Воздушный патруль: измерения и защита беспроводной среды

Точки доступа не только раздают Wi-Fi, но и следят, чтобы вы не подцепили какую-нибудь «кибер-заразу».

Wi-Fi – это просто и удобно, поэтому беспроводные сети повсеместно используются в офисах и общественных местах. Однако за средой Wi-Fi нужно следить, чтобы обеспечивались должные параметры связи (уровень сигнала, доступность подключения), оптимизировать конфигурацию сети, оперативно устранять неполадки. Следить нужно и за безопасностью в сети Wi-Fi – во избежание несанкционированных подключений, DDoS-атак, утечек и других явлений, которые могут иметь самые неприятные последствия.

«СиБ» разбирался, как работают системы мониторинга и защиты сетей Wi-Fi и какие из них можно встретить в Украине.

Следим за качеством

Технологии контроля работы беспроводной сети существуют уже давно и хорошо известны. Одна из них – ***Cisco*** CleanAir, обеспечивающая обнаружение, идентификацию и выявление местоположения источников интерференции (как Wi-Fi, так и других) и уровень опасности от них. Система также умеет находить злонамеренные точки доступа, которые «прячутся» в смещенных частотных каналах или используют нестандартную модуляцию, тем самым CleanAir вносит свой вклад в защиту сети. Если источник интерференции полностью блокирует канал Wi-Fi, система переключается на другой. Также CleanAir запоминает существующие источники помех (микроволновки, беспроводные камеры и т.д.), эта информация может использоваться для оптимизации покрытия. «Индекс качества воздуха» графически отображает величину QoS на уровне радиомодуля, точки доступа, этажа, здания, кампуса, и при падении ниже заданного порога уведомляется администратор.

Система управления ***Aruba*** Airwave обеспечивает мониторинг состояния сети и в реальном времени выдает различные данные в виде инфографики: загруженность и правильность конфигурации сети, распределение трафика по пользователям, типам устройств и т.д., качество VoIP-услуг (MOS-оценка) и другие параметры. Система обнаруживает и наносит на карту подключенные устройства и создает топологическую схему соединений между точками доступа, контроллерами и коммутаторами, что позволяет оценивать влияние устройств друг на друга и находить причины проблем. Также AirWave ведет статистику успешности соединений. Инструмент VisualRF обеспечивает отображение в реальном времени плана помещения с наложением карты покрытия (**рис. 1**), что позволяет наблюдать расположение точек доступа, проблемные места и возможные точки интерференции, а дополнительные диаграммы демонстрируют пороговые значения трафика, загруженность каналов и другие параметры, тем самым можно быстро выявлять проблемное устройство, этаж или здание. Наконец, VisualRF может записывать перемещения устройств и клиентов в пределах покрытия для локализации проблемных мест.

Ruckus Networks, приобретенная в прошлом году компанией ***CommScope***, в составе своего беспроводного решения предлагает систему контроля Ruckus Network Director, которая ведет учет всех точек доступа в сети и с помощью графического интерфейса отображает их состояние. Облачный сервис Ruckus Analytics отслеживает показатели SLA и характеристики работы сети (например, среднее время и процент успешных соединений, продолжительность AP). Сервис автоматически определяет границы нормального поведения каждого элемента сети, впоследствии с помощью машинного обучения выявляются инциденты. Также система показывает, какие клиенты страдают из-за проблем в сети и как именно (медленные соединения, отключения и т.д.).

