УДК 621.391

АНАЛІЗ УРАЗЛИВОСТІ МЕРЕЖІ WI-FI З ПРОТОКОЛОМ БЕЗПЕКИ WPA2

[1]Осокін М.Г., [1]Романов О.І., [2]Романов А.О.
[1]*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського,*
[2]*Факультет телекомунікацій та захисту інформації НАУ*
E-mail: nikitos397@gmail.com; anton3329@gmail.com

Analysis of vulnerability of WI-FI network with WPA2 security protocol

The process of accessing subscribers to a secure WI-FI network using the WPA2 security protocol. Analysis of a new attack technique for reading information called "KRACK" (Key Reinstallation Attacks).

Сьогодні питання захищеності даних є одним з найпріорітетніших в сучасному світі. Цьому приділяють увагу в мережах доступу, мобільного зв’язку, Інтернет та інш. [1,2] Одним з найпопулярніших варіантів доступу являється стандарт 802.1, він же Wi-F з протоколом безпеки WPA2.

WPA2 (Wi-FiProtected Access) - являє собою оновлену програму сертифікації бездротового зв'язку. У WPA2 забезпечена підтримка стандартів 802.1X, а також протоколу EAP (Extensible Authentication Protocol, розширюваний протокол аутентифікації), а також підтримується шифрування відповідно до стандарту AES (Advanced Encryption Standard, вдосконалений стандарт шифрування).

Для протоколу були розроблені механізми аутентифікації під загальною назвою EAP (ExtensibleAuthenticationProtocol). Протокол EAP був створений з метою скасування приватних механізмів аутентифікації і поширення стандартизованих підходів – використання схеми типу "запит-відповідь" (challenge-response) та інфраструктури, заснованої на публічних сертифікованих ключах, призначених для користувачів. Протокол передачі EAP-повідомлень в стандарті 802.1x називається EAPOL (EAP encapsulationover LAN) і в даний час визначено для Ethernet LAN, а також бездротових мереж стандартів серії IEEE 802.11 і LAN, що використовують технології Token Ring і FDDI [3,4].

Розглянемо основні етапи створення захищеного сеансу зв’язку. Сервер аутентифікації, після отримання сертифікату від користувача, використовує 802.1X для створення унікального базового ключа для сеансу зв'язку. TKIP здійснює передачу згенерованого ключа користувачеві і точці доступу, після чого формує ієрархію ключів і систему управління. Для цього використовується двосторонній ключ для динамічної генерації ключів шифрування даних, які в свою чергу використовуються для шифрування кожного пакету даних.

Іншим важливим механізмом є перевірка цілісності повідомлень (Message Integrity Check, MIC). Її використовують для запобігання перехоплення пакетів

даних, зміст яких може бути змінено, а модифікований пакет знову переданий по мережі.

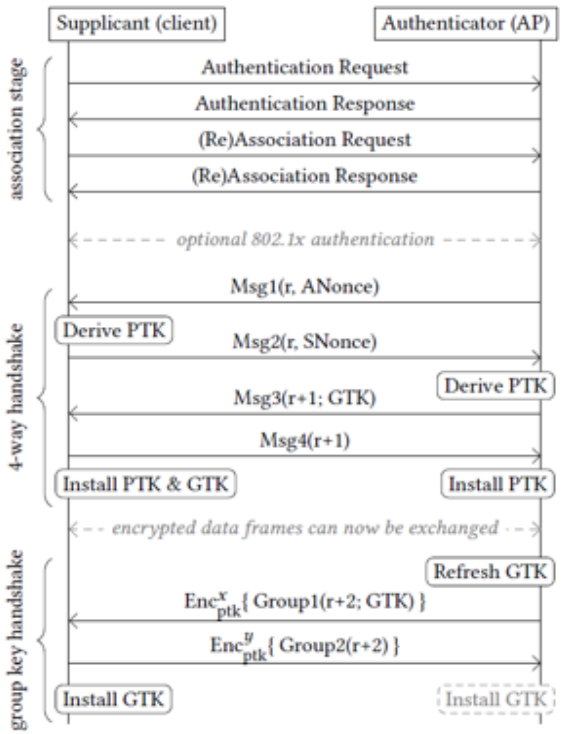

Рис. 1.

