WPA3 – Крупнейшее обновление безопасности Wi-Fi за последние 14 лет

В 2017 году в протоколе WPA2 была обнаружена серьезная уязвимость, получившая название KRACK (Key Reinstallation Attack) – атака с переустановкой ключа. Этот факт, наряду со всеми ранее известными недостатками WPA2, подтолкнул Wi-Fi Alliance к разработке нового стандарта безопасности - WPA3.

Wi-Fi уже давно стал неотъемлемой частью жизни миллионов людей, а с появлением IoT число беспроводных устройств во всем мире постоянно растет, поэтому вопросы защиты Wi-Fi сетей не теряют своей актуальности. Предыдущая версия протокола WPA2 была введена в 2004 году и за последние несколько лет неоднократно была дискредитирована. По этой причине в июле 2018 года Wi-Fi Alliance объявил о начале сертификации устройств, поддерживающих WPA3 (Wi-Fi Protected Access 3) - самого большого обновления безопасности за последние 14 лет.

Новый механизм аутентификации - SAE (Simultaneous Authentication of Equals)

В WPA2 всегда острой проблемой оставалось использование слабых паролей. Если пользователи ставят легкий пароль на беспроводную сеть, то его без труда можно было подобрать с помощью автоматизированных атак с использованием словарей, таких как Dictionary и Brute-Force. Протокол WPA2 никогда не предлагал вариантов для решения этой проблемы. От разработчиков были лишь рекомендации использовать сложные и более надежные пароли. В WPA3 будут приняты меры, позволяющие противодействовать таким атакам.

Для этого в WPA3 был реализован новый механизм аутентификации SAE (Simultaneous Authentication of Equals), который заменяет используемый в WPA2 метод PSK (Pre-Shared Key). Именно в PSK описано четырехступенчатое рукопожатие для установления связи. Этот метод был скомпрометирован KRACK-атакой, которая прерывает серию рукопожатий и пытается повторить запрос на подключение. Неоднократная повторная отправка приветственных сообщений вынуждает участников сети переустановить уже согласованный ключ. Когда жертва переустанавливает ключ, ассоциированные с ним параметры сбрасываются, что нарушает безопасность, которую должен гарантировать WPA2. Таким образом, злоумышленник получает возможность прослушивать трафик и внедрять свои пакеты.

SAE переводится как "одновременная аутентификация равных", и как понятно из названия, согласно этому алгоритму аутентификация устройств производится одновременно и на равных правах. Что это значит?

Разработчики отказались от строгой последовательности действий при авторизации и ушли от того, чтобы считать точку доступа главным устройством в сети при авторизации. Согласно механизму SAE, все устройства в сети (точки доступа и абонентские устройства) работают на равных правах. Поэтому любое устройство может начать отправлять запросы на аутентификацию и в произвольном порядке отправлять информацию по установлению ключей. В результате чего, возможность реализации KRACK-атаки была устранена. С появлением SAE у злоумышленника принципиально не будет возможности прервать процесс аутентификации, "влезая" между точкой доступа и абонентским устройством.

WPA3-Personal и WPA3-Enterprise

В WPA3 по аналогии с WPA2 останется два режима работы: WPA3-Enterprise и WPA3-Personal.

Устройства, использующие WPA3-Personal, получат повышенную защиту от перебора паролей в виде SAE. Даже когда пользователи выбирают пароли, не соответствующие типичным рекомендациям сложности, SAE гарантирует безопасность. Эта технология устойчива к офлайновым брутфорс-атакам, когда взломщик пытается определить сетевой пароль, пытаясь подобрать пароли без сетевого взаимодействия (офлайн).

Кроме этого WPA3-Personal получит дополнительное усиление безопасности в виде "Forward Secrecy". Это решение позволяет устанавливать новый ключ шифрования при каждом новом соединении. При WPA2 можно прослушивать трафик и сохранять зашифрованные данные долгое время, после чего, получив ключ доступа, полученные ранее данные можно расшифровать. С появлением Forward Secrecy это стало невозможно, так как даже если атакующий рано или поздно получит ключ от сети, то он сможет расшифровать только те данные, которые передавались после генерации последнего ключа.

