Безопасность беспроводных LAN

Сергей ГОРДЕЙЧИК
Ведущий специалист
Учебного центра «Информзащита»
MCSE, MCT, CISSP
gordey@itsecurity.ru

Вопросы безопасности являются немаловажным аспектом в проектировании и внедрении локальных беспроводных сетей (Wireless Local Area Network, WLAN). Особенности реализации, связанные с использованием общей среды передачи, выходящей за контролируемый физический периметр, требует использования специфического подхода при обеспечении безопасности WLAN. В данной статье рассматриваются основные угрозы и методы защиты, характерные для беспроводных сетей.

Несанкционированное подключение

В отличие от проводной сети, для подключения к WLAN не требуется получать физический доступ к активному сетевому оборудованию, но достаточно находясь в пределах радиодоступности установить логическую связь (ассоциацию) с точкой доступа.

Как правило, радиосеть далеко выходит за пределы физического периметра, и даже если сеть построена с учетом требований минимизации уровня сигнала, использование мощных беспроводных карточек и направленных антенн позволяет злоумышленнику взаимодействовать с точкой доступа на значительном расстоянии.

Прослушивание трафика

Многие беспроводные карточки поддерживают возможность работы в режиме мониторинга. Этот режим, немного схожий с неселективным режимом адаптеров IEEE 802.3, дает возможность сохранять трафик беспроводной сети даже без установления с ней логической связи. В конкретный момент времени карточка имеет возможность прослушивать только один из каналов, однако большинство сетевых анализаторов беспроводных сетей поддерживают возможность автоматизированного переключения между каналами (channel hoping) для сбора пакетов на всех возможных каналах.

После обнаружения интересующей его беспроводной сети злоумышленник может сконцентрировать внимание на нужном канале и собирать весь трафик этой сети. Как и в случае с несанкционированным подключением, злоумышленник имеет возможность анализировать пакеты, находясь на значительном удалении от точки доступа.

Существует множество разнообразных сетевых анализаторов для WLAN. В качестве примера можно привести программы AirMagnet Laptop, Wildpackets Aeropeak и CommView for WiFi для операционной системы Windows и Ethereal, Kismet для Linux.

Для работы сетевого анализатора необходимо установить в систему специальные драйверы сетевой карты, поддерживающие работу в режиме мониторинга (HostAP, AirJack, Madwifi, IPW2200 для Linux). Драйверы для Windows, как правило, входят в поставку сетевого анализатора.

Уязвимость к отказу в обслуживании

Специфика беспроводной сети делает ее весьма уязвимой для атак, направленных на отказ в обслуживании. На качестве связи могут сказаться погодные условия, незначительное изменение расположения антенны, использование беспроводной сети в соседнем здании либо офисах и т.д. Что касается антропогенных атак, то их можно разделить на три большие группы: использование уязвимостей физического, канального и вышестоящих уровней модели OSI. Подробнее данные типы атак планируется рассмотреть в следующих статьях.

Как показывает практика, превентивных методов защиты от атак, направленных на отказ в обслуживании, не существует. Эту особенность беспроводной сети надо учитывать при планировании и не использовать Wi-Fi для передачи трафика с высокими требованиями к доступности.

Мобильность клиентов

Многие клиенты беспроводных сетей мобильны в буквальном смысле этого слова, т.е. часто изменяют свое месторасположение. Это приводит к тому, что они часто работают с беспроводными сетями, отличными от сети компании. При этом часто не соблюдаются элементарные требования безопасности, и передача ценных данных (зачастую это пароли пользователей, совпадающие с теми, которые используются в сети компании) происходит по незащищенным каналам связи, или хуже того — по каналам, контролируемым злоумышленником.

Для того, чтобы осознать проблемы безопасности клиентов беспроводных сетей, можно представить их в качестве клиентов VPN, получающих доступ к корпоративной сети через агрессивную среду Интернета, в то время, как потенциальные нарушители находятся в одном с ними локальном сегменте. Сейчас мало кто позволит незащищенному клиенту использовать VPN, однако, применение беспроводных сетей без должной защиты клиентов — вполне распространенная практика.

