УДК 004.056:681.5.042

К.В. Савченко
В.В. Вишньовський
О.П. Войтович

ЗАГРОЗИ ТЕХНОЛОГІЇ IoT

Вінницький національний технічний університет;

Анотація

Проведено огляд деяких з існуючих найпопулярніших загроз безпеці технології інтернету речей. А також описано складові частини безпеки технології IoT.

Ключові слова: Інтернет Речей, розумний будинок, автоматизація, безпека, система, протоколи, ботнет, відмова в обслуговуванні, сенсорні мережі, блокчейн.

Abstract

An overview of some of the most common threats to Internet security technology has been reviewed. It also describes the components of the IT security technology.

Keywords: Internet of Things, smart home, automation, security, system protocols, botnet, denial of service, touch networks, blockchain.

Вступ

Інтернет речей (IoT) активно входить в життя міліардів людей. Основною ідеєю IoT є підключення будь-яких пристроїв до інтернету, або один до одного для активної взаємодії. Це дозволить включати кавоварку натисканням кнопки на смартфоні, або вбудувати в одяг чіпи, які будуть вимірювати показники життєдіяльності організму і автоматично викликати екстрені служби в разі порушень. Але зростання кількості підключених пристроїв спричиняє збільшення ризиків безпеці: від завдання фізичної шкоди людям до простою обладнання – це можуть бути навіть трубопроводи або устаткування для виробітку електроенергії. Оскільки ряд об'єктів таких і систем IoT вже піддавалися атакам і було спричинено значні збитки, забезпечення їх захисту виходить на перший план [1].

Результати дослідження

Під інтернетом речей розуміють не тільки побутову і іншу техніку для дому (холодильники, кавоварки, обігрівачі тощо), а й підключені до мережі автомобілі, телевізори, камери спостереження, роботизоване виробництво, розумне медичне обладнання, мережі енергопостачання і безліч промислових систем управління (турбіни, клапани, сервоприводи і т. д.).

Фундамент безпеки інтернету речей складається з чотирьох частин: безпека зв'язку, захист пристроїв, контроль пристроїв і контроль взаємодії в мережі [1].

На цьому фундаменті можна створити потужну і просту в розробці систему безпеки, яка здатна зменшити негативний вплив більшості загроз безпеки для інтернету речей, включаючи цільові атаки.

Канал зв'язку повинен бути захищеним, для цього застосовуються технології шифрування, перевірки автентичності, щоб пристрої знали, чи можуть вони довіряти віддаленій системі. Також важливим завданням є управління ключами для перевірки автентичності даних і достовірності каналів їх отримання [2,3].

Захист пристроїв – це в першу чергу забезпечення безпеки і цілісності програмного коду. Підписання коду потрібне для підтвердження правомірності його запуску, також потрібен захист під час виконання коду, щоб атакуючі не перезаписали його під час завантаження.

В кожен пристрій, до того, як він попаде, до кінцевого користувача, повинна бути вбудована можливість «управління по повітрю» (over-the air, OTA). Оскільки для працівників служби підтримки немає можливості особисто перевіряти кожен пристрій.

Основними компонентами IoT є такі технології: RFID, NFC та WSNs (англ. Wireless Sensor Networks, бездротова сенсорна мережа чи бездротова мережа датчиків) [4].

Найбільш суттєвими загрозами для RFID-системи є десинхронізація, витоки інформації, повторення атак. Десинхронізаційні атаки дозволять відстежувати мітки, визначати їх розташування, блокувати передачу даних від тега до зчитувача [5].

Особливо вразливою є NFC-технологія. Можуть здійснюватися атаки спрямовані на відмову в обслуговуванні (DoS) або прослуховування. Атаки відмови в обслуговування здійснюються шляхом порушення обміну даних між пристроями таким чином, що надіслані відправником дані не можуть бути розшифровані отримувачем. Також можлива підміна чи вставка неправильних даних, наприклад, коли автовідповідач відповідає повільніше, ніж пристрій зловмисника. Для покращення безпеки, рекомендується використовувати захищені канали зв'язку [5].

Бездротові сенсорні мережі є вразливими до різних видів атак на різних рівнях стеку протоколів. Порушення роботи бездротових сенсорних мереж може бути здійснене потужними сторонніми радіочастотного випромінення. Маючи фізичний доступ пристрою, можна зчитувати інформацію, а також повністю його контролювати. Крім того, є адаптовані для датчиків методи атаки спрямованої на відмову в обслуговуванні. Існує й загроза спуфінгу (spoofing), часткової або повної підміни трафіку [5].

Все частіше IoT-пристрої стають частиною ботнетів. Одним з найновіших ботнетів, який з'явився в січні 2018 року є Hide`N Seek (HNS). За час свого існування, нова загроза атакуюча IoT-пристрої, встигла розростись з 12 скомпрометованих пристроїв до 24 000. HNS будується на базі модифікованої версії Mirai і використовує децентралізовану peer-to-peer архітектуру та власний механізм для P2P-комунікацій. Боти здатні виконувати команди по вилученню даних, виконанню коду і втручатися в роботу пристроїв. Поширюється HNS шляхом комбінації словникових брутфорс атак (brute force) і закодованого списку облікових даних, знаходячи в мережі пристрої з відкритими портами Telnet [6].

