АТАКА С ПЕРЕУСТАНОВКОЙ КЛЮЧА (KRACK)

[1]*Бакунова Оксана Михайловна,*
[2]*Бакунов Александр Михайлович,*
[3]*Котлов Александр Алексеевич,*
[3]*Мартыненко Илья Олегович,*
[3]*Гимик Василий Олегович*

Республика Беларусь, БГУИР,
[1]*старший преподаватель, исследователь технических наук, магистр технических наук;*
[2]*старший преподаватель, магистр технических наук;*
[3]*студент*

DOI: https://doi.org/10.31435/rsglobal_wos/12062018/5739

ARTICLE INFO

Received: 15 May 2018
Accepted: 05 June 2018
Published: 12 June 2018

KEYWORDS
security protocols, network security, attacks, key reinstallation, WPA2

ABSTRACT

In the era of IT great attention is paid to data security and confidentiality on the Internet. Despite that often vulnerabilities and exploits can be found in almost every system. Examples of such vulnerabilities can be a defect in architecture or an error in the data-transfer algorithm. Deprecation of standards can also lead to new exploits. As a result it is a necessary to develop new standards or modernize existing ones. This article is about new vulnerability in authorization process of Wi-Fi networks that make use of WPA2 protocol.

Citation: Бакунова О. М., Бакунов А. М., Котлов А. А., Мартыненко И. О., Гимик В. О. (2018) Атака с переустановкой ключа (krack). *Web of Scholar. 6(24),* Vol.1. doi: 10.31435/rsglobal_wos/12062018/5739

Copyright: © 2018 **Бакунова О. М., Бакунов А. М., Котлов А. А., Мартыненко И. О., Гимик В. О.** This is an open-access article distributed under the terms of the **Creative Commons Attribution License (CC BY)**. The use, distribution or reproduction in other forums is permitted, provided the original author(s) or licensor are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Введение. В 2016 году бельгийские исследователи Франк Писсенс (Frank Piessens) и Мэтти Ванхоеф (Mathy Vanhoef) впервые обнаружили уязвимость, позволяющую применить атаку переустановки ключа. Проведя исследования данной уязвимости, в октябре 2017 года ими был выпущен обширный перечень потенциальных атак.

Результаты и обсуждение. С помощью данной уязвимости у злоумышленника появляется возможность изменять и просматривать как отправляемые пакеты, так и получаемые. Это ставит под угрозу конфиденциальность различного рода информации, такой как пароли, переписка, номера и коды кредитных карт и многое другое.

Современные Wi-Fi устройства снабжены системой защиты WPA2, которая, в свою очередь, основана на технологии четырехэтапного рукопожатия принятой в стандарте 802.11i.

Основная концепция четырехэтапного рукопожатия заключается в том, что при подключении к Wi-Fi сети новый клиент с помощью четырех сообщений организует ключи шифрования с передающим устройством. При получении третьего сообщения клиент устанавливает полученные ключи, как активные ключи шифрования, после чего отправляет завершающий, четвёртый, пакет точке доступа, чтобы исключить потерю третьего пакета из-за помех и т.п. В случае получения четвертого пакета точкой доступа, работа продолжается в стандартном режиме, а при его отсутствии, точка доступа отправляет третий пакет заново. При получении третьего пакета повторно клиент сбрасывает счётчики и начинает кодировать сообщение заново. Именно этот этап, с повторной отправкой ключа, позволяет злоумышленнику декодировать сообщение, а в зависимости от используемого протокола, так же получить возможность перехватывать куки, пароли, воспроизводить, расшифровывать или создавать пакеты.

Особенно уязвимым к данной атаке оказался wpa_supplicant версий 2.4 и 2.5, обычно используемый в Linux и android 6.0. При использовании атаки, в данном случае, клиент устанавливает нулевой ключ, вместо того, чтобы заново перезаписать существующий. Эта

уязвимость появилась в результате изменений в стандарте 802.11, который предлагал удалять кодирующую последовательность после генерации кодирующих блоков.

В версии 2.6 это было исправлено, однако, посчитав это некритичным багом, для предыдущих версий исправлений не последовало. Вследствие чего данные версии остаются уязвимыми, как и использующие их программы, такие как Android Wear 2.0. [1]

Результатом атаки является кодирование различной информации одними и теми же блоками кода, вследствие чего у злоумышленника появляется возможность декодировать сообщение, либо, что ещё хуже, выяснить сам ключ.

