МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТРАФІКУ ІНТЕРНЕТ–РЕЧЕЙ

Сабурова С.О, Кадацька О.Й., Рибас К. В., Скалозуб В.В.

Кафедра «Інфокомунікаційної інженерії
імені В.В. Поповського», ХНУРЕ, Україна

E-mail: svitlana.saburova@nure.ua

Abstract

The concept of the Internet of Things is considered, which provides for the possibility of using cloud services for data storage and processing. Distortion and blocking of the transmitted information may be destroyed along the entire route of data from the Internet–device to the cloud service due to the intervention of third parties as an attack, called a "person in the middle". To protect data coming from the Internet of Things to a remote cloud server via public communication networks, it's proposed to use security methods based on hybrid encryption algorithms and creating network traffic patterns.

Інтернет–речей є ключовим напрямком в інфокомунікаціях, обговоренню якого останнім часом приділяють багато уваги. У зв'язку з цим, з'являються нові загрози мережної безпеки для Інтернету–речей, починаючи від атак на енергетичну систему, клонування вузлів сенсорних мереж, перехоплення даних від Інтернету–пристрою і підміни самого пристрою до злому сервісів, на базі яких здійснюється обробка і зберігання даних. Класичні підходи для виявлення таких проблем не завжди підходять, з огляду на те, що для Інтернету–речей використовується велика кількість нових пропрієтарних протоколів, яких зараз налічується близько 25-ти.

Концепція Інтернету–речей передбачає можливість використання хмарних сервісів для зберігання і обробки даних [1] . У свою чергу, хмарний сервіс є сполучною ланкою між Інтернет–пристроєм і людиною, або є кінцевим елементом при зборі даних з датчиків. На всьому маршруті проходження даних від Інтернету–пристрою до хмарного сервісу може відбутися знищення спотворення і блокування інформації, що передається, в силу втручання третіх осіб. Такий вид атаки називається «людина посередині».

Однак, найбільш простий вид атак, який може бути реалізований на рівні доступу, є відправка даних від Інтернету–речей в альтернативний хмарний сервіс, який буде далі розглянуто в роботі – «хибна хмара».

Для отримання доступу до конфіденційних даних, що йде від типової Інтернет–речі до віддаленого хмарного сервісу, пропонується використовувати метод клонування пакетів, що містять конфіденційну інформацію і їх подальшу відправку до дублюючому хмарного сервісу (хибну хмару). Під хмарним сервісом розуміється сукупність програмно-апаратних засобів (серверів), що мають підключення до Інтернет і здійснюють обробку та зберігання даних. У спрощеному варіанті хмарний сервіс може бути представлений Web і Data Base-сервером, який є одним з ключових компонентів модельної мережі для Інтернету–речей.

В умовах реалізації перехоплення і відправки конфіденційних даних на дублюючий сервер необхідно мати доступ до каналу зв'язку або обладнанню на рівні доступу, що відповідає за транспортування даних від Інтернету–речей до хмарного серверу.

В даний час технологія Wi-Fi є найбільш популярною серед безпроводових мереж і використовується для підключення Інтернету–речей в додатках «розумний будинок», «розумне місто» та інш. Для відправки даних на хмарний сервіс Інтернет–речей повинен мати підключення до точки доступу Wi-Fi та мережі провайдера до кінцевого вузла мережі зв'язку загального користування (МЗЗК) [4].

Перехоплення і перенаправлення даних може бути реалізовано в безпосередній близькості до каналу зв'язку на ділянці доступу «Інтернет–речі – точка доступу». Атака може перехопити мережний трафік, що йде до легального хмарного сервісу. Фільтрацію заданих пакетів від другорядного трафіку необхідно виконувати за IP–адресою і портом с призначенням перехоплених пакетів. Пакети, що мають в поле IP–адреса – Адреса легального хмарного сервісу, дублюються та перенаправляються на альтернативний (хибний) хмарний сервер.

Програмна частина має виконувати аналіз заголовків кожного захопленого пакета, і при виявленні в полях Адреса одержувача (мережний рівень) і порт одержувача (транспортний рівень) відповідної адреси і порту легального хмарного сервісу, або IP–адреси Інтернет–речі в поле Адреса відправника, здійснювати копіювання змісту пакета в оперативну пам'ять і подальшу заміну полів Адреса одержувача і порт одержувача на IP–адрес і порт хибного хмарного сервера. Далі здійснити відправку такого пакета в мережу зв’язку зага-льного користування.

