденційної інформації, такої як паролі, ключі шифрування, дані сесії та інші важливі дані.

Принцип роботи Cache-Based Side-Channel атаки

Коли зловмисник може спостерігати шаблони доступу до пам'яті на пристрої жертви, коли він створює кадр фіксації рукостискання Dragonfly, ці шаблони доступу до пам'яті розкривають інформацію про пароль, який використовується. Спостереження за цими шаблонами можливо, якщо зловмисник контролює будь-яку програму на пристрої жертви, і навіть може бути можливим, коли зловмисник контролює код JavaScript у браузері жертви. Шаблони витоку можна використовувати для атаки за словником шляхом імітації шаблонів доступу до пам'яті, пов'язаних із вгаданим паролем, і порівняння цього з виміряними шаблонами доступу (рис. 15).

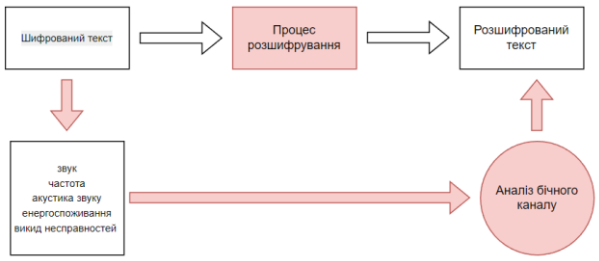

Рис. 15. Методологія здійснення атаки на основі кешу

Як захиститись від атаки Cache-Based Side-Channel

Для захисту від Cache-Based Side-Channel атаки можна використовувати різні заходи, такі як використання апаратних засобів захисту, таких як Intel SGX або AMD SEV, або використання програмних рішень, таких як кеш-пам'ять з рандомізацією і періодичним очищенням. Також можна використовувати захист

від різних видів Side-Channel атак, наприклад, зниження витоків інформації через шумові ефекти, розширення часу виконання інструкцій та інші.

Атака Denial-of-Service

Цей тип атаки спрямований на перешкоджання нормальному функціонуванню бездротової мережі з використанням протоколу WPA3. Для проведення атаки зловмисник намагається затопити мережу великою кількістю запитів або шуму, що призводить до тимчасового відмови в обслуговуванні (DoS) відповідних послуг

Принцип роботи Denial-of-Service атаки

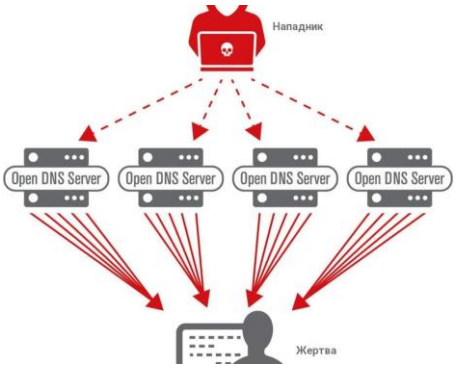

Рис. 16 Методологія здійснення DDoS атаки

Пристрій, який ініціює рукостискання Dragonfly, починає з надсилання кадру фіксації. Обробка цього кадру та генерування відповіді є дорогими з обчислювальної точки зору, особливо якщо реалізовано захист від атак бічного каналу.

Таблиця 3

Типи атак та їх критичність для користувача

Атака	Критичність	Втрачені дані
Downgrade & Dictionary	Висока	Будь-який трафік, включаючи паролі та конфіденційні дані
Security Group Downgrade	Висока	Будь-який трафік, включаючи паролі та конфіденційні дані
Cache-Based Side-Channel	Середня	Ключі шифрування
Denial-of-Service	Низька	Доступ до інтернету

Хоча WPA3 містить метод обміну файлами cookie, щоб запобігти зловмисникам підробляти фрейми фіксації за допомогою фальшивих MAC-адрес, його легко обійти. У результаті зловмисник може перевантажити точки доступу (AP), генеруючи лише 16 підроблених кадрів фіксації в секунду (рис. 16). Ця атака споживання ресурсів спричиняє високе використання ЦП точки доступу, розряджає її батарею, запобігає або затримує підключення інших пристроїв до точки доступу за допомогою WPA3, а також може призупинити або сповільнити інші функції точки доступу.

