DOI 10.36622/VSTU.2023.4.26.008
УДК 004.056

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ, ОСНОВАННЫХ НА ПРИМЕНЕНИИ БЕСПРОВОДНЫХ СЕТЕЙ

Ю.Ю. Громов, П.И. Карасев, А.И. Елисеев, Н.С. Кибец

В работе рассмотрены основные методы защиты от атак на информационные системы, использующие беспроводные сети Wi-Fi. При описании каждого из них были разобраны причины возникновения уязвимостей, которые и повлекли за собой возможность компрометации сети информационной системы со стороны злоумышленника, а также приведены возможные способы их исправления. Были рассмотрены уязвимости таких типов сетей, как WPA2 Personal и WPA2 Enterprise, но больший акцент был сделан именно на первом типе, так как такие сети более повсеместны, их можно встретить повсюду. В первую очередь информация о данных недостатках безопасности представлена для ознакомления, ведь для того, чтобы понять, как обезопасить свою беспроводную сеть, для начала следует выяснить, какие уязвимости существуют и как от них можно защититься. Кроме того, в статье была рассмотрена роль беспроводной сети в общей модели безопасности локальной сети.

Ключевые слова: Wi-Fi, перехват трафика, ИБ, SSID, WPA-2, WEP, handshake, PNL, WPA/WPA2-Personal (PSK), WPA/WPA2-Enterprise (MGT), Man-in-the-Middle, WPS, Brute force, WPS Pixie Dust, PSK, MAC адрес.

Введение

В современном мире беспроводные сети являются неотъемлемой частью повседневной жизни любого человека. Каждый год специалисты ведут работу над все более быстрыми стандартами беспроводных сетей, а также над новыми эффективными и стойкими протоколами шифрования.

Но несмотря на все это, в глобальной паутине все еще находится большое количество маршрутизаторов, безопасность которых оставляет желать лучшего.

Из-за низкой технической осведомленности пользователей, на многих сетевых устройствах до сих установлены заводские, устаревшие обновления безопасности, а также стандартный простой пароль. Этим конечно же пользуются злоумышленники.

Помимо этого, стоит отметить, что многие производители предоставляют очень скудную поддержку своих устройств. В связи с этим, стоит уделять внимание выбору производителя сетевой техники.

Несмотря на все попытки производителей сделать свою продукцию защищенной, атаки все равно происходят, а с каждым годом становятся все изощреннее. Например, для компрометации сети могут использоваться приемы социальной инженерии, с помощью которых возможно осуществить атаки на самих пользователей.

Цели атак могут быть разнообразными: деструктивное влияние на сетевые активы компании, кража персональных данных и т.д.

В связи с этим, стоит уделять внимание безопасности беспроводных сетей, ведь именно сети данного типа часто являются слабым местом сетевой инфраструктуры организации.

Для того, чтобы понимать, как улучшить безопасность беспроводных сетей, нужно знать, какие уязвимости в них могут содержаться. Этому посвящен следующий раздел данной работы.

Способы компрометации беспроводных сетей

В данном разделе будут рассмотрены основные атаки на беспроводные сети, а также способы защиты от них. Многие из них существуют уже много лет, но на некоторых точках доступа, производители которых не выпустили современные обновления прошивки с патчем безопасности для исправления уязвимостей, они все еще могут быть актуальны.

Все атаки будут систематизированы в зависимости от технических особенностей реализации.

Организация поддельных точек доступа

В жилых помещениях, предприятиях используют мобильные устройства, которым необходимо Wi-Fi соединение. Зачастую включено автоматическое подключение к точкам доступа, с которыми когда-либо работали на конкретном устройстве.

Данная атака заключается в том, что устройства подключаются к известной точке доступа, но при этом не проверют ее на факт легитимности [1]. Таким образом, весь трафик может быть перенаправлен к злоумышленнику.

Согласно исследованию в области безопасности корпоративных беспроводных сетей компании Positive Technologies, в 75% проектов с помощью данной атаки удалось перехватить аутентификационные данные пользователей.

