УДК 004.056.57 **Информационные технологии**

Жуков Вадим Сергеевич, *2 курс магистратуры*
МИЭТ, Институт микроприборов и систем управления имени Л.Н. Преснухина (Институт МПСУ), кафедра "вычислительная техника"

МЕТОДЫ ОРГАНИЗАЦИИ БЕСПРОВОДНЫХ ЗАЩИЩЕННЫХ СЕТЕЙ

Аннотация: Цель данной работы заключается в изучении методов организации беспроводных защищенных сетей. В работе дано понятие беспроводной сети, изучены основные принципы организации беспроводных сетей, а также рассмотрены методы организации беспроводных защищенных сетей. В ходе работы применялись такие методы исследования, как анализ, синтез, описание и обобщение. В заключение работы отмечается, что в настоящее время наиболее эффективным и инновационным методом организации беспроводной защищенной сети является комбинация отдельных методов, которая позволяет добиться наилучших результатов.

Ключевые слова: беспроводная сеть, защита, шифрование, доверенная загрузка, Wi-Fi, TrustZone.

Abstract: The purpose of this work is to study the methods of organizing wireless secure networks. The concept of a wireless network, the basic principles of wireless networks, and are considered protected wireless networks. In the course of the work, such research methods as analysis, synthesis, description and generalization were used. In conclusion, it is noted that currently the most effective and innovative method of organizing a wireless secure network is a combination of individual methods that allows you to achieve the best results.

Keywords: wireless network, security, encryption, trusted load, Wi-Fi, TrustZone.

В настоящее время сети, основанные на беспроводных технологиях, развернуты и применяются практически в каждом уголке нашей планеты. Это связано с тем, что они обладают такими характерными преимуществами, как гибкость, удобство работы, а также, что особенно важно, достаточно низкой себестоимостью.

Очевидно, что, как и многие другие современные системы, беспроводные сети обязательно должны соответствовать определенному набору требований, к числу которых можно отнести:

- качество предоставляемых услуг;
- скорость работы сети;
- радиус действия сети;
- защищенность.

Последний из факторов является особенно важным. Попасть в беспроводную сеть намного легче, нежели чем в проводную – достаточно находиться в радиусе действия сети. Несмотря на то, что с каждым годом защита усложняется и применяются более сложные алгоритмы, вероятность получения конфиденциальных данных сторонними лицами до сих пор находится на высоком уровне. Поэтому необходимо со всей серьезностью относиться к вопросам организации беспроводных защищенных сетей.

В связи с вышесказанным можно с уверенностью сказать, что изучение вопросов, которые касаются методов организации беспроводных защищенных сетей, является весьма актуальным в настоящее время.

Под беспроводной сетью понимается такая технология, которая позволяет создать процесс взаимодействия человека с серверами и базами данных с использованием радиочастотных сигналов [1]. Для того, чтобы создать стабильное сетевое подключение, можно использовать несколько способов, такие как Bluetooth, WiFi или WiMax. Разновидности беспроводных сетей полностью идентичны их проводным аналогам (PAN, LAN, MAN, WAN).

В большинстве вариантов беспроводная сеть представляет собой комбинацию узлов доступа и клиентов с беспроводными адаптерами. Узлы

доступа и беспроводные адаптеры должны быть оснащены приемо-передающими устройствами, которые осуществляют обмен данными между собой. Каждому устройству присваивается свой уникальный 48битный MAC-адрес, являющийся полным эквивалентом Ethernet-адреса. Узлы доступа осуществляют взаимосвязь между беспроводными и проводными сетями, обеспечивая беспроводным клиентам доступ к проводным сетям. Каждая беспроводная сеть идентифицируется назначаемым администратором идентификатором SSID. Связь беспроводных клиентов с AP возможна, если они распознают SSID узла доступа. Если в беспроводной сети имеется несколько узлов доступа с одним SSID (и одинаковыми параметрами аутентификации и шифрования), то возможно переключение между ними мобильных беспроводных клиентов [2].

Для защиты от атак на целостность системы IoT нужно убедиться, что только авторизованные лица могут получить доступ. Кроме того, компоненты системы не должны подвергаться опасности (например, заражению вредоносными программами). Если условия безопасности не удовлетворяются, то должны быть приняты все меры по своевременному обнаружению угроз и защиты от них.

Мощным инструментом для защиты целостности является криптопроцессор, в котором хранятся криптографические ключи для защиты информации (TPM). TPM представляет собой стандартный микроконтроллер, который сочетает в себе надёжную криптографическую уникальность с удалёнными функциями управления безопасностью. Поскольку модуль TPM определяется открытыми стандартами, разработчики могу выбирать из множества TPM продуктов от различных производителей.

Защита конфиденциальных данных с помощью шифрования может показаться очевидным, но требуется осторожность, чтобы сделать это правильно. Данные должны использовать шифрование от начала до конца маршрута, чтобы перехватчики не могли расшифровать их.

Шифрование эффективно только в тех случаях, когда алгоритмы имеют высокую энтропию генерации ключей. Для долгоживущих систем применяются обновления с изменением криптографических алгоритмов.

Сохранённые данные должны быть также защищены с помощью шифрования. Одним из методов является перенаправление данных на мощный сервер, где они могут быть легко зашифрованы, вместо локального хранения.

Для важных систем использовать аппаратное обеспечение и стандарты.

Всё программное обеспечение содержит ошибки, которые могут использоваться злоумышленниками. По этой причине критически важные компоненты в IoT системах всегда должны быть основаны на аппаратных средствах безопасности, таких как TPM и SED.