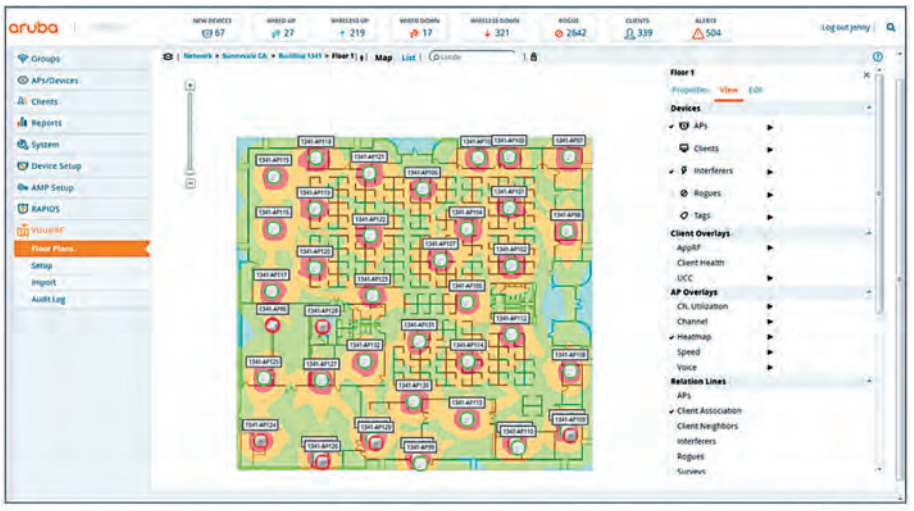

Рис. 1. Интерфейс Aruba AirWave – карта покрытия

Передается воздушным путем

Но можно и так сказать: лучше вообще никуда не подключиться, чем стать жертвой киберпреступников, орудующих в беспроводных сетях. Согласно исследованию ***Symantec***, опубликованному в 2017 году, 92% американцев потенциально подвергали риску свою персональную информацию, пользуясь публичными сетями Wi-Fi. Из них 62% заходили в свою электронную почту, 56% – в социальные сети, 32% – в банковское приложение (или иным способом просматривали финансовую информацию), 29% заходили на рабочую почту. 19% признались, что вводили данные, позволяющие их идентифицировать, такие как день рождения или номер социального страхования. 10% готовы раскрыть персональную информацию или разрешить доступ к своему списку контактов, чтобы получить сильный и бесплатный сигнал Wi-Fi. При этом почти 70% убеждены, что их персональным данным в сетях Wi-Fi ничто не угрожает, а 41% не могут сказать, в чем разница между защищенной сетью и незащищенной. Три четверти опрошенных знают о технологии VPN, но лишь 27% пользуются ею для защиты своих данных.

Другое исследование, проведенное в 2018 году компанией ***Spiceworks*** среди 500 специалистов сферы ИТ в США, показало, что в корпоративном секторе тоже не все ладно. 61% респондентов сообщили, что их сотрудники по работе подключаются к сетям Wi-Fi в кафе, отелях и аэропортах. Только 64% ответили, что персонал знает о рисках, связанных с сетями Wi-Fi, и примерно столько же сказали, что сотрудники пользуются VPN. При этом лишь половина респондентов уверена в защищенности данных, которые хранятся на пользовательских устройствах. 12% признались, что у них хотя бы раз имел место инцидент, связанный с публичной сетью Wi-Fi, еще 34% не знали, были у них взломы или нет, поскольку о многих инцидентах им вообще не известно.

Какие же угрозы подстерегают в сетях Wi-Fi? Они разнообразны – от примитивного подсматривания ввода логина и пароля до злонамеренных точек доступа, предназначенных для ловли незадачливых пользователей.

Самым распространенным типом угроз в сетях Wi-Fi называют атаки типа «человек посередине» (Man-in-the Middle, MitM), она же и самая опасная, поскольку ее нельзя отследить. В некоторых MitM-атаках может использоваться уязвимость протокола определения адреса ARP, преобразующего IP-адреса сети в MAC-адреса: злоумышленники рассылают спуфинговые ARP-ответы (без запроса), пытаясь убедить пользовательские устройства изменить свои таблицы. После этого IP-адреса отправителя и получателя оказываются привязаны к MAC-адресу «человека посередине», который фактически получает возможность перехватывать переписку между обеими сторонами, которые любезно предоставляют ему свои ключи шифрования. Таким образом можно воровать данные учетных записей, реквизиты банковских карт, личную переписку, интеллектуальную собственность. Также можно подделывать перехваченные сообщения – например, подменять реквизиты платежа.

Вариант той же схемы – атаки типа Evil Twin («злой близнец»), основанные на том, что пользовательское оборудование не может различить два радиосигнала, передающих одинаковые идентификаторы сети (SSID). Именно таким образом, как сообщал в 2018 году американский департамент юстиции, хакеры российского ГРУ атаковали ряд организаций: антидопинговые агентства в нескольких странах, компанию Westinghouse, которая поставляет ядерное топливо, в том числе в Украину, а также тестовую лабораторию в швейцарском Шпице, которая имела отношение к расследованию отравления Скрипалей, и Всемирную организацию по запрету химического оружия, где их и поймала полиция Нидерландов.

