РусКрипто

XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ОБЛАЧНЫЕ И ТУМАННЫЕ ТЕХНОЛОГИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Колядин Игорь Витальевич, аспирнат, Самарский университет
Сухов Андрей Михайлович, д.т.н., профессор, Самарский университет
Хайрулов Максим Алексеевич, магистрант, Самарский университет

ТРЕБОВАНИЯ К СИСТЕМЕ БЕЗОПАСНОСТИ ДЛЯ IOT УСТРОЙСТВ

- Минимальный объем вычислительных реурсов
- Максимальная простота использования

Предлагамый подход: ограничение любых запросов к IoT устройству.

Основное взаимодействие устройств с **туманным** (fog) и/или **облачным** (cloud) серверами.

ЭКСПЕРИМЕНТАЛЬНЫЙ ПОЛИГОН

Компоненты:

- Туманный сервер
- Модель IoT устройства (мини компьютер под управлением ОС GNU/Linux)

Программное обеспечение/файлы на туманном сервере:

- Цифровой сертификат для защищенного обмена данными и аутентификации
- ПО для обновления сетевого профиля устройства и сетевой профиль (файл)
- ПО для мониторинга трафика IoT устройства
- ПО для генерации одноразового пароля (двухфакторная аутентификация)

ЦИФРОВЫЕ СЕРТИФИКАТЫ

Цифровые сертификаты являются фундаментальной технологией, обеспечивающей безопасное и масштабируемое взаимодействие в экосистеме IoT.

Цифровые сертификаты размещаются на облачном (туманном) серверах, а также на устройстве интернета вещей.

Цифровые сертификаты предоставляют более безопасный вариант аутентификации по протоколам удаленного доступа (по сравнению с парольной аутентифиацией.

Цифровые сертификаты обеспечивают шифрование данных между туманным (облачным) сервером и IoT устройством.

СЕТЕВОЙ ПРОФИЛЬ УСТРОЙСТВА

Сетевой профиль - конфигурация межсетевого экрана устройства (iptables, ufw, firewalld).

Оригинал сетевого профиля устройства:

- Хранится на туманном сервере
- Периодически загружается на IoT устройство по протоолу удаленного доступа

МОНИТОРИНГ ТРАФИКА IOT УСТРОЙСТВА

Способы определения компрометации устройства:

- Сетевые соединения с адресами, не указанными в сетевом профиле
- Превышение порога объема сетевого трафика устройства

Для проверки объема сетевого трафика устройства использовался протокол **SNMP**.

При подозрении на компрометацию:

- Оповещение администратора/службы информационной безопасности
- Попытка внеочередного обновления сетевого профиля с туманного сервера

ДВУХФАКТОРНАЯ АУТЕНТИФИАЦИЯ

Двухфакторная аутентификация (2FA) — это метод повышения безопасности, который требует от пользователя подтвердить свою личность двумя различными способами (факторами).

В рассматриваемом случае используются следующие факторы для аутентификации:

- Цифровой сертификат
- Одноразовый 6-значный PIN, генерируемый на туманном сервер с помощью алгоритма TOTP

РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Спасибо за внимание!

Колядин Игорь Витальевич
Аспирант, Самарский университет
Email: igor.koladinbzlk@gmail.com
Сухов Андрей Михайлович
Д.т.н., профессор, Самарский университет
Email: sukhov@ssau.ru
Хайрулов Максим Алексеевич
Магистрант, Самарский университет
Email: max.hairulov@mail.ru