Аппаратный подход помогает гарантировать защиту от вредоносных программ и атак, которые типичны в более уязвимом программном обеспечении, которое зачастую не может обновляться для исправления этих ошибок.

Многие системы IoT включают в себя устройства с ограниченными возможностями, такие как крошечные датчики, которые зависят от батарейного питания, или устаревшие устройства. Эти устройства не могут быть обновлены до такой степени, чтобы включать в себя средства безопасности. Тем не менее они не могут быть оставлены без защиты от потенциально враждебной сети. Лучший способ защиты таких систем – размещение на «наложенной» сети, которая изолирует их от атак и обеспечивает конфиденциальность и целостность трафика [3].

Доверенная загрузка – это загрузка операционных систем только с заранее определённых носителей (например, только с жёсткого диска) после успешного завершения специальных процедур, обеспечивающих необходимый уровень безопасности: проверка целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.

В общем случае включает следующие механизмы:

- аутентификация;

- контроль устройства, с которого начинается загрузка ОС;

- контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой ОС;

- шифрование / расшифровка загрузочного сектора, системных файлов ОС, либо шифрование всех данных устройства;

- аутентификация, шифрование и хранение секретных данных, таких как ключи, контрольные суммы и хэш-суммы, выполняются на базе аппаратных средств [4].

Можно выделить следующие этапы доверенной загрузки:

1 Выполнение микропрограммы BIOS. На данном этапе могут быть реализованы следующие механизмы безопасности: проверка целостности микропрограммы, проверка целостности и подлинности настроек CMOS, аутентификация, контроль выбора загрузочного устройства. Этот этап должен быть выполнен производителем.

2 Передача управления загрузочному устройству. На этом этапе BIOS вместо продолжения загрузки может передать управление аппаратному модулю доверенной загрузки. Аппаратный модуль может выполнить аутентификацию, выбор загрузочного устройства, дешифрование и проверку целостности и достоверности загрузочных секторов и системных файлов ОС. Дешифрование загрузочного сектора операционной системы может быть выполнено только на этом этапе.

3 Выполнение загрузочного сектора ОС. На этом этапе также может быть выполнена проверка целостности, достоверности загрузчика, системных файлов и аутентификация. Однако исполняемый код загрузочного сектора ограничен в функциональности вследствие того, что имеет ограничение на размер и размещение кода, а также выполняется до запуска драйверов ОС [4].

Аппаратные модули доверенной загрузки имеют значительные преимущества перед программными средствами. Однако обеспечение

доверенной загрузки не может быть выполнено только аппаратно. При этом можно выделить следующие преимущества аппаратных средств:

- высокая степень защищённости секретной информации о паролях, ключах и контрольных суммах системных файлов;

- возможная засекреченность алгоритмов шифрования, выполняемых аппаратно;

- невозможность запуска компьютера без вскрытия его содержимого;

- в случае шифрования загрузочного сектора невозможно запустить ОС пользователя даже после извлечения аппаратного модуля;

- в случае полного шифрования данных – невозможность получения любых данных после извлечения аппаратного модуля [4].

TrustZone - это аппаратное разделение (виртуализация) ARM-процессора на два изолированных друг от друга «мира» – Secure World и Normal World, позволяющее запущенным в них ОС и приложениям работать независимо друг от друга с использованием одного ядра процессора и набора периферии.

При загрузке процессора сначала загружается специализированная компактная Secure OS, находящаяся в Secure World и контролирующая все коммуникации процессора с внешним миром (контроллеры и периферию). Она же формирует и профиль безопасности (доступные ресурсы, например, объём памяти, доступность внешней периферии и пр.) для «гостевой» (Guest / Rich OS), в которой будет работать «основная» ОС (iOS, Android, Sailfish, Tizen, Linux, Windows и др.) в «нормальном» привычном для нас «мире» Normal World [5].

Таким образом, в ходе выполнения данной работы было рассмотрено понятие и принцип организации беспроводной сети, а также основные методы организации беспроводных защищенных сетей. Можно с уверенностью сказать, что в настоящее время беспроводные сети продолжают активно развиваться и совершенствоваться. Сегодня уже разработано множество приемов защиты и улучшения их работоспособности, однако остаются уязвимости, которые необходимо учитывать. В заключение работы хотелось бы подчеркнуть, что

наиболее эффективным и инновационным методом организации беспроводной защищенной сети является комбинация отдельных методов, которая позволяет добиться наилучших результатов. Примером такового является использование технологии TrustZone в архитектуре ARMv8-M. Исследование данного вопроса позволит в дальнейшем улучшить характеристики беспроводных сетей

Библиографический список:

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. – М.: Инфра-М, 2017. – 416 с.

2. Беделл, П. Сети. Беспроводные технологии [Текст] / П. Беделл. – М.: НТ Пресс, 2008. – 448 с.

3. Кузянин, А.С. Шаги и повышение безопасности технологии Internet of things, IoT [Текст] / А.С. Кузянин // Актуальные вопросы современной техники и технологий: сборник докладов XXIII Международной научной конференции. Научное партнерство «Аргумент». Липецк, 2016. – С. 9-11.

4. Алексеев, Д.М., Иваненко, К.Н., Убирайло, В.Н. Доверенная загрузка как механизм информационной безопасности [Текст] / Д.М. Алексеев, К.Н. Иваненко, В.Н. Убирайло // Влияние науки на инновационное развитие: сборник статей международной научно-практической конференции. Екатеринбург, 2017. – С. 19-20.

5. Доверенная платформа на ARM-процессорах с собственной TrustZone [Электронный ресурс]. Свободный доступ: https://www.aladdin-rd.ru/catalog/trustzone (дата обращения - 28.02.2021 г.).