Секреты в воздухе витают

Прослушивание и анализ передаваемой по беспроводным сетям информации могут предоставить сторонним наблюдателям достаточно данных для успешного проникновения в сеть. В статье описываются плюсы и минусы одного из наиболее часто используемых способов криптозащиты — WEP-методики.

Александр Красоткин

Беспроводные сети с тем же успехом вытесняют кабельную паутину, с которой некогда самобеглые коляски распугивали лошадей на узких городских улочках. Основное достоинство беспроводных технологий — мобильность. Не прерывая работу, участник беспроводной сети может перемещаться из комнаты в комнату, из здания в здание, пересечь несколько часовых поясов, так и не потеряв связь из-за короткого кабеля до розетки. Скорость тоже уже давно не ахиллесова пята беспроводных решений. Сотня мегабит на клиентском порту среднебюджетного оборудования, весьма достаточное подтверждение членства в клубе. В целом стоит честно признать, что аверс монеты весьма привлекателен. Но что с реверсом? Что же является платой за все достоинства?

Подключенные к сети, клиенты связываются между собой не напрямую, а посредством специального узла доступа. Территория, на которой обеспечивается устойчивая связь беспроводного клиента с узлом доступа, называется зоной доступа, или зоной покрытия данного узла. В свою очередь, узлы доступа объединяются между собой волоконно-оптической сетью или радиорелейными мостами. Беспроводная сеть может состоять из нескольких десятков, сотен или тысяч узлов, обеспечивающих покрытие на всей требуемой территории.

Клиент беспроводной сети может перемещаться, переходя из зоны покрытия одного узла доступа в зону покрытия другого. При удалении клиента от узла доступа качество сигнала между беспроводным клиентом и конкретным узлом нередко ухудшается, и тогда реализованные в радиопротоколе средства роуминга дают клиенту команду переключиться на другой узел. Роуминг — это функция, позволяющая пользователю перемещаться от одного узла доступа к другому, не разрывая сетевого соединения. Очевидно, что возможности роуминга в немалой степени зависят от технических характеристик беспроводной сетевой карты и антенны клиента. Лучший узел доступа определяется по качеству сигнала. Производители оборудования используют различные методики оценки этой характеристики. Обычно в число оцениваемых параметров входит сила сигнала и загрузка узла доступа, но не обязательно учитывается расстояние от узла до клиента.

Удобством, как и недостатком беспроводных сетей является доступность физической среды передачи данных — радиоэфира. И если для площадок общественного доступа к сетевым ресурсам (hotspots) такая возможность благо, для офисных сетей доступ за пределами ограниченной территории, определенной стенами предприятия, офиса или квартиры, совершенно излишен. Пространственно зона доступа одного узла представляет собой сферу, радиус которой определен максимальным удалением от центра с сохранением устойчивого качества работы беспроводных клиентов. На практике реальная пространственная зона доступа далека от геометрически красивой фигуры из-за поглощения окружающей физической средой радиосигнала. При одинаковом оборудовании размеры зон доступа в кирпичных и панельных зданиях с железобетонными перекрытиями будут различаться. Надо быть готовым, что, настроив офисную беспроводную сеть, можно не только обеспечить подключение из любой точки офиса, но и из таких неожиданных мест, как чердак, автостоянка или здание напротив. Если для осложнения жизни любителям радиосниферов при прокладке кабельных сетей можно было использовать экранированную витую пару, то в качестве аналогичного решения для физического ограничения пространственной зоны доступа беспроводной сети придется использовать экран из заземленной металлизированной сетки, натянутой по границам зоны доступа. Можно представить, что укладка такого экрана даже в случае небольшой офисной сети сведет на нет все преимущества технологии.

Следует отметить, что максимальное расстояние от клиента до точки доступа напрямую зависит от используемого оборудования. При использовании активных антенн, не особо одобряемых ГКРЧ, расстояние успешного приема/передачи может достигать нескольких километров. В то время как при штатном оборудовании дальность редко превышает сотню метров.

