УДК 004.738.5

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ПРИСТРОЇВ ТА ПОСЛУГ ІНТЕРНЕТУ РЕЧЕЙ

Піхота К.В., Кононова І.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: pihotka19.11@gmail.com

Analysis of security threats to Internet of Things devices and services

The main weaknesses in building the Internet of Things were identified by analyzing major technology threats and providing recommendations (comprehensive security measures) to improve the security of Internet of Things devices and services.

На даний час спостерігається швидкий темп росту пристроїв Інтернету речей, який надає безліч переваг, однак пристрої IoT (internet of things - інтернет речей) можуть надавати реальну загрозу безпеці, тим більше що вони можуть бути легко скомпрометовані і можуть привести до більш серйозних порушень, видалення, спотворення даних і інших проблем.

Експоненціальне зростання IoT призвело до збільшення ризиків для безпеки та конфіденційності. Багато таких ризиків можна віднести до вразливості пристроїв, які виникають внаслідок кіберзлочинності хакерами та неправильного використання системних ресурсів.

Беручи до уваги дослідження, що провела в 2019 компанія Microsoft, яке присвячувалось динаміці впровадження Інтернету речей в компаніях з різних індустрій і країн світу 85% організацій вже мають як мінімум один бізнес-проект в цій сфері, а до 2021 року ця цифра виросте до 94%. При цьому 88% керівників таких проектів усвідомлюють переваги технології для успіху компанії і очікують 30% окупність інвестицій в дворічній перспективі [1].

Тому, необхідно проаналізувати загрози безпеки та визначимо основні проблеми з пристроями і послугами IoT.

Безпека даних являє собою фундаментальну проблему в пристроях і послугах IoT [2]. В контексті IoT доступ до даних може мати не тільки користувач, але і авторизований об'єкт. Це вимагає розгляду двох важливих аспектів: по-перше, механізму контролю доступу та авторизації та другого механізму аутентифікації і управління. Пристрій IoT повинні перевірити, що об'єкт (людина або інший пристрій) авторизований для доступу до послуги. Авторизація допомагає визначити, чи дозволено при ідентифікації об'єкту отримувати послугу. Контроль доступу є невід’ємною частиною контролю доступу до ресурсів шляхом надання або відмови в засобах надання послуг з використанням широкого набору критеріїв.

Авторизація та контроль доступу необхідні для встановлення безпечного з'єднання між кількома пристроями та службами. Основною проблемою в

цьому сценарії є спрощення створення, розуміння і маніпулювання правилами контролю доступу, а також слід враховувати при роботі з конфіденційністю: аутентифікацію та управління ідентифікаціє, оскільки кільком об'єктам розпізнавати один одного за допомогою надійних служб ця проблема є критичною в IoT.

В проведених дослідження, вченими та передовими компаніями, основна увага приділяється безпеці з погляду конфіденційності, що є важливою проблемою для пристроїв і послуг IoT з погляду на те, що об'єкти пов'язані між собою, а дані передаються та обмінюються через Інтернет. Тому, довіра грає важливу роль у встановленні безпечного з'єднання у невизначеною середовищі IoT [3]. На даний час слід розглядати два аспекти довіри: довіра до взаємодій між об'єктами і довіра до системи з точки зору користувачів. Надійність пристроїв IoT, найчастіше, залежить від компонентів пристрою, включаючи обладнання (процесор, пам'ять, датчики) і виконавчі механізми, програмні ресурси (апаратне програмне забезпечення, операційна система, драйвери та додатки, а також джерело живлення). Отже, для підвищення надійності пристроїв повинен існувати ефективний механізм визначення довіри в спільному середовищі IoT.

Розглянемо вплив на цілісність системи з погляду підвищення надійності технології IoT.

Перед усуненням загроз безпеки необхідно спочатку ідентифікувати системні ресурси, які складають IoT, при цьому необхідно розуміти інвентаризацію активів, включаючи всі компоненти IoT, обладнання та послуги, що надаються [4].

Основними активами будь-якої системи IoT є системне устаткування (включаючи будівлі, обладнання і т.д.) , програмне забезпечення, послуги і дані, які пропонуються цими послугами. Виходячи з активів системи, можна класифікувати вплив на цілісність системи, за такими показниками як вразливість, вплив та загроза.

Під вразливістю розуміється слабкі місця в системі або її структурі, які дозволяють зловмиснику виконувати команди, несанкціоновано отримувати доступ до даними і/або проводити атаки типу «відмова в обслуговуванні». Вразливості можуть бути виявлені в різних областях систем IoT, це можуть бути слабкі місця в системному обладнанні або програмному забезпеченні, слабкі місця в політиках і процедурах, використовуваних в системах, а також слабкі сторони самих користувачів системи.

Показник «вплив» в IoT є проблемою або помилкою в конфігурації системи, що дозволяє зловмиснику виконувати дії зі збору інформації. У більшості додатків IoT пристрій може залишитись без нагляду або бути розміщеним в легко доступному для зловмисників, що може стати важливою

проблемою - фізичною атакою, наприклад, пошкодження криптографічних даних, перепрограмування компонент або заміна їх шкідливим пристроєм [5].

Також на цілісність системи впливає показник «загроза» [6]. Загрози можуть виникати з двох основних джерел: люди і природа.

Розглянувши основні проблеми безпеки пристроїв та служб IoT, можна зробити висновок, що вони піддаються ряду поширених загроз, наприклад, віруси та атаки відмови в обслуговуванні і проведення простих заходів для уникнення таких загроз та подолання вразливості системи недостатньо. Таким чином, необхідно забезпечити безперебійний процес реалізації політики, що буде підтримуватися суворими процедурами.

Процес розробки безпеки вимагає глибокого розуміння активів системи з подальшим виявленням різних вразливостей та загроз, які можуть існувати.

Необхідно визначити, що таке активи системи та від чого активи повинні бути захищені. У роботі активи визначені як усі цінні речі в системі, матеріальні та нематеріальні, які потребують захисту. Деякі загальні активи IoT включають системне обладнання, програмне забезпечення, дані та інформацію, а також активи, пов’язані з послугами. Розуміння потенційних атак дозволить розробникам системи краще визначати, на що слід звернути більше уваги для забезпечення коректної та безпечної роботи системи.

Отже, для уникнення ризиків для безпеки та конфіденційності, IoT має бути побудований таким чином, щоб забезпечити простий та безпечний контроль використання, а для цього в першу чергу необхідно забезпечити захист пристроїв і послуг IoT від несанкціонованого доступу як всередині пристроїв, так і ззовні.

Література

1. Интернет вещей, IoT, M2M (мировой_рынок). – Електронний ресурс. – Режим доступу: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA).
2. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges”.
3. M. Abomhara and G. Koien, “Security and privacy in the internet of things: Current status and open issues”.
4. D. Watts, “Security and vulnerability in electric power systems”.
5. D. G. Padmavathi, M. Shanmugapriya et al., “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” arXiv preprint arXiv:0909.0576, 2009.
6. H. G. Brauch, “Concepts of security threats, challenges, vulnerabilities and risks,” in Coping with Global Environmental Change, Disasters and Security. Springer, 2011, pp. 61–106.