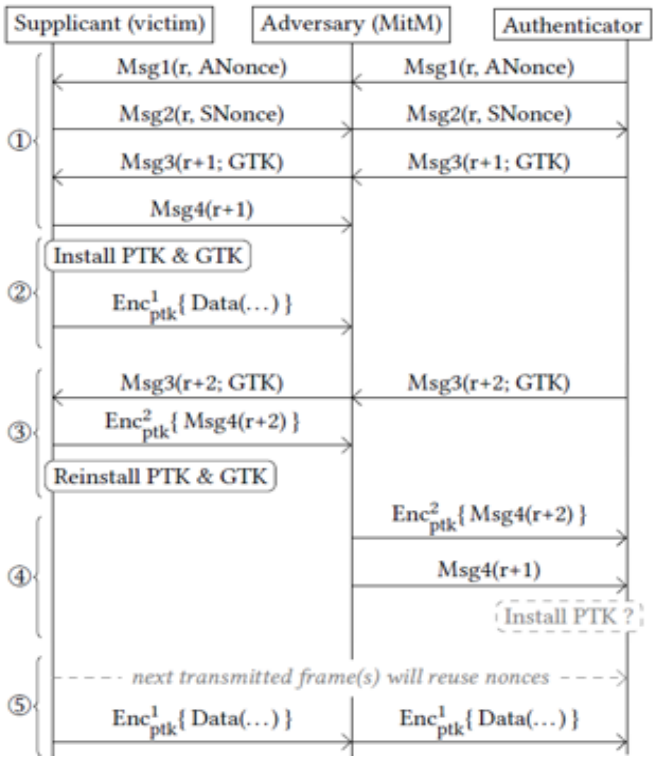

Рис. 2.

На рис.1 зображено алгоритм обміну повідомленнями, коли клієнт з'єднується з аутентифікатором (AP), виконує 4-х стороннє рукостискання і періодично виконує рукостискання в групі.

Однак, під час одного з чергових тестувань, було виявлено нову вразливість, що отримала назву “KRACK” (Key Reinstallation Attacks). Суть вразливості полягає в тому, що зловмисники можуть використовувати нову техніку атаки для зчитування інформації, яка раніше вважалася безпечно зашифрованою. Це може бути використано для крадіжки конфіденційної інформації, наприклад, номерів кредитних карток, паролів, повідомлень у чаті, електронних листів, фотографій тощо. Атака працює проти всіх сучасних захищених мереж Wi-Fi. Крім того, в залежності від конфігурації мережі доступу, зловмисник може впроваджувати шкідливе програмне забезпечення на веб-сайтах.

Уразливість, на яку відбувається атака, знаходиться в 4-кроковому алгоритмі відкриття сеансу протоколу. Цей алгоритм виконується при під'єднанні нового клієнта до захищеної Wi-Fi мережі. Основним завданням алгоритму «рукостискання» є перевірка достовірності пароля, яким захищена дана мережа. Під час «рукостискання» також відбувається погодження нового ключа для шифрування всіх даних, які будуть передані протягом сеансу.

Уразливість KRACK покладається на можливості примусити жертву повторно скористатись вже наявним ключем. Це досягається шляхом маніпуляцій

криптографічними повідомленнями під час «рукостискання». Коли жертва встановлює ключ, вона скидає значення пов'язаних параметрів - лічильники переданих пакетів та отриманих пакетів до початкових значень. Аби убезпечити користувачів від криптоаналізу ключ має бути встановлений лише один раз, але завдяки виявленій можливості маніпулювати процедурою «рукостискання» з'являється практично реалізований спосіб реалізації даної уразливості.

При під'єднанні нового клієнта до мережі Wi-Fi відбувається узгодження спільного ключа шифрування за 4 кроки. Узгоджений ключ потім служить для шифрування всіх «нормальних» пакетів даних. Однак, оскільки окремі повідомлення можуть бути втрачені, точка доступу може повторно відправляти повідомлення третього кроку поки не отримає підтвердження його отримання. Як наслідок, клієнт може отримувати це повідомлення декілька разів. Кожного разу, отримавши таке повідомлення клієнт встановлюватиме наявний ключ шифрування та скидатиме лічильники. Завдяки повторному використанню нонса з'являється можливість атаки на криптографічний протокол: відтворення пакетів, дешифрування та, навіть, підробка їх вмісту.

Ця атака витягує IE RSN (надійний захищений мережевої елемент інформації) з одного кадру EAPOL. RSN IE - це необов'язкове поле, яке виступає в якості контейнера до ідентифікатора ведучого ключа Pairwise (PMKID), який створюється маршрутизатором, коли користувач намагається підключитися до мережі WiFi. PMK грає важливу роль в 4-сторонньому рукостисканні, яке використовується для аутентифікації як відомого клієнтського і маршрутизаторного встановленого ключа (PSK), так і бездротового пароля мережі. «PMKID обчислюється з використанням HMAC-SHA1, де ключ є PMK, а частина даних являє собою конкатенацію фіксованої строкової мітки «PMK Name», MAC-адресу точки доступу і MAC-адресу станції».

На рис. 2 зображена атака переустановлення ключів на 4-позиційне рукостискання, коли жертва все ще приймає повторні передачі відкритого тексту повідомлення 3, якщо встановлено PTK.

По суті, KRACK дозволяє зловмисникові здійснити атаку типу man-in-the-middle і примусити учасників мережі виконати реінсталляцію ключів шифрування, які захищають трафік WPA2. До того ж якщо мережа налаштована на використання WPA-TKIP або GCMP, зловмисник зможе не тільки прослуховувати трафік WPA2, а й здійснювати інжект пакетів в дані жертви.

