ПРИЛОЖЕНИЕ Г

ПЕРЕЧЕНЬ НАУЧНЫХ РАБОТ

АТАКИ НА IEEE 802.11 БЕСПРОВОДНЫЕ СЕТИ

Фролов В.В.
Научный руководитель – д.т.н., доц. Халимов Г.З.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина, 14, каф. БИТ)
E-mail: frolvlad@gmail.com, тел. (057) 338-43-65

В данной работе будет рассмотрена безопасность IEEE 802.11 беспроводных сетей, также известных как Wi-Fi сети. На текущий момент Wi-Fi сети можно разделить на два метода аутентификации: открытая аутентификация и аутентификация с общим ключём. В Wi-Fi сетях с откры0й аутентификацией не применяются никакие алгоритмы шифрования. Для защищённых – существует несколько алгоритмов для обеспечения безопасности: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA, WPA2).

Я начну рассмотрение с алгоритма для обеспечения безопасности Wired Equivalent Privacy (WEP). Данный алгоритм был одобрен Институтом Инженеров Электроники и Радиоэлектроники (IEEE) в 1997 году. Существует две разновидности WEP: WEP-40, WEP-104. В настоящее время данная технология является устаревшей, так как её взлом может быть осуществлён в течение нескольких минут. Тем не менее, данный алгоритм продолжает широко использоваться.

В октябре 2000-го года появилась первая статья, поисывающая проблемы алгоритма WEP и атаки, которые могут быть огранизованы с использованием его уязвимостей. В 2001 году была принята спецификация WEP-104, но она не решила проблемы WEP, так как изменения коснулись только длинны ключа. Слабые места в алгоритме:

- механизмы обмена ключами и проверки целостности данных
- способ аутентификации
- алгоритм шифрования
- малая разрядность ключа и вектора инициализации

Основой для WEP стал поточный шифр RC4, преимуществом которого является возможность использования ключа переменной длинны и высокая скорость работы. Для подсчёта контрольных сумм используется алгоритм CRC32.

На данный момент существуют такие атаки на WEP:

- FMS-атака (Fluhrer, Martin, Shamir) – самая первая атака на сети с WEP-шифрованием, появилась в 2001 году. Основана на анализе передаваемых векторов инициализации. Для проведения атаки нужно как минимум полмиллиона пакетов. После обновления протокола эта атака неуспешна.

- Атака KOREK’A. Для взлома необходимо уже несколько сотен тысяч пакетов.
- PTW-атака (Pyshkin, Tews, Weinmann). В основе лежит прослушивание большого количества ARP-пакетов (Address Resolution Protocol). Достаточно 10.000-100.000 пакетов. Самая эффективная атака на сеть с WEP-шифрованием. Данную атаку можно вычислить по большому количеству ARP-пакетов, которые генерируются в сеть.

WPA и WPA2 (Wi-Fi Protected Access) — представляет собой обновленную программу сертификации устройств беспроводной связи. Технология WPA пришла на замену технологии защиты беспроводных сетей WEP. Плюсами WPA являются усиленная безопасность данных и ужесточенный контроль доступа к беспроводнымсетям. 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.

Но на данный момент WPA и WPA2 также имеют уязвимости, но эти уязвимости не позволяют узнать ключ.

- 6 ноября 2008 года на конференции PacSec был представлен способ, позволяющий взломать ключ TKIP, используемый в WPA, за 12-15 минут. Этот метод позволяет прочитать данные, передаваемые от точки доступа клиентской машине, а также передавать поддельную информацию на клиентскую машину. Данные, передаваемые от клиента к маршрутизатору, пока прочитать не удалось.
- В 2009 году сотрудниками университета Хиросимы и университета Кобе, Тосихиру Оигаси и Масакату Мории был разработан и успешно реализован на практике новый метод атаки, который позволяет взломать любое WPA соединение без ограничений, причем, в лучшем случае, время взлома составляет 1 минуту.
- 23 июля 2010 года была опубликована информация об уязвимости Hole196 в протоколе WPA2. Используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ.

Необходимо заметить, что соединения WPA, использующие более защищённый стандарт шифрования ключа AES, а также WPA2-соединения, не подвержены этим атакам.

Уже существует набор утилит для обнаружения сетей, перехвата передаваемого через беспроводные сети трафика и реализации известных атак. Этот набор объединён под названием Aircrack-ng. Но для реализации атаки необходимо выполнять рутинные действия, которые можно автоматизировать. Таким образом я реализовал утилиту, которая автоматизирует выполнение известных атак на WEP, а в дальнейшем и WPA алгоритмы.