Якщо IP-адреса легального хмарного сервера була невідома, то здійснюється аналіз структури трафіку від Інтернету–речей. Основні характеристики трафіку Інтернет–речей можуть значно відрізнятися в залежності від типу пристрою (сенсорний вузол, актуатор, комбінований пристрій і т. д.), а також виду виконуваного завдання [2].

Для виявлення даних від Інтернету–речей і подальшої їх відправки на хибний хмарний сервер спочатку визначалася IP–адреса легального хмарного сервісу. Для цього необхідно проаналізувати поведінку трафіку від Інтернету–речі і отримати параметри основних характеристик. Протокол MQTT має стандартизований формат обміну повідомленнями між Інтернет–річей і MQTT–брокером, як показано на рисунку 1.

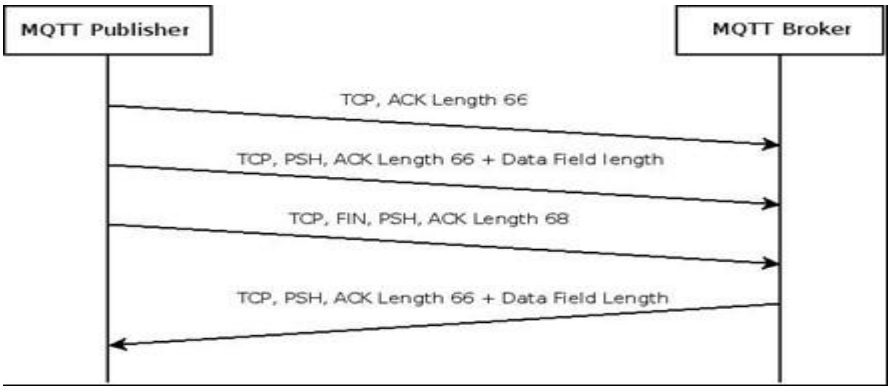

Рис. 1. Обмін повідомленнями між Інтернет-річчю і MQTT–брокером

Першим критерієм для фільтра мережного трафіку протоколу MQTT є виявлення 4 послідовно вихідних пакетів від Інтернету– речей, а саме:

– пакету, що сигналізує про початок передачі даних (транспортний протокол TCP);
– пакету з даними від Інтернету–речей (транспортний протокол TCP);
– протоколу прикладного рівня MQTT;
– пакету сигналізації про закінчення передачі даних (транспортний протокол TCP);
– пакету, що підтверджує отримання даних MQTT–брокером (протокол прикладного рівня MQTT).

Для фільтрації пакетів по даним критеріям необхідно здійснити порівняння поля Адреса відправника в пакеті, що йде від Інтернету–речей, і поля Адреса одержувача в пакеті, що йде від сервера. Цей критерій допустимо за умови, якщо пакет від сервера отримано не далі, ніж через 7 пакетів після пакета від послуги Інтернету–речей, і при їх збігу здійснювалося порівняння полів даних. Якщо поля даних виявлялися ідентичні, то включався лічильник, який при досягненні певного значення записував IP–адреса сервера одержувача, IP–адреса Інтернет–речі і порт одержувача в оперативно-запам'ятовуючому пристрою (ОЗП) для подальшого використання при дублюванні пакетів. Цей критерій підходить для аналізу трафіку за умови використання протоколів мережного рівня IPv4, IPv6, транспортного рівня UDP, TCP і використанні протоколу прикладного рівня MQTT.

Також в якості критерію для фільтрації трафіку Інтернету–речей здійснюється аналіз всіх захоплених пакетів на предмет їх схожості на базі непрямих характеристик. Для цього можна використовувати масив з структур, що містять IP–адреса відправника, адресу порту відправника, IP–адреса одержувача, передбачуваний тип даних (символи або число), розмір поля даних пакета (з не-великим ймовірним відхиленням в залежності від типу перехоплених даних), масив з 3 і більше чисел, що зберігають час надходження останніх 3 і більше пакетів даного типу, і лічильник кількості перехоплених пакетів. Дана структура описує кількість отриманих пакетів, схожих між собою. У разі, якщо більше 3 пакетів мали схожі адреси та порти відправника, адреса одержувача, тип даних, розмір поля даних і тимчасова різниця між двома послідовно що йдуть пакетами була приблизно дорівнює різниці інших двох послідовно йдуть пакетів, в ОЗП записувалося значення адреси одержувача, адреса відправника та порт одержувача для подальшого використання при дублюванні пакетів. Цей критерій доцільно використовувати для аналізу трафіку інтернет-речі за умови використання протоколів мережного рівня IPv4, IPv6 і протоколів транспортного рівня UDP, TCP, однак вивчення структури інформаційного обміну може зайняти деякий час.

Після визначення IP–адреси сервера одержувача (легальний хмарний сервіс), IP-адреси Інтернет–речі і порту одержувача, кожен пакет, який підходить під дані критерії, дублюється і записується в ОЗП. Потім відбувається заміна IP–адреси сервера і порту одержувача на адресу сервера дублювання даних і порт 10001[3].

Для захисту даних, що надходять від Інтернету–речей до віддаленого хмарного сервера через мережі зв’язку загального доступу пропонується використовувати методи захисту трафіку Інтернет–речей на базі використання алгоритмів гібридного шифрування.

Розглянемо алгоритми RSA-512 і AES-128, які вимагають великих обчислювальних потужностей від Інтернету–речей і не підходять для малопотужних додатків, реалізованих на базі мікроконтролерів, що мають 8–ми або 16–ти бітну розрядність цифрового процесорного

приладу (ЦПП) – AVR або ARM, також, як і пристрої з малим об'ємом пам'яті. Приклад такого алгоритму складається з наступної послідовності кроків, як показано на рисунку 2.

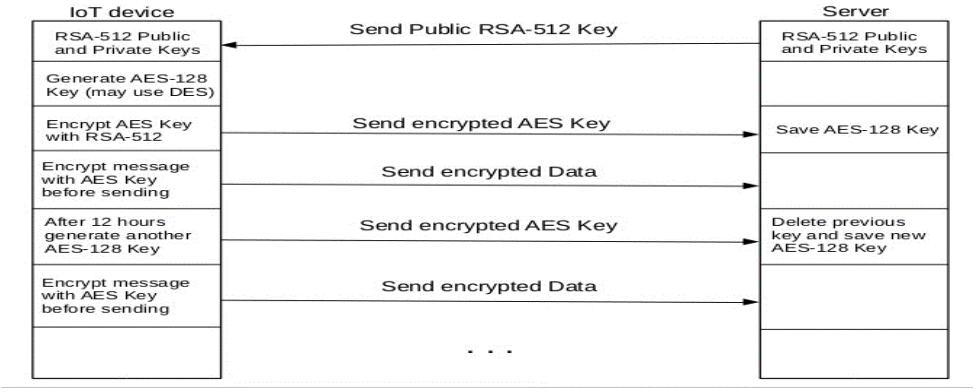

Рис. 2. Алгоритм гібридного шифрування для Інтернету–речей

Розглянемо покрокову роботу алгоритму гібридного шифрування для Інтернету–речей:

Крок 1. Генерація відкритого і закритого ключів на сервері для організації асиметричного шифрування (наприклад RSA–512).

Крок 2. Генерація відкритого і закритого ключів для мікроконтролера і їх запис в пам'ять Інтернет–речі.

Крок 3. Проводиться обмін відкритими ключами між сервером і Інтернет–річчю.

Крок 4. Інтернет-річ генерує за допомогою набору випадкових символів ключ для симетричного шифрування (наприклад, DES).

Крок 5. Отриманий ключ симетричного шифрування шифрується за допомогою відкритого ключа та відправляється на сервер.

Крок 6. На сервері відбувається дешифрування і запис у ПЗП симетричного ключа за допомогою закритого ключа.

Крок 7. Усі наступні дані, що відправляються з Інтернету–речі, шифруються за допомогою симетричного ключа, наявного на Інтернет–речі і сервері.

Крок 8. В залежності від складності дешифрування симетричного ключа методом повного перебору (bruteforce) через заданий час потрібно повторити Кроки 4-7.

Метод захисту трафіку Інтернет–речей на базі створення патернів мережного трафіку.

Метод передбачає внесення випадкових змін в структуру інформаційного обміну між Інтернет–річчю і хмарним сервером, а також використання декількох портів на сервері для створення нетипового для Інтернету–речі трафіку.

Даний метод підійде для більшості Інтернету–речей, включаючи малопотужні 8-ми розрядні мікроконтролери.

Розглянемо наступну послідовність кроків, як показано на рисунку 3.

