

СПОСОБЫ МИНИМИЗАЦИИ РИСКА ВТОРЖЕНИЯ ДЛЯ БЕСПРОВОДНЫХ СЕТЕЙ

Безопасность жизненно важна для беспроводных сетей, так как коммуникационные сигналы при их распространении через радио эфир 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.

Ключевые слова: беспроводные сети, безопасность, стандарт 802.11, WPA, WEP.

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 (далее 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. Такая точка представляет собой неавторизованную точку доступа, включенную в сеть (рис.1). Какой-нибудь служащий может приобрести точку доступа и установить ее в своем офисе, не понимая, каковы последствия этого для безопасности сети. Хакер также может разместить точку доступа в здании, умышленно подключив незащищенную точку доступа к корпоративной сети.

В подставной точке доступа, как правило, не активизируется система шифрования, и она будет представлять собой открытую дверь для любого, кто захочет получить доступ к корпоративной сети, находясь вне здания. Эта проблема актуальна не зависимо от того, установлена беспроводная сеть или нет. Кто-то может подключить подставную точку доступа и к полностью проводной сети Ethernet.



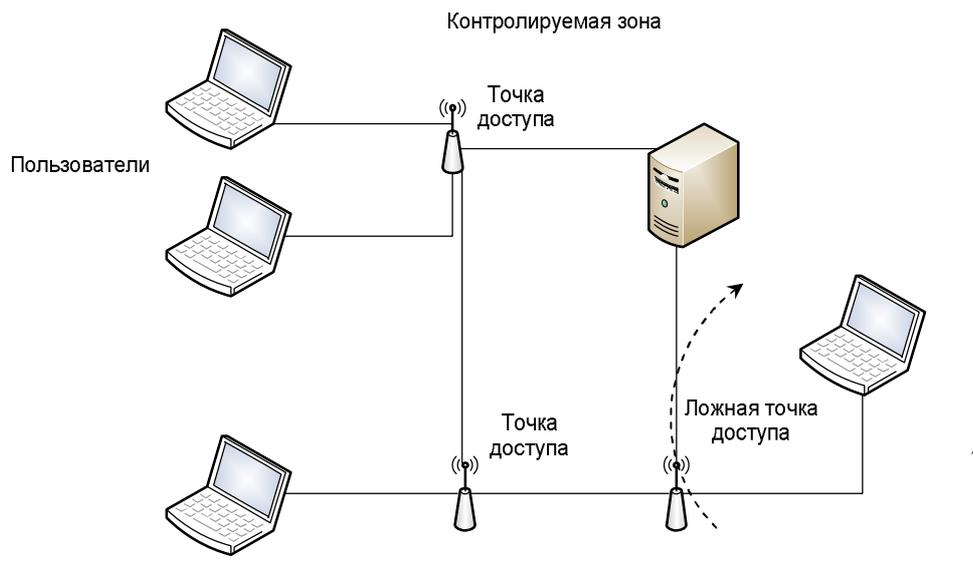


Рис.1. Неавторизованная точка доступа, включенная в сеть

Для противодействия неавторизованному доступу в беспроводной сети используется взаимная аутентификация, осуществляемая между клиентскими устройствами и точками доступа. Аутентификация — это подтверждение идентичности пользователя или устройства. В беспроводной сети должны применяться методы, позволяющие базовой станции удостовериться в идентичности клиента, и наоборот. Это позволяет удостовериться в "законности" пользователя и в том, что он устанавливает соединение с легитимной точкой доступа. Кроме того, точки доступа должны проходить процедуру аутентификации на коммутаторах, что исключает появление в сети подставных точек доступа.

В подставной точке доступа, как правило, не активизируется система шифрования, и она будет представлять собой открытую дверь для любого, кто захочет получить доступ к корпоративной сети, находясь вне здания. Эта проблема актуальна не зависимо от того, установлена беспроводная сеть или нет. Кто-то может подключить подставную точку доступа и к полностью проводной сети Ethernet.