Первым этапом должно стать внедрение в протокол конфиденциальности данных проверки, установлен ли уже используемый сетью ключ. Если это так, то отменяется сброс связанных с этим счётчиков и перезапись ключа. Это предотвратит возможность атаки, по крайней мере, если злоумышленник не использует для перестановки старый ключ, перед повторной установкой текущего. А также, при использовании данных мер защиты, важно, чтобы счётчик повторных запросов рукопожатий с ключом только увеличивался. Иначе злоумышленник может попытаться использовать старое сообщение, чтобы жертва временно установила старый ключ, впоследствии переустановив актуальный.

Второй этап – убедиться, что конкретный ключ установлен лишь единожды за время сессии рукопожатия в сущность, реализующую протокол конфиденциальности данных. Когда клиент получает повторно переданное сообщение 3, он должен ответить, но не переустанавливать ключ сеанса. Это можно сделать, добавив логическую переменную. Она инициализируется в состоянии false и установить значение true при создании нового PTK в PTK-START. Если значение переменной true при вводе PTK-DONE, то PTK установлен, а переменной присваивается значение false. Если значение переменной false при вводе PTK-DONE, установка PTK пропускается.

На данный момент идёт активное обсуждение модернизации протокола безопасности, а также происходит отслеживание устройств, критически уязвимых к данной атаке.

Выводы. На примере данной уязвимости можно подчеркнуть необходимость пересмотра стандартов безопасности с некоторой периодичностью. Так же, при оценке уровня стойкости шифрования следует обращать внимание не только на математический алгоритм шифрования, но и на логическую структуру механизмов распределения, обновления и утилизации ключей, токенов, так как это может стать причиной уязвимости всего алгоритма, в обход математической составляющей.

ЛИТЕРАТУРА

1. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [Электронный ресурс] – Режим доступа: https://papers.mathyvanhoef.com/ccs2017.pdf.

2. О. Н. Образцова, О. М. Бакунова, Д. М. Кугач, А. В. Хомяков Практико-ориентированное обучение в сфере информационных технологий в БГУИР и сотрудничество вуза с ведущими компаниями IT // Проблемы современного образования: материалы VIII международной научной конференции, 10-11 сентября 2017. – Прага: Vědecko vydavatelské centrum «Sociosféra-CZ», 2017 - С.38-41

3. Бакунов А. М., Бакунова О. М., Калитеня И. Л., Образцова О. Н. Профориентация как предпосылка выбора профиля обучения // Непрерывная система образования "школа-университет". Инновации и перспективы: сборник статей Международной научно-практической конференции (23-24 февраля 2017 г.) - Минск: БНТУ, 2017. - С. 35-37.

4. Бакунов А. М., Бакунова О. М., Калитеня И. Л., Образцова О. Н. Применение ИКТ в образовательном процессе специальности «Программное обеспечение информационных технологий» специализации «Программное обеспечение обработки экономической и деловой информации» / Подготовка специалиста-профессионала в различных видах деятельности : [электронный ресурс] : материалы Республиканской научно-практической конференции с международным участием, Гомель, 23-24 ноября 2017 г. - Гомель : Гомельский областной институт развития образования, 2017. - С. 43 - 46.

5. О. М. Бакунова, О. Н. Образцова, Силинский, Р. А. Дистанционные технологии как способ оптимизации трудовых процессов инженеров испытательной лаборатории / // Дистанционное обучение – образовательная среда XXI века : материалы X международной научно-методической конференции (Минск, 7 - 8 декабря 2017 года). – Минск: БГУИР, 2017. – С. 286.

6. Бакунова О. М., Калитеня И. Л., Бакунов А. М., Малиновская Т. И. Применение ИКТ для оказания образовательных услуг лицам с особыми потребностями на примере изучения системы 1С дистанционно // Непрерывное профессиональное образование лиц с особыми потребностями: сборник статей международной науч.- практической конференции (Минск, 14 - 15 декабря 2017 года). – Минск: БГУИР, 2017. – С. 41 – 43.