Соколов Никита Дмитриевич,

студент III курса, ОГАПОУ «УАвиаК-МЦК»,

г. Ульяновск

Руководитель ***Зорина М.А.,***

преподаватель ОГАПОУ «УАвиаК-МЦК», г. Ульяновск

БЕЗОПАСНОСТЬ СЕТИ Wi-Fi: МИФ ИЛИ РЕАЛЬНОСТЬ?

Актуальность. На сегодняшний день все больше и больше появляется «разоблачающих» публикаций о взломе какого-либо очередного протокола или технологии, компрометирующего безопасность беспроводных сетей Wi-Fi. Но, так ли это на самом деле и чего стоит бояться, а также как сделать, чтобы доступ в вашу сеть был максимально защищен? Подготовленный обзор поможет свести воедино все применяющиеся на сегодня технологии шифрования и авторизации радиодоступа. В данной работе мы постарались показать, что правильно настроенная беспроводная сеть представляет собой непреодолимый барьер для злоумышленника.

Цель. Создать основные правила по организации и настройке частной Wi-Fi-сети, для защиты от хакерского взлома.

Для начала ознакомимся со списком возможных информационных похищений в беспроводной сети Wi-Fi, настройке которой не было уделено должного внимания:

- доступ к ресурсам LAN, через диски и ресурсы пользователя Wi-Fi-сети;
- подслушивание трафика, которое ведет к извлечению из него всей информации;
- сеть информации проходит искаженной;

• интернет-траффик «уходит» в чужие руки, так сказать происходит его воровство;

• серверы сети и ПК пользователей оказываются под атакой злоумышленников (например: Denial of Service, глушение радиосвязи);

• организуется поддельная точка доступа и ее внедрение;

• от имени вашей сети происходит противоправная деятельность, рассылка спама.

Всякое взаимодействие точки доступа (сети) и беспроводного клиента, построено на аутентификации и шифровании. Разберемся более детально.

Аутентификация – есть право общения между собой клиента и точки доступа с подтверждением.

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

Параметры беспроводной сети, а именно ее имя (SSID), постоянно анонсируются точкой доступа в широковещательных beacon пакетах. Кроме ожидаемых настроек безопасности, передаются пожелания по QoS, по параметрам 802.11n, поддерживаемых скорости, сведения о других соседях и многое другое. А как клиент представляется точке, определяет аутентификация. Рассмотрим возможные варианты:

• Open – открытая сеть, в ней все подключенные устройства авторизованы одновременно;

• Shared – ключом или паролем проверяется подлинность подключаемого устройства;

• EAP – по протоколу EAP внешним сервером должна быть проверена подлинность подключаемого устройства.

Открытость сети не значит, 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. Таковы алгоритмы шифрования:

- None – данные передаются в открытом виде, здесь отсутствует шифрование;
- WEP – имеется разная длина статического или динамического ключа (64 или 128 бит), он основан на алгоритме RC4;
- CKIP – это ранний вариант TKIP, является проприетарной заменой WEP от Cisco;
- TKIP – дополнительные проверки и защита, является улучшенной заменой WEP;
- AES/CCMP – дополнительные проверки и защита, но наиболее совершенный алгоритм, основанный на AES256.

В гостинице, в кафе Интернет предоставляется в системе гостевого доступа, а комбинация Open Authentication, No Encryption там широко используется. Чтобы подключиться к беспроводной сети и имени будет достаточно. Любое подключение комбинируется с дополнительной проверкой на Captive Portal. Где можно запросить подтверждение (логин-пароль, согласие с правилами и так далее) путем редиректа пользовательского HTTP-запроса на дополнительную страницу.

Применение механизма авторизации EAP в сети приводит к тому, что после успешной аутентификации клиента точкой доступа, где последняя просит клиента авторизоваться у инфраструктурного RADIUS-сервера (рисунок 1).

