УДК 004.7

И.И. Пархоменко, кандидат технічних наук, доцент, В.А. Чижова
(Национальный авиационный университет, Украина)

ПРОБЛЕМЫ БЕЗОПАСНОТИ СИСТЕМ БЕСПРОВОДНОГО ДОСТУПА И МЕТОДЫ ИХ ЗАЩИТЫ

Безопасность жизненно важна для беспроводных сетей, так как коммуникационные сигналы при их распространении через радиоэфир доступны для перехвата. Компании и индивидуальные пользователи должны осознавать потенциально существующие проблемы и принимать контрмеры. В этой статье рассмотрены основные проблемы безопасности и способы защиты беспроводных сетей.

Введение. Беспроводные сети открывают новую эру возможностей для передачи данных, недоступных в проводном мире. Быстрота развертывания, простой доступ к информации и возможность масштабирования – все это означает, что могут быть удовлетворены запросы совершенно новых групп пользователей, причем такими способами, которые были недоступны всего несколько лет назад.

Однако все эти преимущества одновременно являются и недостатками беспроводных систем доступа, так как, проблемы возникающие в безопасности беспроводных сетей обусловлены природой беспроводных сигналов.

Целью статьи есть исследование проблем безопасности беспроводных систем доступа, а также демонстрация защиты всех областей сети; минимизации риска вторжения, используя проверенные методы защиты(такие как сетевые экраны, аутентификация, шифрование). *Исследование основных проблем* Основной проблемой беспроводных сетей является то, что они не имеют практически никакой защиты. Дело в том, что беспроводная сеть использует радиосигнал с четко определенным набором характеристик, поэтому любой, желающий уделить достаточное количество времени и усилий отслеживанию этих сигналов, сможет найти способ перехватить и прочитать данные, содержащиеся в них.

Эта проблема — *простота перехвата радиочастотного трафика* – может быть решена путем остановки вещания SSID с точки доступа. Точка доступа (дальше ТД) обычно передает SSID (Service Set ID – набор основных служб), когда позволяет клиенту присоединиться к себе. Поэтому для защиты WLAN необходимо запрограммировать ТД только отвечать клиентам, которые уже знакомы со всеми деталями BSS (Basic Service Set – основной набор услуг). Это означает, что при попытке клиента соединиться с ТД она запрашивает у него информацию о ключе шифрования WEP и SSID, перед тем как предоставить ему доступ.

Эта политика безопасности работает хорошо в беспроводной среде WLAN до тех пор, пока технически грамотный, но незнакомый с проблематикой безопасности пользователь устанавливает «ложную» ТД, поскольку хочет иметь собственную ТД, связанную с WLAN. В таком случае для противодействия неавторизованного доступа, используют взаимную аутентификацию.

Еще одной из важных проблем беспроводных сетей является то, что *все пароли опубликованы, задокументированы и представляют собой значения «по умолчанию» в беспроводном пространстве*, построенном из специального оборудования. Для того чтобы предотвратить несанкционированный доступ, очень важно не оставлять изначальные значения паролей неизменными навсегда. Кроме того, в паролях не следует использовать легко угадываемые имена.

Существует еще проблема безопасности беспроводных сетей, связанная с протоколом ARP, которая состоит в том, что он представляет опасность для системы защиты из-за возможности спуфинга (о*т англ, spoofing — имитация соединения, получение доступа обманным путем*). Так, хакер может ввести в заблуждение станцию, посылая ей через подставное сетевое устройство фиктивный ARP-ответ, содержащий IP-адрес легитимного сетевого уст-

ройства и MAC-адрес подставного. Это приведет к тому, что все легитимные станции сети автоматически обновят свои ARP-таблицы, внеся в них ложные данные. В результате станции будут передавать пакеты подставному устройству, а не легитимной точке доступа или маршрутизатору. Для предотвращения атак с использованием спуфинга ARP поставщики предлагают защищенный ARP (secure ARP, SARP). Этот усовершенствованный ARP обеспечивает специальный защищенный туннель между каждым клиентом и беспроводной точкой доступа или маршрутизатором, который игнорирует все ARP-ответы, не связанные с клиентом, находящимся на другом конце этого туннеля.

Основными же методами защиты информации на механизм доступа беспроводных сетей являются шифрование и аутентификация. Также использование решений RADIUS или VPN для аутентификации и туннелирования хорошо действует в качестве дополнительной защиты.

Одним из широко используемых технологий шифрования для защиты информации есть *стандарт WEP*. Он является опциональным стандартом шифрования и аутентификации, используемый на уровне MAC; его поддерживают радиоплаты интерфейса сети и точки доступа многих производителей. WEP выполняет три функции: предотвращение неавторизованного доступа в сеть, выполняет проверку каждого пакета и защищает данные от недоброжелателей. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. В основе WEP лежит поточный шифр RC4, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Для подсчета контрольных сумм используется CRC32. Все атаки на WEP основаны на недостатках шифра RC4, таких, как возможность коллизий векторов инициализации и изменения кадров. Для всех типов атак требуется проводить перехват и анализ кадров беспроводной сети. В зависимости от типа атаки, количество кадров, требуемое для взлома, различно. С помощью программ, таких как *Aircrack-ng*, взлом беспроводной сети с WEP шифрованием осуществляется очень быстро и не требует специальных навыков. Поэтому в настоящее время это технология считается устаревшей, так как не обеспечивает надлежащую защиту данных.

