УДК 004.7
Вовкостріл А.І.[1]
Лізунов С.І.[2]
[1] студент ЗНТУ
[2] канд. техн. наук, доцент ЗНТУ

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ЗАКРИТИХ WI-FI МЕРЕЖ

Дослідження бельгійського університету KU Leuven знайшли серйозні недоліки WPA2-протоколу, що забезпечує захист сучасних захищених мереж Wi-Fi. Зловмисник, що знаходиться в зоні дії жертви, може використовувати ці недоліки та застосовувати для атаки на повторну установку ключів (KRACK). Таким чином, може бути викрадена конфіденціальна інформація, що вважалась раніше захищеною: номери кредитних карток, паролі, повідомлення чату, електронні листи, фотографії і т.д. [1]

Зловмисник може розшифрувати всі дані, що передає жертва, використовуючи повторну установку універсального ключа шифрування. При криптографічному рукостисканні не гарантується безпека одноразового використання параметрів, що пов'язані з використовуваним ключем. Зловмисник при перехваті ключа шифрування компрометує жертву переустановкою вже використовуваного ключа. Зв'язані параметри (інкрементний номер пакету що передається (nonce) та номер пакету що приймається (лічильник повторів)) скидаються до початкового значення..[1,2]

Коли новий клієнт приєднується до мережі, він виконує чотиристоронне рукостискання для узгодження нового ключа шифрування. Як тільки ключ встановлено, він буде використовуватись для шифрування нормальних фреймів даних з використанням протоколу шифрування. Так як повідомлення можуть бути втрачені чи скинуті, точка доступу повторно передає повідомлення про підтвердження сеансу, якщо воно не отримало відповідного пакета для підтвердження, тому клієнт може отримувати це повідомлення декілька разів. Зловмисник може змусити повідомлення некоректно скидатися, в результаті чого клієнт отримує його і перевстановлює той самий ключ шифрування та скидає інкрементний номер пакету передачі (nonce), отримуючи лічильник повтору, що використовується протоколом шифрування. Таким чином, викликаючи навмисне повторне використання, пакети можуть бути відтворені, дешифровані та/або підроблені. Цей метод можливий для використання в атаці групового ключа, PeerKey, TDLS і узгодженняшвидкого переходу BSS.[1,2]

Дешифрування потоку можливе тому, що атака перевстановлення ключа приводить до відновлення nonce (також відомих як номери пакетів чи вектори ініціалізації) до початкового значення. Тобто один і той же ключ

шифрування використовується із повторюваним декілька разів значенням nonce. Це призводить до того що всі протоколи WPA2 повторно використовують кеш-поток при шифруванні пакетів.

Можливість дешифрування пакетів може бути використана для дешифрування пакетів TCP SYN, що дозволяє зловмиснику отримати порядкові номери TPC з'єднання та захопити його. Після цього зловмисник може не зважати на використання WPA2 та виконати найбільш розповсюджену атаку на мережі Wi-Fi: внесення шкідливих даних в незашифровані HTTP-з'єднання (вводити вимагання чи шантаж, тобто шкідливе програмне забезпечення на сайти, що відвідує жертва).[1]

В небезпеці знаходяться жертви, що використовують протокол шифрування WPA-TKIP чи GCMP замість AES-CCMP.

Проти цих протоколів шифрування можливе не тільки розшифрування, а й підробка та введення пакетів, так як ці протоколи використовують повторне використання nonce. GCMP використовує один і той же ключ аутентифікації в в обидві сторони зв'язку, тому ключ може бути відновлено. Як рішення цієї проблеми, підтримка GCMP на даний момент розвертається під назвою Wireless Gigabit (WiGig) та очікується її прийняття в найближчі декілька років.

Напрям, в якому пакети можуть бути дешифровані чи підроблені, залежить від атаки на рукостискання. Якщо спрощено атакувати чотиристоронніє рукостискання, зловмисник може дешифрувати і підробити пакети, відправлені клієнтом. Коли атака відбувається на рукостискання Fast BSS Transition (FT), є можливість розшифрувати і підробити пакети відправлені клієнту. Більшість атак також здатні відновлювати одноадресні, широкомовні чи багатоадресні кадри. [1]

Важливою деталлю є той факт, що наведені атаки не відновлюють пароль від мережі Wi-Fi, не відновлюють будь-які частини нового ключа шифрування що узгодився під час чотиристороннього рукостискання.

На даному етапі розслідування можливість KRACK можна нейтралізувати за допомогою оновлень безпеки пристроїв, які дозволять встановлювати ключ шифрування тільки раз. Постачальники, чиї продукти протестували дослідники, отримали повідомлення про недоліки ще в липні 2017 року. У серпні до процесу також підключилася координаційний центр CERT-CC, який розіслав повідомлення про вразливості. [1]

Оновлення безпеки гарантують, що ключ встановлюється тільки один раз, що запобігає атаці. Тому користувачі повинні переконатися, що всі пристрої оновлені, а також повинні оновити прошивку маршрутизатора. Що робити, якщо немає оновлень безпеки для мого маршрутизатора або точки доступу, або якщо він не підтримує 802.11r. Домашні маршрутизатори або AP, ймовірно, не вимагають оновлень безпеки. Замість цього, головним чи-

ном, корпоративні мережі повинні будуть оновити свою мережеву інфраструктуру.

Є можливість спробувати зменшити атаки на маршрутизатори і точки доступу, відключивши клієнтські функції (наприклад, використовувані в режимах ретранслятора) і 802.11r (швидкий роумінг).[1]

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Breaking WPA2 by forcing nonce reuse [Електронний ресурс]. – Режим доступу: https://www.krackattacks.com/#demo

2. Mathy Vanhoef, Frank Piessens - Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.