Для противодействия неавторизованному доступу в беспроводной сети используется взаимная аутентификация, осуществляемая между клиентскими устройствами и точками доступа. Аутентификация — это подтверждение идентичности пользователя или устройства. В беспроводной сети должны применяться методы, позволяющие базовой станции удостовериться в идентичности клиента, и наоборот. Это позволяет удостовериться в "законности" пользователя и в том, что он устанавливает соединение с легитимной точкой доступа. Кроме того, точки доступа должны проходить процедуру аутентификации на коммутаторах, что исключает появление в сети подставных точек доступа.

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 (*от 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 устройства и MAC-адрес подставного. Это приведет к тому, что все легитимные станции сети автоматически обновят свои ARP-таблицы, внося 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.

Среди серьезных угроз со стороны профессиональных взломщиков является атака типа "отказ в обслуживании" (denial of service, DoS) — это нападение, в результате которого беспроводная сеть приходит в негодность или ее работа блокируется. Одной из разновидностей DoS-атак является метод грубой силы (brute-force attack). Массовая рассылка пакетов, для которой задействуются все ресурсы сети, в результате чего она прекращает работу — это вариант DoS-атаки, выполненной методом грубой силы. В Internet можно найти программные средства, позволяющие хакерам вызывать интенсивную передачу пакетов в беспроводных сетях. Хакер может провести DoS-атаку методом грубой силы путем отправки бесполезных пакетов серверу с других компьютеров сети. Это вызывает существенные непроизводительные расходы в сети и не позволяет использовать ее пропускную способность легитимным пользователям.

Другим способом приостановки работы большинства беспроводных сетей, особенно тех, в которых используется метод обнаружения несущей (carrier sense access) является использование мощного радиосигнала, заглушающего все остальные и делающего таким образом точки доступа и радиоплаты бесполезными. Протоколы, такие как 802.11b, позволяют сигналу DoS-атаки иметь доступ к среде передачи столь долго, сколько захочется хакеру.

Однако попытка проведения атаки на сеть с использованием мощного радиосигнала может оказаться весьма рискованной для хакера. Поскольку для проведения такой атаки мощный передатчик должен располагаться в непосредственной близости от помещения, в котором развернута беспроводная сеть, ее владелец может обнаружить хакера, используя средства обнаружения, входящие в состав сетевых анализаторов. После того как источник преднамеренных помех будет найден, его владельцу придется прекратить атаку и даже, возможно, сесть на скамью подсудимых.

Иногда отказ в обслуживании беспроводной сетью возникает вследствие непреднамеренных действий. Так, сети стандарта 802.11b работают в переполненном спектре частот, а такие устройства, как беспроводные телефоны, микроволновые печи и устройства Bluetooth, могут вызвать существенное снижение производительности сетей этого стандарта. Помехи же могут вообще воспрепятствовать работе сети. Кроме того, превосходной целью для DoS-атак могут служить некоторые механизмы защиты сети. Например, механизм защищенного доступа к Wi-Fi (Wi-Fi protected access, WPA) уязвим для атак типа "отказ в обслуживании". WPA использует математический алгоритм для аутентификацию пользователей сети. Если какой-то пользователь попытается получить к ней доступ и пошлет два пакета неавторизованных данных в течение одной секунды, WPA сочтет, что стал объектом атаки, и прекратит работу сети.

Наиболее эффективный способ противодействия атакам типа "отказ в обслуживании" — это изоляция компьютера в тщательно охраняемой комнате и отключение его от всех сетей, включая Internet. Но это невозможно в отношении беспроводных сетей.

Наиболее действенной защитой от DOS-атак является разработка и соблюдение строгих правил безопасности. Такие действия, как установка и обновление брандмауэров, постоянно обновляемые антивирусные средства, установка свежих "заплат", ликвидирующих бреши в системе безопасности, использование длинных паролей и отключение неиспользуемых сетевых устройств должны стать повседневной практикой для всех компаний и домовладельцев.

Можно защитить беспроводную сеть от атак типа "отказ в обслуживании", обеспечив сопротивляемость зданий проникновению в них радиосигналов извне.