Данная атака реализуется следующим образом: на каждом устройстве, которое использует беспроводное подключение к глобальной паутине, существует специальное хранилище PNL, в котором содержится упорядоченный список идентификаторов ESSID, к которым станция подключалась в прошлом. Если мобильное устройство найдет сеть, идентификатор которой содержится в PNL, то произойдет подключение.

В зависимости от технических особенностей атакуемой сети существуют следующие разновидности данного типа атаки:

- на открытую точку доступа, не использующую шифрование трафика;
- на персональную сеть, защищенную WPA/WPA2-Personal (PSK) [2];
- на корпоративную сеть, защищенную WPA/WPA2-Enterprise (MGT).

Для того, чтобы осуществить атаку на открытую сеть, достаточно создать ее копию, также сделав общедоступной, и вынудить подключиться устройство атакуемого. Возможно применение фишинга (например, с помощью вэб формы авторизации пользователя, которая зачастую используется в городских общественных сетях).

В случае же с атакой на сети WPA/WPA2-Personal (PSK) преградой может стать незнание пароля сети. Для пользователя может показаться необычным и подозрительным отсутствие пароля у сети, у которой он всегда был.

Дальнейший вектор атаки может быть очень разнообразен:

- классическая атака «человек посередине» (англ. Man-in-the-Middle);
- атака на внутренний портал компании, при которой может быть совершена фишинг атака или доставка полезной нагрузки в корпоративную или домашнюю локальную сеть.

Для того, чтобы нагляднее показать, как работает данный класс атак, был создан тестовый стенд, состоящий из двух устройств и, собственно, беспроводной точки доступа.

С помощью специального сетевого адаптера, который поддерживает AP и неразборчивый режимы, удалось создать поддельную точку доступа. Далее с помощью отправки специальных пакетов деаутентификации удалось вынудить стендовый хост-жертву переподключиться к ненастоящей сети с таким же именем. Таким образом, весь трафик начинает идти через компьютер злоумышленника. Упрощенная схема атаки представлена на рис. 1.

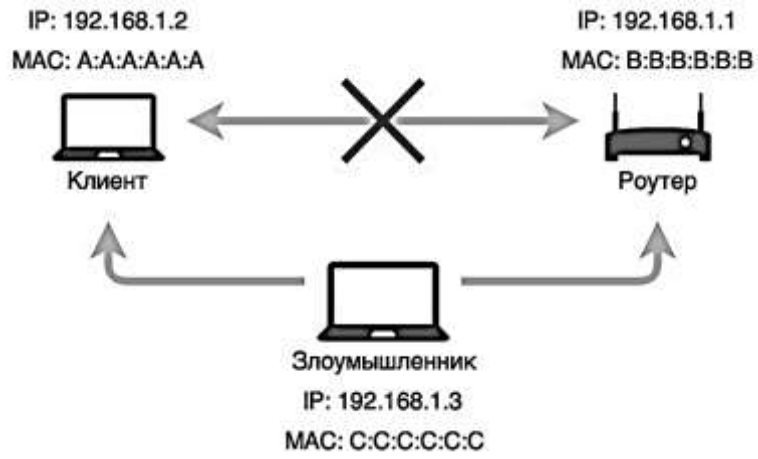

Рис. 1. Пример атаки «человек посередине»

Для того, чтобы защититься от атак данного класса, следует:

– не использовать незащищенные беспроводные сети;
– использовать собственную, доверенную точку доступа;
– выключить автоматическое подключение к известным Wi-Fi сетям;
– использовать многофакторную аутентификацию;
– использовать VPN.

Уязвимость в WPS PIN

Для начала стоит разобраться, что такое WPS, как он работает и зачем он нужен.

WPS (Wi-Fi Protected Setup) – стандарт полуавтоматического создания беспроводной сети. Данная технология упрощает процесс подключения пользователей к точке доступа [3] (рис. 2).

Можно воспользоваться следующими способами подключения к сети:

– используя аппаратную кнопку PBC на точке доступа;
– используя NFC;
– используя специальный код аутентификации.