Метод KRACK універсальний і працює проти будь-яких пристроїв, підключених до Wi-Fi мережі. Тобто в небезпеці абсолютно всі користувачі Android, Linux,iOS, macOS, Windows, OpenBSD, а також численні IoT-пристрої.

Якщо жертва все ще приймає повторні передачі відкритого тексту повідомлення 3 після встановлення сеансового ключа, наша атака переустановки ключа проста. По-перше, атакуючий використовує на основі каналу MitM атаку, щоб вона могла керувати повідомленнями рукостискання [5,6]. Потім вона блокує

повідомлення 4, що надходить на аутентифікатор. Це проілюстровано на стадії 1 на рис.2. Відразу після надсилання повідомлення 4 жертва встановить PTK і GTK.

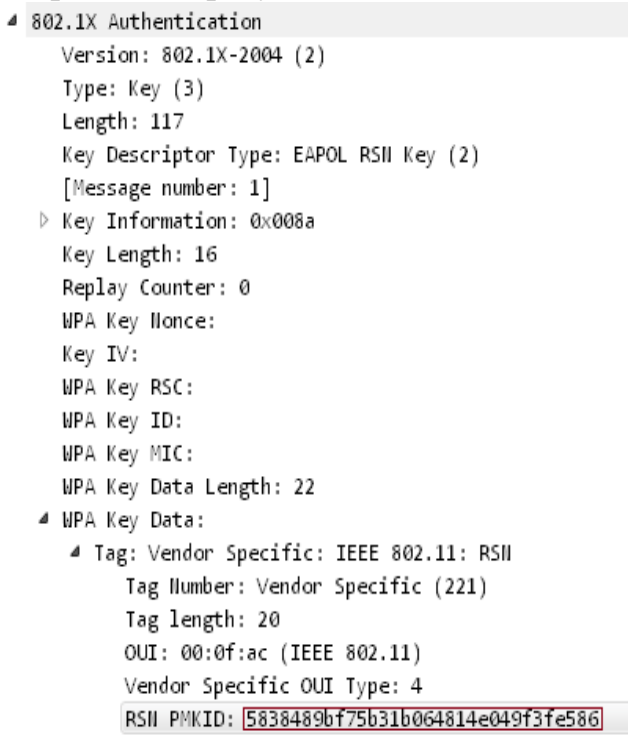

Рис. 3.

У цей момент жертва також відкриває порт 802.1x і починає передавати звичайні кадри даних. Потім, на третьому етапі атаки, аутентифікатор повторно передає повідомлення 3, оскільки він не отримав повідомлення 4. Атакуючий пересилає повторно передане повідомлення 3 жертві, змушуючи його перевстановити PTK і GTK. В результаті він скидає лічильник nonce і replay, що використовується протоколом конфіденційності даних. Таким чином, ми можемо контролювати кількість nonces, які будуть повторно використані. Більш того, атакуючий завжди може знову виконати атаку, деавторизуючи клієнта, після чого він знову з'єднається з мережею і виконає нове 4-позиційне рукостискання. На рис. 3 можна побачити приклад тестового «спійманого» ключа RSNPMKID.

Для уникнення атак такого роду, слідує оновити програмне забезпечення смартфону/ПК/роутера, адже ця вразливість допущена в самому протоколі і уникнути від потенціальної шкоди можна лише в тому випадку, якщо оновити обладнання [7]. Також, конфіденційність даних забезпечить використання VPN і протоколу HTTPS, під час користування мережею інтернет.

Література

1. Романов О.І., Осокін М.Г. Аналіз рівня безпеки сигналізації SS7. Матеріали 12-ої МНТК «Проблеми телекомунікацій», Київ, 2018 р. С 131-134.
2. Письменний І.С., Романов А.О. Мережа підприємства с програмним забезпеченням ASTERIISK PBX на основі PLC, Київ, 2018 р. С 119-122.
3. Атака против WPA2, позволяющая перехватить трафик WiFi-сети [Електронний ресурс] – Режим доступу: https://www.opennet.ru/opennews/art.shtml?num=47392.
4. Мария Нефёдова, Новая методика упрощает взлом паролей WPA и WPA2 в сетях 802.11i/p/q/r [Електронний ресурс] – Режим доступу: https://xakep.ru/2018/08/07/802-11-pass-hack/.
5. Мария Нефёдова, Опубликована подробная информация о проблемах WPA2 [Електронний ресурс] – Режим доступу: https://xakep.ru/2017/10/16/wpa2-krack-2/.
6. Лука Сафонов, Новая техника атаки WPA2, не требующая наличия клиента на AP [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/jetinfosystems/blog/419383/.
7. Mathy Vanhoef, Key Reinstallation Attacks. Breaking WPA2 by forcing nonce reuse [Електронний ресурс] – Режим доступу: https://www.krackattacks.com.