МАТЕРІАЛИ XXVII МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ

2023

ТОМ 4

ХАРКІВ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 27-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ
«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

10 – 12 травня 2023 р.

Том 4

КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2023

УДК 004:[621.317+621.391](06)

27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2023. – 192 с.

В збірник включені матеріали 27-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті».

Видання підготовлено факультетом інфокомунікацій
Харківського національного університету радіоелектроніки

61166 Україна, Харків, просп. Науки, 14
тел./факс.: (057) 7021397

E-mail: mref21@nure.ua

Програмний комітет конференції

Снігуров А.В. к.т.н., декан факультету ІК
Безрук В.М. д.т.н, зав. каф. ІМІ
Лемешко О.В. д.т.н., зав. каф. ІКІ
Захаров І.П. д.т.н., зав. каф. ІВТ

УДК 004.032.2:621.391

ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

Поддельський В.М.
Науковий керівник – ас. каф. ІМІ, Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м.Харків, Україна
E-mail: vladyslav.poddelskyi@nure.ua

This report discusses the growing popularity of smart homes with the development of the Internet of Things (IoT), which offers a variety of solutions to help people in their daily lives. Smart homes are designed to perform functions such as security, privacy, energy management, and other functions based on the needs of the homeowner. The aim of this work is to study the issue of privacy and security in smart homes, as well as to identify potential types of attacks and countermeasures. It also discusses various types of attacks, including physical attacks, denial-of-service attacks, and man-in-the-middle attacks, and suggests defence methods such as cryptographic algorithms to protect the storage and transmission of information.

На сьогоднішній день, з розвитком інтернету речей (IoT), розумні будинки стали більш доступними та популярними серед споживачів. IoT пропонує безліч рішень, які можуть допомагати людям у повсякденному житті. Розумні будинки є одним із найкращих варіантів. Як правило, такі будинки проектуються для виконання певних функцій, таких як безпека, конфіденційність, управління енергоспоживанням, та інших функцій.

Метою цієї доповіді є дослідження питання конфіденційності та безпеки розумного будинку, а також виявлення можливих видів атак та способів протидії їм. В роботі було розглянуто наступні види атак, такі як фізичні атаки, атаки типу “відмова в обслуговуванні” (DoS), “людина посередині” та інші[1].

Бездротова сенсорна система може бути вразлива до атак типу “відмова в обслуговуванні”, яка відбувається коли зловмисник використовує ПК для передачі повідомлення задля втручання в радіочастотний канал. Ця атака здійснюється шляхом безперервної передачі повідомлень з метою перевантаження каналу, що призводить до некоректної роботи датчика, так як він не може передати інформацію на сервер[2].

Атаки типу “людина посередині” також впливають на роботу всієї системи. В залежності від того, для чого зловмисник проводить атаку, ціль може різнитися. Наприклад, якщо атака направлена на порушення роботи, це може здійснюватися шляхом відправки хибних даних.

Фізичні атаки стосуються можливості зловмисника отримати фізичний доступ до сенсорів та пристроїв. Цей доступ дає змогу ряду атак бути спрямованими на знищення або викрадення пристроїв, незаконну модифікацію коду і отримання конфіденційної інформації, такої як дані авторизації, криптографічні ключі тощо.

В роботі було розглянуто методи захисту від більшості видів атак. Ключовим методом для забезпечення безпеки від кібератак є криптографічний метод. Криптографічні алгоритми використовуються для безпечного зберігання та передачі інформації. Існує два методи криптографічного шифрування – це симетричне та асиметричне. Симетричний алгоритм шифрування використовує один ключ, а асиметричний алгоритм використовує два різні[3].

Криптографічні алгоритми з асиметричним ключем потребують більше обчислювальної потужності та пам’яті, ніж симетричні алгоритми. Симетричний метод шифрування більш підходить для системи розумного будинку, оскільки датчики не мають достатньо ресурсів для виконання складної та ресурсоємної криптографії з відкритим ключем.

Таким чином, можна зробити висновок, що завдяки розвитку Інтернету речей (IoT) розумні будинки стали дуже популярними серед споживачів. Вони можуть значно полегшити повсякденне життя, забезпечуючи безпеку, конфіденційність, управління енергоспоживанням та інші функції. Однак, вони можуть бути вразливими до різних видів кібератак, таких як фізичні атаки, атаки типу DoS та атаки типу «людина посередині». Для того, щоб захистити систему від цих атак, необхідно використовувати криптографічні методи та інші методи захисту. Крім того, слід дотримуватися заходів безпеки, таких як контроль доступу та захист мережі від зловмисників.

Список використаних джерел

1. Fei Hu. (2016). Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. CRC Press.

2. Young, C. (2019). Smart Home: Digital Assistants, Home Automation, and the Internet of Things.

3. Buchanan, M. (2020). The Smart Home Manual: How to Automate Your Home to Keep Your Family Entertained, Comfortable, and Safe. HomeTechHacker.

АЛФАВІТНИЙ ПЕРЕЛІК