Достоинства WPA3-Personal:

- Пользователи могут выбирать пароли, которые легче запомнить, не задумываясь о

безопасности;
- Новые алгоритм SAE обеспечивающий улучшенную защиту за счет изменения алгоритма авторизации;
- Шифрование данные Forward Secrecy, защищает трафик данных, даже если пароль был скомпрометирован;

Корпоративные сети чаще используют Enterprise-протокол безопасности. WPA3-Enterprise также будет улучшен за счет усиления ключа шифрования с 128 бит до 192 битов. Разработчики считают такую длину ключа избыточной для большинства сетей, однако, его будет более чем достаточно для особо ценной информации.

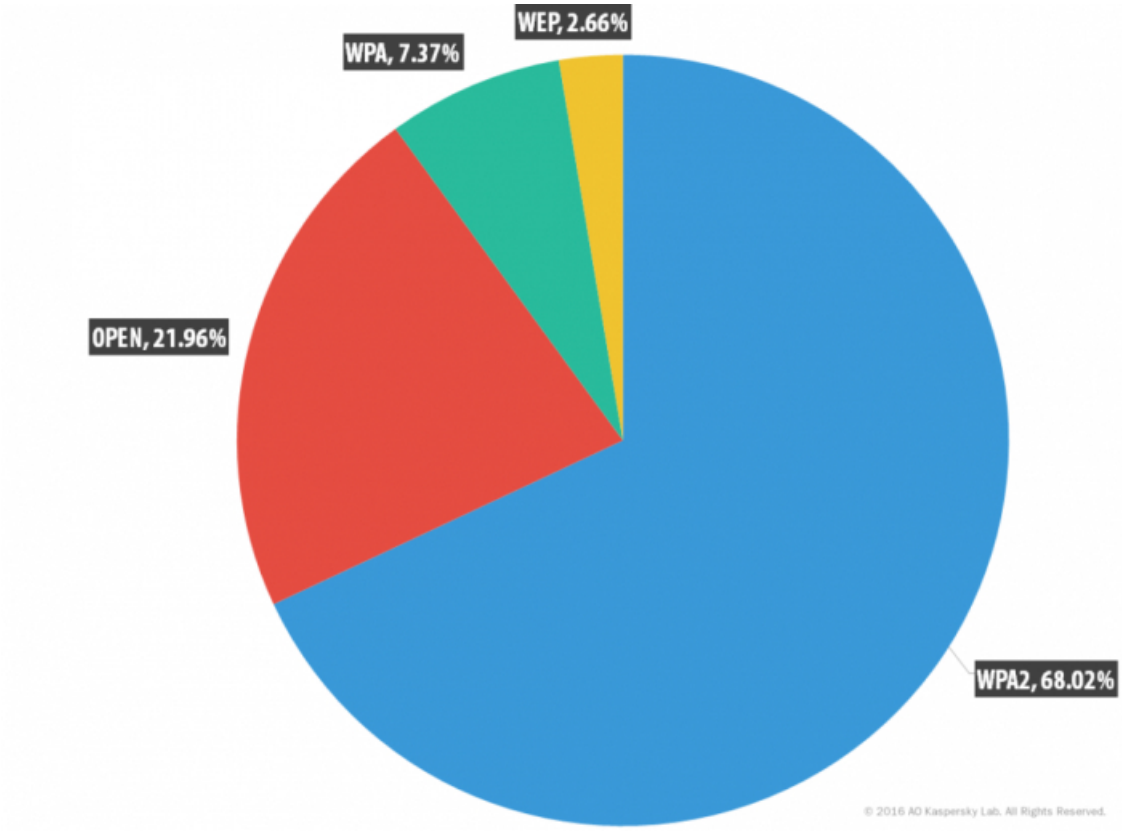
При 192-разрядном шифровании будет использоваться целый ряд сложных криптографических инструментов, протоколов аутентификации и функций формирования ключей:

- 256-bit Galois/Counter Mode Protocol (GCMP-256)
- 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
- 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

При этом WPA3 сохраняет обратную совместимость с устройствами, использующими WPA2.

Открытые Wi-Fi сети станут безопасными благодаря Enhanced Open

Пользователи получают доступ к сетям Wi-Fi повсюду: дома, в офисе, в гостиницах, на остановках и в торговых центрах. Доступ к незащищенным сетям в этих местах представляет собой риск того, что кто-то может перехватить персональные данные. Согласно статистики лаборатории Касперского, проанализировавшей 32 миллиона точек доступа Wi-Fi, более 20% устройств используют открытые беспроводные сети:



Стоит ли говорить о том, что следует подключаться только к безопасным и защищенным сетям? Всегда существуют ситуации, когда открытая Wi-Fi сеть является единственным возможным вариантом получения доступа к сети Интернет. Не редки случаи, когда в открытой сети среди большого количества устройств оказывается атакующий, прослушивающий трафик в фоновом режиме. Чтобы устранить эти риски, Wi-Fi Alliance разработал решение для открытых сетей, которое получило название Enhanced Open.

