АВТОР: АНДРЕЙ ВЛАДИМИРОВ

ОБОРОНА ВОЗДУШНЫХ ЗАМКОВ

БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ КОРПОРАТИВНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

ДАВНО ПРОШЛИ ТЕ ВРЕМЕНА, КОГДА ЕДИНСТВЕННОЙ ДОСТАТОЧНО БЕЗОПАСНОЙ И РАЗУМНОЙ АЛЬТЕРНАТИВОЙ УЖЕ ВЗЛОМАННОМУ WEP БЫЛИ ГРОМОЗДКИЕ В АДМИНИСТРИРОВАНИИ ВЧК НА БАЗЕ IPSEC ИЛИ, ПО КРАЙНЕЙ МЕРЕ, КОМБИНАЦИИ PPTP И MPPE. ТЕМ НЕ МЕНЕЕ НЕ СТОИТ РАССЛАБЛЯТЬСЯ.

Прорехи, специфические для беспроводных сетей различных стандартов 802.11 (речь пойдет только о них, так как нельзя объять необъятное), по-прежнему существуют. Защита этих сетей так же требует пристального внимания. Проводным сетям никогда не сравниться с беспроводными в удобстве пользования, особенно когда речь идет о подключении мобильных компьютеров. С другой стороны, беспроводные сети никогда не будут настолько же безопасны по сравнению с их медными и оптико-волоконными собратьями. Это, как говорил известный герой Ильфа и Петрова, медицинский факт. И отталкиваясь от данного факта, взвесив все «за» и «против», рано или поздно всем придется сделать выбор между полноценной защитой беспроводных сетей и защитой от беспроводных сетей и устройств.

Защита от беспроводных сетей и устройств

Сначала рассмотрим последний, более простой случай. Предположим, вы решили, что для вашего предприятия или компании беспроводные сети будут скорее проблемой, чем решением проблем, а ассоциированные риски слишком велики и приведут к неприемлемым затратам для их уменьшения. Кроме того, существуют ситуации, когда развертывание беспроводных сетей категорически противопоказано, вне зависимости от уровня защищенности передаваемых по ним данных. Речь идет об объектах, которые должны быть защищены от электромагнитных утечек всеми возможными способами. Не вдаваясь в тонкости радиотехнического шпионажа, упомянем, что исходящий высокочастотный сигнал может модулироваться при взаимодействии с другими электромагнитными сигналами на объ-

екте и, таким образом, «выносить наружу» потенциально ценную информацию. Далее, широкополосные сигналы сетей 802.11a/b/g и, особенно, 802.11n идеально подходят для маскировки сигналов продвинутых радиозакладок методом наложения. Соответственно, если помещение, в котором работают со сверхсекретными данными, не является неприступной клеткой Фарадея, беспроводных сетей и устройств в нем быть не должно. Для этого необходимо:

- четко прописать запрет на использование любых беспроводных устройств и каналов связи на территории объекта в политиках информационной безопасности и ясно обозначить административные последствия нарушения этого запрета;
- физически изъять беспроводные интерфейсы из всех используемых на территории объекта устройств, включая КПК, сетевые принтеры и смартфоны. Если для некоторых устройств это технически невозможно, то они просто не должны использоваться на территории объекта и для хранения конфиденциальных данных предприятия, организации или компании;
- установить распределенную систему мониторинга частот, используемых стандартами 802.11a/b/g/n (а также Bluetooth), для обнаружения, локализации и изъятия несанкционированных устройств. Главное — помнить, что, если вы запретили использование беспроводных сетей и устройств на подконтрольной территории, это отнюдь не значит, что их там нет.

Защита беспроводных сетей

Теперь о том, как защитить ваши беспроводные сети и устройства от несанкционированного доступа и утечек конфиденциальной информации. Однозначного и абсолютного решения этой проблемы на сегодняшний момент нет. «Используйте WPA» — рекомендация очень распространенная, но, увы, отражающая непонимание советчиками всей полноты современных угроз беспроводной безопасности. Для эффективного противостояния этим угрозам необходим целый комплекс мер — как технических, так и административных. Основанные на стандарте 802.11i, WPA1 и WPA2 (как PSK, так и Enterprise) — безусловно важные, но далеко не единственные составляющие части такого комплекса. Проиллюстрируем это утверждение, перечислив основные текущие проблемы безопасности беспроводных сетей и устройств.

— Несанкционированные устройства

Варьируются от личных точек доступа и ноутбуков, приносимых сотрудниками в офис, до «продвинутых» мобильников и беспроводных принтеров, подключенных к проводным сетям с включенным при этом позабытым 802.11 интерфейсом. В большинстве случаев эти устройства не защищены. Взлом несанкционированного клиентского устройства может привести к не менее плачевным последствиям, чем подсоединение к несанкционированной точке доступа.

— Неправильные настройки сетей

К таковым относятся слабые ключи WPA PSK, которые можно определить перебором по словарю. На сегодняшний день для этого наиболее эффективна Elcomsoft Distributed Password Recovery, с использованием графических процессоров видеокарт nVIDIA для взлома. WPA Enterprise также имеет проблемы конфигурации, связанные с методами аутентификации пользователей. EAP-MD5 и EAP-LEAP не безопасны и могут быть взломаны. Также не рекомендуется использовать PAP и MS-CHAP внутри тоннелей EAP-TTLS. Если проверка сертификатов сервера на клиентских машинах не включена, то и EAP-TTLS, и более распространенный EAP-PEAP могут быть атакованы посредством установки фальшивой точки доступа, дополненной модифицированным RADIUS-сервером (FreeRADIUS с установленной заплатой freeradius-wpe). Так что сами по себе ни WPA PSK, ни WPA Enterprise — не панацея, их нужно еще и уметь правильно настроить.

— Непростительные ошибки настройки сетей

До сих пор встречаются как полностью открытые беспроводные сети (от 10 до 20%, по статистике наших недавних боевых выездов), так и сети, использующие WEP (до 30%, по той же статистике, если не принимать во внимание хотспоты). Наш рекорд по взлому WEP с помощью полностью автоматизированного wesside-ng, одной из утилит aircrack-ng, — три с небольшим минуты. К слову, достаточно часто доводилось встречать точки доступа с WPA1, по умолчанию использовавшие TKIP для защиты одноадресного, а WEP — многоадресного и широковещательного трафика. Каждый сетевой администратор может легко представить, сколько бед может натворить хакер, получивший полный доступ к широковещательной и групповой передаче данных на сети.

— Прорехи безопасности коммерческих хотспотов

До сих пор все из установленных в общественных местах хотспотов, которые доводилось встречать, уязвимы к сбрасыванию клиента из сети с помощью любой беспроводной DoS-атаки и дальнейшему подсоединению вместо него или попутно с ним. Кроме того, хакеры могут свободно перехватывать весь посылаемый через хотспот незащищенный трафик, к примеру похищая cookies для логина вместо легитимного пользователя с помощью таких утилит, как Hamster. Львиная доля проблем безопасности хотспотов связана с отсутствием на них защиты данных на канальном уровне, которая реализована в стандарте 802.11i. Защита отдельных протоколов на 6-7-м уровнях OSI-модели никак не может служить ей полноценной заменой и имеет свои уязвимости (смотрите, например, использование Omen для атак против SSL/TLS).

— Беспроводные атаки по отказу в обслуживании

Стандарт 802.11w, предназначенный для аутентификации фреймов управления и способный предотвратить самые простые и распространенные на сегодняшний день беспроводные DoS-атаки деаутентификации и деассоциации, должен был быть ратифицирован еще в апреле этого года. Сейчас срок его ратификации перенесен на декабрь 2009 года, и это самое раннее, на что можно рассчитывать. В то же время количество известных беспроводных DoS-атак продолжает расти чуть ли не в геометрической прогрессии с появлением новых классов таких атак. К ним относятся RTS/CTS-атаки (внедрены в Metasploit как cts_rts_flood.rb), атаки на EAPOL, так называемые «аутоиммунные атаки», заставляющие точки доступа отсоединять клиентские устройства, забивание 802.11b-канала переводом клиентского устройства в режим PLME_DSSSTESTMODE, 802.11e/n-атаки против порядковых номеров окон (Block ACK DoS) и атаки по сбиванию ширины 802.11n-канала до 20 МГц. Недоработанный стандарт 802.11w, защищающий только фреймы деаутентификации, деассоциации и действия (802.11e) и его уже внедренная пре-имплементация (Cisco MFP — Management Frames Protection) от этих атак совершенно не помогают.