Хакеры ГРУ использовали популярный инструмент для пен-тестов – устройство Wi-Fi Pineapple, мощные антенны, батарею и LTE-модем. Оборудование размещалось в багажнике припаркованного автомобиля или в рюкзаке, с которым сотрудник заходил в здание (**рис. 2**). По мнению руководителя отдела исследований FireEye Джона Халквиста, которое приводит издание Wired, такая тактика говорит о нахальстве и агрессивности. «Делать это физически – рискованно и дерзко, – сказал Халтквист. – Конечно, есть вероятность быть пойманным и разоблаченным, но это открывает для них новые возможности для проникновения в сети, которые иначе могли быть затруднены».

Но вообще для атак Evil Twin можно обойтись даже без специализированного оборудования, используя обычный смартфон с возможностью раздачи Wi-Fi, который транслирует поддельный SSID. Расчет делается на то, что большинство клиентов Wi-Fi автоматически подключаются к сети, идентификатор которой они помнят. Если целью атаки является

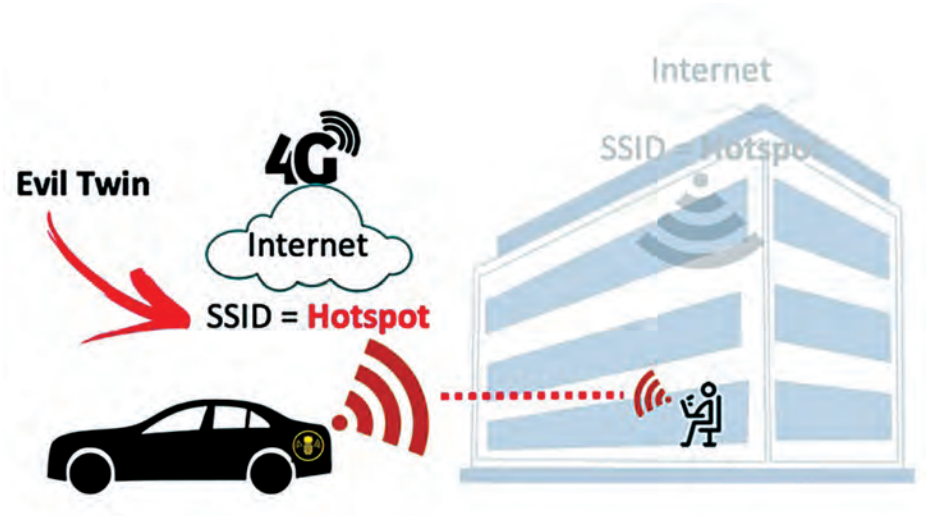

Рис. 2. Атака хакеров ГРУ с помощью Evil Twin (схема WatchGuard)

загруженная открытая сеть, жертвы подключаются к поддельной AP в течение нескольких секунд. Если же убедить пользовательское устройство перейти на фиктивную AP не удается, злоумышленники могут прибегнуть к деаутентификационной атаке, посылая поток поддельных сообщений о прерывании соединения.

MitM-атака может быть основана и на социальной инженерии. Злонамеренная точка доступа (Rogue AP) генерирует сигнал, который имитирует, например, легальную сеть отеля или кафе и ведет на портал авторизации, неотличимый от настоящей страницы. В примере, которые приводит компания ***Lookout***, такой портал предлагал пользователю загрузить поддельный сертификат для дальнейшего бесплатного пользования интернет-доступом, что в дальнейшем позволяло расшифровывать трафик Gmail и других приложений.

Чтобы был порядок

Защитой сетей Wi-Fi занимаются WIPS – системы предотвращения вторжений в беспроводную среду. WIPS сканируют радиочастоты, распознают злонамеренные и неверно сконфигурированные точки доступа, неавторизованные подключения, спуфинг MAC-адресов и другие нежелательные явления, а также пресекают их и/или извещают отдел безопасности. В простейшем случае WIPS представляет собой коробочное решение, для крупных организаций оно включает специализированные точки доступа (сенсоры), которые устанавливаются в защищаемых зонах и сканируют эфир.

WIPS предлагают производители как систем безопасности, так и оборудования беспроводного доступа. Gartner в обзоре систем предотвращения вторжений для проводных и беспроводных сетей за 2019 год относит к квадранту лидеров в этом направлении компании ***Cisco***, ***HPE*** (***Aruba***) и ***Extreme Networks***, в соседних квадрантах к ним близки ***Huawei***, ***Fortinet***, ***CommScope*** (***Ruckus Networks***) и ***Alcatel Lucent Enterprise***.

Как устроены беспроводные IPS, можно посмотреть на примере Aruba (подразделение HPE). У этого производителя точки доступа могут работать в трех режимах: обслуживания клиентов, радиомониторинга (AM) и спектрального мониторинга (SM). В последнем случае устройство только сканирует частоты и классифицирует нарушителей, тогда как в режиме AM оно может также их блокировать. Точки доступа также могут работать в гибридном режиме, сочетая обслуживание и сканирование. Лицензия RFProtect в составе операционной системы для мобильных контроллеров обеспечивает дополнительные функции мониторинга и блокирования нарушителей.

Инструмент RAPIDS, входящий в состав системы управления AirWave, обнаруживает злонамеренные AP на основе данных, полученных от собственных точек доступа. Кроме того, он сканирует сеть на предмет наличия сторонних AP, включенных в сеть через проводные интерфейсы, а также находит неавторизованные устройства за пределами зон покрытия (это делается с помощью приложения под Windows, после установки которого пользовательские устройства играют роль дополнительных сенсоров). Система автоматически ведет список авторизованных точек доступа, чтобы они не обозначались как злонамеренные.

RAPIDS классифицирует точки доступа и устройства на основе правил, по мере поступления новой информации статус может меняться. Например, если обнаружен слабый сигнал от соседской AP, она классифицируется как «предположительно сосед». Если эта точка доступа внезапно начинает излучать сильный сигнал, она переходит в категорию «предположительно Rogue AP», о чем извещается персонал. Если же затем будет выявлено, что AP включена в сеть через проводной интерфейс, ее переклассифицируют как «Rogue AP», что считается высшим уровнем угрозы и подлежит немедленному расследованию. Также возможна дополнительная градация угроз от 1 до 10.

Блокирование злонамеренных AP осуществляется вручную и автоматически. Если выявлено проводное подключение такой AP, соответствующий порт коммутатора отключается. Беспроводное блокирование происходит двумя способами. Точка доступа может форсировать деаунтификацию, посылая соответствующие пакеты чужой AP и клиентскому устройству. Поскольку большинство терминалов автоматически пытаются переподключиться к сети, AP рассылает эти пакеты регулярно (примерно каждые 15 мс). Метод увязания (pit-tarring, tar-pitting) состоит в том, что когда пользовательское устройство пытается переподключиться, «своя» точка доступа выдает ответ, которым пытается переключить его на фальшивый канал или SSID. В конце концов клиентское устройство осознает, что связь не работает (это может занять от 500 мс или даже потребовать вмешательства пользователя). Блокировка дает время персоналу физически удалить нарушителей.

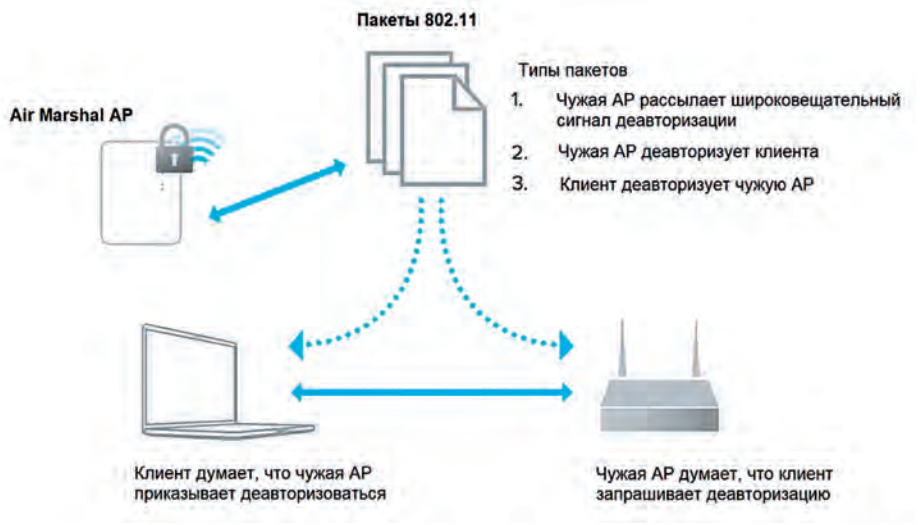

Рис. 3. Блокирование злонамеренных AP в Air Marshal

Правила блокировки тоже могут быть разными; например, в режиме «защита подтвержденных рабочих станций» сеть не позволяет устройствам, классифицированным как свои, подключаться к другим точкам доступа, что обеспечивает защиту важных данных. В режиме «защита SSID» автоматически блокируются все чужие AP, это оберегает пользователей от вредоносного оборудования (а также от ухудшения качества обслуживания при подключении к чужим сетям).

Cisco предлагает два решения для беспроводного доступа: Catalyst/Aeronet и Meraki, в каждом из которых реализована своя система предотвращения вторжений. В первой линейке она называется Cisco wIPS. В качестве сенсоров выступают точки доступа нескольких видов: локальные (обслуживают клиентов и проводят ограниченное сканирование), мониторинговые (непрерывное сканирование), локальные с wIPS-подобным локальным режимом (обслуживание клиентов с более продолжительным сканированием) и устройства с модулем беспроводной защиты (WSM), который берет на себя проверку эфира, тогда как сама AP работает с клиентами. На точках доступа можно включить генерацию файлов для расследования инцидентов (forensics).

Точки доступа Cisco Meraki либо обслуживают клиентов, при случае проводя сканирование на том же канале (можно также прописать обязательные сканы в заданное время суток), либо работают в режиме предотвращения вторжений – Air Marshal. Также есть устройства с дополнительным радиомодулем, выделенным для сканирования. Точки доступа выявляют злонамеренные AP в окрестностях, а также подключенные к проводным интерфейсам. Помимо этого, система отслеживает VIP-устройства, которые ни при каких условиях не должны подключаться к чужим AP, (корпоративные ноутбуки, POS-терминалы, сканеры штрихкодов и т.д.), и извещает персонал, если эти устройства начинают передавать пакеты, не находясь в корпоративной сети. Air Marshal блокирует Rogue APs с помощью разных вариантов деаутентификации: рассылкой сигнала от имени чужой AP широковещательно или по MAC-адресам устройств, либо же дополнительно могут рассылаться запросы деавторизации от имени клиента (**рис. 3**). Это гарантирует защиту и тех устройств, которые могут находиться в спящем режиме и игнорировать сообщения деавторизации от Rogue AP.

WatchGuard – производитель систем безопасности, известный, в том числе, решениями для защиты беспроводной среды. Концепция Trusted Wireless предполагает защиту от шести типов угроз (злонамеренные AP и клиенты; соседские AP и случайные подключения к ним клиентов; точки доступа типа Evil Twin; режим Ad-Hoc, когда подключенное к сети устройство раздает Wi-Fi другим и, как следствие, открывает им доступ к LAN; ошибки конфигурирования AP). В то же время добропорядочные сторонние точки доступа могут работать на той же территории. WatchGuard может предложить несколько точек доступа со встроенной функциональностью WIPS. Производитель особенно гордится тем, что в ходе испытаний, проведенных в прошлом году компанией ***Miercom***, точка доступа WatchGuarrd AP325 показала обнаружение и предотвращение 11 видов угроз.

WIPS-система компании ***Arista*** (в 2018 году купившей Mojo Networks, когда-то известную как AirTight) совмещает в себе функции собственно WIPS и контроллера. Система автоматически классифицирует обнаруженные беспроводные устройства как авторизованные, злонамеренные и внешние. В результате, как утверждается, администраторы избавлены от необходимости прописывать сложные правила и вручную проверять эти устройства, а также благодаря точности классификации можно автоматически блокировать нарушителей, не боясь помешать работе собственной или соседской сети. Система умеет вычислять местоположение нарушителей, а также сохраняет архивные данные о том, где посторонние устройства находились в прошлом. WIPS также отвечает за анализ эфира, выявление потенциальных проблем и их классификацию (неправильное распределение каналов, низкая скорость передачи данных и т.д.). Возможны несколько сценариев использования WIPS: например, как дополнительную систему безопасности поверх существующей сети Wi-Fi (кстати, то же самое предлагает и WatchGuard) или для обеспечения режима запрета Wi-Fi в режимных помещениях.

Вообще обнаруживать нарушителей так или иначе умеют все точки доступа. Простые советы, которые можно встретить в Интернете, таковы: изолировать гостевую сеть от корпоративной с помощью устройства доступа, транслирующего несколько SSID; шифровать трафик с помощью WPA2 или WPA3; своевременно обновлять прошивки; следить, чтобы точка доступа была включена только в рабочее время. А также – не полагаться на безопасность в публичных хотспотах, а использовать VPN. Не факт, что это полностью убережет, но жизнь злодеям усложнит.

Василий ТКАЧЕНКО, **СиБ**