Несмотря на все удобство, именно последний способ содержит неисправимую уязвимость в механизме работы. Рассмотрим данную уязвимость подробнее.

.

WPS Pin состоит из 8 цифр, последняя является контрольной суммой предыдущих семи. Чтобы найти валидный код, в худшем случае нужно перебрать 10^7 (10000000) вариантов, но благодаря данной уязвимости можно поступить иначе.

В авторизации по протоколу WPS предполагается, что клиент должен отправить точке доступа некоторые пакеты M1-M7. Так, если первые четыре цифры кода неверны, то точка доступа сообщит нам об этом после отправки пакета M4. Если же первые четыре цифры верны, а в последующих присутствует ошибка, то мы узнаем об этом после отправки сообщения M6 [4]. Таким образом, можно сильно сократить количество переборов до $10^4 + 10^3 = 11000$. Данный факт может сэкономить очень много времени атакующему.

Ранее данная атака была популярна, но сейчас во многих организациях существуют строгие политики безопасности, в которых прописаны меры по предотвращению атак типа «Brute force». Она может потерять свою актуальность для тех сетевых устройств, производители которых позаботились о безопасности своих клиентов.

Защитные средства и механизмы для предотвращения онлайн атак можно обойти с помощью оффлайн атаки на протокол WPS, которая будет рассмотрена далее.

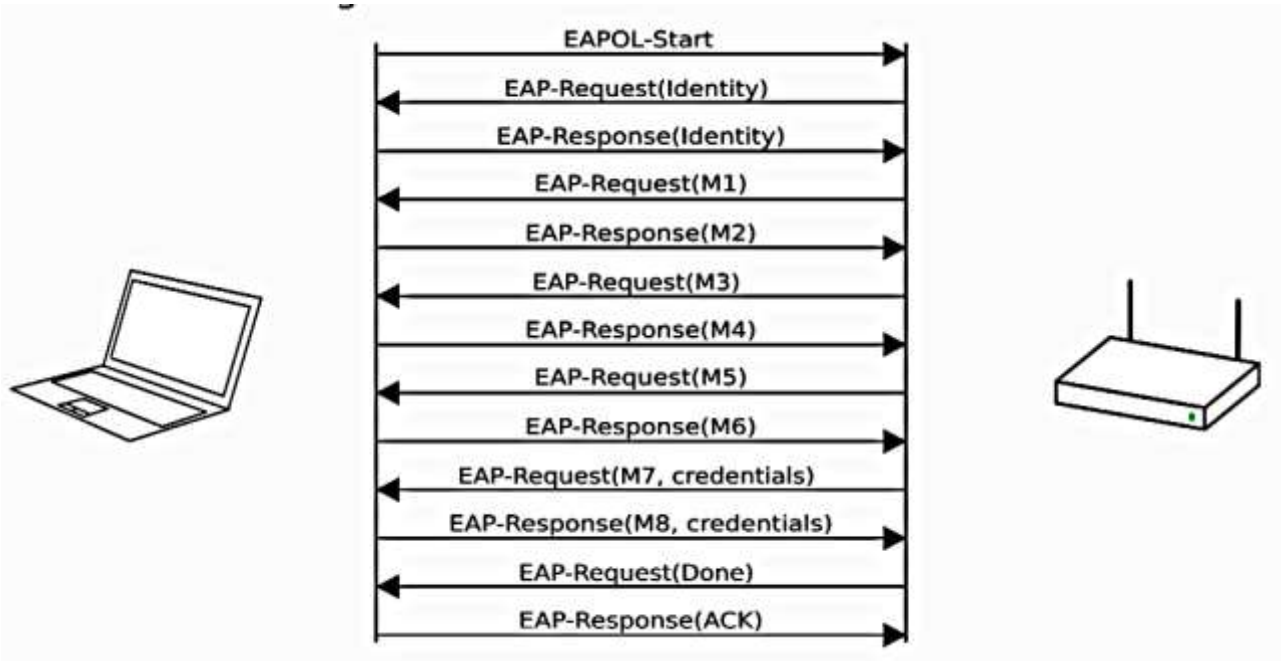

Рис. 2. Процесс аутентификации с помощью WPS

Самым лучшим способом защиты от атак на WPS – это его отключение. Если технология WPS все же нужна, стоит поддерживать программное обеспечение маршрутизаторов в актуальном состоянии. Данная атака далеко не новая, уязвимость по перебору WPS в большей части сетевых устройств уже исправлена.

