УДК 62

ПОДХОД К БЕЗОПАСНОСТИ СЕТИ Wi-Fi

Лобанов Анатолий Анатольевич
магистрант
Сибирский государственный университет телекоммуникаций
и информатики, Новосибирск
lobanov.anatoly54@gmail.com

Аннотация. В последнее время появилось много «разоблачающих» публикаций о взломе какого-либо очередного протокола или технологии, компрометирующего безопасность беспроводных сетей. Так ли это на самом деле, чего стоит бояться, и как сделать, чтобы доступ в вашу сеть был максимально защищен? Данный обзор поможет свести воедино все применяющиеся технологии шифрования и авторизации радио-доступа. Попробуем показать, что правильно настроенная беспроводная сеть представляет собой непреодолимый барьер для злоумышленника (до известного предела, конечно).

Ключевые слова: безопасность; информация; Wi-Fi; беспроводная сеть.

APPROACH TO SAFETY OF THE Wi-Fi NETWORK

Lobanov Anatoly Anatolyevich
undergraduate
Siberian state university of telecommunications and informatics
Novosibirsk

Abstract. Recently there were many «exposing» publications about breaking of any next protocol or the technology, compromising safety of wireless networks. Whether so it actually of that it is worth being afraid and how to make that access to your network was most protected? This review will help to bring together all being applied technologies of enciphering and radio access authorization. Let's try to show that correctly adjusted wireless network represents an insuperable barrier to the malefactor (to a known limit, certainly).

Key words: safety; information; Wi-Fi; wireless network.

Основы.

Что же теоретически может получить злоумышленник в беспроводной сети, настройке которой не было уделено должного внимания? Далее приведен примерный список:

- доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через неё – и к ресурсам LAN;
- подслушивание трафика, извлечение из него конфиденциальной информации;
- искажение проходящей в сети информации;
- воровство интернет-траффика;
- атака на ПК пользователей и серверы сети (например, Denial of Service или даже глушение радиосвязи);
- внедрение поддельной точки доступа;
- рассылка спама, противоправная деятельность от имени вашей сети.

Любое взаимодействие точки доступа (сети), и беспроводного клиента, построено на следующем:

Аутентификации – как клиент и точка доступа представляются друг другу и подтверждают, что у них есть право общаться между собой;

Шифровании – какой алгоритм скремблирования передаваемых данных применяется, как генерируется ключ шифрования, и когда он меняется.

Параметры беспроводной сети, в первую очередь ее имя (SSID), регулярно анонсируются точкой доступа в широковещательных beacon пакетах. Помимо ожидаемых настроек безопасности, передаются пожелания по QoS, по параметрам 802.11n, поддерживаемых скорости, сведения о других соседях и прочее. Аутентификация определяет, как клиент представляется точке. Возможные варианты:

- **Open** – так называемая открытая сеть, в которой все подключаемые устройства авторизованы сразу;
- **Shared** – подлинность подключаемого устройства должна быть проверена ключом / паролем;
- **EAP** – подлинность подключаемого устройства должна быть проверена по протоколу EAP внешним сервером.

Открытость сети не означает, что любой желающий сможет с ней работать. Чтобы передавать в такой сети данные, необходимо совпадение применяющегося алгоритма шифрования, и соответственно ему корректное установление шифрованного соединения.

Алгоритмы шифрования таковы:

- **None** – отсутствие шифрования, данные передаются в открытом виде;
- **WEP** – основанный на алгоритме RC4 шифр с разной длиной статического или динамического ключа (64 или 128 бит);
- **CKIP** – проприетарная замена WEP от Cisco, ранний вариант TKIP;
- **TKIP** – улучшенная замена WEP с дополнительными проверками и защитой;
- **AES/CCMP** – наиболее совершенный алгоритм, основанный на AES256 с дополнительными проверками и защитой.

Комбинация **Open Authentication, No Encryption** широко используется в системах гостевого доступа вроде предоставления Интернета в кафе или гостинице. Для подключения нужно знать только имя беспроводной сети. Зачастую такое подключение комбинируется с дополнительной проверкой на Captive Portal путем редиректа пользовательского HTTP-запроса на дополнительную страницу, на которой можно запросить подтверждение (логин-пароль, согласие с правилами и т.п).