На первый взгляд, несанкционированный доступ к среде передачи данных бесполезен при использовании криптозащиты. На деле же несколько иначе.

Один из наиболее часто используемых способов криптозащиты — WEP-методика. Это симметричный способ шифрования, когда для кодирования и декодирования данных используется один и тот же кодирующий ключ, состоящий из двух частей. Одна часть — секретный ключ — хранится у получателя и отправителя. Вторая — вектор инициализации — генерируется случайным образом на системе отправителя. На основании этих двух значений вычисляется псевдоуникальный кодирующий ключ.

Данные между сетевыми системами передаются в виде пакетов. Структурно каждый пакет состоит из двух частей — заголовка и тела. В заголовке хранится служебная информация, в частности идентификатор сети, аппаратные адреса получателя и отправителя. В теле передаются сами данные и значение контрольной суммы передаваемых данных, используемое получателем для проверки их целостности. Для каждого нового сетевого пакета применяется новый кодирующий ключ. Причем кодируется только тело пакета. В заголовок добавляется значение вектора инициализации, соответствующее кодирующему ключу для данного пакета. Содержание заголовка не кодируется и передается в открытом виде.

Если используемый системой генератор случайных чисел достаточно качественный в статистическом отношении, то проведенная операция шифрования обеспечивает шумоподобный характер передаваемых данных, что, в теории, без знания секретного ключа делает возможность декодирования перехваченного сообщения очень длительным процессом даже при всех мощностях современной вычислительной техники.

При расшифровке пакета получателем программа кодирования инициализируется секретным ключом и извлеченным из полученного пакета значением вектора инициализации. После расшифровки тела сетевого пакета система вычисляет контрольную сумму полученных данных и сравнивает ее со значением контрольной суммы, переданной отправителем в этом же пакете. При положительном результате данные начинают обрабатываться, и отправителю передается подтверждение удачного приема. В противном случае отправитель повторно осуществляет передачу.

Реализованный в WEP механизм криптозащиты должен быть устойчив к взлому. Но обе стороны, как отправитель, так и получатель, должны обладать секретным ключом, используемым вместе с вектором инициализации для кодирования и декодирования информации. Однако, к примеру, в стандарте 802.11b не оговорен механизм обмена ключами между сторонами. В результате при интенсивном обмене данными реальна ситуация повторного использования значений векторов инициализации с одним и тем же секретным ключом. Особенность реализованного алгоритма криптозащиты приводит к тому, что, имея два сетевых пакета, зашифрованных одним кодирующим ключом, можно не только расшифровать данные, но и вычислить секретный ключ. Это позволяет не только декодировать всю перехваченную информацию, но и имитировать активность одной из сторон.

Можно попробовать «скрыть» от посторонних беспроводную сеть, используя одну из особенностей этой технологии. Для однозначного определения беспроводных сетей используются уникальные идентификаторы, позволяющие клиентам различить несколько перекрывающихся беспроводных сетей. Узел доступа может работать в режиме оповещательной передачи «маячковых» сигналов, содержащих значение идентификатора своей сети. Приняв такой сигнал, пользователь определяет, что он вошел в зону доступа какой-либо беспроводной сети. Установив на своем оборудовании идентификатор сети, переданный «маячковым» сигналом, пользователь подключается к ней. Если отключить широковещательную передачу узлом доступа «маячковых» сигналов с идентификатором сети, то теоретически такая сеть становится скрытой. Пользователь, находясь в зоне доступа такой скрытой сети, не получает «маячковых» сигналов от узла доступа. Следовательно, он не может определить идентификатор сети. А если у него нет идентификатора, подключиться к сети он «как бы» не может. Для подключения к «скрытой» таким образом сети легитимным участникам необходимо будет вводить значение сетевого идентификатора вручную.