Атака «WPS PIXIE DUST»

Уязвимость, эксплуатируемая в данной атаке, была обнаружена одним зарубежным исследователем в сфере информационной безопасности в конце 2014 года. Так, уязвимость кроется в алгоритме аутентификации, а точнее в реализации его производителями сетевого оборудования на конкретных устройствах [5].

Для выбора метода аутентификации, который будет использоваться при подключении клиента к точке доступа, используется фреймворк аутентификации EAP.

Рассмотрим подробнее EAP запрос (M1), EAP ответ (M2), EAP запрос (M3).

Таблица 1

Сообщения M1-M3 и передаваемые в них данные

Отправитель -> получатель	Сообщение	Передаваемые данные
Роутер – клиент	M1	N1, Description, PKE
Клиент – роутер	M2	N1, N2, Description, PKR, Auth
Роутер – клиент	M3	E-Hash1, E-Hash2

В табл. 1 обозначено:

N1 – 128-битное случайное число, сгенерированное клиентом.

PKE – открытый ключ клиента.

N2 – 128-битное случайное число, сгенерированное роутером.

PKR – открытый ключ роутера.

Auth – хэш от первых двух сообщений.

```
E-Hash1 = HMAC-SHA-256 (E-S1 | PSK1 | PKE | PKR)
E-Hash2 = HMAC-SHA-256 (E-S2 | PSK2 | PKE | PKR)[6]
```

PSK1 состоит из первых 4 цифр WPS, PSK2 – последние 4 цифры.

В сообщении M4 клиент посылает сообщение о том, что ему известен ПИН код. В M5 роутер посылает аутентификационные данные точки доступа. Проблема заключается в том, что числа E-S1 и E-S2 должны быть случайными, но у техники некоторых производителей они либо предопределены, либо алгоритм их вычисления известен. На современных точках доступа WPS зачастую активирован по умолчанию, поэтому при аудите безопасности следует отдельно обратить внимание на проверку защищенности подключения с помощью данной технологии на конкретном устройстве. Основные меры по защите следующие:

– не использовать WPS;
– устанавливать последние доступные обновления;
– использовать технику, которая на момент использования поддерживается производителем.

Атака на WEP шифрование

WEP – довольно старый стандарт защиты беспроводных сетей, был создан в конце 20 века. Для шифрования трафика используется временный ключ [7]. Проблема заключается в том, что к каждому пакету данных добавляется несколько байт этого ключа. Для успешной атаки на 64 битный достаточно иметь 200000 пакетов, для 128 битного около 5000

В настоящее время данный протокол практически не используется и встретить его на реальных точках доступа очень сложно, поэтому подробнее атака на WEP в данной статье не будет рассмотрена. Не следует использовать данный протокол на реальных точках доступа в локальных сетях, он давно не обеспечивает какой-либо защиты передаваемой по радиоканалу информации.

WPA/WPA2 PSK перехват HANDSHAKE

Данная атака может сработать на тех точках доступа, на которых, следуя стандарту WPA/WPA2 personal, отсутствует сервер аутентификации radius. То есть пароль одинаковый для всех клиентов сети. Когда клиент пытается подключиться к точке доступа, происходит «четверное рукопожатие» (4-ways handshake). Это требуется для генерации PTK, который используется для шифрования трафика между клиентом и точкой доступа. Ключ является сессионным, то есть действует в рамке одного подключения. После этого все устройства получают PMK. Этот же ключ статичен до того момента, как поменяется SSID сети. Схема четверного рукопожатия приведена в рис. 3. Прослушав четверное рукопожатие, можно произвести атаку по подбору PSK (пароля) [8].