Сети Wi-Fi Enhanced Open предоставляют пользователям неавторизованное шифрование данных, что значительно усиливает безопасность. Защита прозрачна для пользователя и основана на

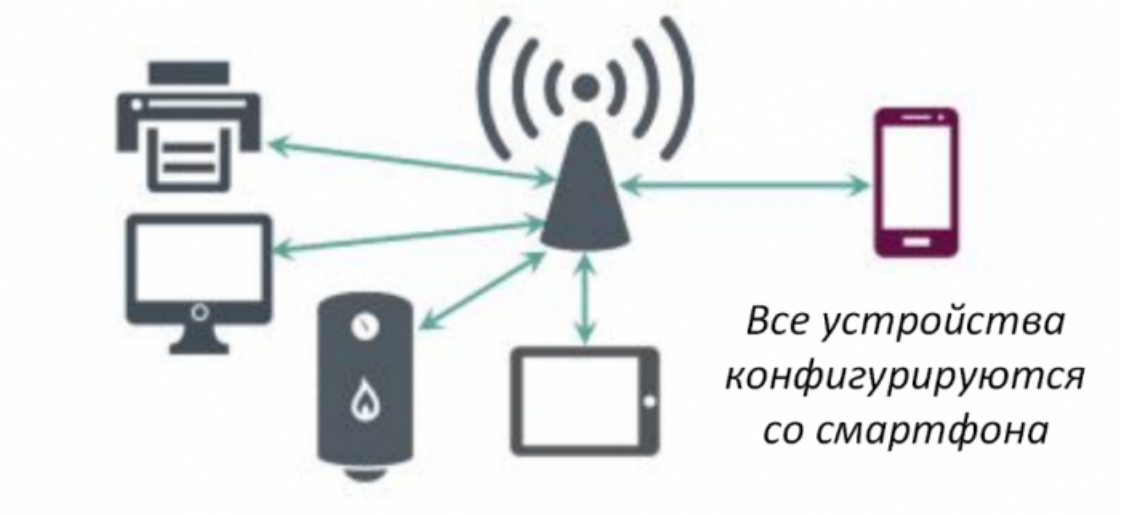
шифровании Opportunistic Wireless Encryption (OWE), определенного в спецификации Internet Engineering Task Force RFC8110 и спецификации беспроводного шифрования Wi-Fi Alliance, Opportunistic Wireless Encryption Specification, которые были разработаны для защиты от пассивного прослушивания. Таким образом, даже просто подключившись к открытой сети с защитой WPA3 весь трафик по умолчанию будет шифроваться.

Конец эпохи "забывания паролей". Разработан простой способ авторизации в сети Wi-Fi - Easy Connect

Wi-Fi Alliance разработал простой способ аутентификации Wi-Fi Easy Connect. Изначально он сделан для малопроизводительных IoT-устройств, но скорее всего этот способ авторизации понравится и простым пользователям. Подключить устройство к беспроводной сети можно будет путем сканирования его QR-кода.

Wi-Fi Easy Connect позволяет пользователям безопасно добавлять новое устройство в существующую Wi-Fi сеть, используя терминал с более надежным интерфейсом, например смартфон или планшет. По сути это может быть любое устройство, способное сканировать QR-код и запускать протокол Device Provisioning Protocol (DPP) разработанный Wi-Fi Alliance.

Выбранное устройство считается конфигуратором, а все остальные устройства являются дочерними для него и используют конфигуратор для подключения к сети:



Пользователь устанавливает безопасное соединение с дочерним устройством, сканируя его QR-код. Это запускает протокол DPP и автоматически предоставляет ключи, необходимые для доступа к сети.

Easy Connect обеспечивает простоту и гибкость сетей Wi-Fi:

- Не нужно запоминать и вводить пароли при подключении новых устройств;
- Упрощает настройку и подключение устройств с помощью QR-кода;
- Позволяет подключать к Wi-Fi сети устройства с отсутствующим пользовательским интерфейсом (датчики умных домов и элементы IoT);
- Easy Connect не связан с WPA3 поэтому его смогут использовать устройства, поддерживающие как WPA2 так и WPA3;
- Позволяет заменять точку доступа без необходимости повторной регистрации всех устройств;