УДК 004.056.53

Докшин А.Д.,
студент
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича
Россия, г. Санкт-Петербург
Даньшина А.В.,
студент
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича
Россия, г. Санкт-Петербург
Ковцур М.М.,
кандидат технических наук
доцент кафедры «Защищенные системы связи»
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича
Россия, г. Санкт-Петербург
Юркин Д.В., кандидат технических наук
доцент кафедры «Защищенные системы связи»
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича
Россия, г. Санкт-Петербург

ИССЛЕДОВАНИЕ ПОДХОДОВ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ БЕСПРОВОДНОЙ СЕТИ НА ОСНОВЕ LDAP

Аннотация: *В данной статье рассмотрен принцип организации безопасности беспроводных сетей семейства IEEE 802.11. Небольшие Wi-Fi сети, как правило, защищены с помощью одной общей парольной фразы для каждой SSID, но этот подход крайне небезопасен и неэффективен. Решение*

данной проблемы заключается в реализации RADIUS аутентификации пользователей при подключении к Wi-Fi сети. В статье представлены различные LDAP решения, позволяющие организовать централизованную аутентификацию пользователей корпоративной беспроводной сети.

Ключевые слова: *IEEE 802.11, безопасность беспроводных сетей, RADIUS, Windows Active Directory, FreeIPA.*

Annotation: *This article discusses the principle of organizing the security of wireless networks of the IEEE 802.11 family. Small Wi-Fi networks are usually secured with a single shared passphrase for each SSID, but this approach is extremely insecure and inefficient. The solution to this problem is to implement RADIUS authentication of users when connecting to a Wi-Fi network. This article presents various LDAP solutions that allow centralized authentication of corporate wireless network users.*

Key words: *IEEE 802.11, wireless network security, RADIUS, Windows Active Directory, FreeIPA.*

На данный момент, беспроводная сеть является объектом постоянного внимания. Системные администраторы и ИТ-директора признают, что небезопасные сети Wi-Fi являются одним из общих векторов атаки.

Многие Wi-Fi сети защищены с помощью одного общего SSID и парольной фразы. Но этот подход является небезопасным и неэффективным, когда речь заходит о предоставлении доступа к беспроводной сети вашей организации. Если общий SSID или парольная фраза состоят из большого количества символов, то велика вероятность того, что они попадут в открытые источники. Любой желающий может увидеть эту информацию. В некоторых случаях сигнал Wi-Fi достигает соседнего здания, парковки или тротуара. Поэтому, когда человек получает SSID или парольную фразу, ему даже не нужно быть в офисе, чтобы получить доступ к сети организации. Помимо угроз безопасности, защита сетей Wi-Fi с помощью SSID или парольных фраз также малоэффективны [1]. Когда люди увольняются из организации, администраторам приходится менять пароли, из-за чего могут возникнуть дополнительные сложности .

Решение этой проблемы заключается в уникальной аутентификации пользователя при доступе к сети. Такой подход устраняет общую парольную фразу и гарантирует, что администратору не придется менять пароль каждый раз, когда сотрудник покидает организацию.

Централизованная аутентификация в этом случае организовывается с использованием IEEE 802.11 и требует развертывание AAA сервера на сети, а также организации взаимодействия пользователей и сетевого оборудования с этим сервером [2]. Данная задача решается с помощью протоколов EAP и RADIUS. Существует несколько решений, реализующих приведенные протоколы .

RADIUS протокол, используется для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах. RADIUS обеспечивает защиту сетей, предоставляя каждому пользователю свой собственный набор учетных данных [3].

FreeRADIUS является одной из самых популярных реализаций RADIUS – сервера, так как программное обеспечение находится в свободном доступе. Для настройки FreeRADIUS пользователю придется работать с конфигурационными файлами, что не всегда бывает удобно. Однако, для работы сервера авторизации требуется централизованная база данных пользователей, а также протокол взаимодействия с этой базой. В качестве такого протокола может выступать LDAP.

Active Directory (AD) – LDAP база данных, разработанная для операционной системы Microsoft Server, в которой хранятся данные в виде объектов. Объект – это отдельный элемент, например пользователь, группа, приложение, устройство или принтер. Объекты обычно определяются как ресурсы, такие как принтеры или компьютеры, или как субъекты безопасности – такие как пользователи или группы [4].

Active Directory благодаря удобному графическому интерфейсу пользуется популярностью у системных администраторов. Основной службой в Active Directory являются доменные службы, которые хранят информацию о каталоге и

обрабатывают взаимодействие пользователя с доменом. AD проверяет доступ, когда пользователь входит в устройство или пытается подключиться к серверу по сети. AD контролирует, какие пользователи имеют доступ к каждому ресурсу. При этом аутентификация пользователей проводится с использованием протокола LDAP. Базы данных, поддерживающие этот протокол, получили название LDAP, часто применяют для централизованнго хранения пользовательских идентификаторов. Примером LDAP базы данных является Active Directory.

Основные конкуренты Active Directory, которые предоставляют аналогичные функции AD – это Red Hat Directory Server, Apache Directory, FreeIPA и OpenLDAP.

FreeIPA LDAP база данных для операционной системы Linux. Загрузка программного обеспечения осуществляется бесплатно. Преимуществом является то, что помимо взаимодействия в консоли, FreeIPA имеет удобный графический интерфейс, что позволяет комфортно взаимодействовать с базой данных. Так же интерфейс и функционал аналогичен Active Directory. Помимо схожего интерфейса, FreeIPA возможно использовать совместно с Active Directory [5].

OpenLDAP – наиболее широко используемая реализация LDAP с открытым исходным кодом. Как решение с открытым исходным кодом, загрузка программного обеспечения бесплатна, но настройки на физическом оборудовании – нет. OpenLDAP чрезвычайно гибок и может использоваться для аутентификации множества различных типов ресурсов, но в конечном итоге все они используют протокол LDAP.

Исследование показало, что для организации аутентификации пользователей беспроводной сети могут использоваться различные решения, включая LDAP базы данных. Однако, при реализации программы импортозамещения возникает задача проверки совместимости существующих решений с операционными системами отечественного производителя. Таким

образом, актуальной задачей является тестирование совместимости OpenLDAP и FreeIPA на базе операционной системы Astra Linux.

Использованные источники:

1. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты WI-FI сетей / В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 47-51.

2. Ковцур М.М., Симанов М.С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11 / В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 т.. 2019. С. 537-541.

3. Юркин Д.В., Исаченков П.А., Патрикеев А.И. Улучшение вероятностно – временных характеристик протоколов инкапсуляции 802.11 / Вопросы кибербезопасности. 2016. № 2 (15). С. 46-53.

4. Красов А.В., Штеренберг С.И., Голузина Д.Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей / Электросвязь. 2019. № 11. С. 39-47.

5. Виткова Л.А., Головлева Ю.А., Гераськина В.С, Мустафаев Р.А. Конвергенция информационных технологий для повышения безопасности информационного пространства / Вестник молодых ученых Санкт - Петербургского государственного университета технологий и дизайна. 2018. № 1 С. 131-135.