В ходе «прослушивания» трафика атакующий может получить следующие данные:

– SSID точки доступа;
– ANonce, SNonce;
– MAC адреса клиента и точки доступа;
– значение MIC, сгенерированное действительным ключом PTK.

Таким образом, происходит перебор возможных значений PSK. Для каждого из них по алгоритму вычисляются PMK и PTK. С помощь PTK происходит вычисление значения MIC. Если оно равно перехваченному значению, то PSK валиден.

Данная атака является устаревшей и требует огромных мощностей для осуществления сложных вычислений. Помимо этого, она может быть нецелесообразна, если нужно быстро получить доступ к сети.

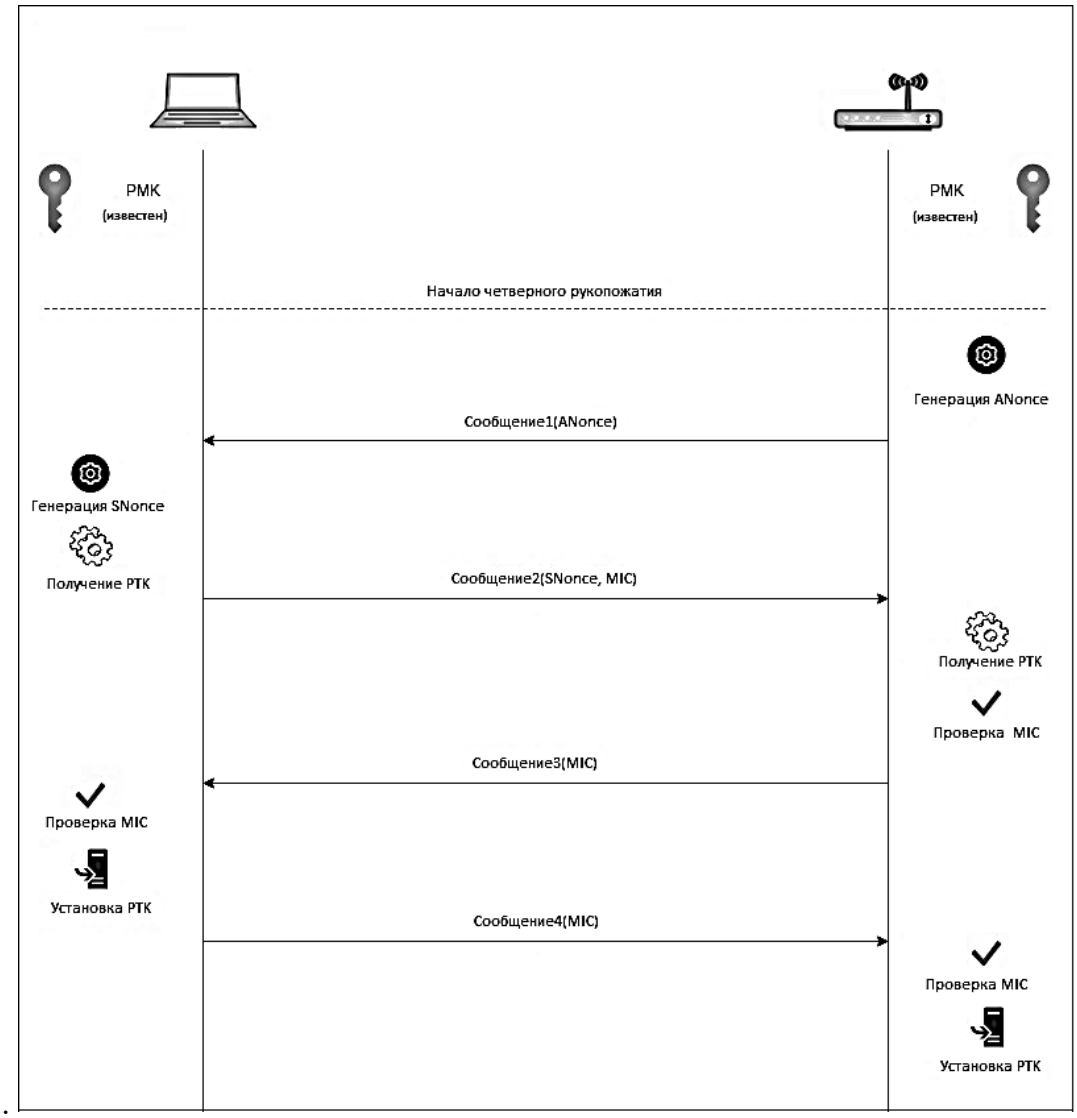

Рис. 3. Упрощенная схема четверного рукопожатия.