К сожалению для администраторов и владельцев беспроводной сети, пассивное прослушивание и анализ передаваемой информации могут предоставить сторонним наблюдателям достаточно данных для успешного проникновения в сеть. Для сбора информации достаточно войти в зону покрытия сети и, воспользовавшись рабочей станцией с беспроводным сетевым интерфейсом, подключить программный анализатор сетевого трафика (к примеру, Aircrack). Если WEP-кодирование не включено (обычная заводская настройка оборудования), наблюдатель видит в открытом виде все данные, передаваемые в сети. Если WEP-кодирование все-таки включено, то (следует заметить) кодируются только передаваемые в сетевом пакете данные, а заголовок пакета передается в открытом виде. Из анализа заголовка можно извлечь информацию об идентификаторе сети, аппаратных адресах узлов доступа и клиентов сети, а также значение вектора инициализации, используемого получателем для дешифровки полученных данных. Как видим, прослушивание и анализ перехваченных сетевых пакетов делает попытки сокрытия беспроводной сети с помощью отключения широковещательной передачи узлами доступа «маячковых» сигналов несостоятельными.

Использование механизма идентификации клиентов по аппаратным адресам сетевых интерфейсов для доступа к сетевым ресурсам — не самая лучшая идея. Перехватив и проанализировав сетевой трафик, можно за короткое время получить список аппаратных адресов всех активных клиентов. Задача же изменения аппаратного адреса своего сетевого интерфейса давно решена. Под Linux-подобными операционными системами достаточно воспользоваться стандартной системной утилитой, а для Windows-систем надо трудиться несколько больше, переставляя драйвер сетевого интерфейса или устанавливая дополнительную утилиту.

Простор действий злоумышленников вышеописанным далеко не ограничен. Одна из наиболее неприятных вещей — появление в сети «посредников». Данный вид атаки использует функцию роуминга клиентов в беспроводных сетях. Злоумышленник на своей рабочей станции имитирует узел доступа с более мощным сигналом, чем реальный узел доступа. Клиент беспроводной сети автоматически переключается на новый узел, передавая на него весь свой трафик. В свою очередь, злоумышленник передает этот трафик реальному узлу доступа под видом клиентской рабочей станции. Таким образом, система злоумышленника включается в обмен данными между клиентом и узлом доступа как посредник, что и дало название данному виду атаки — Man-In-The-Middle. Эта атака опасна тем, что позволяет взламывать защищенные соединения (VPN), устанавливаемые по беспроводной сети, вызывая принудительную реавторизацию VPN-клиента. В результате злоумышленник получает авторизационные данные скомпрометированного им клиента. Сама среда передачи данных также предоставляет возможность силовой атаки на беспроводные сети. Цель подобного нападения — снижение производительности сети или ухудшение качества сетевого обслуживания вплоть до полного паралича. В процессе нападения злоумышленник передает трафик, объем которого превышает возможности пропускной способности сетевого оборудования, или сетевые пакеты со специально нарушенной внутренней структурой. Или имитирует команды узла доступа, вызывает отключение клиентов и т. д., и т. п. Злоумышленник может избирательно атаковать как отдельную рабочую станцию или точку доступа, так и всех клиентов сети. DoS-атака может быть и непреднамеренной. Например, вызванная включением радиопередающего оборудования, работающего на той же частоте, что и беспроводная сеть.

Возможно, DoS-атака не так изящна, как проникновение в сеть путем взлома криптозащиты, зато убийственно эффективна. С учетом того, что нельзя избирательно ограничивать доступ к физической среде передачи данных в беспроводных сетях (радиоволнам), вероятно, придется смириться с существованием этой потенциальной уязвимости данной технологии.

Вышеописанное отнюдь не является строгой рекомендацией отказаться от использования беспроводных технологий. Беспроводные сети становятся настолько же распространенным сервисом, как и сотовая телефонная связь (защита информации в которой тоже далеко не безупречна). Достигнуто многое, но главное — существуют возможности дальнейшей эволюции. А пока не стоит облегчать задачу взломщикам, пренебрегая пусть немногими и не совсем совершенными средствами безопасности.