Існує також ботнет DoubleDoor, який використовує комбінований обхід фаєрвола (Juniper Netscreen) з експлуатацією багів безпосередньо в цільових пристроях [7].

Порівняльна характеристика загроз в IoT наведено в таблиці 1.

Таблиця 1 – Порівняльна характеристика загроз в IoT

№	Технологія	Загрози	Рішення
1	RFID	Десинхронізація, витік інформації, DoS, MITM.	Використовувати захищені канали зв'язку.
2	NFC	Relay-атака, підміна приймача.	Автентифікація, блокчейн.
3	WSNs	MITM.	Автентифікація , блокчейн.
4	IoT-пристрій	Брутфорс, зараження шкідливим програмним забезпеченням.	Міжмережеве екранування, стійка автентифікація, захист ПЗ.
5	Інтернет	MITM, підміна IP-адрес та всі загрози притаманні для Інтернет.	Використання традиційних методів захисту, шифрування трафіку.

Для захисту від втручання в код програми та підміна показників датчиків, слід використати технологію блокчейн. Блокчейн є розподіленою базою даних, яка потенційно доступна кожному [8]. Завдяки використанню блокчейн, є можливість протидіяти шахрайству, управління ідентифікацією, проведення транзакцій, верифікація стану елементів різних систем, забезпечення цілісності даних. Основними областями застосування блокчейна в IoT стануть ідентифікація пристроїв і забезпечення цілісності даних. Використовуючи взаємодію блокчейн та Інтернет речей можна вирішити ряд проблем з безпекою, а саме:

- блокчейн може використовуватися для відстеження вимірювань даних сенсора та запобігання дублюванню будь-якими іншими шкідливими даними;
- автентифікація та безпечна передача даних.

Витрати на розгортання та експлуатацію IoT можуть бути зменшені через блокчейн, оскільки немає посередника. Також пристрої IoT безпосередньо можуть бути адресовані за допомогою блокчейна, забезпечуючи історію підключених пристроїв для усунення несправностей.

Висновки

Концепція IoT містить в собі величезний потенціал можливостей. Але поруч з цими можливостями виникає цілий спектр загроз безпеки, в тому числі з соціальними наслідками. Завдяки використанню

технології блокчейн, можна вирішити ряд значних проблем з безпекою в IoT.

Проведено огляд складових частин технології інтернету речей. Описано основні аспекти забезпечення безпеки IoT. Розглянуто найпоширеніші загрози безпеці IoT-пристроїв. Проведений аналіз є основою для подальшої розробки системи безпеки представника технології IoT, а саме Розумного будинку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Эталонная архитектура безопасности интернета вещей (IoT). Часть 1 [Електронний ресурс]. – Режим доступу: URL https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 - Назва з екрану
2. Владислав Васильович Вишньовський, Олеся Петрівна Войтович Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс]– Режим доступу: https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2017/paper/view/2738 – Назва з екрану
3. Катерина Володимирівна Савченко, Олеся Петрівна Войтович Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс]– Режим доступу: https://conferences.vntu.edu.ua/index.php/all–fitki/all–fitki–2017/paper/view/2736 – Назва з екрану
4. Kateryna Savchenko, Vladislav Vyshnovskiy. System bezpieczeństwa inteligentnego domu // Materiały konferencyjne. 54. Konferencja studenckich kół naukowych Pionu Hutniczego [Електронний ресурс] – Режим доступу: http://www.kolanaukowe.agh.edu.pl/ph/dzialalnosc/ /54.%20Konferencja%20SKNPH%20 – %20zeszyt.pdf – Назва з екрану
5. Lisa Goeke, Security Challenges of the Internet of Things [Електронний ресурс]. – Режим доступу: URL https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1 – Назва з екрану
6. Обнаружены сразу два новых IoT-ботнета: Masuta и Hide `N Seek [Електронний ресурс]. – Режим доступу: URL https://xakep.ru/2018/01/25/masuta-and-hns/ - Назва з екрану
7. IoT-ботнет DoubleDoor обходит защитные решения с помощью комбинации двух эксплоитов [Електронний ресурс]. – Режим доступу: https://xakep.ru/2018/02/16/doubledoor/– Назва з екрану
8. Why blockchain and IoT are best friends [Електронний ресурс]. – Режим доступу: URL https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/ - Назва з екрану

Савченко Катерина Володимирівна — студентка групи 1БС-17м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: katiasv96@gmail.com

Вишньовський Владислав Васильович — студент групи 1БС-17м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: vyshnovskyi@outlook.com

Науковий керівник:
Войтович Олеся Петрівна — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна

Savchenko Kateryna — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: katiasv96@gmail.com

Vyshnovskyi Vladyslav — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: vyshnovskyi@outlook.com

Supervisor:
Voitovych Olesya — phd. Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine