МЕТОДЫ ОГРАНИЧЕНИЯ ДОСТУПА В БЕСПРОВОДНЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Катковский М. М.

Шпак И. И. – канд. техн. наук, доцент

Рассматриваются средства ограничения доступа для противодействия кибератакам в беспроводных сетях. Особое внимание предлагается уделить обновлённым программам сертификации устройств беспроводной связи WPA и WPA2 (Wi-Fi Protected Access). Даются рекомендации по выбору оптимального с различных точек зрения способа использования технологии WPA2 применительно к конкретной сети.

Для противодействия кибератакам в [1, 2] предлагается использовать разрабатываемую (ещё незаконченную) программно-техническую систему мониторинга корпоративной сети, позволяющую производить её аудит (своевременно обнаруживать кибератаки и другие несанкционированные вторжения в сеть) в реальном масштабе времени.

Поскольку разработка предлагаемой в [1, 2] системы мониторинга ещё не завершена, в настоящем докладе сделана попытка временно использовать для противодействия кибератакам в беспроводных коммуникациях средства, описанные в [2]. К ним относятся средства ограничения доступа (фильтрация MAC-адресов, использование режима скрытого идентификатора SSID [2], методы аутентификации (Open Authentication и Shared Key Authentication), шифрования (WEP, TKIP-, CKIP), WPA и WPA-2) [2]. При этом особое внимание в докладе предлагается уделить обновлённым программам сертификации устройств беспроводной связи WPA и WPA2 (Wi-Fi Protected Access). Технология WPA пришла на замену технологии защиты беспроводной Wi-Fi сети WEP. Плюсами WPA являются усиленная безопасность данных и ужесточённый контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств как на аппаратном уровне, так и на программном. На данный момент WPA и WPA2 разрабатываются и продвигаются организацией Wi-Fi Alliance.

Основные понятия. В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации). Стоит заметить, что в WPA2 поддерживается шифрование в соответствии со стандартом AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования), который имеет ряд преимуществ над используемым в WEP RC4, например, гораздо более стойкии криптоалгоритмом. Большим плюсом при внедрении EWPA является возможность работы технологии на существующем аппаратном обеспечении Wi-Fi. Некоторые отличительные особенности WPA: 1) усовершенствованная схема шифрования RC4; 2) обязательная аутентификация с использованием EAP; 3) система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.

Аутентификация пользователей. Wi-Fi Alliance даёт следующую формулу для определения сути WPA:

WPA = 802.1X + EAP + TKIP + MIC

Видно, что WPA, по сути, является суммой нескольких технологий. Как упомянуто выше, в стандарте WPA используется расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (иначе называют мандатом), подтверждающего его право на доступ в сеть. Для этого права пользователь проходит проверку по специальной базе зарегистрированных пользователей. Без аутентификации работа в сети для пользователя будет запрещена. База зарегистрированных пользователей и система проверки в больших сетях, как правило, расположены на специальном сервере (чаще всего RADIUS).

Следует отметить, что WPA имеет упрощённый режим. Он получил название Pre-Shared Key (WPA-PSK). При применении режима PSK необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты, клиентские адаптеры). Если пароли совпадают с записями в базе, пользователь получит разрешение на доступ в сеть.

WPA2 определяется стандартом IEEE 802.11i, принятым в июне 2004 года, и призванным заменить WPA. В нём реализовано CCMP и шифрование AES, за счет чего WPA2 стал более защищённым, чем свой предшественник. С 13 марта 2006 года поддержка WPA2 является обязательным условием для всех сертифицированных Wi-Fi устройств.

В докладе даются рекомендации по выбору оптимального с различных точек зрения способа использования технологии WPA2 применительно к конкретной сети.

Список использованных источников:

1. Катковский П.Ю., Пачинин В.И., Сечко Г.В., Шпак И.И. Методы ограничения доступа в hot-spot сетях // Современные средства связи: материалы XVII Междунар. науч.-техн. конф., 16–18 сент. 2012 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2012. – 332 с. – С. 198.

2. Катковский П.Ю., Шпак И.И. Противодействие кибератакам в беспроводных коммуникациях // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 228-229.