УДК 004.5

Н. О. Черневський
В. А. Шатайло

ДОСЛІДЖЕННЯ ПРОБЛЕМ КОНФІДЕНЦІЙНОСТІ ТА СПОСОБИ ЇХ ВИРІШЕННЯ У ГАЛУЗІ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький Національний Технічний Університет

Анотація
В даній статті було розглянуто проблеми конфіденційності в індустрії Інтернету речей та розроблено потенційні стратегії їх ефективного вирішення, для забезпечення безпечної та орієнтованої на конфіденційність екосистеми Інтернету речей.
Ключові слова: Інтернет речей, IoT, захист інформації, конфіденційність, кібербезпека, захист даних.

Abstract
This article examined privacy issues in the Internet of Things industry and developed potential strategies to effectively address them to ensure a secure and privacy-oriented Internet of Things ecosystem.
Keywords: Internet of things, IoT, information protection, privacy, cyber security, data protection.

Вступ

Останнім часом Інтернет речей набув великої популярності, завдяки його здатності полегшувати наше життя та автоматизувати різні процеси. Він широко застосовується в області домашньої автоматизації, охорони здоров'я, виробництва та інших галузях. Кількість підключених пристроїв швидко зростає, а компанії активно працюють над розробкою нових продуктів Інтернету речей. Його популярність пояснюється потужним потенціалом у поліпшенні ефективності та оптимізації різних секторів. Проте, разом з цим з'являється загроза несанкціонованого проникнення в систему, яке може поставити під загрозу конфіденційність та безпеку [1].

Аналіз сучасного стану питання та обґрунтування задачі

Зі зростанням кількості підключених пристроїв, що обмінюються даними, з’являються потенційні ризики безпеки. Зловмисники, намагаючись отримати несанкціонований доступ до систем Інтернету речей, часто використовують різні методи. Одними з таких методів є перехоплення комунікації між підключеними пристроями або використання вразливостей у програмному забезпеченні пристроїв. Хакери можуть скористатися слабкими паролями, незахищеними Wi-Fi мережами або вразливостями в програмному забезпеченні пристроїв для отримання доступу до системи [4].

Після успішного взлому, зловмисники можуть здійснювати широкий спектр небажаних дій. Наприклад, вони можуть збирати та використовувати особисті дані користувачів, отримані від підключених пристроїв. Вони також можуть перехоплювати контроль над цими пристроями, що дає їм можливість керувати ними віддалено. Найбільш тривожною ситуацією є вплив на фізичне середовище, коли зловмисники здатні викликати шкоду або небезпеку шляхом маніпуляцій з критично важливими пристроями. У зв'язку з цим, для ефективного запобігання взлому систем Інтернету речей необхідно приділяти увагу як програмним, так і апаратним засобам безпеки. Ось кілька методів які допоможуть запобігти взлому [2, 3].

Методи програмного запобігання взлому:

- Автентифікація та авторизація: Рекомендується використовувати механізми автентифікації для перевірки легітимності підключених пристроїв і користувачів. Кожен пристрій повинен мати унікальні облікові дані та паролі для забезпечення безпеки.
- Шифрування: Всі дані, що передаються між пристроями або зберігаються на сервері, мають бути зашифрованими, щоб запобігти перехопленню та несанкціонованому доступу до них.
- Оновлення програмного забезпечення: Виробники повинні регулярно випускати оновлення програмного забезпечення, що містить патчі та виправлення вразливостей. Користувачі повинні вчасно встановлювати ці оновлення, щоб забезпечити постійну безпеку системи.

- Моніторинг та виявлення вторгнень: Використання систем моніторингу та виявлення вторгнень (Intrusion Detection and Prevention Systems) може допомогти виявити незвичайну активність або спроби вторгнення в систему. Це дозволяє швидко реагувати та запобігати можливим атакам.
- Фільтрація та блокування шумів: Використання фільтрів та систем блокування шумів може зменшити вплив зовнішніх радіоперешкод на пристрої Інтернету речей. Це дозволяє забезпечити стабільну та надійну роботу системи, навіть у середовищах з високим рівнем радіоперешкод.

Методи апаратного запобігання взлому:

- Криптографічні модулі: Використання апаратних криптографічних модулів допомагає забезпечити безпеку ключів та шифрування даних на апаратному рівні. Це ускладнює завдання зловмисникам, які намагаються отримати доступ до захищених даних.
- Захист мережі: Забезпечення безпеки мережі, через яку підключені пристрої обмінюються даними, є важливим аспектом. Використання захищених протоколів зв'язку, таких як TLS (Transport Layer Security), може допомогти уникнути перехоплення та незаконного доступу до даних.
- Екранування та захист від електромагнітних перешкод: Використання екранів та захисних покриттів може зменшити вплив зовнішніх електромагнітних сигналів на пристрої. Це допомагає забезпечити нормальну роботу системи навіть при наявності радіоперешкод.

Висновки

Під час розгляду даної теми було проаналізовано потенційні ризики безпеки, пов'язані з зростанням кількості підключених пристроїв Інтернету речей. Досліджено способи перехоплення комунікації та використання вразливостей у програмному забезпеченні для незаконного доступу, а також запропоновано шляхи їх усунення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРТ

1. Безпека інтернету речей [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Безпека_інтернету_речей

2. IoT Security Challenges and Problems [Електронний ресурс]. – Режим доступу: https://www.balbix.com/insights/addressing-iot-security-challenges/

3. 11 Biggest security challenges & solutions for IoT - Peerbits [Електронний ресурс]. – Режим доступу: https://www.peerbits.com/blog/biggest-iot-security-challenges.html

4. IoT Security Issues, Threats, and Defenses [Електронний ресурс]. – Режим доступу: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses

Черневський Назар Олександрович — студент групи 2СП-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький Національний Технічний Університет, Вінниця, e-mail: chernevskijnazar@gmail.com

Шатайло В'ячеслав Андрійович — студент групи 2СП-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький Національний Технічний Університет, Вінниця, e-mail: viacheslavshatailo@gmail.com

Chernevskyi Nazar Oleksandrovich — student of group 2SP-21b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: chernevskijnazar@gmail.com

Shatailo Viacheslav Andriyovych — student of group 2SP-21b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: viacheslavshatailo@gmail.com