Шифрование **WEP** скомпрометировано, и использовать его нельзя (даже в случае динамических ключей).

Широко встречающиеся термины **WPA** и **WPA2** определяют, фактически, алгоритм шифрования (TKIP либо AES). В силу того, что уже довольно давно клиентские адаптеры поддерживают WPA2 (AES), применять шифрование по алгоритму TKIP нет смысла.

Разница между **WPA2 Personal** и **WPA2 Enterprise** состоит в том, откуда берутся ключи шифрования, используемые в механике алгоритма AES. Для частных (домашних, мелких) применений используется статический ключ (пароль, кодовое слово, PSK (Pre-Shared Key)) минимальной длиной 8 символов, которое задается в настройках точки доступа, и у всех клиентов данной беспроводной сети одинаково. Компрометация такого ключа (сказали другу, уволен сотрудник, украден ноутбук) требует немедленной смены пароля у всех оставшихся пользователей, что реалистично только в случае небольшого их числа. Для корпоративных применений, как следует из названия, используется динамический ключ, индивидуальный для каждого работающего клиента в данный момент. Этот ключ может периодический обновляться по ходу работы без разрыва соединения, и за его генерацию отвечает дополнительный компонент – сервер авторизации, и чаще всего это RADIUS-сервер.

Если с WPA2 Personal (WPA2 PSK) всё достаточно просто, то корпоративное решение требует дополнительного рассмотрения (рис. 1).

Таблица 1

Все возможные параметры безопасности

Свойство	Статический WEP	Динамический WEP	WPA	WPA 2 (Enterprise)
Идентификация	Пользователь, компьютер, карта WLAN	Пользователь, компьютер	Пользователь, компьютер	Пользователь, компьютер
Авторизация	Общий ключ	EAP	EAP или общий ключ	EAP или общий ключ
Целостность	32-bit Integrity Check Value (ICV)	32-bit ICV	64-bit Message Integrity Code (MIC)	CRT/CBC-MAC (Counter mode Cipher Block Chaining Auth Code – CCM) Part of AES
Шифрование	Статический ключ	Сессионный ключ	Попакетный ключ через TKIP	CCMP (AES)
Распределение ключей	Однократное, вручную	Сегмент Pairwise Master Key (PMK)	Производное от PMK	Производное от PMK
Вектор инициализации	Текст, 24 бита	Текст, 24 бита	Расширенный вектор, 65 бит	48-бит номер пакета (PN)
Алгоритм	RC4	RC4	RC4	AES
Длина ключа, бит	64/128	64/128	128	до 256
Требуемая инфраструктура	Нет	RADIUS	RADIUS	RADIUS

WPA2 Enterprise.

