

ЗАСІБ ЗАХИСТУ ФУНКЦІОНАЛУ І БЕЗПЕКИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ І МОДИФІКАЦІЇ В ПРИСТРОЯХ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

Вінницький національний технічний університет

Анотація

Проаналізовано мережу та проблеми безпеки в пристроях інтернету речей. Запропоновано засіб захисту функціоналу і безпеки від несанкціонованого доступу і модифікації в пристроях IoT.

Ключові слова: інтернет речей, безпека IoT.

Abstract

Network and security issues in Internet of Things devices are analyzed. The means of protection of functionality and security against unauthorized access and modification in IoT devices is offered.

Keywords: internet of things, IoT security.

Вступ

Концепція IoT була сформована в результаті розвитку засобів радіочастотної ідентифікації (RFID) (для взаємодії пристроїв між собою і оточенням). Значним поштовхом для розвитку інтернету речей послужив розвиток технологій, а також інтерес до даної тематики з боку більшості світових компаній. На даний момент практично всі великі компанії зі світовим ім'ям усвідомили, що дана концепція буде затребувана в найближчі кілька років. З цієї причини в їх складі з'явилися робочі групи, що займаються даною проблематикою. Уряди країн в свою чергу також виділяють фінансові кошти на грантовій основі для розвитку даного напрямку науки і техніки[1].

Метою даного дослідження є забезпечення інформаційної безпеки Інтернету речей для захисту функціоналу і безпеки від несанкціонованого доступу і модифікації шляхом вибору оптимального алгоритму способів захисту.

Для досягнення мети необхідно розв'язати такі задачі:

- проаналізувати роботу IoT;
- проаналізувати можливі загрози і способи захисту.

Аналіз роботи IoT

Інтернет речей - це більш тісна інтеграція реального та віртуального світу, в якому спілкування здійснюється між людьми та пристроями [2].

У загальному значенні під Інтернетом речей розуміється сукупність різноманітних приладів, датчиків, пристроїв, об'єднаних в мережу за допомогою будь-яких доступних каналів зв'язку, що використовують різні протоколи взаємодії між собою і єдиний протокол доступу до глобальної мережі. У ролі глобальної мережі для Інтернет-речей зараз використовується мережа Інтернет. Спільним протоколом є IP[3].

При практичній реалізації IoT існує ряд проблем:

- проблема енергоспоживання;
- проблема стандартизації;
- проблема живлення датчиків;
- проблема децентралізованого управління;
- проблема самоврядування;
- проблема конструкції;
- проблема безпеки.

Аналіз загроз безпеки та запропоновані способи захисту

На сьогоднішній день існує ряд проблем для безпечної реалізації Інтернету речей. Віддалене розташування пристроїв і автоматизація збільшує їх незахищеність до несанкціонованого доступу і модифікації. Найбільшою загрозою є здійснення атаки «відмови в обслуговуванні», метою якої є порушення коректного функціонування сенсорної мережі.

Шкідливий код може поширюватися скориставшись уразливими місцями та помилками в конфігурації. Зловмисники можуть установлювати програмне забезпечення збору даних, які дають можливість витягання конфіденційної інформації. Хостовий захист є досить ефективним, так як в ньому використовується ряд технологій, такі як: шифрування, розмежування доступу до системних ресурсів, захист на основі репутації і поведінки, захист від шкідливих програм, пісочниця. Таким чином, залежно від потреб конкретної системи IoT, об'єднання цих технологій може забезпечити ефективний захист кожного пристрою. Пісочниця і розмежування доступу до ресурсів забезпечать захист входів і виходів в системі, так як вони обмежують мережеві підключення до додатків і перевіряють вхідний і вихідний потік трафіку, захищають від переповнення буфера, цілеспрямованих атак, налаштовує роботу додатків, але при цьому дозволяють зберігати контроль над пристроєм. Такі кроки ще можуть використовуватися для запобігання несанкціонованого використання, блокування конфігурації та налаштувань пристрою, також для зміни привілеїв користувачів. Хостовий захист дає можливість аудиту та допомагає відстежувати події безпеки. Технології на основі політик можуть працювати навіть в середовищах без підключення до інформаційної мережі або при обмеженій обчислювальній потужності, необхідної для використання традиційних технологій. Поєднання потрібних технологій має залежати від конкретних ситуацій, але наведені вище засоби можуть об'єднуватися для захисту пристроїв, навіть в середовищах з обмеженими обчислювальними ресурсами.

Висновки

Отже, було проаналізовано можливі загрози і способи їх попередження. Виявлено, що безпека IoT повинна бути комплексною – всі напрямки загроз повинні усуватися в поєднанні з надійним підписом коду і моделлю перевірки, також хостовий захист може допомогти захистити пристрої від багатьох небезпек.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Что такое Интернет вещей(IoT)? // електрон. текст. дані URL: <https://riot.org/2016/04/04/что-такое-интернет-вещей-iot/>
2. Найдич А. «Интернет вещей» — реальность или перспектива? // електрон. текст. дані URL: <https://compress.ru/article.aspx?id=24290>
3. Росляков А. В. ИНТЕРНЕТ ВЕЩЕЙ : Учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. - Самара : ПГУТИ, 2015 - 136 с.

Маковійчук Ірина Олександрівна — студентка групи ІБС-176, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: ira.konoplitska@gmail.com

Науковий керівник: **Маліновський Вадим Ігорович** — к.т.н., доцент каф. Захисту інформації, Вінницький національний технічний університет, м. Вінниця

Makoviichuk Iryna O. — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : ira.konoplitska@gmail.com

Supervisor: **Malinovskiy Vadim I.** — PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia