РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

УДК 004.056.53

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕТЯХ СВЯЗИ

Молдаш Айнур Бауржанкызы
Студент 4-курса специальности радиотехника, электроника и телекоммуникации ЕНУ им. Л.Н.Гумилева, Астана, Казахстан.
Научный руководитель – Амирова А.С

В наше время имеется очень большое количество технологий и методов обмена данными между пользователями. И наиболее часто для передачи данных используются беспроводные сети. Отличие беспроводных сетей заключается в том, что в данном случае используются различные преобразователи среды, нежели коммутаторы и сетевые кабели. Преобразователи трансформируют сообщение в радиоволны, и транслируют ее в эфир, следовательно радиоволны поступают на приемник, который в свою очередь выполняет аналогичное действие- преобразовывает радиоволны обратно в сообщение. Беспроводные сети удобны в том случае, когда протягивание кабеля невозможно или финансово убыточно. Я не имею ввиду, что беспроводная сеть лучше проводной сети, напротив она уступает ей во многом. Беспроводные сети бывают: Wi-Fi, 4G сети, 3G сети, GPRS сети, Bluetooth. В данной статье будут рассмотрены беспроводные сети на базе Wi-Fi.

С каждом годом все больше растет спрос на беспроводную сеть связи. Также растет количество устройств подключенных к этим сетям. И тем самым мы получаем главную проблему информационных технологии- как защитить информация от постороннего доступа к сети.

На данном рисунке показано, что аутентификация на ряду с шифрованием обеспечивает нам защищенную беспроводную сеть, и что друг без друга они не могут защитить ту информацию, которую мы передаем друг другу через беспроводную сеть передачи данных.

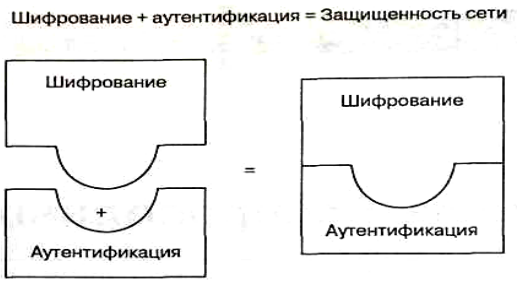

Рисунок 1 – Защита от несанкционированного доступа в сеть обеспечивается благодаря аутентификации и шифрованию.

Аутентификация - это процесс проверки достоверности. Иными словами, проверяет правильно ли пользователь ввел пароль, который находится в его базе данных, сохраненного ранее.

Шифрование - это преобразование сообщений от несанкционированного доступа третьих лиц для сохранения безопасности данных.

Самые главные уязвимости и пути защиты беспроводной сети связи.

На рисунке 2 изображена схема метода, по которому злоумышленник может перехватить наше сообщение.

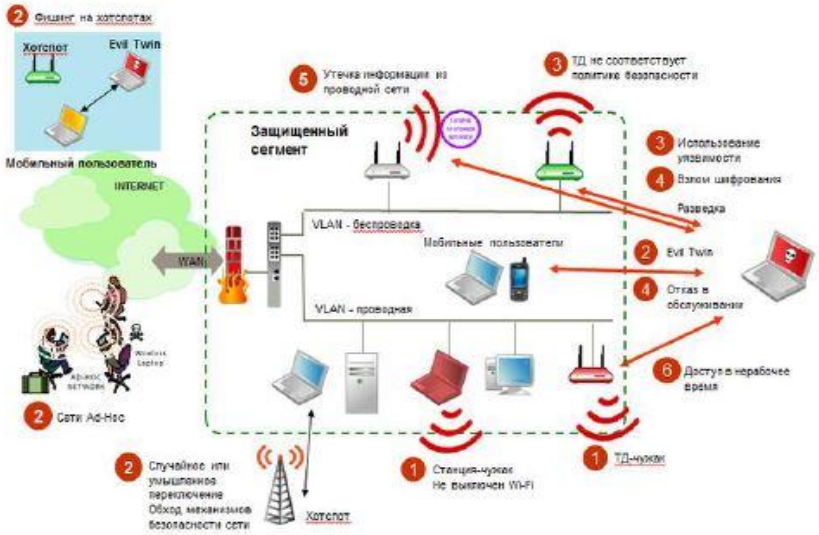

Рисунок 2 – Схема главных атак

Существуют различные механизмы безопасности беспроводных сетей: wired equivalent privacy (WEP), wi-fi protected access (WPA).

Самым первым разработанным стандартом обеспечения безопасности был WEP, который использует криптографический алгоритм RC4, со статическим распределением ключей шифрования для аутентификации подключившихся пользователей.

Одна из самых главных уязвимостей протокола WEP это то, что отсутствует механизм контроля ключей. Мы подбираем ключ шифрования, передаем этот ключ пользователям и потом, мы его никогда не изменяем. Каждый пользователь кому известен этот ключ, без особого труда, расшифрует весь зашифрованный вами трафик. В результате нарушается конфиденциальность данных, и злоумышленник может получить доступ к беспроводной сети.

WEP- продукты исследовались продолжительное время и предполагалось, что хакинг ключей с помощью Airsnot и WEPcrack уже не актуален, так как против этих инструментов мы имеем ряд обратных действий. Но это была лишь самая большая ошибка. Притом, что сорок процентов устройств не прошли тестирование на хакинг ключей, некоторые поставщики даже отступили назад, потому что их конечный продукт был уязвимее, нежели прежний.

Многие пользователи используют протокол WEP, который позволяет работать нам с ключами, продолжительность которых преобладает стандартные 104 бита. В плане маркетинга понятно почему, а в техническом плане мы не видим в этом смысла. Даже если мы попытаемся подобрать ключ разрядностью в 104 бита методом перебора, у нас уйдет значительное время, нежели прогнозируемое время вселенной, и поэтому нет необходимости увеличивать разрядность ключа. Но ущерб от этого бесспорный: использование ключей, у которых нестандартная длина, может привести к тому, что продукты различных компании могут быть несовместимы.

Из этого можно сделать вывод, что WEP- не такой продукт, на который можно положиться, если вы глубоко решили защитить вашу беспроводную сеть. Наша радость, что есть более надежные механизмы безопасности сети.

Консорциум wi-fi Alliance инициативно продвигают WPA-продукт, который разработали производители, так как они боятся, что после уязвимостей WEP-протокола, снизятся их продажи беспроводных устройств.

WPA значительно повышает безопасность беспроводных сетей тем, что позволяет создать новейший протокол temporal key integrity protocol (TKIP), который обеспечивает эффективно применять ключи шифрования. Самым главным достоинством WPA является то что для разных сеансов используются разные ключи шифрования. При каждом новом

соединении клиента-сервера генерируется повторно новый ключ. Числа могут быть случайными, для каждого соединения активизируется автономно.

Если использовать PSK (Pre-Shared Key), заранее разосланный ключ, то безопасность сети будет значительнее. Если мы сочинили пароль, у которого длина значительно мала, то злоумышленник может схватить наши пакеты, которые мы передаем, и после регенерирует ключ PSK, который использовался. И все что он перехватил останется для нас скрытым, мы не сможем обнаружить.

Если, конечно, мы будем задавать 64-х символьные шестнадцатеричные пароли, то и наша с вами сеть будет защищена. Тестирование дало результаты, что восьми-символьный PSK злоумышленник может хакнуть за пару дней.

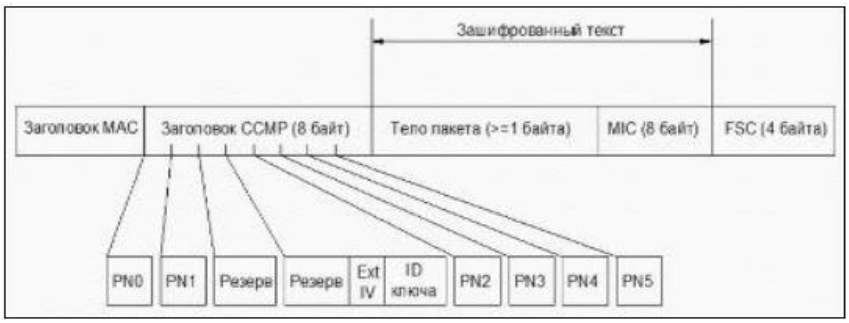

Рисунок 3 – Схема зашифрованного WPA-2

Если использовать WPA протокол наряду с механизмом аутентифиувции 802.1X, то это обеспечит наивысшую степень защиты нашей беспроводной сети. Придется установить RADIUS-сервер, который может работать с механизмом 802.1X и поддерживает обработку цифровых сертификатов. Radius (remote authentication in Dial-In user service)- протокол, использующийся для реализации авторизации, аутентификации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием.

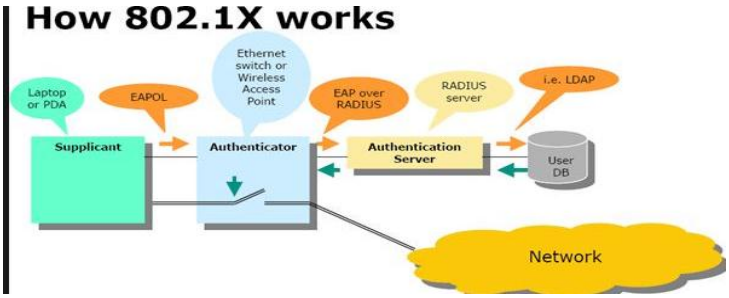

Рисунок 4 – Структурная схема работы механизма аутентификации 802.1X

В современном мире информационных технологи дуэт WPA протокола и механизма аутентификации 802.1X считают великолепнейшим для беспроводных сетей.

Для того, чтобы окончательно обезопасить вашу сеть, необходимо задать пароль, который будет включать более двенадцати символов. Также если вы утеряли ключ PSK, желательно поменять на новый на всех ваших устройствах.

Список использованных источников

1. «Беспроводные сети. Первый шаг»/ Джим Гейер.-М.: Издательство: Вильямс, 2005
2. «Современные технологии беспроводной связи» / Шахнович И.-М.: Техносфера, 2004
3. «Криптография и безопасность сетей» / Фороузан Б.Ф.-ЭКОМ, 2008