Специфика защиты беспроводных сетей

Статья инженера центра технической поддержки Cisco посвящена вопросам защиты современных беспроводных сетей. Автор кратко рассматривает основные типы таких сетей и потенциальные угрозы для этого вида связи. Уделено внимание организации обнаружения и устранения атак на беспроводные сети.

Ирина Ильина-Сидорова
iilyinas@cisco.com

С момента ратификации стандарта IEEE 802.11b в 1999 г. беспроводные ЛВС (локальные вычислительные сети, или Local Area Network, LAN) получили широкое распространение. Сегодня их можно встретить и в офисах, и в конференц-залах, на промышленных складах, в школьных классах, кафе и торговых центрах, в историческом центре города.

Специфика защиты беспроводных сетей, прежде всего, заключается в их отличии от сетей проводных. Беспроводные ЛВС, ввиду их широковещательной природы, требуют реализации дополнительных механизмов для:

- аутентификации абонентов (user authentication) с целью предотвращения несанкционированного доступа к сетевым ресурсам;
- обеспечения конфиденциальности данных (data privacy) с целью обеспечения целостности и защиты при передаче по общедоступному радиоканалу.

Безусловно, наряду с уникальными для беспроводных технологий проблемами безопасности существует ряд общих для проводных и беспроводных технологий проблем. Как правило, это атаки более высокого уровня, неселективные к используемой технологии доступа (фишинг и т. п.). Однако и здесь возможны варианты беспроводной специфики, например в случае DoS-атак. Интересной особенностью беспроводных сетей является организация публичного и незащищенного доступа, приводящая к целому классу проблем безопасности, совершенно несвойственных проводным сетям.

В целом можно сказать, что большое значение играет совершенно другая организация доступа к физической среде. В отличие от проводных подключений, в случае подключения беспроводного у нас присутствуют следующие моменты:

1. Может оказаться проблематичным достоверно определить местоположение клиента (точку подключения), особенно в случае разреженной беспроводной сети.
2. Трафик всегда передается по разделяемой среде (shared medium), то есть практически всегда имеется возможность для прослушивания и вмешательства в канал передачи данных (безусловно, успешность таких действий не гарантирована).
3. Местоположение сетевого устройства также неочевидно для подключающегося клиента, что облегчает злоумышленнику возможность выдать нелегитимное устройство за точку подключения к сети.
4. Клиентское устройство не зафиксировано в пространстве, более того, даже в случае неподвижного клиента мы не можем требовать подключения к одной и той же точке доступа в сеть, роуминг — это нормальное поведение клиентского устройства (этот факт существенно затрудняет обнаружение попыток имперсонификации).
5. Кроме того, в случае Mesh-сетей мы имеем дополнительный класс инфраструктурных атак[1], где сетевые устройства не могут быть достоверно определены (т. е. мы не можем сказать, является upstream/downstream peer[2] легитимным или же нет);

Подытоживая: мы не можем быть уверены в клиенте, не можем быть уверены в точке подключения и в канале передачи,

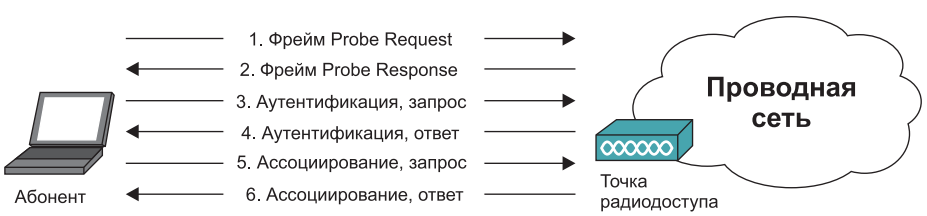

Рис. 1. Аутентификация в беспроводной сети

[1] Инфраструктурные атаки — атаки на сетевую инфраструктуру организации.
[2] Upstream/downstream peer — в данном случае устройство сетевой инфраструктуры (точка доступа) в Mesh-сети. Это может быть как RAP (Root Access Point, корневая точка доступа), так и MAP (Mesh Access Point сетевая точка доступа). Основной особенностью Mesh-сетей является то, что пользовательский трафик передается от одной точки к другой (а затем покидает Mesh-сеть через RAP). Злоумышленник может пытаться встроить нелегитимную точку доступа в эту цепочку.