Як захиститись від DDos атаки

Для захисту від атаки DDoS, можна використовувати різні заходи, які дозволяють виявляти та блокувати аномальний трафік, наприклад, за допомогою системи виявлення вторгнень (IDS) або системи запобігання вторгнень (IPS). Додатково, можна налаштувати мережу з використанням механізмів контролю доступу та обмеження швидкості передачі даних, що допоможе зменшити ймовірність успішної атаки DDoS.

Висновки. Зважаючи на зростаючу популярність технологій Wi-Fi, безпека мережі Wi-Fi стає все більш важливою. Адже за допомогою WIFI передаються не лише звичайні фото та відео, але й дані банківських рахунків, особиста інформація та конфіденційні дані. Зважаючи на те , що WPA2 широко використовується на багатьох пристроях, він має певні вразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до конфіденційних даних, та WPA3 був розроблений для усунення цих вразливостей і забезпечення більш високого рівня безпеки бездротових мереж. Також WPA3 забезпечує нові функції, такі як одночасна автентифікація рівних (SAE) і посилений захист від атак грубої сили.

Проте, незважаючи на покращення, що пропонує WPA3 впровадження цього протоколу може бути вповільненим через те, що є потреба в оновленні мережевого обладнання, що підтримує цей стандарт. Більше того WPA2 залишається стандартом, який можна використовувати для захисту безпровідних мереж, в тому випадку якщо оновлення мережевого обладнання є неможливим.

Підсумовуючи, вибір між WPA2 та WPA3 буде в першу чергу залежати від декількох факторів, включаючи вимоги до безпеки мережі, наявність обладнання, що підтримує новий стандарт, і готовність користувачів модернізувати свої пристрої. Оскільки бездротові мережі продовжують відігравати важливу роль у нашому повсякденному житті, важливо, щоб користувачі усвідомлювали наслідки свого вибору для безпеки і вживали відповідних заходів для захисту своїх мереж від несанкціонованого доступу.

Список літератури

[1] Аналіз захищеності wifi мереж. URL: [Електронний ресурс] https://tech.vernadskyjournals. in. ua/ journals/2021/2_2021/part_1/18.pdf.

[2] Web Titan Most Common Wireless Network Attacks. [Електронний ресурс] https://www. webtitan. com/blog/most-common-wireless-network-attacks/ # : ~:text=Packet%20Sniffing%3A%20Interception%20of%20Unencrypted%20Traffic&text=Packet%20sniffing%20is%20one%20of,as%20those%20using%20WEP%20encryption.