Основной мерой по защите беспроводных сетей от данной атаки является использование длинных и сложных паролей, подбирать которые просто нецелесообразно или вовсе невозможно.

Надежный пароль можно создать следующими способами:

– придумать алгоритм для составления паролей;
– воспользоваться генератором паролей и хранить пароль в менеджере паролей или ином защищенном хранилище.

WPA/WPA2 PSK PMKID атака

Данная атака появилась относительно недавно. Используемая в ней уязвимость была найдена в 2018 году при тестировании на безопасность протокола WPA3.

Особенность данной уязвимости заключается в том, что для атаки не требуется подключение клиентов к точке доступа, нужно лишь взаимодействие между ней и атакующим [9].

В атаке используется первое сообщение четверного рукопожатия, которое содержит некоторое значение PMKID, которое по умолчанию добавляют современные маршрутизаторы. Формула вычисления PMKID представлена на рис. 4 [10].

PMKID = HMAC-SHAI-128(PMK , "PMK Name" | MAC_AP | MAC_STA)

PMK = PBKDF2(Passphrase , SSID , 4096)

Рис. 4. Хеш-функция для вычисления PMKID

MAC адреса легко узнать, строка "PMK Name" постоянна. PMK можно найти с помощью перебора, затем высчитать хэш по алгоритму, представленному в формуле, и сопоставить перехваченному ранее значению PMKID.

Таким образом, можно получить данные для аутентификации без подключенных клиентов к этой беспроводной сети.

Чтобы защититься от данной атаки, как и в случае с предыдущей, следует использовать надежные пароли, которые не были слиты в публичных базах. Это единственный действенный способ противодействия данной атаке. Перебор хеш-функций обычно производится по словарю паролей, поэтому сгенерированный длинный пароль является неплохим способом защиты, так как делает бессмысленными попытки подобрать валидный хеш.

Атака EAP Downgrade на корпоративные беспроводные сети WPA Enterprise (MGT)

Сети WPA Enterprise (рис. 5) созданы для бизнеса, в частности, для крупных компаний, которые обладают обширной сетевой инфраструктурой. В процессе аутентификации задействуется специальный сервер аутентификации Radius.

Авторизация в сети происходит по уникальной для каждого пользователя связке «логин:пароль».

Рис. 5. Схема сети WPA Enterprise.

Существует множество протоколов аутентификации между клиентом и сервером Radius. Атаки на протоколы аутентификации нельзя отнести к популярным способам компрометации сети, поэтому в данной работе уязвимости всех известных протоколов аутентификации затронуты не будут.

Как уже говорилось ранее, в сетях, использующих WPA Enterprise, можно провернуть атаку по подмене точки доступа. Несмотря на всю сложность топологии сети, существует множество инструментов для ее реализации.

Для начала стоит рассмотреть возможный вектор атаки на такую сеть, если до этого была выполнена подмена легитимной беспроводной точки доступа.

Метод шифрования EAP [11] инициируется точкой доступа. В обычных сетях протоколы аутентификации должны выбираться по принципу от надежного к менее надежным, атакующему это невыгодно, поэтому он может обмануть

клиентов и заставить их использовать небезопасные протоколы. На рис. 6. представлена схема атаки, использующей данную идею [12].

Данной атаке в большей мере подвержены мобильные устройства, количество которых обычно не столь велико в корпоративной сети, так как их алгоритмы поиска наилучших беспроводных точек доступа работают довольно агрессивно. Но не исключена возможность проведения данной атаки и с обычными стационарными рабочими станциями и ноутбуками, оснащенными беспроводной сетевой картой.

