Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Сокрута В.В. Обеспечение безопасности беспроводных сетей // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2015. – № 07(декабрь). – АРТ 31-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В.В. Сокрута
Студент 4-го курса, факультет естественных,
математических и компьютерных наук
ФГБОУ ВПО «НГПУ им. Козьмы Минина»
Научный руководитель: Поначугин А.В., доцент
г. Нижний Новгород, Нижегородская область,
Российская Федерация

Обеспечение безопасности беспроводных сетей

Ключевые слова: беспроводные локальные сети, шифрование, 802.1X.

Аннотация: В статье рассмотрены основные алгоритмы обеспечения безопасности в корпоративных беспроводных сетях.

Согласно собранным данным, что за 2013 год Россия вошла в первую десятку ведущих стран мира по денежным расходам на IT – оборудование, уступая Западным странам Европы [2].

Сейчас почти в каждом доме есть Интернет, и ежедневно через эту глобальную сеть проходит огромный поток информации и совершается большое количество различных операций. Большинство бизнес-процессов также осуществляются с помощью современных электронных технологий [1].

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Преимущества WLAN (Wireless Local Area Network).

Основные преимущества беспроводной сети - это отсутствие затрат на прокладку кабелей, что может сэкономить средства для организации, а так же свобода перемещений и возможность использовать различные мобильные устройства, что удобно для конечного пользователя.

Тем не менее, без строгой безопасности для защиты сетевых ресурсов, внедрение WLAN могло предложить ложную экономию. С Wired Equivalent Privacy (WEP), старый механизм безопасности 802.1x WLAN, мог легко поставить под угрозу сеть. Это отсутствие безопасности заставили многих осознать, что беспроводные сети могут привести к большим проблем, чем того они стоят.

Преодоление недостатков WEP.

WEP, шифрование конфиденциальных данных для WLAN, определенным в протоколе 802.11b, не оправдал ожидания. Использование редко меняющихся статических клиентских ключей контроля доступа сделало WEP криптографически слабым. Криптографические атаки позволили злоумышленникам просматривать все входящие и сходящие данные точки доступа.

Недостатки WEP:

- Статичные ключи, которые редко меняются пользователями.
- Используется слабая реализация алгоритма RC4.
- Последовательность исходного вектора слишком коротка и довольно быстро делает “круг”. В результате происходит повторение ключей.

Решение проблемы WEP.

Сегодня WLAN созрели и получили инновационные методы и стандарты безопасности, которые будут использоваться долгие годы. WLAN

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

сделали более гибким, создавая решения, которые позволили быстро устранять обнаруженные недостатки. Примером может послужить добавление протокола аутентификации 802.1x к инструментам безопасности WLAN. Этот протокол предлагает способ защиты сети от вторжений, находящейся за точкой доступа, а так предоставляет динамические ключи и укрепляет шифрование WLAN.

Протокол 802.1X является гибким, так как основан на Расширяемом Протоколе Аутентификации (EAP). EAP (IETF RFC 2284) является весьма гибким стандартом. 802.1x охватывает диапазон методов аутентификации EAP, включая MD5, TLS, TTLS, LEAP, PEAP, SecurID, SIM и AKA.

Более продвинутые типы EAP, такие как TLS, TTLS, LEAP и PEAP обеспечивают взаимную аутентификацию, которая ограничивает тип атаки man-in-the-middle путем аутентификации сервера к клиенту в дополнении к аутентификации клиента к серверу. Кроме того эти методы EAP создают основу, которая может быть использована для генерации динамических ключей WEP.

Методы туннелирования EAP-TTLS и EAP-PEAP также предоставляют взаимную аутентификацию с другими методами, которые используют знакомые способы аутентификации через ввод ID и пароля пользователя, т.е. EAP-MD5, EAP-MSCHAP V2, в целях проверки подлинности клиента на сервере. Этот метод аутентификации проходит через защищенный туннель TLS шифрования, который заимствует методы из проверенного временем HTTPS, который используется при онлайн транзакциях кредитных карт. В случае EAP-TTLS через тоннель могут быть использованы устаревшие методы аутентификации, такие как PAP, CHAP, MS CHAP и MS CHAP V2.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

В октябре 2001 года Wi-Fi альянс представил новый алгоритм шифрования, который заменяет WEP под названием WPA (Wi-Fi Protected Access). Этот стандарт, ранее известный как Safe Secure Network, разрабатывался для работы с существующими продуктами использующими стандарт 802.11 для обратной совместимости, при этом не имея недостатков предыдущего стандарта.

WPA был создан Wi-Fi альянсом, который владеет торговой маркой Wi-Fi и сертифицирует устройства, который используют их технологии. WPA использует разные случайно генерируемые ключи для разных пользователей. Так же существует режим PSK (PreSharedKey) - общий ключ на всех.

Одно из главных улучшений WPA по сравнению с WEP этот система TKIP (протокол целостности временного ключа) которая динамически изменяет ключ по мере его использования. Так же используется новый алгоритм проверки целостности кода MIC, который не позволяет изменять содержимое пакетов, возможность проведения таких атак были недостатком WEP. В MIC используется счетчик кадров, который предотвращает выполнение повторных атак.

WPA 2 и WPA имеют как сходства так и отличия. WPA 2 использует алгоритм шифрования AES. Если клиент используя WPA устанавливал слабый пароль, была возможность подобрать его, перехватив траффик, и получить доступ к точке. В WPA 2 подобрать пароль потребует больше времени и ресурсов.

Для доступа к сети с использованием 802.1x используются три компонента:

- конечный пользователь, устройство, которое запрашивает доступ,

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- устройства доступа, такие как маршрутизаторы и коммутаторы,
- сервер аутентификации (RADIUS сервер)

Эта архитектура может использовано децентрализовано, к примеру иметь несколько серверов аутентификации, что может быть удобно для организаций с большим парком техники.

Когда EAP используется по LAN, пакеты инкапсулируются в EAPOL сообщения. Форматы пакетов EAPOL определены в спецификации 802.1x. EAPOL сообщения передаются между конечным пользователем и беспроводной точкой доступа. RADIUS протокол используют для обмена данным между аутентификатором и сервером RADIUS.

Процесс аутентификации начинается когда конечный пользователь подключается к сети WLAN. Аутентификатор (беспроводная точка доступа) принимает запрос и создает виртуальный порт с конечным пользователям. Аутентификатор действует как прокси для конечного пользователя и обращается с просьбой предоставить доступ к серверу аутентификации уже от своего имени. Аутентификация происходит по такому плану:

- конечный пользователь отправляет начальное EAP сообщение.
- аутентификатор EAP запрашивает у пользователя идентификационные данные.
- Ответ конечного пользователя проксируется и перенаправляется к серверу аутентификации.
- Сервер аутентификации запрашивает учетные данные у конечного пользователя, а так же передает ему свои учетные данные (при использовании взаимной аутентификации).

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- Клиент проверяет информацию о сервере (при использовании взаимной аутентификации), а затем отправляет свои учетные данные на сервер, чтобы идентифицировать себя.
- Сервер принимает или отклоняет запрос клиента на подключение.
- Если конечный пользователь принят, аутентификатор изменяет виртуальный порт с пользователем на полный авторизованный доступ к сети.
- При отклонении запроса аутентификатор изменяет виртуальный порт пользователя на неавторизированный доступ.

Беспроводные сети в сочетании с мобильными устройствами это правильное направление развития локальных сетей. Появление протокола WPA2 в сочетании с 802.1X приблизило уровень безопасности беспроводных сетей к приемлемому уровню для корпоративного сегмента, а так же позволяет администратору сети переключиться с вопросов безопасности на более важные задачи и делает работу конечных пользователей гибкой и мобильной.

Список литературы:

1. Мигалова К.С., Поначугин А.В. Проблема безопасности электронных платежей // Перспективы развития науки, Международная научно-практическая конференция. Ответственный редактор: Сукиасян Асатур Альбертович. Уфа, 2015. С. 134-137;
2. Поначугин А.В. Современные компьютерные сети в России // Наука сегодня сборник научных трудов по материалам международной научно-практической конференции: в 4 частях. Научный центр «Диспут». 2015. С. 58-59;
3. Электронная библиотека RoyalLib.com, Росс Джон "Wi-Fi. Беспроводная сеть": http://royallib.com/read/ross_dgon/Wi_Fi_besprovodnaya_
4. set.html#794771;
5. CCNA Security 640-554 Official Cert Guide ISBN-10: 1-58720-446-0
6. Cherita Corbett: Current Flaws, New Standards, and Today’s Alternatives:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Security for 802.11 Wireless Networks: http://www.prism.gatech.edu/~gt0369c/Security_survey.pdf;
7. How 802.1x authentication works. Jim Burns 2003;
8. InterlinkNetworks: Introduction to 802.1X for Wireless Local Area Networks: www.lucidlink.com/media/pdf_autogen/802_1X_for_Wireless_LAN.pdf.

Рекомендовано к публикации:
Н.В. Камеровой, кандидат исторических наук, доцент,
профессор Российской Академии Естествознания
гл.редактор журнала «Академия педагогических идей «НОВАЦИЯ»

Дата поступления в редакцию: 29.12.2015 г.
Опубликовано: 30.12.2015 г.