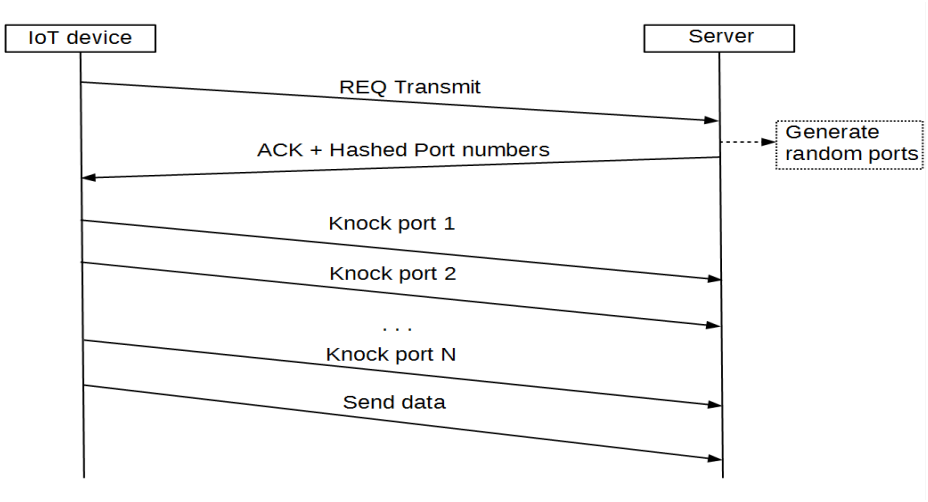

Рис. 3. Структура інформаційного обміну для методу portknocking

Крок 1. Хешування всієї інформації, що знаходиться в полі даних всіх пакетів, що відправляються з Інтернет–речі (наприклад, за допомогою алгоритму MD5).

Крок 2. Внесення випадкових затримок перед черговим циклом відправки даних (диференціювання часу) з Інтернету–речі.

Крок 3. Використання з боку сервера декількох IP–адрес для прийому даних, що дозволить Інтернет–речі випадковим чином записувати різні значення в поле Адреса приймача.

Крок 4. Використання методу portknocking перед початком кожної передачі даних.

Метод portknocking полягає в зверненні до певних портів для розблокування доступу до порту, по якому, в кінцевому підсумку, відбувається передача даних. В даному випадку пропонується перед кожною передачею даних (або раз в певний період) проводити зміну портів передачі даних за допомогою даного методу. Для цього Інтернет–річ попередньо відправляє запит на передачу даних. Сервер у відповідь надсилає хешований список портів для передачі, а потім пристрій робить поперемінні запити до кожного порту і відправляє дані за обраним портом.

Крок 5. Створення помилкового потоку даних.

Запропонований метод дозволяє значно збільшити складність перехоплення трафіку від Інтернету–речі, що дасть можливість зберегти конфіденційну інформацію.

Висновки

Концепція Інтернет–речей передбачає можливість використання хмарних сервісів для зберігання і обробки даних. У свою чергу, хмарний сервіс є сполучною ланкою між Інтернет–пристроєм і людиною, або є кінцевим елементом при зборі даних з датчиків. На всьому маршруті проходження даних від Інтернету–пристрою до хмарного сервісу може відбутися знищення спотворення і блокування інформації, що передається, в силу втручання третіх осіб. Такий вид атаки називається «людина посередині».

Для захисту даних, що надходять від Інтернету–речей до віддаленого хмарного сервера через мережі зв'язку загального доступу пропонується використовувати такі методи захисту на основі:

- алгоритмів гібридного шифрування;
- створення патернів мережного трафіку.

Література:

1. Y.2060 Огляд Інтернету–речей. Міжнародний союз електрозв'язку, сектор стандартизації, 06/2012.

2. Эталонная архитектура безопасности Интернета–вещей, Источник: [Електронний ресурс] – Режим доступу до ресурсу: https://www.antimalware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 – 2017.

3. Тестування мереж зв'язку наступного покоління. / А. Б.Васильєв, Д. В. Тарасов, Д. В. Андрєєв, А. Е. Кучерявий., 2008. – 140 с

4. Росляков А. В. Интернет–вещей: Учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. – Самара: ПГУТИ, 2015. – 136 с.

Villy, B. Iversen Teletraffic Engineering Handbook. COM Center Technical University of Denmark Building 343, DK-2800 Lyngby Tlf.: 4525 364