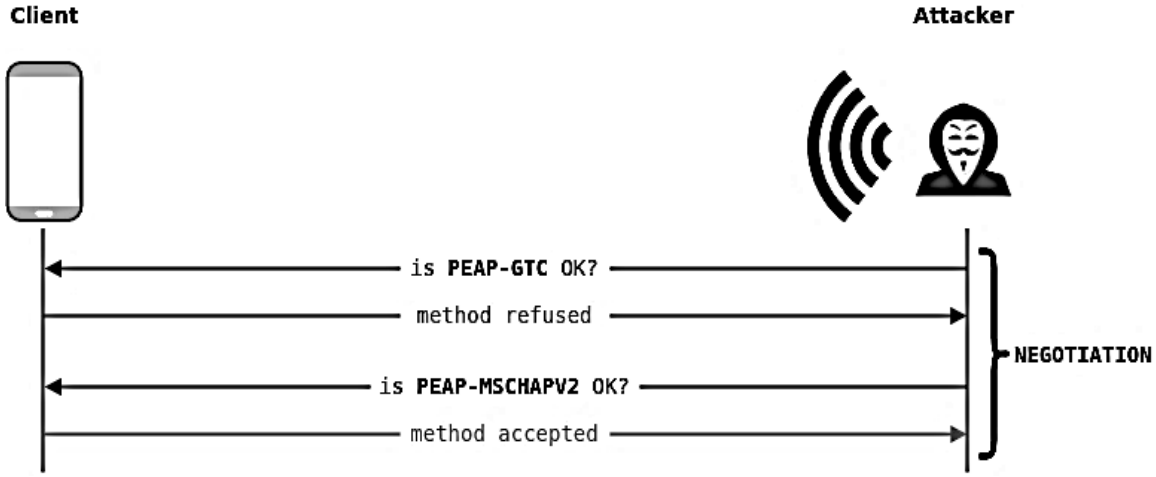

Рис. 6. Схема атаки EAP downgrade.

Лучшим способом защиты от данной атаки – запретить использование сети мобильными устройствами.

Заключение

В случае с рассматриваемым нами типом сетей, порой приходится ставить под угрозу безопасность персональных данных пользователей.

Но разработка защитных механизмов не стоит на месте. Например, актуальным является стандарт WPA3, который смог избавиться от некоторых недоработок предыдущих стандартов.

Для обеспечения безопасности беспроводных сетей следует использовать наиболее свежие, актуальные механизмы шифрования, которые может предоставить вендор оборудования. Помимо этого, очень важной составляющей общей безопасности сетевой инфраструктуры является своевременное обновление используемого программного обеспечения. Важно проводить мониторинг новых уязвимостей с целью предотвращения их влияния на устройства.

В критической инфраструктуре все же стоит отдать предпочтение классическим проводным сетям. Всегда есть вероятность наличия в оборудовании уязвимостей нулевого дня, которые могут быть найдены злоумышленником, поэтому стоит отказаться от использования таких сетей.

Немаловажным аспектом для обеспечения безопасности беспроводных сетей является выбор вендора для сетевого оборудования, а также поддержка с его стороны имеющейся техники. Как уже было сказано ранее, обновления безопасности очень важны, так как без них повышается риск компрометации сети, что может поставить под угрозу конфиденциальность данных.

Список литературы

1. Аудит WPA2-Enterprise с помощью атаки Evil Twin. – URL: https://codeby.net/threads/audit-wpa-2-enterprise-s-pomoschju-ataki-evil-twin.59920/ (дата обращения: 10.02.2023).

2. LIFARS Wi-Fi Network Penetration Testing with a Synopsis of Ontology to Enhance the Security (дата обращения: 3.03.2023).

3. Wi-Fi Protected Setup. – URL: https://ru.wikipedia.org/wiki/Wi-Fi_Protected_Setup#%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_WPS (дата обращения: 15.02.2023).