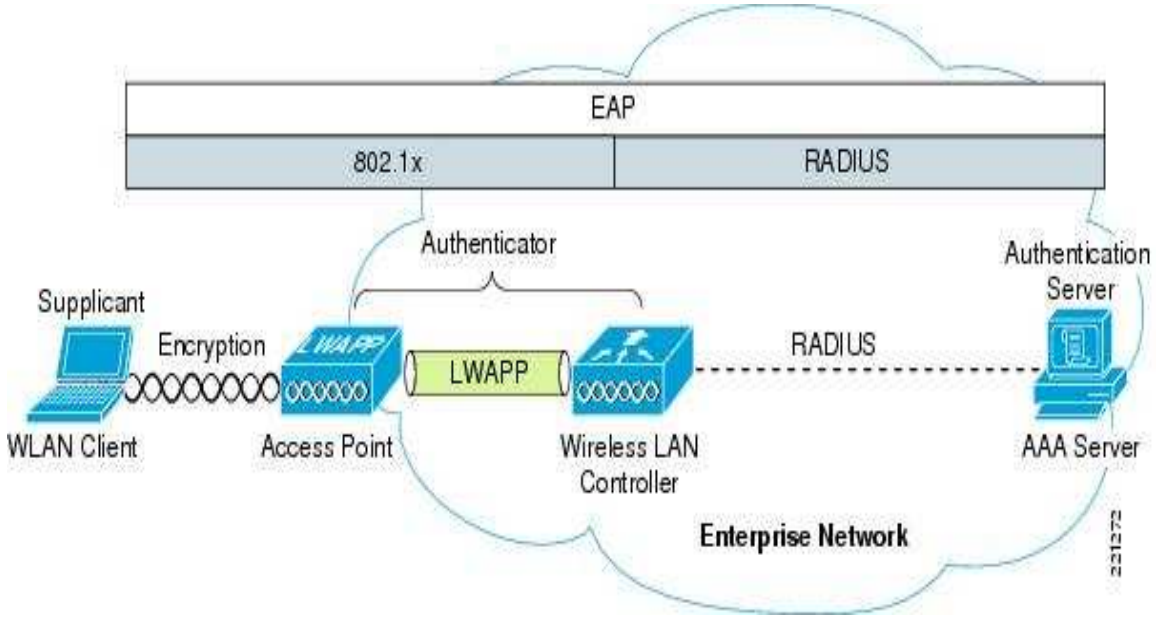

Рисунок 1. WPA2 Enterprise

Здесь мы имеем дело с дополнительным набором различных протоколов. На стороне клиента специальный компонент программного обеспечения, supplicant (обычно часть ОС) взаимодействует с авторизующей частью, AAA сервером. В данном примере отображена работа унифицированной радиосети, построенной на легковесных точках доступа и контроллере. В случае использования точек доступа «с интеллектом» всю роль посредника между клиентов и сервером может на себя взять сама точка. При этом данные клиентского суппликанта по радио передаются сформированными в протокол 802.1x (EAPOL), а на стороне контроллера они оборачиваются в RADIUS-пакеты.

Применение механизма авторизации EAP в сети приводит к тому, что после успешной (почти наверняка открытой) аутентификации клиента точкой доступа (совместно с контроллером, если он есть) последняя просит клиента авторизоваться (подтвердить свои полномочия) у инфраструктурного RADIUS-сервера (рис. 2):

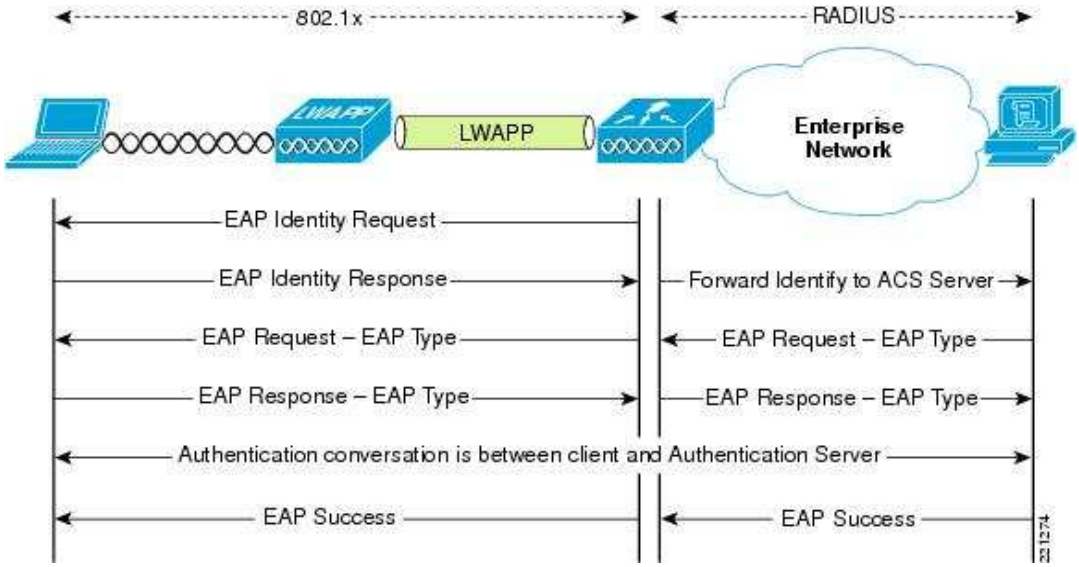

Рисунок 2. Механизм авторизации EAP

Использование **WPA2 Enterprise** требует наличия в сети RADIUS-сервера. На сегодняшний момент наиболее работоспособными являются следующие продукты:

