

ЗАХИСТ ІНФОРМАЦІЇ ТЕХНОЛОГІЇ «ІНТЕРНЕТ РЕЧЕЙ»

Автор Чемериський Є. Г.

(науковий керівник — д.т.н., с.н.с, проф. Степанов М. М.)

Інтернет речей (Internet of Things, IoT), як і будь-яка швидко розвивається технологія, відчуває ряд «хвороб зростання», серед яких найбільш серйозною є проблема безпеки. Але чим викликана ця небезпека?

Збої чийхось «розумних» годин або фітнес-трекерів особливої шкоди, крім розлади їх господарів, не принесуть. Але ось злом IoT-пристроїв, які входять в системи і сервіси M2M, зокрема, інтегровані в критичну інфраструктуру, загрожує непередбачуваними наслідками. У цьому випадку ступінь їх безпеки повинна відповідати важливості тієї чи іншої інфраструктури: транспортної, енергетичної чи інший, від яких залежить життєдіяльність людей і робота економіки.

Для IoT-пристроїв безпеку полягає, перш за все, в цілісності коду, перевірці автентичності користувачів (пристроїв), встановлення правами володіння (включаючи генеруються ними дані), а також можливістю відображення віртуальних і фізичних атак. Але по факту, більшість з працюючих сьогодні IoT-пристроїв елементами захисту не забезпечені, мають доступні ззовні інтерфейси управління, дефолтних паролі, тобто, мають всі ознаки веб-вразливості.

Існуюча проблема безпеки IoT-пристроїв виникла не через технічну неграмотність їх розробників. Тут грає роль тверезий розрахунок: швидкість виходу на ринок дає перевагу перед конкурентами, нехай і ненадовго, і навіть за рахунок низького порога захищеності. Таким чином можна зробити висновок, що розробники порушують принцип наскрізної інформаційної безпеки, а саме — Інтернет безпека повинна закладатися на початковій стадії проектування продукту або послуги і підтримуватися аж до завершення їх життєвого циклу.

Так захист інформації в IoT можна розділити на наступні три етапи: безпека на етапі розробки та проектування, безпека на етапі розробки програмного забезпечення та прошивок, етап впровадження.

Для забезпечення захисту на першому етапі розробник повинен виконати наступні пункти:

- налаштування апаратних інтерфейсів, а саме усунення надлишкового функціоналу(наприклад UART який необхідний в разі налаштування і тестування системи), обмежити введення виконуваних команд
- налаштування завантажувача ОС
- використання спеціалізованих технології пайки, що ускладнюють процес налагодження чіпу — Ball grid array, system on chip
- видалення маркувань

На другому етапі все повинно бути в рамках SDLC (Systems development life cycle), код програми повинен бути аудированим, проводити iot hardening —

процес посилення захищеності системи з метою зниження ризиків від можливих загроз. Даний процес застосовується до всіх компонентів системи, тим самим, в ідеальному випадку, роблячи її неприступною фортецею).

Щоб забезпечити захист на етапі впровадження бажано для підвищення рівня захисту використовувати сторонні модулі захисту, оновлення.

Одною з найрозповсюдженіших типів атак є підбір паролів доступу до адміністративної панелі (Brute-force attack). Тому для забезпечення захисту від атак такого типу достатньо використовувати міжмережевий екран або IPS система (Intrusion Prevention System — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через Інтернет), які при досягненні критичного рівня некоректних підключень можуть їх блокувати.

Для забезпечення захисту CVE exploit (це "словник" відомих вразливостей, що має строгу характеристику по описаним критеріям) атак необхідно виконувати своєчасне оновлення та патчинг системи, тим самим мінімізуючи їх загрозу. Більшість таких загроз характерна для такого обладнання як маршрутизатори.

Ще деякі з варіантів атаки це підміна оновлень або підміна команд для виконання будь-яких функцій, які виникають при незахищеності каналу передачі даних. Для вирішення цієї проблеми підходить тунелювання трафіку та перевірка оригінальності кінцевих пристроїв, шляхом перевірки сертифікату безпеки.

Так само є варіант отримання зловмисником фізичного доступу до пристрою, внаслідок чого він може виконати реінжиніринг прошивки, спробувати її модифікувати, додати або видалити якийсь функціонал. В цьому випадку допоможе використання SIEM (Security information and event management) системи, яка забезпечує аналіз в реальному часі подій (тривог) безпеки, що надходять від мережевих пристроїв і додатків. У нашому випадку, збираючи контрольні суми прошивок IoT пристроїв, то таку модифікацію можна детектувати і вчасно ізолювати.

Що стосується оновлення системи, то оновлення має відбуватися не тільки для програмного функціоналу самого пристрою, але і ОС в рамках якої воно функціонує, пов'язане стороннє програмне забезпечення, з яким воно функціонує, канал оновлення повинен бути захищений, але якщо такої можливості немає, то потрібно шифрувати самі оновлення. Також необхідно розносити самі поновлення в часі, щоб підвищити відмовостійкість системи в цілому.

Убезпечити управління IoT пристроїв можна за рахунок впровадження інфраструктури відкритих ключів, тим самим роблячи пристрої довіреними. Атрибути і ролі пристроїв можна прописувати в сертифікатах безпеки, що забезпечить єдину консоль управління пристроями.

Отже хоч технологія досить нова та не зовсім захищена, але існують варіанти як підвищити її захист вже існуючими методами.

Перелік посилань

1. Росляков А.О. Интернет вещей [Текст] : учебное пособие по направлению подготовки «Инфокоммуникационные технологии и системы связи» 11.03.02 — бакалавриат и 11.04.02 - магистратура / А.В. Росляков, С.В. Ваяшин, А.Ю. Гребешков. — Самара : ПГУТИ, 2015. — С.136.
2. Остапов С.Е. Технології захисту інформації : навч. посіб. / Остапов С. Е., Євсєєв С. П., Король О. Г. // Харків. нац. екон. ун-т. — Харків : ХНЕУ, 2013. — С. 475
3. С.К. Варлатая, М.В. Шаханова. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс. — М.: Проспект, 2015. — С. 216
4. Пономарев В.С. Методи та моделі розроблення комп'ютерних систем і мереж : монографія — Харків : ХНЕУ, 2008. — С. 316
5. Защита информации. Инсайд : информационно-методический журнал / учредитель и издатель: ООО "Издательский дом "Афина". — Санкт-Петербург : Афина, 2006 — С. 29

Анотація

В даній статті проаналізовані основні проблеми та вразливі місця захисту інформації Інтернету речей. Наведено можливі причини виникнення цих проблем. Наведенні типові види атак на інформаційну систему та методи протидії цим атакам.

Ключові слова: Інтернет речей, захист інформації.

Abstract

This article analyzes the main issues and vulnerabilities of protection information of technology Internet of things. The possible causes of these problems are presented. Show typical types of attacks on the information system and methods of counteracting these attacks.

Key words: Internet of Things, information protection