— Атаки против клиентских устройств

Все, что улучшилось за последние два года, в основном относится не к защите, а к совершенствованию подходов и инструментарию атакующих: пентестеры должны обратить свое внимание на совместное использование Karmetasploit, airbase-ng, ISR-

АВТОР: АНДРЕЙ ВЛАДИМИРОВ

АВТОР: АНДРЕЙ ВЛАДИМИРОВ

Evilgrade и Ferret. Современные атаки против клиентских беспроводных устройств можно разделить на три большие категории: атаки на механизмы ассоциации с сетями, атаки на механизмы защиты (взлом того же WEP или WPA-PSK у отдельно взятого устройства) и атаки переполнения буфера против драйверов клиентских устройств. Все клиентские устройства, которые подключались к незащищенным или недостаточно защищенным на канальном уровне сетям (хотспоты и кратковременные ад-хок-соединения в этом плане обычно фатальны), следует считать уязвимыми. А самой эффективной атакой против любого клиентского устройства является его физическое похищение, которое может стать катастрофическим, если для подключения к корпоративной беспроводной сети используется аутентификация самих устройств, а не их пользователей.

Предупрежден – значит вооружен

Имея хотя бы приблизительное представление о том, что могут сделать атакующие, можно переходить к рассмотрению возможных мер обороны от вышеперечисленных угроз. Поскольку речь идет, в первую очередь, о защите беспроводных сетей крупных организаций или компаний, начнем с политик беспроводной безопасности.

Они должны полностью покрывать как минимум такие важные области:

- предназначение и связанные с ним ограничения пользования беспроводными сетями. Скажем, служащие компании не должны подключаться к гостевой сети, а сама гостевая сеть должна иметь доступ в интернет и никуда более, клиентские устройства не должны соединяться с каналом точка-точка между двумя офисами, работники одного отдела не должны сидеть на беспроводной сети другого;
- должностную ответственность за поддержку, обслуживание и безопасность беспроводных сетей;
- уровни доступа к беспроводным сетям и устройствам для технических специалистов и пользователей;
- информацию, разрешенную и запрещенную к передаче через беспроводные каналы;
- инвентаризацию и учет всех беспроводных устройств без исключения, действия при их потере или похищении;
- минимальный необходимый уровень технической защиты беспроводных сетей. Например, использование только WPA Enterprise с EAP-PEAP и сильными паролями пользователей, наличие распределенной wIDS/wIPS, сохранение журналов и учетных записей централизованного мониторинга беспроводных сетей, сегментация сетей, регулярное обновление драйверов клиентских устройств;
- правила пользования беспроводными сетями и устройствами и их нарушения;
- действия при подозрении на беспроводную атаку: формальное расследование, установление причин проблемы, устранение последствий, отчетность;
- проведение регулярных аудитов беспроводной безопасности для ее реалистичной оценки, выявления и устранения слабых сторон.

Если эти вещи четко не определены и не расписаны, ни о какой безопасности корпоративных беспроводных сетей речи идти не может. Будет хаос, плодящий разнообразные уязвимости. Очень трудно соблюдать (и заставлять соблюдать других) то, что не обозначено и не описано должным образом. И только когда это сделано, имеет смысл концентрироваться на технических деталях.

Технические меры защиты

Начнем с базовых технических мер защиты. Зона покрытия беспроводной сети должна быть ограничена по максимуму, чтобы не привлекать излишнего внимания и заставить потенциальных атакующих находиться как можно ближе к подконтрольной вам территории, где их гораздо проще заметить и отследить. Делается это посредством регуляции силы выходного сигнала точек доступа и правильного расположения самих точек доступа и внешних антенн. Помните, что дальность покрытия сетей стандарта 802.11n может превышать таковую для сетей других 802.11-стандартов в 1,5-4 раза, тогда как дистанция работы сетей 802.11a — наименьшая.

Также для уменьшения заметности сетей значения ESSID не должны содержать информацию, которая может заинтересовать атакующих: название компании, отдела, адрес, имена, тип используемого оборудования и т.д. А вот использовать «скрытые ESSID» не имеет смысла. С одной стороны, их элементарно узнать, с другой, не вдаваясь в технические подробности, отметим, что сокрытие ESSID на самом деле уменьшает безопасность клиентских устройств, заставляя их «выплевывать» больше информации в процессе поиска сети для подсоединения.

Еще одна «традиционная» мера защиты беспроводных сетей — фильтрация по MAC-адресам. Она способна несколько задержать атакующих, но ненадолго. О скидывании легитимного клиента и подсоединении вместо него уже говорилось при обсуждении проблем безопасности хотспотов. При этом поддержка базы разрешенных и запрещенных MAC'ов для крупной беспроводной сети может быть очень трудоемким и неблагодарным

Об авторе

Андрей Владимиров – соучредитель компании «Arhont Ltd» с 2001 года, глава по безопасности, CISSP, CCNP, CCDP, CWNA, TIA Linux+. Обнаружил и опубликовал ряд уязвимостей Cisco IOS, протокола EIGRP и механизмов сегментации VLAN.
Соавтор книг «Wi-Foo: The Secrets of Wireless Hacking» (была переведена на 5 языков) и «Hacking Exposed Cisco Networks», а также автор многочисленных публикаций на различные темы в сфере информационной безопасности в профессиональной и популярной периодической прессе. В настоящее время активно работает над вторым изданием «Wi-Foo: The Secrets of Wireless Hacking».
Принимал участие в аудитах безопасности беспроводных сетей и бета-тестировании защиты 802.11-устройств ряда крупных корпораций, включая General Electric, Renault, Marriot, Proxim, Belkin, Netgear, а также Royal Ascot Race Course. Помимо прикладной работы, в основном связанной с безопасностью протоколов маршрутизации и коммутации, архитектурой проводных и беспроводных сетей и расследованием компьютерных преступлений, активно участвует в профильном обучении специалистов, разработке корпоративных политик, стандартов и руководств безопасности, консалтинге по получению и соответствию ISO27001, Basel II, SOX, FSA и другим аккредитациям.

делом. А вот разделить проводные и беспроводные сети компании наиболее безопасным образом, отсекая неиспользуемые на беспроводной сети протоколы и лишние потоки данных и принимая меры против подделки ARP- и DHCP-пакетов, атак на VLANы и STP на всех вовлеченных коммутаторах, — хороший пример классической эшелонированной обороны, которым не стоит пренебрегать.

Теперь про собственно WPA. WPA PSK не должен применяться для защиты крупных корпоративных сетей по целому ряду причин. Все пользователи знают (или могут легко узнать) общий ключ, который сохранен на их мобильных компьютерах. Эти компьютеры могут быть утеряны или похищены, а пользователи могут проболтаться. Смена ключа, регулярная или в связи с подозреваемой утечкой, на большом количестве хостов представляет значительную административную проблему. А если ключ не менять, то рано или поздно произойдет утечка или же настойчивая атака перебором может закончиться успехом. Таким образом, сфера применения WPA PSK в корпоративной среде строго ограничена: защитой небольших отдельных гостевых сетей, защитой кратковременных инсталляций (ад-хок и временные сети на деловых встречах и конференциях) и случаями, когда клиентские устройства (например, считыватели баркодов, сетевые принтеры) не поддерживают WPA Enterprise и для них желательно создать отдельный VLAN под защитой WPA PSK. Во всех остальных случаях установки и настройки WPA Enterprise должны быть тщательно продуманы и спланированы. RADIUS-серверов должно быть как минимум два, с протоколом дублирования (VRRP, heartbeat и т.д.) между ними, иначе любая серьезная проблема с RADIUS-сервером сделает использование сети невозможным. Теперь что касается выбора EAP. Какие типы и установки EAP не следует выбирать, было обсуждено при описании проблем безопасности беспроводных сетей. Из оставшейся выборки наиболее безопасным является EAP-TLS, при условии защиты клиентских сертификатов паролями, иначе похищение сертификата (обычно вместе с мобильным компьютером, на котором он сохранен) открывает доступ к сети. Неудивительно, что EAP-TLS и наиболее неудобен в плане администрирования и поддержки: необходимо открывать свою CA, выписывать сертификат на каждый беспроводной хост и удостоверяться, что пользовательские сертификаты защищены сильными паролями. Более комфортным в использовании и распространенным на современных сетях является EAP-PEAP, который безопасен, при условии выбора достаточно сильных паролей MS-CHAPv2, запускаемого EAP-PEAP внутри TLS-тоннеля. Есть и более экзотические безопасные конфигурации WPA Enterprise с EAP-TTLS (вплоть до использования EAP-TLS внутри EAP-TTLS) и Cisco EAP-FAST (небезопасен в анонимном режиме). Но, в любом случае, клиентские устройства должны всегда быть настроены на проверку сертификата сервера и подключение исключительно к авторизованным, легитимным RADIUS-серверам.

