МЕТОДЫ ЗАЩИТЫ Wi-Fi СЕТЕЙ

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

Королев А.И – к.т.н.,доцент

С момента ратификации стандарта IEEE 802.11 беспроводные сети получили широкое распространение в производственных, общественных местах, а также жилых помещениях. Удобство и легкость реализации данной технологии также дает возможность и злоумышленникам с такой же легкостью осуществить сетевую атаку. Сети стандарта IEEE 802.11 подвержены угрозам нарушения конфиденциальности, целостности, доступности, а также ряду специфических угроз, причиной которых может быть нефиксированная природа связи и открытость среды передачи данных, а также уязвимости системы аутентификации, криптографических протоколов, программного обеспечения и уязвимости, обусловленные человеческим фактором.

Рассмотрим беспроводные сети стандарта IEEE 802.11 как объект угроз информационной безопасности и проведем их классификацию по конфигурации используемых средств защиты.

На сегодняшний день существуют следующие классы беспроводных сетей:

1) Открытые беспроводные сети.

2) Беспроводные сети, использующие базовую аутентификацию.

3) Беспроводные сети с WEP-шифрованием.

4) Беспроводные сети, применяющие протокол TKIP (WPA) и аутентификацию с использованием общих PSK-ключей.

5) Беспроводные сети, применяющие протокол TKIP (WPA) и аутентификацию по протоколам IEEE 802.1x и EAP.

6) Беспроводные сети, применяющие улучшенный алгоритм шифрования AES и аутентификацию с использованием общих PSK-ключей.

7) Беспроводные сети, применяющие улучшенный алгоритм шифрования AES и аутентификацию по протоколам IEEE 802.1x и EAP.

8) Беспроводные сети, использующие виртуальные частные сети как механизм защиты.

Для беспроводных сетей стандарта 802.11 все средства и методы защиты можно условно разделить на следующие три типа:

– средства и методы аутентификации;

– средства криптографической защиты передаваемых данных;

– дополнительные средства защиты.

Если рассматривать технологии защиты беспроводных сетей стандарта IEEE 802.11 в целом, то можно выделить следующие методы защиты:

– методы ограничения доступа (смена настроек, отключения широковещания ESSID, белые и черные списки ACL на основе MAC-адресов, использование политик безопасности и др.);

– методы шифрования (WEP-шифрование, WPA-шифрование, WPA2-шифрование);

– методы аутентификации (открытая аутентификация, аутентификация с общим ключом, аутентификация по MAC-адресу, аутентификация с общим ключом, аутентификация 802.1x);

– организационные методы защиты (мероприятия по предотвращению нарушений путем информирования сотрудников, мероприятия по обнаружению, мероприятия по восстановлению, объектовые мероприятия защиты при функционировании информационной системы, мероприятия по предотвращению, мероприятия по обнаружению).

К основным средствам и методам аутентификации относятся:

– базовая аутентификация (открытая аутентификация, аутентификация с совместно используемым ключом, аутентификация по MAC-адресу);

– аутентификация с использованием общих PSK-ключей;

– аутентификация по IEEE 802.11 и протоколу EAP (Extensible Authentication Protocol) с использованием RADIUS-сервера.

К основным средствам и методам криптографической защиты относятся:

– шифрование с использованием статических WEP-ключей;

– шифрование с использованием протокола TKIP;

– применение улучшенного алгоритма шифрования (AES).

К дополнительным средствам защиты, не предусмотренным производителями оборудования, можно отнести:

– создание виртуальных частных сетей (VPN);

– применение системы обнаружения атак (IDS).

Данные методы звщиты актуальны на сегодняшний день и используются как в промышленных так и в домашних сетях.

Список использованных источников:

1. Иванов П. Беспроводные сети: час настал.// Журнал сетевых решений LAN, 2002, №4, сс.103–108.
2. Хофф С. Безопасность сетей WLAN не дается даром.// Журнал сетевых решений LAN, 2003, №3, сс.44–49.