УДК 004.7

Неучитываемые особенности и уязвимости Wi-Fi. Надежная и стабильная беспроводная сеть.

А. В. Иванов
Московский физико-технический институт (государственный университет), Москва, Россия

Проанализировано создание надежной и безопасной беспроводной сети. Речь идет о моментах, на которые следует обратить внимание при проектировании сети, рассказано об инструментах моделирования, типичных решениях топовых производителей, перспективных технологиях. При этом сделан упор на среду передачи — радиоволны, а также рассмотрены некоторые нюансы беспроводной технологии.

Ключевые слова: Wi-Fi, безопасность беспроводной сети, стабильная связь, CleanAir, AirDefense.

В настоящее время сети Wi-Fi распространены повсеместно и зачастую имеют огромные зоны покрытия, включающие целые районы городов. Технология прочно вошла нашу жизнь и поселилась во многих устройствах, начиная с мобильных телефонов и заканчивая холодильниками.

С точки зрения безопасности следует учитывать не только угрозы, свойственные любым, в том числе и проводным сетям, но также и среду передачи сигнала. В беспроводных сетях получить доступ к передаваемой информации проще, чем в проводных, равно как и повлиять на канал передачи данных.

Особенности беспроводной связи с точки зрения безопасности

Wi-Fi сети в сравнении с проводными сетями имеют ряд существенных отличий, о которых зачастую забывают.

В них нет «контролируемой среды» — кабеля, к которому можно приставить охрану через 5 метров и пропускать весь трафик через системы обнаружения и предотвращения вторжений IDS/IPS. Среда передачи — радиоволны, которые можно как принимать с мобильника, проходя мимо, так и глушить с помощью микроволновки. И размер зоны покрытия не позволяет окружить сеть забором, а еще лучше куполом.

За совсем небольшие деньги пользователь может купить маршрутизатор и развернуть Wi-Fi сеть «из коробки» с конфигурацией по-умолчанию, что является одной из наиболее распространенных угроз. При этом пользователи могут находиться в любой точке зоны покрытия, а беспроводные устройства видеть друг друга.

Исходя их этих и других причин, злоумышленникам гораздо удобнее атаковать именно Wi-Fi, чем проводные сети [1].

Невозможно построить аналог безопасной проводной сети. Однако можно максимально приблизиться к этому. Попробуем наметить первоочередные шаги, исходя из определяющего отличия — среды передачи.

Построение сети

Прежде всего, требуется выбрать производителя беспроводного оборудования. Флагманами являются Cisco, Motorola и Aruba Networks.

Cisco — лидер сетевой индустрии. Любое решение, построенное на Cisco, должно работать хорошо. Цена соответствующая. Типовая система — ряд точек доступа, трафик с которых передается на отдельный контроллер, который занимается дальнейшей обработкой пакетов.

Aruba Networks — один из основных конкурентов Cisco. Типовое решение отличается от последней размещением контроллера в облаке.

Решения от **Motorola** предполагают децентрализованность. Их точки доступа способны пропускать трафик через себя в соответствии с настройками, которые точки получают с контроллера. Есть режим работы, при котором контроллером становится одна из точек доступа, а при ее недоступности автоматически выбирается новая из оставшихся [2].

Есть и другие, например новичок на рынке Ubiquiti UniFi. Собственно разница между оборудованием различных производителей в собственных наработках и цене. Чем решение дешевле, тем больше его приходится допиливать напильником.

Иванов Александр Владимирович, студент 4 курса кафедра Защиты Информации.
E-mail: ksandrfreeman@rambler.ru

Статья поступила в редакцию 14 июня 2014 г.

Хотя это не относится напрямую к безопасности, некоторые моменты могут в критичный момент повлиять на работу сети самым неожиданным способом. Нужно удостовериться, что железо предназначено для работы в вашем регионе (обычно это указано в полном имени устройства, например, Motorola AP-0650-66030-EU относится к Европе). Могут потребоваться лицензии на подключения точек доступа к контроллеру и контракты на обновление прошивок (неудобно будет в запарке покупать возможность обновиться и закрыть новонайденную уязвимость). К тому же стандарт 802.1x не описывает взаимодействие между точками, и разные производители используют разные технологии, что может привести к некорректной работе с оборудованием других производителей или даже собственным оборудованием других типов.

Вот теперь начинается самое интересное. Нужно спроектировать саму сеть, ее конфигурацию, систему безопасности, политику.

Требуется провести радиообследование помещения, основываясь на плане здания, свойствах перекрытий, информации о соседних сетях. Поможет в этом среда моделирования, например **TamoGraph Site Survey** [3]. Требуется определить зоны покрытия, наличие интерференции (любой достаточно мощный источник, работающий в вашей частоте, доставит массу хлопот — микроволновка, например). Но моделирование не заменит реального обследования и тем более мониторинга уже работающей сети.

У **Cisco** есть технология CleanAir 2.0 [4] для выявления и обхода радиопомех. Кроме того, она предоставляет возможность мониторинга частотного спектра на предмет угроз информационной безопасности (атак типа DoS, пиратских точек доступа и т. д.).

А технология Cisco Rogue AP Containment позволяет гасить сигнал вражеских точек доступа. При этом снижается качество работы невалидной ТД до неудовлетворительного уровня — приходит около 10 % пакетов. Но возможность подключиться к «чужаку» все же остается. Может снижаться качество работы основной сети — заявлено снижение скорости до 20 %, на деле встречается и 50 % [5].

При составлении политики безопасности будет разумно:

- разделять права доступа не только по персональной идентификации, но и по таким признакам, как идентификация и текущее состояние устройства, время суток, местоположение пользователя;
- использовать динамические VLAN для упрощения взаимодействия пользователей с системой безопасности, для доступа к сервисам зон X и Y будет требоваться SSID-X(Y) и метод аутентификации X(Y);
- включить обеспечение безопасности мобильных устройств пользователей в общую систему безопасности (такие устройства постоянно появляются как внутри подконтрольной зоны, так и вне ее — высок риск того, что злоумышленники этим воспользуются);
- не разделять безопасность проводного и беспроводного сегментов (сеть едина, атаковать проводную сеть можно через беспроводную и наоборот, также это касается сбора статистики и вообще любой служебной информации о работе сети).

Motorola предлагает AirDefense Enterprise — систему предотвращения беспроводных вторжений с множеством интересных возможностей. Она состоит из центрального сервера, распределенных сенсоров, собирающих информацию и передающих ее на сервер и консоли администратора. Этого решение позволяет заниматься мониторингом сети, контролировать соблюдение заданных политик, а также защищать конечные устройства пользователей (антивирус, межсетевой экран, отслеживающее беспроводные события и конфигурацию телефона [6]).

Кроме того, система включает в себя:

- Обнаружение чужаков. С помощью нерезглашаемого алгоритма система находит неавторизированные подключения, и основываясь на планах защищаемых помещений(включая характеристики перекрытий) выясняет физическое местонахождение нарушителя. Дальше им занимаются специально обученные люди. Также можно вести историю перемещений.
- Автоматизированная защита. Система умеет блокировать неавторизированные подключения как в беспроводном сегменте, так и в проводном. В отличии от Cisco, Motorola может точечно блокировать коммуникации и попытки ассоциаций с устройством.
- Инструментарий аналитики и расследования инцидентов. Система хранит историю за несколько месяцев и может предъявить ход событий с шагом в минуту.
- Диагностика состояния сети и помощь в устранении проблем. Система собирает огромное количество информации, которое используется для обнаружения перегруженных каналов, неправильно сконфигурированных устройств и т. п.

За вами остается настройка командного центра и точек доступа. На этом почти все. Нужно уделить внимание некоторым нюансам.

Нюансы

От выбранной скорости зависит зона и форма покрытия. На более высоких скоростях чувствительность приемника меньше. А на низких скоростях можно подключиться с большего расстояния, если появилось низкоскоростное подключение — скорее всего кто-то пытается пробиться извне. К тому же служебная и широковещательная информация отправляются на минимальной разрешенной скорости. Низкие скорости разумно отключить, дабы не давать злоумышленникам возможность сбора информации с ближайшей сопки.

Кроме того, сеть должна быть стабильной. Не имея возможности нормально посмотреть котиков через свою сеть, сотрудники будут подключаться к соседним доступным точкам доступа. И вся безопасность полетит к чертям.

Возможно, потребуется снизить мощности точек доступа для более стабильной связи – не только сигнал точки доступа должен достичь клиента, но и сигнал клиента должен достичь точки. Типичная ситуация: мощность Wi-Fi клиентов в районе — 40 мВт, а точек доступа — 100мВт. Клиент видит сеть, она у него неплохо ловится, но сам он не может до нее достучаться.

Также далеко не самым известным фактом является то, что у большинства клиентских устройств мощность передатчика снижена на «крайних» каналах, чтобы не задевать соседние диапазоны. Если клиентские устройства будут плохо ловить, требуется перейти на другие каналы [7].

«Непересекающиеся» каналы 1/6/11 все же пересекаются:

1/6 и 6/11 — на ~ –20 dB;
1/11 — на ~ –36 dB;
1/13 — на ~ –45 dB.

Технология широкополосная, и полностью удержать сигнал в рамках полосы в 22 МГц невозможно. Попытка поставить две точки доступа, настроенные на соседние «неперекрывающиеся» каналы, близко друг от друга приведет к тому, что каждая из них будет создавать соседке серьезные помехи. Такой шум способен целиком забить любой полезный Wi-Fi сигнал из соседней комнаты, или блокировать ваши коммуникации целиком. Не следует ставить точки слишком близко друг с другом в желании максимально качественного покрытия.

Существуют режимы совместимости b-g (ERP Protection) и a/g-n (HT Protection). В обоих режимах работы скорость падает. Если у вас сеть построена на 802,11n, а у соседа на 802,11g, и его трафик долетает до вас, то ваша точка упадет в режим совместимости — того требует стандарт. Либо отключаем такой режим, либо уговариваем владельца соседней сети.

Это далеко не все особенности, но их описание потребуют еще не одну статью. Так что стандарты нам в помощь.

Выводы

Сети Wi-Fi существенно отличаются от проводных и обладают рядом непривычных особенностей. Требуется применять комплексные и продуманные методы построения и защиты стабильной безопасной сети и при этом не влиять на функционирование соседних сетей, даже если их активность подозрительна. Cisco и Motorola предлагают инструменты для защиты, средства мониторинга и администрирования, но они не являются панацеей. Без грамотного планирования, без учета множества нюансов ничего не выйдет. И даже в таком случае мы не получим абсолютно защищенную сеть, лишь приблизимся к уровню защиты проводной. Но отказаться от беспроводных сетей немыслимо, ибо достоинства с лихвой перекрывают недостатки.

Литература

1. *Белорусов Д. И., Корешков М. С.* WiFi-сети и угрозы информационной безопасности. // Специальная техника. — 2009. № 6. — 4 с.

2. Оптимальная производительность беспроводных сетей // MotorolaSolutions.com: портал. URL: http://www.motorolasolutions.com/RU-RU/Business+Solutions/Technologies/Wireless+IP+Networks/WiNG+5+WLAN+Solutions (дата обращения: 24.06.2014).

3. Планирование и обслуживание Wi-Fi сетей // TamoGraph Site Survey: сайт. URL: http://www.tamos.ru/ products/wifi-site-survey (дата обращения: 24.06.2014).

4. Технология Cisco CleanAir // Cisco.com : портал. URL: http://www.cisco.com/web/RU/downloads/broch/Cisco-CleanAir-RUS.pdf (дата обращения: 24.06.2014).

5. Rogue Management in a Unified Wireless Network // Cisco.com: портал. URL: http://www.cisco.com/c/en/us/sup-port/ docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html (дата обращения: 24.06.2014).

6. *Бандурян А.* Motorola AirDefense Enterprise // Компьютерное обозрение. 2010. № 12. URL: http://ko.com.ua /motorola_airdefense_enterprise_49016 (дата обращения: 24.06.2014).

7. Iphone Test Report Fcc // Appleinsider.com: портал. URL: http://images.appleinsider.com/iphone-test-report-fcc-4.pdf (дата обращения: 24.06.2014).

Unregarded features and vulnerability of Wi-Fi. Reliable and stable wireless network

A. V. Ivanov
Moscow Institute of Physics and Technology (State University), Moscow, Russia

This article is devoted to the creation of safe and secure wireless network. It is a matter of the moments that should pay attention in the course of network design, about the modeling tools, the typical solutions of top manufacturers, perspective technologies. Emphasis is thus placed on the medium — radio waves, and also reported about some nuances of wireless technology.

Keywords: Wi-Fi, wireless network security, stable connection, CleanAir, AirDefense.

Bibliography — 7 references. *Received June 14, 2014*