«бонус» — затруднены выявление и локализация потенциального клиента-злоумышленника. Все, кроме первого, маловероятно в случае проводного подключения.

Кроме того, необходимо учитывать логическое деление беспроводных сетей.

Помимо корпоративных сетей с гостевым сегментом, для беспроводных сетей необходимо рассмотреть случаи организации публичного доступа (такого, например, как Wi-Fi в аэропортах, на конференциях и в торговых центрах), где нам необходимо обеспечить подключение самого широкого класса устройств, не имея возможности проконтролировать меры по безопасности на них; а также служебные сегменты сетей (Mesh-сети), которые в силу самой природы разделяемого доступа к среде передачи не могут быть надежно изолированы от окружающего мира. Необходимо также напомнить, что корпоративная сеть и ее гостевой сегмент не могут считаться полностью изолированными ни друг от друга, ни от внешнего мира — в зависимости от используемых технологий подключения, некоторый объем информации о сети будет доступен стороннему наблюдателю.

Все вышеперечисленное делает задачу защиты беспроводных сетей весьма интересным и комплексным мероприятием.

Итак, на какие же потенциальные угрозы необходимо обратить внимание в беспроводных сетях? Вот их перечень:

- сбор информации о сети;
- сбор информации о клиентах;
- имперсонификация с целью получения доступа к сети;
- имперсонификация с целью получения контроля над клиентом;
- отказ в обслуживании (зачастую совмещенный с предыдущими пунктами).

Список в таком виде выглядит аналогично списку угроз для проводных сетей. Однако это верно только на первый взгляд.

Рис. 2. Информация, предоставляемая в beacon-фрейме

Для сбора информации злоумышленник может использовать как активное, так и пассивное сканирование.

Чем любопытно пассивное сканирование, так это принципиальной невозможностью его выявления. То есть, в отличие от проводных сетей, в беспроводных сетях мы обязаны учитывать тот факт, что (как минимум) следующие данные известны стороннему наблюдателю:

- название/идентификатор нашей сети (Service Set Identifier, SSID);
- используемые алгоритмы шифрования для подключения (AES, TKIP);
- используемая схема аутентификации (MAC Auth, Static key, EAP, WebAuth или их комбинации);
- поддерживаемые скорости подключения;
- производитель используемого оборудования и его узлов (беспроводного чипсета);
- количество клиентов беспроводной сети и их состав (эта информация будет неполной, однако злоумышленник может принять меры для ее уточнения);
- примерное расположение точек доступа в нашей сети (эта информация важна для последующих атак с имитацией точек доступа, а также для попытки предотвращения определения физического положения атакующего методом триангуляции);
- используемые протоколы оптимизации работы в беспроводных сетях (capability information) — это может послужить базой для атаки на конкретный алгоритм и способствовать определению модели используемого оборудования;
- характерные для сети источники помех (может использоваться для сокрытия следов в случае DoS-атак).

Даже этот минимальный набор — уже достаточно существенный объем данных.

В зависимости от данных, полученных на данном этапе, а также от требуемого результата, злоумышленник может перейти к этапу атаки на инфраструктурные устройства — или к этапу имитации устройства доступа для последующих атак на клиентские устройства. Необходимо отметить, что получение контроля над беспроводными инфраструктурными устройствами может преследовать разные цели: это и атаки на клиентские устройства, и атака на сетевую инфраструктуру компании, и получение доступа ко внутренним доверенным сетям.

Попытки атаки как на инфраструктурные, так и на клиентские устройства могут быть обнаружены средствами беспроводных систем обнаружения атак (Wireless Intrusion Protection System, wIPS). Также эти системы проводят обнаружение активного сканирования, которое, по сути, является попыткой начала установления соединения.

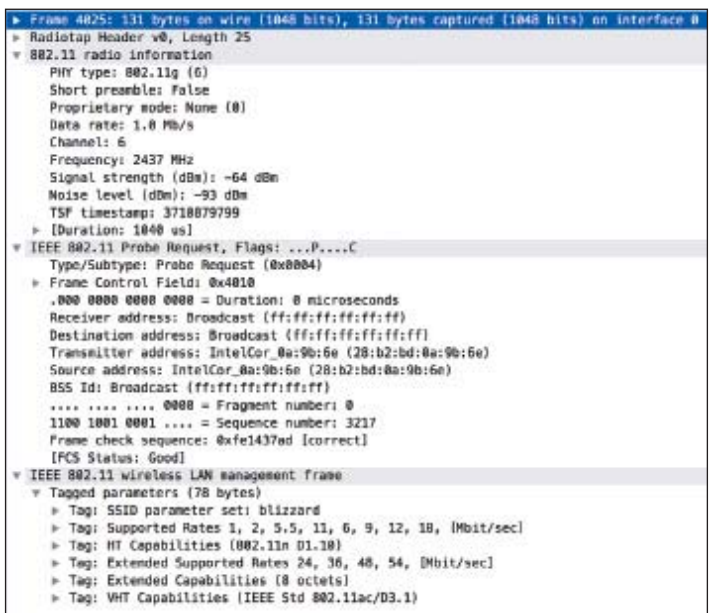

Рис. 3. Информация, предоставляемая в probe-request-фрейме

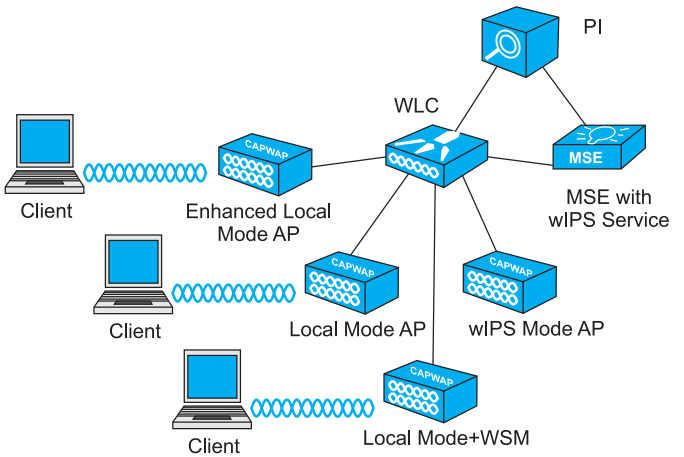

Рис. 4. Архитектура беспроводной сети с wIPS

В общих чертах, wIPS получает информацию от точек доступа, анализирует ее и, аналогично классической IPS, старается выявить паттерны, свидетельствующие о наличии атаки.

Это могут быть попытки профилирования сетевой инфраструктуры с помощью активного сканирования, попытки взломать шифр, используемый для доступа к сети, попытки имперсонификации (например, подмена MAC-адреса) для преодоления сетевой аутентификации, а также известные атаки на протоколы.

Кроме того, wIPS способны коррелировать события, обнаруживая более сложные схемы атаки, например имитацию помех, вынуждающую клиента переподключиться и приводящую к возможности расшифровки трафика между клиентом и точкой доступа, с последующей посылкой deauth-фреймов (Deauthentication frame) клиенту (DoS-атака, заставляющая клиента отключиться) и одновременным внедрением в сеть с имперсонификацией в сторону точки доступа от лица этого клиента, с перехватом аутентифицированной сессии и установлением доступа к доверенной сети.

К сожалению, зачастую можно наблюдать, как беспроводные атаки остаются незамеченными достаточно продолжительное время, будучи замаскированными под неустойчивое подключение или перегрузку среды передачи. Понятно, что такого рода проблемы невозможны в проводных сетях. В этом случае можно только рекомендовать более внимательно относиться к предупреждениям wIPS и проводить тщательное расследование инцидентов.

Также внимательно нужно относиться к случаям выявления беспроводных клиентов вне территории предприятия (в случае зон с раздельным доступом — в неожиданной зоне) или «прыжков» клиентов по карте, конечно, если доступно позиционирование клиентов на программном обеспечении (ПО) для сетевого мониторинга.