Во время прошлогодней выставки-конференции Infosecurity Moscow 2005 Учебный центр «Информзащита» совместно с компанией Positive Technologies провел эксперимент, позволивший оценить, насколько специалисты в области безопасности серьезно относятся к беспроводным сетям.

С этой целью была развернута беспроводная сеть-приманка (honeynet), позволявшая после

некоторых усилий получить доступ к Internet. Каково же было удивление исследователей, когда оказалось, что многие из участников Infosecurity не только не прочь использовать чужую беспроводную сеть, но получают с ее помощью корпоративную почту. При этом многие из них, как потом выяснилось при личной беседе, не представляют, что их трафик может анализировать не только владелец ресурса, но и любой находящийся рядом приемник.

Бесконтрольность беспроводных сетей

Зачастую владелец сети и ее администраторы даже не подозревают, что на предприятии развернута беспроводная сеть. Дешевизна беспроводных устройств, их распространенность и простота использования делает Wi-Fi серьезным каналом утечки корпоративной информации.

Сотрудник может подключить к локальной сети беспроводную точку доступа или настроить на своем ноутбуке сетевой мост между беспроводным адаптером и локальной сетью. Он может забыть отключить беспроводной адаптер после работы с домашней сетью и т. п. Все это дает ему, а не исключено, что и внешнему злоумышленнику, возможность получения доступа к корпоративным данным.

Однажды, в ходе выездного обучения, проводились практические работы по курсу "Безопасность беспроводных сетей" и слушатели обнаружили "несанкционированную" точку доступа. При анализе трафика было обнаружено, что эта точка доступа не только позволяет неаутентифицированные подключения, но и выдает IP-адреса с корпоративного сервера DHCP. Оказалось, что один из сотрудников компании решил "поэкспериментировать" со своей домашней точкой доступа на работе и подключил AP к сети предприятия. В результате слушатели обнаружили не учебный, а вполне реальный инцидент.

Защита беспроводных сетей

В ходе разработки в беспроводные сети были заложены возможности защиты от несанкционированного подключения и прослушивания. Первым из предложенных стандартов защиты был WEP (Wired Equivalent Privacy), использующий криптографический алгоритм RC4 со статическим распределением ключей шифрования для аутентификации подключающихся клиентов и шифрования передаваемого трафика. Однако в 2001 г. были публично продемонстрированы уязвимости данного протокола, позволяющие атакующему восстановить ключ WEP после перехвата определенного количества зашифрованных данных. Атаки на WEP получили дальнейшее развитие, и в 2004 г. появились так называемые KoreK-атаки, позволяющие атакующему получить ключ после перехвата гораздо меньшего объема данных, чем в оригинальном варианте. Кроме того, управлять статическим распределением ключей в случае большого количества клиентов практически невозможно.

Современные механизмы защиты

Поскольку WEP не обеспечивает адекватного уровня безопасности, для защиты беспроводных сетей довольно широко используются средства построения виртуальных частных сетей. В этом случае канальный уровень OSI признается небезопасным, а вся беспроводная сеть приравнивается к сети Интернет, доступ из которой в корпоративную сеть возможен только по каналу, защищенному средствами VPN на основе PPTP, IPSec в туннельном режиме или L2TP+IPSec. Однако использование VPN накладывает ряд ограничений на использование беспроводных сетей. Исчезает прозрачность, для работы с сетью требуется активизировать беспроводное подключение. И так достаточно небольшая пропускная способность беспроводного канала дополнительно утилизируется за счет служебного трафика протокола организации виртуальной частной сети. Могут возникать разрывы VPN соединения при интенсивном переключении между точками доступа.

Современная подсистема безопасности семейства стандартов 802.11 представлена двумя спецификациями: WPA и 802.11i. Первая из них, как и WEP, задействует для защиты трафика алгоритм RC4, но с динамической генерацией ключей шифрования. Устройства, поддерживающие 802.11i, в качестве алгоритма шифрования используют AES. Оба протокола, и 802.11i, и WPA для аутентификации устройств могут применять как статически распределяемый ключ, так и технологию 802.1X.