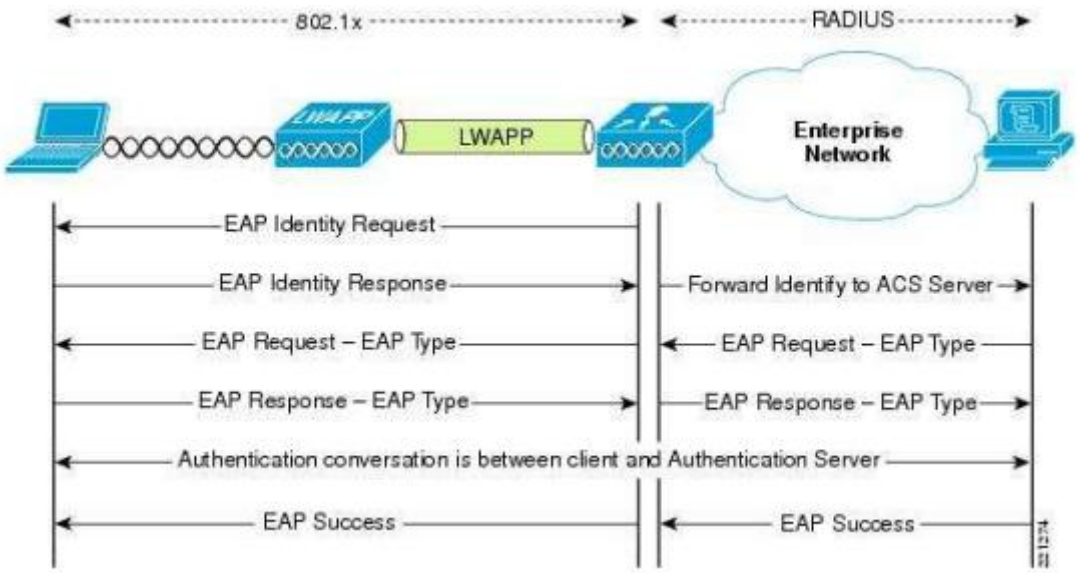

Рисунок 1. **Механизм авторизации EAP**

Как Вы считаете, злоумышленнику чтобы взломать вашу сеть, много нужно будет сделать? Для Open Authentication, No Encryption – ничего! Достаточным условием будет подключиться к сети. Так как радиосреда открыта заблокировать сигнал, который распространяется в разные стороны непросто. Сетевой трафик виден так же, как будто атакующая сторона подключилась в провод, в хаб, в SPAN-порт коммутатора, это при наличии соответствующих клиентских адаптеров, позволяющих прослушивать эфир.

Сегодня у администраторов и обычных пользователей сетей имеются все средства необходимые для надёжной защиты Wi-Fi. При условии отсутствия явных ошибок (взять, например, человеческий фактор) уровень безопасности можно обеспечить, а также сохранить ценность информации в такой сети. Предлагаем ознакомиться с разработанными нами основными правилами при организации и настройке частной Wi-Fi-сети (не общедоступной), правила таковы:

1. технологию применения VPN, где обеспечивается максимальный уровень безопасности, следует использовать в корпоративных сетях;

2. использовать по возможности 802.1X (если точка доступа поддерживает, имеется RADIUS-сервер);

3. всегда быть знакомым с инструкцией и документацией сетевых устройств, а так же знать протоколы или технологии шифрования, которые ими поддерживаются;

4. использовать только новые технологии, такие как Advanced Encryption Standard (AES);

5. не использовать по радио протокол SNMP, web-интерфейс и telnet, а так же не настраивать AP;

6. использовать возможность управлять доступом клиентов по MAC-адресам (Media Access Control);

7. запретить трансляцию в эфир идентификатора SSID (опция может называться «closed network»);

8. запретить доступ для клиентов с SSID по умолчанию «ANY», а так же не следует использовать в своих сетях простые SSID;

9. использовать направленные антенны, не использовать радиоканал по умолчанию, располагать антенны как можно дальше от окон, внешних стен здания;

10. использовать максимально длинные и сложные ключи и пароли, где 128-бит это будет минимум;

11. оставляйте информацию о паролях конфиденциальной;

12. пользуйтесь частой сменой статических ключей и паролей, а проводить эту работу должен администратор;

13. используйте сложный пароль, состоящий из букв и цифр для доступа к настройкам точки доступа;

14. используйте организацию разделяемых ресурсов средствами NetBEUI;

15. используйте вручную распределяемые статические IP-адреса между легитимными клиентами;

16. установите файерволлы на всех ПК внутри беспроводной сети, а так же используйте минимум протоколов внутри WLAN (например, только HTTP и SMTP).

Да, угроза была, есть и будет и человеческий фактор не идеален, но используя приведенные выше правила безопасности, можно избежать или выстоять от запланированного хакерского взлома. Лишь тогда Ваше использование беспроводных сетей Wi-Fi будет безопасным и спокойным.

Вывод. Мы можем с уверенностью сказать, что правильно настроенная частная беспроводная сеть и соблюдение правил безопасности представляет собой непреодолимый барьер для злоумышленника.

СПИСОК ЛИТЕРАТУРЫ:

1. Гейер Д. Беспроводные сети. Первый шаг. / Д. Гейер – М.: Издательство «Вильямс», 2005. – 192 с.

2. Пролетарский А.В. Беспроводные сети Wi-Fi (2-е издание) / А.В. Пролетарский – М.: НОУ «ИНТУИТ», 2016. - 284 с.

3. URL:http://habrahabr.ru

4. URL:http://www.juniper.net

5. URL:http://www.oszone.net

6. URL:http://www.wi-fi.ru