[3] Defence express Захист WIFI на передовій.
[4] [Електронний ресурс] https://defenceua.com/minds_and_ideas/chomu_vazhlivo_maskuvati_wi_fi_na_peredovij_vkraj_vazhlivij_material_dlja_vsih_hto_na_perednomu_kraji_ta_ne_tilki-7948.html.
[5] Небезпека Wi-Fi у публічних місцях: поради IT-спеціалістів. [Електронний ресурс] https: // shpalta.media/2020/08/12/nebezpeka-wi-fi-u-publichnix-miscyax-poradi-it-specialistiv/.
[6] Typical Wi-Fi attacks Splone Blog. [Електронний ресурс] https://splone.com /blog/ 2020/ 10/ 13/ typical-wi-fi-attacks/.
[7] Wi-Fi Security: WEP vs WPA or WPA2.
[8] [Електронний ресурс] – https: // www.avast.com/c-wep-vs-wpa-or-wpa2.
[9] What is KRACK? [Електронний ресурс] https://www.kaspersky.com / resource-center / definitions/krack.
[10] Білевська О.С. Аналіз Вразливостей Програм Сертифікації WPA2 та WPA3 Мережі Wi-Fi [Електронний ресурс] – http://www.tech.vernadskyjournals.in.ua/journals/2021/3_2021/15.pdf.
[11] Mathy Vanhoef, Eyal Ronen, Dragonblood. Analysing WPA3's Dragonfly Handshake of WPA3 and
[12] EAP-pwd. [Електронний ресурс] – http: // wpa3.mathyvanhoef.com.
[13] Mathy Vanhoef, Key Reinstallion Attacks. Breaking WPA2 by forcing nonce reuse. [Електронний ресурс] – http://www.krackattacks.com.
[14] Що таке WPA3, чим кращий за WPA2 і чи варто його вмикати. [Електронний ресурс] https://rootnation.com/ua/articles-ua/tech-ua/ua-wpa3-vs-wpa2/.
[15] Harkins, D. The Dragonfly Key Exchange. [Електронний ресурс] https: //www. rfc-editor. org/rfc/ rfc7664.html.
[16] Key Reinstallation Attacks. [Електронний ресурс] – https://www.krackattacks.com.
[17] Wi-Fi in drones. [Електронний ресурс] https://dronesgator.com/need-wifi-to-fly-a-drone/.
[18] Богданов О.С., Бурак Н.Є. Особливості захисту мережі Wi-Fi з протоколом шифрування WPA3.
[19] [Електронний ресурс] https://sci.ldubgd.edu.ua/bitstream/123456789/9277/1/Bohdanov.pdf.
[20] KRACK Attack Detection.
[21] [Електронний ресурс] https://www.fing.com /news/krack-attack-detection-protection.
[22] І.Р. Опірський, 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. 2021. С. 31-42.
[23] Опірський І.Р., Тютіков О.Ю. Проблематика побудови концепції «Розумного міста» // «Захист інформації». Том 2. Випуск №22. Київ: НАУ, 2020р. С. 114-119.

УДК 004.056.55

Opirskyy I., Maksymiv N., Zhenchur M. Security research of Wi-Fi Protected Access 3 (WPA3) standard

Abstract. *Wi-Fi technology is very relevant nowadays, as wireless communication has become a necessary part of our everyday life. Wi-Fi allows you to connect to the Internet on various devices, such as smartphones, tablets, laptops, TVs, and others. In addition, Wi-Fi technology is constantly evolving and improving. New technology standards, such as 802.11ax (Wi-Fi 6), allow for improved data transfer speeds and greater resistance to interference and interference. However, with the popularity of Wi-Fi technology comes a greater threat to network security. Therefore, it is important to improve security methods and encryption algorithms for Wi-Fi networks to ensure their safety and security. The study of vulnerabilities of Wi-Fi WPA2 and WPA3 wireless communication protocols is very relevant due to the fact that wireless networks are an integral part of the modern world. Since hacker attacks on wireless networks have become widespread, researching WPA2 and WPA3 vulnerabilities is very important for ensuring the security of Wi-Fi networks. After all, WPA2 and WPA3 protocol vulnerabilities can be exploited by attackers to gain unauthorized access to the network and obtain sensitive information such as passwords and user data. This paper will cover such topics as the vulnerabilities of securing WIFI networks using WPA2 and WPA3, the main means of protection against attacks, and a comparative characterization of these two security methods.*

Keywords: *Wi-Fi, WPA2, WPA3, cybercrime, security, cryptography, defense.*

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.

Максимів Назар Васильович, студент, кафедра захисту інформації, Національного університету «Львівська політехніка».
Nazar Maksymiv, student, Department of Information Security, Lviv Polytechnic National University.

Женчур Марія Володимирівна, студентка, кафедра захисту інформації, Національного університету «Львівська політехніка».
Maria Zhenchur, student, Department of Information Security, Lviv Polytechnic National University.

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