Технология 802.1X служит для аутентификации клиента перед получением доступа к канальному уровню технологии Ethernet даже при наличии физического подключения. Для аутентификации используется протокол EAP и его варианты (PEAP, EAP-TTLS, LEAP). В качестве сервера аутентификации может выступать сервер, реализующий необходимые расширения протокола RADIUS. Серьезным достоинством 802.1X является тот факт, что она может использоваться как в проводной, так и беспроводной сети. Т.е. компания может внедрить 802.1X для Wi-Fi, а затем, по мере обновления активного сетевого оборудования задействовать ту же инфраструктуру для аутентификации проводных клиентов.

Очень часто в рекомендациях по обеспечению безопасности беспроводных сетей фигурирует требование к отключению широковещательной рассылки идентификатора сети (SSID broadcast, guest mode и т.д.). В этом случае точка доступа прекращает рассылать широковещательные пакеты beacon с идентификатором сети и другой служебной информацией, облегчающей клиенту настройку.

Это может затруднить обнаружение беспроводной сети злоумышленником, обладающим невысокой квалификацией, но так же и усложнить настройку клиентских устройств (особенно, если точка доступа работает на граничных каналах).

Еще один часто используемый механизм доступа — авторизация по MAC-адресам имеет смысл использовать только как дополнительный механизм защиты, но не как основной, поскольку он довольно легко обходится злоумышленниками.

Выбор технологии обеспечения безопасности

Беспроводные сети можно условно разделить на домашние (SOHO), общедоступные и корпоративные. В каждом из этих случаев имеют смысл разные подходы к обеспечению безопасности сети, поскольку модели угроз различаются для каждого из типов сетей.

В SOHO сетях применяются как технологии построения VPN (например, PPTP, сервер которого встроен во многие беспроводные маршрутизаторы, или IPSec-PSK), так и WPA-PSK (т.е. с аутентификацией на общих ключах). Однако при выборе в качестве протокола защиты WPA-PSK следует помнить, что любой протокол аутентификации, основанный на паролях, уязвим для атак восстановления парольной фразы по перехваченной сессии. Соответственно, для защиты беспроводной сети следует выбирать достаточной устойчивый к подбору пароль (согласно многим рекомендациям, состоящий как минимум из 20 символов).

Для защиты корпоративных сетей наибольшей популярностью пользуются решения на основе технологии 802.1X или средств построения виртуальных частных сетей. И та, и другая технология позволяет задействовать уже имеющиеся в корпоративной сети компоненты, такие, как инфраструктура открытых ключей, серверы RADIUS, шлюзы VPN для защиты от перехвата трафика и несанкционированного подключения к беспроводной сети. Достоинство VPN -- возможность задействовать существующее оборудование, программные продукты и опыт, накопленный при эксплуатации традиционных виртуальных частных сетей. Дополнительным плюсом внедрения 802.1X служит возможность дальнейшего переноса этой технологии и в локальную сеть, поскольку все больше и больше проводных коммутаторов поддерживают 802.1X.компоненты, такие, как инфраструктура открытых ключей, серверы RADIUS, шлюзы VPN для защиты от перехвата трафика и несанкционированного подключения к беспроводной сети. Достоинство VPN -- возможность задействовать существующее оборудование, програ мные продукты и опыт, накопленный при эксплуатации традиционных виртуальных частных сетей. Дополнительным плюсом внедрения 802.1X служит возможность дальнейшего переноса этой технологии и в локальную сеть, поскольку все больше и больше проводных коммутаторов поддерживают 802.1X.

В конце, но не последнюю очередь

Решение о внедрении беспроводной сети, как и любое внедрение IT-технологии, должно сопровождаться анализом рисков, разработкой политики безопасности и инструкций администраторов и пользователей по работе с внедряемой технологией. При развертывании Wi-Fi в крупной сети следует подумать о механизмах централизованного управления настройками точек доступа и клиентских станций. Поскольку требования к безопасности беспроводной сети отличаются от проводной, стоит разделить эти сети с помощью межсетевого экрана. Желательно контролировать настройки рабочих станций и точек доступа как с помощью активных средств (сканеров уязвимостей) так и с помощью беспроводных систем обнаружения атак. Последние помогут так же решить проблему подключения несанкционированных беспроводных устройств. БТ

Продолжение следует.