Нужно сказать, что качественные, детализированные карты существенно облегчают работу такого рода, позволяя легко различить, к примеру, false positive (ошибочное (ложное) срабатывание wIPS), возникшее при проходе клиента через двусветный зал (при этом клиент как бы переместился на этаж выше и обратно), и попытку имитации MAC-адреса (например, если клиент «бьется» между офисной зоной и газоном у входа в здание). К сожалению, не всякая беспроводная инфраструктура изначально готова к позиционированию клиентов на карте. Именно поэтому выше мы упоминали о том, что неточное позиционирование клиента — один из вызовов разработчикам защиты беспроводных сетей.

Для классического позиционирования необходимо, чтобы один и тот же клиент обнаруживался тремя точками доступа с достаточной силой сигнала. Это позволяет вычислить положение клиента. Такой метод не всегда приносит хорошие результаты. Он сильно зависит от расположения точек доступа: при неудачном расположении позиционирование будет доступно лишь на некоторых участках сети, что сводит на нет потенциальный эффект. Кроме того, он требует, чтобы точки доступа тратили свои ресурсы на сканирование эфира и передачу данных об обнаруженных клиентах. В идеале необходимы дополнительные точки доступа, которые будут работать исключительно в режиме сканирования, однако это удорожает конечное решение. Реализация позиционирования существенно отличается от производителя к производителю. К прмеру, решение от компании Cisco включает в себя модули Hyperlocation, позволяющие осуществить позиционирование с точностью до метра.

Рис. 5. Тонкая настройка обнаружения атак на Cisco PI

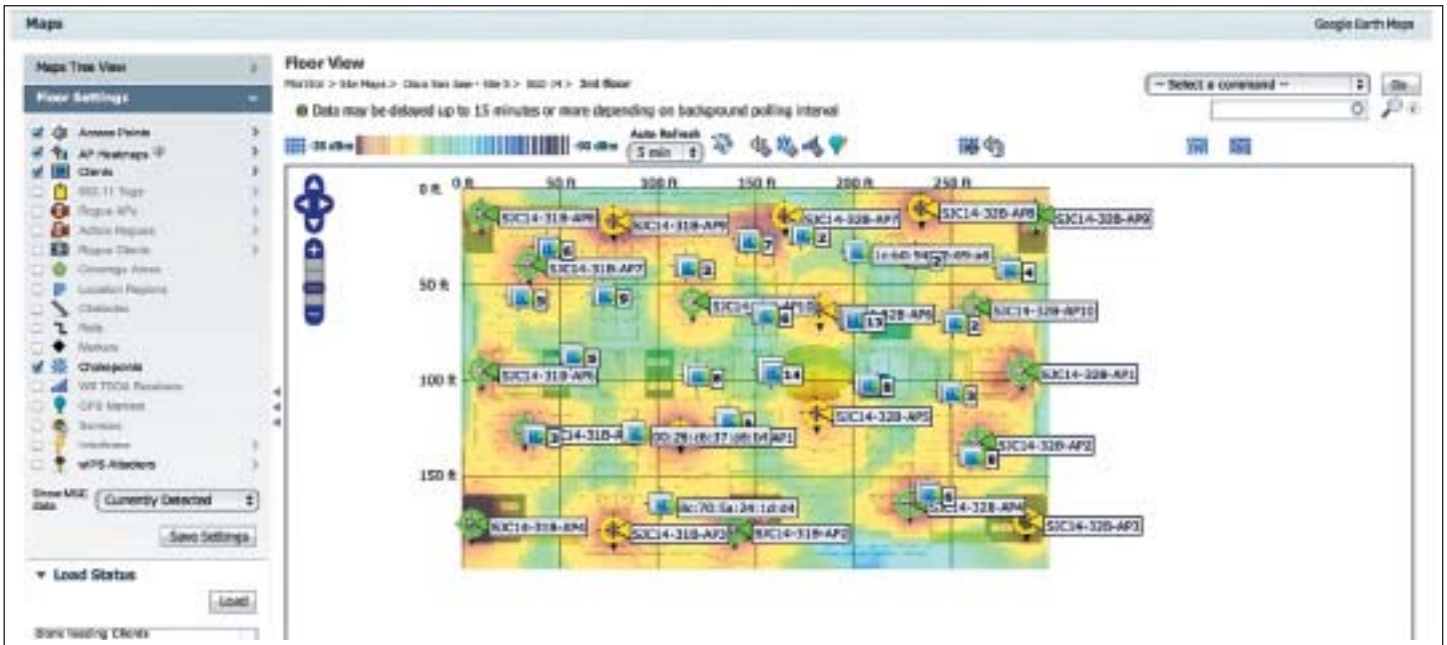

Рис. 6. Пример карты с клиентами

Безусловно, ограничиться обнаружением атак было бы недостаточно. Однако следует отметить, что — опять-таки в силу открытой природы беспроводных сетей — применять ответные меры следует с осторожностью.