4. Безопасность в сетях Wi-Fi. Часть 2 - WPS. – URL: https://interface31.ru/tech_it/2014/07/bezopasnost-v-setyah-wi-fi-chast-2-wps.html (дата обращения: 23.02.2023).

5. WPS Pixie Dust Attack — Взлом Wi-Fi сети за 5 минут. Описание уязвимости. – URL: https://habr.com/ru/articles/280796/ (дата обращения: 1.03.2023).

6. Dominique Bongard «Online bruteforce attack on WiFi Protected Setup» Hack.lu 2014 CTF (дата обращения: 2.03.2023).

7. Методы аутентификации клиентов беспроводных сетей. – URL: https://wiki.merionet.ru/seti/34/metody-autentifikacii-klientov-besprovodnyx-setej/ (дата обращения: 3.03.2023).

8. How does WPA/WPA2 WiFi security work, and how to crack it? – URL: https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it?accept-cookies=1 (дата обращения: 17.03.2023).

9. Атака PMKID на беспроводные точки доступа. – URL: https://codeby.net/threads/ataka-pmkid-na-besprovodnye-tochki-dostupa.79384/ (дата обращения: 17.03.2023).

10. Wireless Penetration Testing https://reconshell.com/wireless-penetration-testing (дата обращения: 23.03.2023).

11. rfc5247 Extensible Authentication Protocol (EAP) Key Management Framework.

12. EAP Downgrade Attacks. – URL: https://web.archive.org/web/20220517091227/https://solstice.sh/2019/09/10/eap-downgrade-attacks/ (дата обращения: 24.03.2023).

Тамбовский государственный технический университет
Tambov State Technical University

МИРЭА – Российский технологический университет
MIREA – Russian Technological University

Поступила в редакцию 15.11.2023

Информация об авторах

Громов Юрий Юрьевич – д-р техн. наук, профессор, Тамбовский государственный технический университет, e-mail: gromovtambov@yandex.ru.

Карасев Павел Игоревич – канд. техн. наук, МИРЭА – Российский технологический университет, e-mail: karasev@mirea.ru.

Елисеев Алексей Игоревич – канд. техн. наук, Тамбовский государственный технический университет, e-mail: alekseyeliseev@ya.ru.

Кибец Николай Сергеевич – студент, МИРЭА – Российский технологический университет, e-mail: kibets.n.s@edu.mirea.ru.

METHODS FOR PROTECTING INFORMATION SYSTEMS BASED ON WIRELESS NETWORKS

Yu.Yu. Gromov, P.I. Karasev, A.I. Eliseev, N.S. Kibets

The paper discusses the main methods of protection against attacks on information systems using wireless Wi-Fi networks. When describing each of them, the reasons for the occurrence of

vulnerabilities, which entailed the possibility of compromising the information system network by an attacker, were analyzed, and possible ways to correct them were also given. The vulnerabilities of such types of networks as WPA2 Personal and WPA2 Enterprise were considered, but greater emphasis was placed on the first type, since such networks are more ubiquitous and can be found everywhere. First of all, information about these security flaws is presented for your information, because in order to understand how to secure your wireless network, you first need to find out what vulnerabilities exist and how you can protect yourself from them. In addition, the article examined the role of a wireless network in the general local network security model.

Keywords: Wi-Fi, Traffic interception, IBM, SSID, WPA-2, WEP, Handshake, PNL, WPA/WPA2-Personal (PSK), WPA/WPA2-Corporate (MGT), Man-in-the-Middle, WPS, Brute force, WPS Pixie Dust, PSK, MAC Address.

Submitted 15.11.2023

Information about the authors

Yurii Yu. Gromov – Dr. Sc. (Technical), professor, Tambov State Technical University, e-mail: gromovtambov@yandex.ru.

Pavel I. Karasev – Cand. Sc. (Technical), MIREA – Russian Technological University, e-mail: karasev@mirea.ru.

Aleksey I. Eliseev – Cand. Sc. (Technical), Tambov State Technical University, e-mail: alekseyeliseev@ya.ru.

Nikolay S. Kibets – student, MIREA – Russian Technological University, e-mail: kibets.n.s@edu.mirea.ru.