- **Microsoft Network Policy Server (NPS), бывший IAS** – конфигурируется через MMC, бесплатен, но необходимо приобрести Microsoft Windows;
- **Cisco Secure Access Control Server (ACS) 4.2, 5.3** – конфигурируется через веб-интерфейс, имеет широкий функционал, позволяет создавать распределенные и отказоустойчивые системы;

- **FreeRADIUS** – бесплатен, конфигурируется текстовыми конфигами, в управлении и мониторинге не совсем удобен
- **Juniper Steel-Belted Radius Enterprise Edition:**

– Расширенное управление сетью: определяет и помогает устанавливать, кто может подключаться к сети, когда и на какой период времени. Стандартизирует и внедряет унифицированную проверку подлинности и обеспечения безопасности сети. Внедряет эффективные средства контроля за пользователями и их доступом к сети.
– Полная совместимость в гетерогенных средах: обеспечивает контроль AAA практически для всех типов и методов развертывания сетей. Обеспечивает поддержку кросс-платформенных развертываний, с применением устройств различных производителей и методов множественной проверки подлинности. Беспрепятственно взаимодействует со всеми популярными хранилищами учетных данных пользователей.
– Централизация проверки подлинности и управления: централизация проверки подлинности пользователей и управления упрощает процедуры и обеспечивают расширенную защиту сетей, а также соблюдение корпоративных политик безопасности.
– Защита инвестиций в сетевую инфраструктуру: беспрепятственно взаимодействует с оборудованием сетевого доступа, независимо от применяемых стандартов и производителей оборудования.
– Удобное конфигурирование, администрирование и техническое обслуживание: Такие функции, как интерфейс управления на основе браузера, централизованное администрирование и репликация упрощают конфигурирование и техническое обслуживание, уменьшая вероятность ошибок конфигурирования. Это дает возможность быстрее подключать к сети устройства и пользователей.
– Безопасные подключения: защищает учетные записи пользователей и данные, предотвращая несанкционированное отслеживание обмена данными в беспроводных сетях и другие атаки, одновременно соблюдая требования, предъявляемые наиболее загруженными сетями.
– Непревзойденная надежность: обеспечивает абсолютно надежную работу с минимальными простоями и потерями производительности, что повышает рентабельность инвестиций.

При этом контроллер внимательно наблюдает за происходящим обменом информацией, и дожидается успешной авторизации, либо отказа в ней. При успехе RADIUS-сервер способен передать точке доступа дополнительные параметры (например, в какой VLAN поместить абонента, какой ему присвоить IP-адрес, QoS профиль и т.п.). В завершении обмена RADIUS-сервер дает возможность клиенту и точке доступа сгенерировать и обменяться ключами шифрования (индивидуальными, валидными только для данной сессии) (рис. 3):

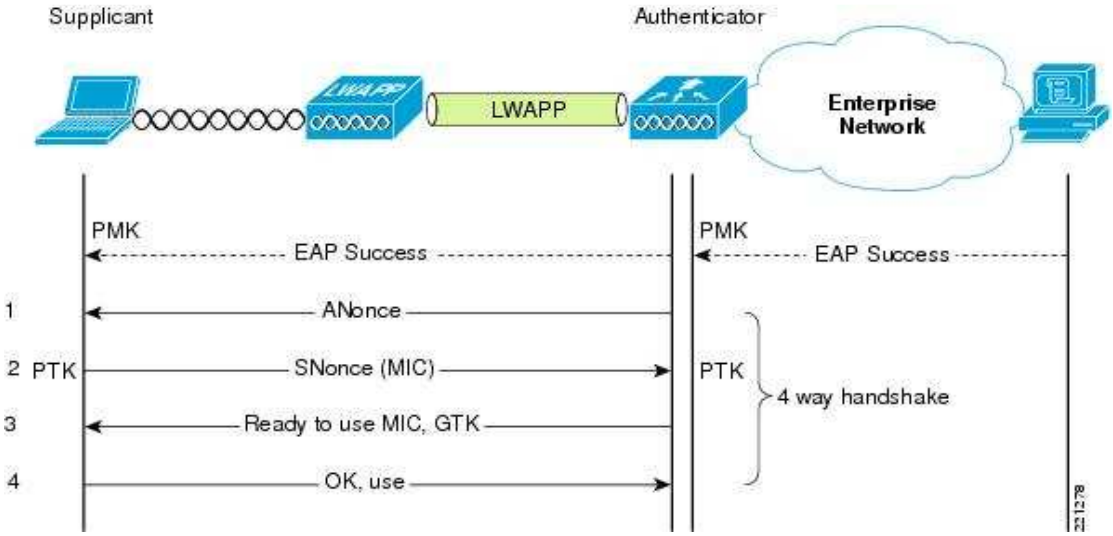

Рисунок 3. Алгоритм авторизации с участием RADIUS-сервера EAP

Сам протокол EAP является контейнерным, то есть фактический механизм авторизации дается на откуп внутренних протоколов. На настоящий момент значимое распространение получили следующие:

– **EAP-FAST** (Flexible Authentication via Secure Tunneling) – разработан фирмой Cisco. Позволяет проводить авторизацию по логину-паролю, передаваемому внутри TLS туннеля между суппликантом и RADIUS-сервером;

– **EAP-TLS** (Transport Layer Security). Использует инфраструктуру открытых ключей (PKI) для авторизации клиента и сервера (суппликанта и RADIUS-сервера) через сертификаты, выписанные доверенным удостоверяющим центром (CA). Требует выписывания и установки клиентских сертификатов на каждое беспроводное устройство, поэтому подходит только для управляемой корпоративной среды. Сервер сертификатов Windows имеет средства, позволяющие клиенту самостоятельно генерировать себе сертификат, если клиент – член домена. Блокирование

клиента легко производится отзывом его сертификата (либо через учетные записи);

– **EAP-TTLS** (Tunneled Transport Layer Security) аналогичен EAP-TLS, но при создании туннеля не требуется клиентский сертификат. В таком туннеле, аналогичном SSL-соединению браузера, производится дополнительная авторизация (по паролю или другим способом);

– **PEAP-MSCHAPv2** (Protected EAP) – схож с EAP-TTLS в плане изначального установления шифрованного TLS туннеля между клиентом и сервером, требующего серверного сертификата. В дальнейшем в таком туннеле происходит авторизация по известному протоколу MSCHAPv2;

– **PEAP-GTC** (Generic Token Card) – аналогично предыдущему, но требует карт одноразовых паролей (и соответствующей инфраструктуры).

Все эти методы (кроме EAP-FAST) требуют наличия сертификата сервера (на RADIUS-сервере), выписанного удостоверяющим центром (CA). При этом сам сертификат CA должен присутствовать на устройстве клиента в группе доверенных (что нетрудно реализовать средствами групповой политики в Windows). Дополнительно, EAP-TLS требует индивидуального клиентского сертификата. Проверка подлинности клиента осуществляется как по цифровой подписи, так (опционально) по сравнению предоставленного клиентом RADIUS-серверу сертификата с тем, что сервер извлек из PKI-инфраструктуры (Active Directory).

Поддержка любого из EAP методов должна обеспечиваться суппликантом на стороне клиента. Стандартный, встроенный в Windows XP/Vista/7, iOS, Android обеспечивает как минимум EAP-TLS, и EAP-MSCHAPv2, что обуславливает популярность этих методов. С клиентскими адаптерами Intel под Windows поставляется утилита ProSet, расширяющая доступный список. Это же делает Cisco AnyConnect Client.

Насколько это надежно?

Итак, что же нужно злоумышленнику, чтобы взломать вашу сеть? Для Open Authentication, No Encryption – ничего. Достаточно подключиться к сети и всё. Поскольку радиосреда открыта, сигнал распространяется в разные стороны, заблокировать его непросто. При наличии соответствующих клиентских адаптеров, позволяющих прослушивать эфир, сетевой трафик виден так же, как будто атакующая сторона подключилась в провод, в хаб, в SPAN-порт коммутатора.

Рисунок 4. Окно Cisco AnyConnect Client

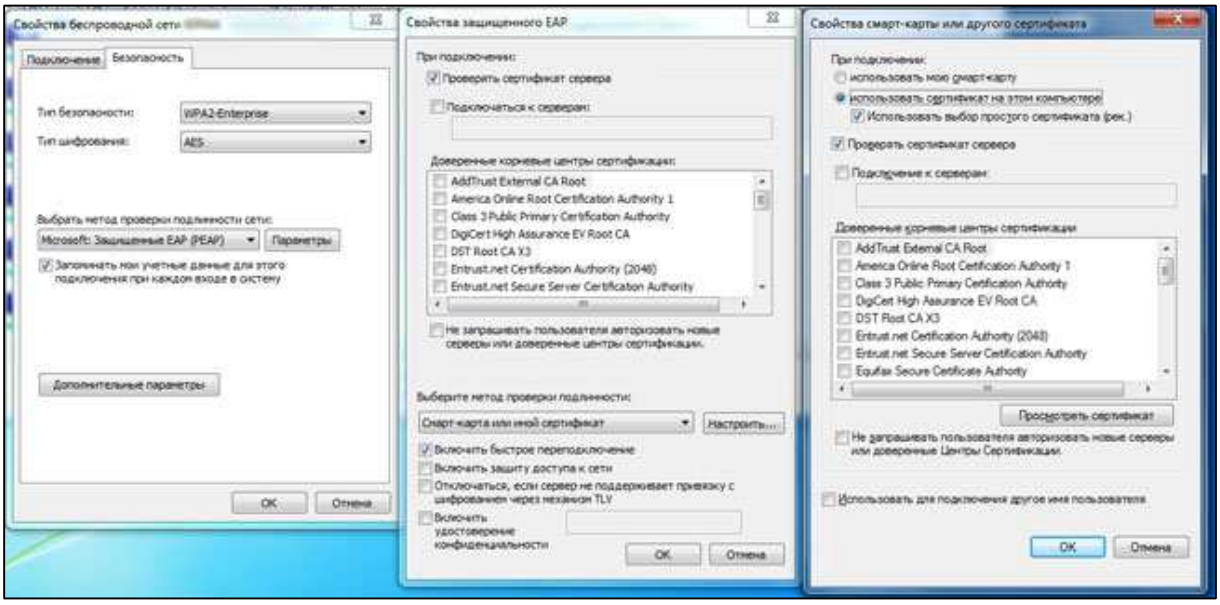

Рисунок 5. Окна настроек беспроводных сетей в MS Windows 7

Для шифрования, основанного на WEP, требуется только время на перебор и одна из многих свободно доступных утилит сканирования.

Для шифрования, основанного на TKIP либо AES прямое дешифрование возможно в теории, но на практике случаи взлома не встречались. Можно попробовать подобрать ключ PSK, либо пароль к одному из EAP-методов. Распространенные атаки на данные методы не известны.

Получить доступ к сети, защищенной EAP-FAST, EAP-TTLS, PEAP-MSCHAPv2 можно, только зная логин-пароль пользователя (взлом как таковой невозможен). Атаки типа перебора пароля, или направленные

на уязвимости в MSCHAP также не возможны либо затруднены из-за того, что EAP-канал «клиент-сервер» защищен шифрованным туннелем.

Доступ к сети, закрытой PEAP-GTC возможен либо при взломе сервера токенов, либо при краже токена вместе с его паролем.

Доступ к сети, закрытой EAP-TLS возможен при краже пользовательского сертификата (вместе с его приватным ключом, конечно), либо при выписывании валидного, но подставного сертификата. Такое возможно только при компрометации удостоверяющего центра, который в нормальных компаниях берегут как самый ценный IT-ресурс.

Поскольку все вышеозначенные методы (кроме PEAP-GTC) допускают сохранение (кэширование) паролей/сертификатов, то при краже мобильного устройства атакующий получает полный доступ без лишних вопросов со стороны сети. В качестве меры предотвращения может служить полное шифрование жесткого диска с запросом пароля при включении устройства.

Таким образом, на сегодняшний день у обычных пользователей и администраторов сетей имеются все необходимые средства для надёжной защиты Wi-Fi, и при отсутствии явных ошибок (пресловутый человеческий фактор) всегда можно обеспечить уровень безопасности, соответствующий ценности информации, находящейся в такой сети. Основные же правила при организации и настройке частной Wi-Fi-сети (если нет задачи сделать её общедоступной) таковы:

1. Максимальный уровень безопасности обеспечит применение VPN – эту технологию следует использовать в корпоративных сетях.
2. Если есть возможность использовать 802.1X (например, точка доступа поддерживает, имеется RADIUS-сервер) – ей следует воспользоваться (впрочем, уязвимости есть и у 802.1X).
3. Перед покупкой сетевых устройств внимательно ознакомиться с документацией. Узнать, какие протоколы или технологии шифрования ими поддерживаются. Проверить, поддерживает ли эти технологии шифрования ваша ОС. Если нет, то скачайте апдейты на сайте разработчика. Если ряд технологий не поддерживается со стороны ОС, то это должно поддерживаться на уровне драйверов.
4. Обратить внимание на устройства, использующие WPA2 и 802.11i, поскольку в этом стандарте для обеспечения безопасности используется новый Advanced Encryption Standard (AES).

5. Если точка доступа позволяет запрещать доступ к своим настройкам с помощью беспроводного подключения, то использовать эту возможность. Настраивать AP только по проводам. Не стоит использовать по радио протокол SNMP, web-интерфейс и telnet.
6. Если точка доступа позволяет управлять доступом клиентов по MAC-адресам (Media Access Control, в настройках может называться Access List), использовать эту возможность. Хотя MAC-адрес и можно подменить, тем не менее это дополнительный барьер на пути злоумышленника.
7. Если оборудование позволяет запретить трансляцию в эфир идентификатора SSID, использовать эту возможность (опция может называться «closed network»), но и в этом случае SSID может быть перехвачен при подключении легитимного клиента.
8. Запретить доступ для клиентов с SSID по умолчанию «ANY», если оборудование позволяет это делать. Не следует использовать в своих сетях простые SSID – стоит придумать что-нибудь уникальное, не завязанное на название организации и отсутствующее в словарях. Впрочем, SSID не шифруется и может быть легко перехвачен (или подсмотрен на ПК клиента).
9. Располагать антенны как можно дальше от окон, внешних стен здания, а также ограничивайте мощность радиоизлучения, чтобы снизить вероятность подключения «с улицы». Использовать направленные антенны, не использовать радиоканал по умолчанию.
10. Всегда использовать максимально длинные ключи. 128-бит – это минимум (но если в сети есть карты 40/64 бит, то в этом случае с ними вы не сможете соединиться). Никогда не прописывайте в настройках простые, «дефолтные» или очевидные ключи и пароли (день рождения, 12345), периодически их меняйте (в настройках обычно имеется удобный выбор из четырёх заранее заданных ключей – сообщите клиентам о том, в какой день недели какой ключ используется).
11. Не давать никому информации о том, каким образом и с какими паролями вы подключаетесь (если используются пароли). Искажение данных или их воровство, а также прослушивание траффика путем внедрения в передаваемый поток – очень трудоемкая задача при условиях, что применяются длинные динамически изменяющиеся ключи. Поэтому хакерам проще использовать человеческий фактор.

12. Если используются статические ключи и пароли, стоит позаботиться об их частой смене. Делать это лучше одному человеку – администратору.
13. Обязательно использовать сложный пароль для доступа к настройкам точки доступа.
14. По возможности не использовать в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее. Нецелесообразно разрешать гостевой доступ к ресурсам общего доступа.
15. По возможности не использовать в беспроводной сети DHCP – вручную распределить статические IP-адреса между легитимными клиентами намного безопаснее.
16. На всех ПК внутри беспроводной сети установить файерволлы, не устанавливать точку доступа вне брандмауэра, использовать минимум протоколов внутри WLAN (например, только HTTP и SMTP). Дело в том, что в корпоративных сетях файерволл стоит обычно один – на выходе в интернет, взломщик же, получивший доступ через Wi-Fi, может попасть в LAN, минуя корпоративный файерволл.
17. Регулярно исследовать уязвимости своей сети с помощью специализированных сканеров безопасности (в том числе хакерских типа NetStumbler), обновлять прошивки и драйвера устройств, устанавливать обновления для ОС.

Список использованных источников

1. URL:http://habrahabr.ru
2. URL:http://www.juniper.net
3. URL:http://www.cisco.com
4. URL:http://www.oszone.net
5. URL:http://ru.wikipedia.org
6. URL:http://www.wi-fi.ru

Впервые данная статья была опубликована в сборнике материалов IV Международной научно-практической конференции «Теория и практика актуальных исследований» (15 мая 2013 г., Краснодар).