Однако все вышеперечисленное само по себе не решает сложную проблему атак на клиентские устройства. Для того чтобы противостоять подобным атакам, необходимо:

- своевременно обновлять и залатывать драйверы клиентских устройств. Для проверки уязвимости драйверов можно использовать Wifidenum, доступный на сайте Aruba Networks;
- удостоверяться, что в профилях клиентских устройств сохранены данные о подсоединении исключительно к высокозащищенным на канальном уровне сетям. В идеале, там должны быть только сети вашей компании, обороняемые с помощью WPA Enterprise. Если это позволяют политики компании, вынос рабочих мобильных компьютеров за пределы ее территории должен быть максимально ограничен, равно как и использование публичных беспроводных сетей сотрудниками в командировках. Профили компьютеров, которые могли подключаться к беспроводным сетям вне компании, должны проверяться и очищаться системными администраторами. Также желательно полностью запретить использование персональных и домашних беспроводных компьютеров и других устройств в бизнес-целях;
- по возможности выключать поддержку ад-хок-соединений у клиентских устройств;
- заботиться о правильности установок и обновлений персональных брандмауэров и антивирусов клиентских устройств (помня при этом, что ни то ни другие особо не защищают от прямых атак на сами беспроводные драйверы, а также от фишинга, фальш-обновлений а-ля ISR-evilgrade и беспроводных утечек информации);
- запретить пользователям менять беспроводные настройки клиентских устройств, так же как и настройки персональных брандмауэров и антивирусов, и тщательно следить за выполнением этого запрета;
- своевременно обнаруживать и устранять несанкционированные, подозрительные точки доступа и источники DoS-атак.

Для успешного воплощения последнего пункта необходима установка современной распределенной беспроводной IDS/IPS. В настоящее время промышленные, централизованно контролируемые точки доступа обычно имеют встроенную функциональность обнаружения, журналирования и предотвращения атак. Использование такой функциональности более эффективно, чем разворачивание независимой wIDS/wIPS, так как гарантирует полное совпадение зон покрытия и частот самих беспроводных сетей и этих защитных систем. В то время как технически предотвращение и блокирование большинства беспроводных DoS-атак (частая прелюдия для взлома клиентских устройств) и установки «зловредных» точек доступа хакерами пока не реалистично, их точная географическая локализация и физическое устранение остаются единственными работающими методами обороны. Для их результативности желательно, чтобы зона покрытия беспроводных сетей более-менее совпадала с зоной видеонаблюдения, а охранники компании, организации или предприятия были обучены оперативному реагированию на сообщения о наличии подозрительных устройств и хакеров в этих зонах.

Заключение

Следует отметить, что, даже имея полноценную систему беспроводной защиты — от политик безопасности и соответствующих контрольно-управленческих механизмов до продвинутых, корректно настроенных и поддерживаемых технических средств, все равно стоит следовать принципу «доверяй, но проверяй». При возможности, регулярно пользуйтесь услугами внешних профессиональных аудиторов безопасности для профилактического обнаружения слабых звеньев защиты ваших беспроводных сетей и своевременного их устранения. То, что очень хорошо выглядит на бумаге, в рекламе «самых безопасных решений» производителей или докладах системных администраторов, может совершенно не соответствовать реальности. Вспомним, что когда-то и WEP считался практически неуязвимым. **it**

АВТОР: АНДРЕЙ ВЛАДИМИРОВ