Так, в случае работы в помещении крупного офисного центра практически всегда в процессе настройки wIPS будет выявлено множество ложных срабатываний по обнаружению rogue AP («вражеских» точек доступа). Это нормальное явление, поскольку подавляющее их большинство является точками доступа соседнего предприятия, работающими в той же среде передачи. Попытка автоматической реакции на них отключением (shun) будет представлять собой, по сути, DoS-атаку на соседскую сеть и, безусловно, повлечет за собой неприятные последствия.

В случае критической инфраструктуры основной реакцией на обнаруженную wIPS-атаку должна быть именно человеческая реакция группы реагирования на инциденты. Проще говоря, для критичных событий сетевой специалист с беспроводным сканером должен немедленно проследовать в ту часть сети, где обнаружена проблема. Это позволит своевременно устранить угрозу. В качестве сканера может использоваться как ноутбук со специализированным ПО, так и отдельное устройство.

Понятно, что как только система wIPS подаст сигнал об обнаружении не контролируемой нами точки доступа, вещающей наш SSID, необходимо сразу же заняться выяснением того, что именно ведет передачу. Например, мы можем встретиться с беспроводным устройством, имитирующим легитимную точку доступа, а на деле представляющим из себя устройство MITM[3], собирающее информацию об устанавливаемых сетевых соединениях и устанавливающее на клиентские системы шпионское ПО (например, модифицируя на лету ответы HTTP-сервера клиенту).

Конечно, это лишь один вариант из богатого набора атак, которые возможны в беспроводных сетях.

К счастью, для подавляющего большинства инсталляций будет достаточно обращать внимание на события и предупреждения, генерируемые wIPS, — и незамедлительно реагировать, конечно же. Для критичных мест необходимо также предусмотреть регулярный обход с включенным беспроводным сканером и последующим разбором собранной информации.

Вышеописанная реакция на инциденты — это важная составляющая политики беспроводной безопасности, которая, в свою очередь, является частью общей политики безопасности компании. Подробное рассмотрение этого вопроса выходит за рамки статьи, поэтому лишь вкратце упомянем о том, какие этапы необходимо пройти при выработке такой политики и поддержании ее в актуальном состоянии. Как и ранее, во многом они будут близки этапам, выполняемым для проводных сетей:

1. Выполнить оценку рисков.
2. Определить и задокументировать возможные уязвимые места и меры по их устранению.
3. Получить поддержку от руководства.
4. Обеспечить взаимодействие между отделами и вовлеченными лицами.
5. Обеспечить непрерывный мониторинг и аудит.
6. Запланировать ответные меры, расследование инцидентов, структуру отчетов на случай успешной атаки.
7. Регулярно пересматривать и дополнять политику по мере необходимости.
8. Опубликовывать все вносимые изменения и проводить своевременное обучение персонала.

* * *

Резюмируя вышесказанное, подчеркнем, что безопасность беспроводных сетей имеет определенную специфику. На сегодня безопасная беспроводная сеть — вполне достижимая цель, требующая, однако, определенных финансовых вложений и, безусловно, высокой квалификации сотрудников, вовлеченных в ее организацию. ■

Рис. 7. Платы нелегальных беспроводных устройств

[3] MITM (Man-in-the-Middle), буквально — «человек посередине», т. н. «атака посредника». Вид атаки, когда злоумышленник, подключившись к каналу связи, осуществляет вмешательство в протокол передачи, перехватывает, удаляет или искажает информацию, подменяет сообщения, которыми обмениваются корреспонденты, причем никто из них не догадывается о присутствии в канале постороннего. — Прим. ред.