УДК 004.732

Гусейнов Н.Э., Гашимов Р.Г.

ПРОЕКТИРОВАНИЕ И БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Азербайджанский Технический Университет, г. Баку, Азербайджан

В представленной статье приведены результаты исследования беспроводных локальных сетей. При проектирование и эксплуатации беспроводных сетей следует уделять большое внимание защите информации. Технических проблем сетей много. Данная статья посвящена анализу способов безопасной передачи информации в локальных и корпоративных сетях. Предлагается проводить сканирование радиодиапазона нескольких точек для выявления методов шифрования. Анализ показал, что в корпоративных сетях шифрование WPA2-Enterprise является на сегодняшний день самым надежным, часто используется тип аутентификации EAP. Протоколы защиты беспроводных сетей EAP-TLS/TTLS входят в стандарт 802.1x и используют для обмена данными между клиентом и RADIUS инфраструктуру открытых ключей. Сочетание этих ключей обеспечивает надежную защиту беспроводных локальных сетей. Цифровые сертификаты нужно делать для каждого Wi-Fi устройства. Это длительный процесс, поэтому сертификаты обычно используются только в Wi-Fi-сетях, требующих максимальной защиты. В то же время можно легко отозвать сертификат и заблокировать клиента. При проектировании Wi-Fi-сетей часто нарушаются принципы безопасности, совершаются однотипные ошибки. Исследования показали, что следует ограничить возможность подключения сторонних устройств к локальной вычислительной сети, например, используя аутентификацию по протоколу 802.1x. Протокол встроен в операционные системы и специальные программные пакеты. Режим работы 802.1x. самый распространенный и надежный. Здесь аутентификатор разрешает или запрещает доступ в сеть. Использование сервера RADIUS защищает от перехвата пакетов.

Ключевые слова: беспроводные сети, шифрование, локальные сети, протокол, аутентификация.

Постановка проблемы

Беспроводные локальные вычислительные сети, беспроводные сети Wi-Fi, технологические сети вошли в нашу повседневную жизнь. Почти во всех мелких и крупных компаниях в той или иной степени выделены беспроводные сети для удобства работы сотрудников компании. В отличие от традиционных кабельных сетей доступа, где электрический провод или оптоволокно, как правило, являются контролируемой средой передачи данных, беспроводные сети относятся к неконтролируемой среде передачи данных.

Новые возможности, которые открываются при использовании беспроводных сетей, а также удобство для конечных пользователей в руках злоумышленника превращаются в новые риски информационной безопасности. К физическим ограничениям относятся уровень сигнала и чувствительность приемопередатчика. С учетом этой особенности размываются границы периметра сети, теперь внешний злоумышленник может подключиться к локальной сети и превратиться в злоумышленника внутреннего [1].

Устройства, подключенные к корпоративной сети и создающие собственную локальную сеть, нелегитимное пользовательское оборудование беспроводной сети, часто встречающиеся примеры угроз сети.

Уязвимости беспроводных локальных вычислительных сетей и устройств много. Вот некоторые из них:

– некорректно сконфигурированные точки доступа;

– использование слабого шифрования;

– неотключенный WPS;

– отсутствие ограничений при доступе из беспроводной сети предприятия в локальную сеть предприятия;

– некорректно сконфигурированные пользовательские устройства.

Анализ последних исследований и публикаций

Устройства, имеющие доступ к корпоративной вычислительной сети или беспроводной локальной вычислительной сети, могут спровоцировать утечку информации. В частности, им может быть корпоративный ноутбук с включенной программной точкой доступа. Причем включение программной точки доступа может быть результатом целенаправленной атаки, и пользователь об этом может даже не догадываться. Примером такой уязвимости может служить тот же принтер с беспроводным модулем. Злоумышленник через уязвимость получает административный доступ и заменяет прошивку на принтере на модифицированную, получая бесконтрольный доступ к сети компании и радиопространству вокруг принтера. Большинство производителей принтеров оперативно устраняют подобные уязвимости в своих устройствах. Решением этой проблемы может быть частые обновления микропрограммного обеспечение оргтехники системными администраторами [2].

При определенных условиях можно взломать практически любое шифрование. WEP-шифрование взламывается за несколько минут. WPA-PSK- и WPA2-PSK-шифрование тоже может быть взломано. Типы шифрования WPA-PSK и WPA2-PSK подвержены атакам с использованием перебора паролей. Да, этот процесс может быть довольно долгим, но, если мощностей и времени достаточно, вполне результативным. WPA-Enterprise с парольным доступом взломать сложно, но при некотором количестве вычислительных ресурсов можно. Широко известно, что WEP-шифрование имеет низкую криптостойкость и использовать его противопоказано, но при этом данный вид шифрования все еще часто используется [3].

Протокол WPS является уязвимым и не рекомендуется к использованию, хотя иногда он имеет дополнительные механизмы защиты от перебора ключей [4].

Главной ошибкой администраторов компании является отсутствие контроля над устройствами, подключаемыми к внутренней сети компании, что приводит к повальной установке пользователями собственных уязвимых точек доступа.

Есть множество практических решений. Например, можно провести сканирование радиодиапазона нескольких центральных точек, в частности, мегаполиса, чтобы выяснить, какие типы шифрования используются и какую полезную информацию можно получить от работающих точек беспроводного доступа. Статистика по типам используемого шифрования показывает, что многие компании владельцев беспроводной локальной вычислительной сети не заботятся о безопасности, часто используют WEP-шифрование или поддерживают протокол WPS. При целевых атаках злоумышленник в рамках разведки на местности сможет идентифицировать множество компаний. А если рассматривать статистику по идентифицированным компаниям, только некоторые из них имеют должный уровень защищенности [5].

Постановка задачи

Цель статьи исследовать безопасное шифрование беспроводных локальных вычислительных сетей.

Изложение основного материала исследования

Анализ показывает, что единственное шифрование, которое можно считать надежным на сегодняшний день – это WPA2-Enterprise+802.1x с использованием сертификатов (рисунок).

В режиме WPA2-Enterprise решаются проблемы, касающиеся распределения статических ключей и управления ими, а его интеграция с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в этом режиме требуются такие регистрационные данные, как имя и пароль пользователя, сертификат безопасности или одноразовый пароль, аутентификация же осуществляется между рабочей станцией и центральным сервером аутентификации.

Корпоративные сети с шифрованием WPA2-Enterprise строятся на аутентификации по протоколу 802.1x через RADIUS-сервер.

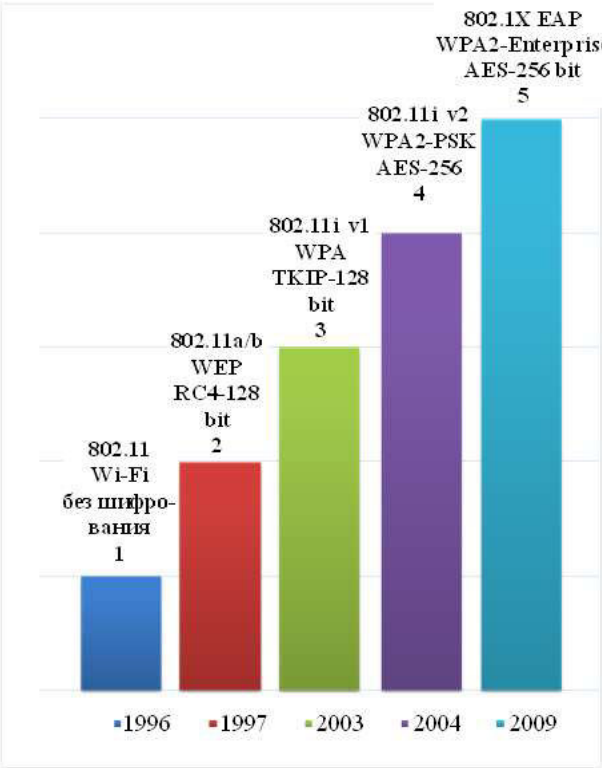
Протокол 802.1x (EAPOL) определяет методы отправки и приема запроса данных аутентификации и обычно встроен в операционные системы и специальные программные пакеты.

802.1x предполагает три роли в сети:

– клиент (supplicant) – клиентское устройство, которому нужен доступ в сеть;

– сервер аутентификации (обычно RADIUS);

– аутентификатор – роутер/коммутатор, который соединяет множество клиентских устройств с сервером аутентификации и отключает/подключает клиенсткие устройства.



Типы сетей в зависимости от надежности

Есть несколько режимов работы 802.1x, но самый распространенный и надежный следующий:

– аутентификатор передает EAP-запрос на клиентское устройство, как только обнаруживает активное соединение;

– клиент отправляет EAP-ответ – пакет идентификации. Аутентификатор пересылает этот пакет на сервер аутентификации (RADIUS);

– RADIUS проверяет пакет и право доступа клиентского устройства по базе данных пользователя или другим признакам, и затем отправляет на аутентификатор разрешение или запрет на подключение. Соответственно, аутентификатор разрешает или запрещает доступ в сеть.

Использование сервера RADIUS позволяет отказаться от PSK и генерировать индивидуальные ключи, валидные только для конкретной сессии подключения. Проще говоря, ключи шифрования невозможно извлечь из клиентского устройства. Защита от перехвата пакетов обеспечивается с помощью шифрования по разным внутренним протоколам EAP, каждый из которых имеет свои особенности.

Среди наиболее часто используемых типов аутентификации EAP можно назвать EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-Fast и Cisco LEAP.

EAP-MD-5 (Message Digest Challenge, проверка свертки сообщения) – метод аутентификации EAP, предоставляющий поддержку базового уровня протокола EAP. Метод EAP-MD-5 обычно не рекомендуется для применения в локальных сетях Wi-Fi, т.к. он допускает восстановление пароля пользователя. Он обеспечивает только одностороннюю аутентификацию, а не взаимную идентификацию клиента Wi-Fi и сети.

EAP-TLS (Transport Layer Security, протокол защиты транспортного уровня) – обеспечивает взаимную аутентификацию клиента и сети на базе сертификатов. Для выполнения аутентификации используются сертификаты клиента и сервера. Этот метод можно применять для динамической генерации ключей WEP для пользователя и сеанса, чтобы защитить последующую связь между клиентом беспроводной сети и точкой доступа. Один из недостатков EAP-TLS – необходимость управления сертификатами как на стороне клиента, так и на стороне сервера. В крупных беспроводных локальных сетях эта задача может быть трудновыполнимой.

EAP-TTLS (Tunneled Transport Layer Security, туннелированный протокол защиты транспортного уровня). Этот метод защиты предусматривает основанную на сертификате, взаимную аутентификацию клиента и сети через зашифрованный канал, а также средство получить динамические, ключи WEP на сеанс, в расчете на пользователя. В отличие от EAP-TLS, для работы EAP-TTLS требуются только сертификаты сервера.

Метод EAP-FAST (Flexible Authentication via Secure Tunneling, гибкая аутентификация по защищенному туннелю) был разработан компанией Cisco. Вместо сертификатов для взаимной аутентификации используются регистрационные данные PAC (Protected Access Credential), которыми может динамически управлять сервер аутентификации. Данные PAC могут предоставляться (один раз) клиенту как вручную, так и автоматически. Ручные методы включают доставку на диске или с использованием защищенных сетей. Автоматическая доставка предусматривает внутриполосную эфирную передачу.

LEAP (Lightweight Extensible Authentication Protocol, облегченный расширяемый протокол аутентификации) – разновидность метода аутентификации EAP, используемый преимущественно в беспроводных локальных сетях Cisco Aironet.

Передаваемые данные шифруются с использованием динамически генерируемых ключей WEP. Поддерживается взаимная аутентификация.

PEAP (Protected Extensible Authentication Protocol, защищенный расширяемый протокол аутентификации) – метод безопасной передачи аутентификационных данных по сетям 802.11 Wi-Fi, включающий унаследованные протоколы на базе паспортов. Для связи между клиентами PEAP и сервером аутентификации используется туннелирование. Подобно конкурирующему стандарту TTLS, PEAP позволяет проверять подлинность клиентов локальной сети Wi-Fi с использованием только сертификатов сервера. Таким образом, упрощается реализация и администрирование защищенных локальных сетей Wi-Fi. PEAP – совместная разработка Microsoft, Cisco и RSA Security.

Максимальную защиту сети Wi-Fi обеспечивает только WPA2-Enterprise и цифровые сертификаты безопасности в сочетании с протоколом EAP-TLS или EAP-TTLS. Сертификат – это заранее сгенерированные файлы на сервере RADIUS и клиентском устройстве. Клиент и сервер аутентификации взаимно проверяют эти файлы, тем самым гарантируется защита от несанкционированных подключений с чужих устройств и ложных точек доступа. Протоколы EAP-TTL/TTLS входят в стандарт 802.1x и используют для обмена данными между клиентом и RADIUS инфраструктуру открытых ключей (PKI). PKI для авторизации использует секретный ключ (знает пользователь) и открытый ключ (хранится в сертификате, потенциально известен всем). Сочетание эти ключей обеспечивает надежную аутентификацию.

Цифровые сертификаты нужно делать для каждого беспроводного устройства. Это трудоемкий процесс, поэтому сертификаты обычно используются только в Wi-Fi-сетях, требующих максимальной защиты. В то же время можно легко отозвать сертификат и заблокировать клиента.

Сегодня WPA2-Enterprise в сочетании с сертификатами безопасности обеспечивает надежную защиту корпоративных Wi-Fi-сетей. При правильной настройке и использовании взломать такую защиту практически невозможно «с улицы», то есть без физического доступа к авторизованным клиентским устройствам. Тем не менее, администраторы сетей иногда допускают ошибки, которые оставляют злоумышленниками «лазейки» для проникновения в сеть. Проблема осложняется доступностью софта для взлома и пошаговых инструкций, которыми могут воспользоваться даже дилетанты.

При проектировании и эксплуатации Wi-Fi-сетей часто нарушаются принципы безопасности, причем, как правило, совершаются однотипные ошибки:

– ошибки на этапе проектирования;

– отсутствие разграничения между сетьми и основной сетью предприятия;

– кабельная и беспроводная сети между собой должны иметь разграничение;

– доступ в корпоративную сеть из сети должен быть ограничен только требуемыми адресами и сервисами.

Выводы

Существует множество решений по защите и мониторингу беспроводных сетей и радиодиапазона. Такие решения предлагают и крупные производители сетевого оборудования.

Рекомендуется проводить периодическую проверку офисных помещений и радиоэфира на наличие подобных устройств и ограничить возможность подключения сторонних устройств к локальной вычислительной сети предприятия, например, используя аутентификацию по протоколу 802.1x. Необходимо не допускать утечек паролей или использовать общие пароли. Данная ошибка пересекается с похожей ошибкой при проектировании, но при этом является самостоятельной ошибкой, потому что как бы грамотно ни была спроектирована защита, на этапе эксплуатации часто возникают множественные нарушения. Для собственных устройств пользователей желательно создать выделенную сеть без доступа к основной сети предприятия.

Защита беспроводных локальных вычислительных сетей – задача комплексная. Основные рекомендации вытекают из основных ошибок, перечисленных выше: разграничение доступа в/из сети; проведение радиопланирования при проектировании сети; использование Wireless Intrusion Prevention System (WIPS); использование систем управления доступом к сети с возможностью профилирования и оценки состояния.

К проектированию беспроводных сетей нужно подходить обстоятельно, уделяя должное внимание вопросам безопасности. Правильная настройка позволяет приблизить защищенность Wi-Fi к уровню защищенности проводной сети с внедренным протоколом 802.1x.

СПИСОК ЛИТЕРАТУРЫ

1. *Росс Дж.* Wi-fi. Беспроводные сети. Установка. Конфигурирование. Использование: Пер. с англ. В.А. Ветлужских – М.: НТ Пресс, 2005. – 312 с.

2. *Гейер Дж.* Беспроводные сети. Первый шаг: Пер. с англ. – М.: Издательский дом «Вильяме», 2005. – 192 с.

3. *Гордейчик С.В., Дубровин В.В.* Безопасность беспроводных сетей. – М.: Горячая линия – Телеком, 2008. – 288 с.

4. *Борисов В.И., Щербаков В.Б., Ермаков С.А.* Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11 // Информация и безопасность. – 2008. – Т. 11. – № 3. – С.431-434.

5. *Широкополосные* беспроводные сети передачи информации / Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.Л. – М.: Техносфера, 2005. – 592 с.

Поступила в редакцию 02.10.2017

ПРОЕКТУВАННЯ І БЕЗПЕКА БЕЗДРОТОВИХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Гусейнов Н.Е., Гашимов Р.Г.

У представленій статті були досліджені бездротові локальні мережі. При проектуванні і експлуатації бездротових мереж слід приділяти велику увагу захисту інформації. Технічних проблем мереж багато. Дана стаття присвячена аналізу способів безпечної передачі інформації в локальних і корпоративних мережах. Пропонується проводити сканування радіодіапазону декількох точок для виявлення методів шифрування. Аналіз показав, що в корпоративних мережах шифрування WPA2-Enterprise є на сьогоднішній день найнадійнішим, часто використовується тип аутентифікації EAP. Протоколи захисту бездротових мереж EAP-TLS/TTLS входять в стандарт 802.1x і використовують для обміну даними між клієнтом і RADIUS інфраструктуру відкритих ключів. Поєднання цих ключів забезпечує надійний захист бездротових локальних мереж. Цифрові сертифікати потрібно робити для кожного Wi-Fi-пристрою. Це тривалий процес, тому сертифікати зазвичай використовуються тільки в Wi-Fi-мережах, які вимагають максимального захисту. У той же час можна легко відкликати сертифікат і заблокувати клієнта. При проектуванні Wi-Fi-мереж часто порушуються принципи безпеки, відбуваються однотипні помилки. Дослідження показали, що слід обмежити можливість підключення сторонніх пристроїв до локальної обчислювальної мережі, наприклад, використовуючи аутентифікацію по протоколу 802.1x. Протокол вбудований в операційні системи і спеціальні програмні пакети. Режим роботи 802.1x найпоширеніший і надійний. Тут аутентифікатор дозволяє або забороняє доступ в мережу. Використання сервера RADIUS захищає від перехоплення пакетів.

Ключові слова: бездротові мережі, шифрування, локальні мережі, протокол, аутентифікація.

DESIGN AND SAFETY OF WIRELESS LOCAL COMPUTER NETWORKS

Huseynov N.E., Hashimov R.H.

Azerbaijan Technical University, Baku, Republic of Azerbaijan

In the provided article wireless local area networks were probed. In case of design and maintenance of wireless networks it is necessary to pay the big attention to information security. There are a lot of technical issues of networks. This article is devoted to the analysis of methods of safe information transfer on the local and corporate area networks. It is offered to carry out scanning of a radio-frequency range of several access points for detection of cryptography techniques. The analysis showed that encoding WPA2 Enterprise is the most reliable today in corporate networks, EAP authentication type is often used. Protocols of protection of wireless networks EAP-TLS/TTLS are included into the standard 802.1x and use the infrastructure of public keys for a data interchange between the client and RADIUS. The combination of these keys provides reliable protection of wireless local area networks. Digital certificates should be created for each Wi-Fi device. It is a long process, therefore certificates are usually used only on the Wi-Fi-networks requiring the maximum protection. At the same time it is possible to withdraw easily the certificate and to disable the client. In design of Wi-Fi networks the principles of safety are often broken, the same mistakes are made. Research showed that it is necessary to restrict a possibility of connection of third-party devices to a local computer network, for example, using authentication according to the protocol 802.1x. The protocol is built into operating systems and special software packages. Operation mode 802.1x is the most widespread and reliable. Here the authenticator resolves or forbids access to a network. Use of the RADIUS server protects from interception of packets.

Keywords: wireless networks, encoding, local area networks, protocol, authentication.

REFERENCES

1. Ross Dzh. Wi-fi. Besprovodnyie seti. Ustanovka. Konfigurirovanie. Ispolzovanie: Per. s angl. V.A. Vetluzhskih [The book of Wi-Fi Install, Configure, and Use]. NT Press, Moscow, 2005. 312 p. (*in Russian*).

2. Geyer Dzh. Besprovodnyie seti. Pervyiy shag: Per. s angl. [Wireless. The first step]. Izdatelskiy dom «Vilyame», Moscow, 2005. 192 p. (*in Russian*).

3. Gordeychik S.V., Dubrovin V.V. Bezopasnost besprovodnyih setey [Wireless security]. Goryachaya liniya – Telekom, Moscow, 2008. 288 p. (*in Russian*).

4. Borisov V.I., Scherbakov V.B., Ermakov S.A. Spektr uyazvimostey besprovodnyih setey standarta IEEE 802.11 [The spectrum of vulnerabilities of wireless networks standard IEEE 802.11]. *Informatsiya i bezopasnost*, 2008, vol. 11, no. 3, pp. 431-434. (*in Russian*).

5. Vishnevskiy V.M., Lyahov A.I., Portnoy S.L., Shahnovich I.L. Shirokopolosnyie besprovodnyie seti peredachi informatsii [Broadband wireless data transmission network]. Tehnosfera, Moskow, 2005. 592 p. (*in Russian*).