Сравнительный анализ основных протоколов безопасности, используемых в сетях IEEE 802.1x корпоративного сегмента

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

Рагула О.В.

Киринович И.Ф. – доцент, к.ф-м.н

Целью работы является анализ основных протоколов безопасности беспроводных сетевых соединений, применяемых в сетях корпоративного сегмента.

Одним из условий передачи данных в сетях корпоративного сегмента является совпадение применяющегося алгоритма шифрования с корректно установленным шифрованным соединением. Можно назвать следующие алгоритмы шифрования:

CKIP – проприетарная замена WEP от Cisco, ранний вариант TKIP;

TKIP – улучшенная замена WEP с дополнительными проверками и защитой;

AES/CCMP – наиболее совершенный алгоритм, основанный на AES256 с дополнительными проверками и защитой.

WPA и WPA2 (Wi-Fi Protected Access) – представляет собой обновлённые протоколы безопасности и программу сертификации устройств беспроводной связи. Плюсами WPA являются усиленная безопасность данных и более жесткий контроль доступа к беспроводным сетям. Немаловажной характеристикой является также совместимость между множеством беспроводных устройств, как на аппаратном уровне, так и на программном. Сравнительную характеристику протоколов безопасности можно представить в таблице в следующем виде.

Таблица – Сравнение основных протоколов безопасности в сетях IEEE 802.1x

Свойство	WPA (Enterprise)	WPA 2 (Enterprise)
Идентификация	Пользователь, компьютер	Пользователь, компьютер
Авторизация	EAP или общий ключ	EAP или общий ключ
Целостность	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code – CCM) Part of AES
Шифрование	Попакетный ключ через TKIP	CCMP (AES)
Распределение ключей	Производное от PMK	Производное от PMK
Вектор инициализации	Расширенный вектор, 65 бит	48-бит номер пакета (PN)
Алгоритм	RC4	AES
Длина ключа, бит	128	до 256
Требуемая инфраструктура	RADIUS	RADIUS

Основные технические отличия WPA от WPA2 состоят в технологии шифрования и в используемых протоколах шифрования. В WPA используется протокол TKIP, в WPA2 – протокол AES. На практике это значит, что чем современнее алгоритм шифрования, тем обеспечивается более высокая степень защиты беспроводной сети. Например, протокол TKIP позволяет создавать ключ аутентификации размером до 128 бит, AES – до 256 бит. И в отличие от TKIP, в CCMP управление ключами и целостностью сообщений осуществляется одним компонентом, построенным вокруг AES с использованием 128-битного ключа, 128-битного блока, в соответствии со стандартом шифрования FIPS-197.

Список использованных источников:
1. https://technet.microsoft.com/ru-ru/network/bb545365.aspx
2. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
3. http://standards.ieee.org/getieee802/download/802.11-2012.pdf
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: ДМК Пресс, 2012. — 592 с