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 сетей. 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 шифрование. 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 несколько 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 к ней, 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 все данные, проходящие через него в сеть или из нее, в зависимости от набора правил, установленных сетевым администратором. Например, брандмауэр может отсеивать данные от неизвестного источника или файлы, связанные с определенным источником (вирусы). Или он может пропускать все данные, передающиеся из локальной сети в Интернет, но пропускать только конкретные их типы из Интернета. Наиболее общим использованием брандмауэра сети является шлюз в Интернет, как показано на рис.2. Брандмауэр отслеживает все входящие и исходящие данные между локальной сетью на одной стороне и Интернетом на другой. Такой тип брандмауэра предназначен для защиты компьютеров в сети от неавторизованного доступа из Интернета.

В беспроводной сети брандмауэр может быть также расположен на шлюзе между беспроводными точками доступа и проводной сетью. Такой брандмауэр изолирует беспроводную часть сети от проводной сети, поэтому недоброжелатели, подключившие свои компьютеры к сети без разрешения, не могут использовать беспроводное подключение для выхода в Интернет или проводную часть сети. На рис. 3 показано местоположение брандмауэра в беспроводной сети.



Рис.2. Шлюз в Интернет

Самым простым вариантом использования брандмауэра для беспроводной сети является использование встроенного в точку доступа. Некоторые сочетают функции беспроводной точки доступа с широкополосным маршрутизатором и свитчем Ethernet, поэтому поддерживают как проводных, так и беспроводных сетевых клиентов.

Изолируя подключение между сетевыми узлами от другого сетевого трафика, VPN может добавлять еще один уровень защиты. VPN является кодированным каналом передачи, который соединяет две сетевые конечные точки через «туннель данных». VPN пересылает данные через одну или более промежуточную сеть к точке назначения в другой сети. Туннельный клиент VPN инкапсулирует имеющиеся пакеты данных или фреймы путем добавления нового заголовка с трассировочной информацией, которая инструктирует их о способе достижения конечной точки VPN. Путь прохождения через промежуточные сети называется туннелем. В конечной точке туннеля VPN-сервер удаляет туннельный заголовок и отправляет данные к точке назначения, определяемой полями заголовков. Точная форма туннеля не оказывает никакого влияния на данные, так как данные воспринимают туннель как соединение точка-точка. Многие эксперты по сетевой защите рекомендуют VPN как эффективный способ защиты беспроводной сети от недоброжелателей и неавторизованных пользователей.

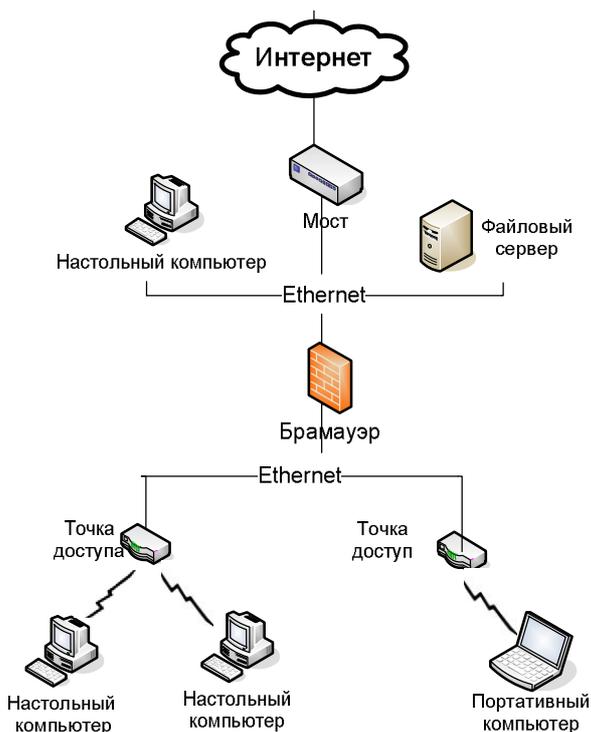


Рис.3. Местоположение брандмауэра в беспроводной сети

Вывод. 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.

ЛИТЕРАТУРА

1. Росс Дж. Wi-Fi. Беспроводная сеть / Джон Росс - М.: НТ Пресс. – 2007. – 322 с.
2. Гейер Дж. Беспроводные сети. Первый шаг / Джим Гейер. – М.: «Вильяме». – 2005. – 189с.
3. Барнс К. Защита от хакеров беспроводных сетей / Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле и др. – М.: ДМК-Пресс. – 2005. – 476с.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Юдін О.К.