*Стандарт 802.11i позволяет повысить защищенность беспроводных локальных сете*й. Протокол *TKIP* — это частное решение, основанное на использовании временного 128-разрядного ключа, совместно используемого клиентами и точками доступа. TKIP комбинирует временный ключ с MAC-адресом клиентского устройства, а затем добавляет относительно длинный 16-октетный вектор инициализации для создания ключа, посредством которого будут шифроваться данные. Эта процедура гарантирует, что каждая станция будет использовать различные ключевые потоки для шифрования данных. TKIP использует RC4 для шифрования, что аналогично применению WEP. Основное отличие от WEP состоит в том, что TKIP изменяет временные ключи после передачи каждых 10 тыс. пакетов. Это дает динамический метод распределения, благодаря чему значительно повышается безопасность сети. Преимущество применения TKIP состоит в том, что компании, уже имеющие основанные на механизме WEP точки доступа и радиоплаты интерфейса сети, могут модернизировать их до уровня TKIP с помощью относительно простых, встраиваемых "заплаток". Кроме того, оснащенное только WEP оборудование сможет взаимодействовать с TKIP-устройствами, используя WEP.

*Помимо временного решения TKIP, стандарт 802.11i содержит протокол улучшенного стандарта шифрования (advanced encryption standard, AES), который обеспечивает более надежное шифровани*е. Проблема, связанная с AES, состоит в том, что для его реализации требуется большая вычислительная мощность, чем та, которой обладают большинство точек доступа, предлагаемых сегодня на рынке. Поэтому компаниям для применения AES придется модернизировать аппаратное обеспечение своих беспроводных локальных сетей, чтобы оно поддерживало производительность, необходимую для применения алгоритма AES.

Из-за недостатков со спецификацией WEP-шифрования многие производители беспроводного сетевого оборудования и разработчики программного обеспечения адаптировали стандарт 802.1x. Этот стандарт определяет структуру, которая может поддерживать неско-

лько различных форм аутентификации, включая сертификаты, смарт-карты и однократные пароли, все из которых обеспечивают большую защиту, чем управление доступом, интегрированное в 802.11.

Стандарт на защищенный доступ к Wi-Fi (Wi-Fi protected access, WPA), предложенный Альянсом Wi-Fi, обеспечивает модернизацию WEP за счет одновременного использования метода шифрования с динамическим ключом и взаимной аутентификации. Клиенты WPA используют различные ключи шифрования, которые периодически меняются. Из-за этого взломать алгоритм шифрования намного сложнее. По сути, WPA 1.0 представляет собой текущую версию стандарта 802.11i, который включает механизмы TKIP и 802.1x. За счет комбинации этих двух механизмов обеспечивается шифрование с динамичным ключом и взаимная аутентификация, т.е. то, что необходимо для беспроводных локальных сетей. WPA 2.0 полностью совместим со стандартом 802.11.

Фильтрация MAC – это один из самых простых путей для минимизации угрозы целого ряда атак. В случае применения MAC-фильтрации точка доступа проверяет MAC-адрес источника каждого получаемого ею фрейма и отказывается принимать фреймы с MAC-адресом, не соответствующим ни одному из особого списка, программируемого администратором. Следовательно, MAC-фильтрация обеспечивает простейшую форму аутентификации. Главным недостатком использования фильтрации MAC-адресов заключается в необходимости административного контроля. Процесс фильтрации MAC-адресов должен постоянно записываться и контролироваться для максимальной эффективности. Еще одним недостатком есть то ,что если кто-то прослушивает трафик, он может определить MAC-адреса по их фиксированному месту в передаваемых пакетах информации. Мониторируя процесс работы сети, хакер может попытаться получить доступ в нее, используя те MAC-адреса, которые давно не используются.

Для защиты компьютера в сети от неавторизованного доступа целесообразно использовать также брандмауэр. Брандмауэр является прокси-сервером, фильтрующим данные, проходящие через него в сеть или из нее, в зависимости от набора правил, установленных сетевым администратором.

Выводы. Все средства обеспечения защиты в беспроводных сетях, рассмотренные выше, должны использоваться в комплексе, это позволит максимально защитить сеть от несанкционированного доступа. Но и нельзя забывать, что каждый день становятся известны новые слабые места в протоколах и программах, поэтому нельзя считать свою сеть полностью защищенной.

Список литературы

1. Wi –Fi . Беспроводная сеть. Джон Росс. Издание НТ Пресс, Москва 2007 год, 322 с.
2. Беспроводные сети. Первый шаг. Джим Гейер. Издание «Вильяме», Москва 2005 год,189с.
3. Защита от хакеров беспроводных сетей. Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле, Джеффри Посланс, Дэвид М. Зенджан, Нил О’Фаррел. Издание ДМК-Пресс,Москва 2005 год, 476с.
4. WEP. http://ru.wikipedia.org