УДК 621.396

А. О. Паламарчук

О.О. Семенова

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Анотація

Розглянуто потенційні загрози, що супроводжують на кожному шляху розвитку мереж Інтернету речей, а також запропоновані методи вирішення питань загроз. Запропоновані рішення мають потенціал забезпечити безпеку мереж Інтернету речей на стабільно високому рівні.

Ключові слова: Інтернет речей, безпека, захист інформації.

Abstract

The potential threats that accompany each path of development of the Internet of Things are discussed, as well as proposed methods for addressing the threat. The proposed solutions have the potential to ensure the security of the Internet of Things at a consistently high level.

Keywords: Internet of Things, security, information protection.

Вступ

Інтернет речей розширює поняття самого «Інтернету» відповідними технологіями, такими як традиційний Інтернет, мобільні та сенсорні мережі тощо. Кожна «річ» Інтернету речей під'єднана до «Інтернет», ці «речі» також комунікують одне з одним. IoT одночасно володіє великим потенціалом, гнучкістю, масштабованістю, але є також ризик проблем з безпекою, на який не потрібно закривати очі. Через масове поширення даної технології виникає щоразу більше питань до її безпеки, і без відповідних рішень не буде подальшого розвитку, або він стане дуже повільним [1].

Метою даної роботи є дослідження проблеми загроз і обґрунтування способів забезпечення безпеки в мережах IoT.

Результати дослідження

На даний момент є низка загроз для безпеки Інтернету речей на його різних рівнях.

На рівні сприйняття: спуфінг-атаки, радіоглушіння, підслуховування, PDoS-атаки, відключення вузлів і т. д.

На рівні мережі: selective forwarding attack (зловмисник займає кілька нод і не дає конкретним пакетам даних проходити), sinkhole-атаки, MiM-атаки, атаки червоточини (wormhole attack), флуд-атаки HELLO-flood, атаки Сивілли тощо.

На рівні підтримки: підробка даних, DDoS-атаки, неавторизований доступ тощо.

На програмному рівні: сніфери та логери, TCP Hijacking, DDoS-атаки тощо.

Обладнання, що використовується в IoT, як, наприклад, різного роду датчики, шлюзи, GPS та інші подібні девайси, потребують відповідного ефективного захисту. Відкритий проєкт з безпеки вебзастосунків OWASP (Open Web Application Security Project) зайнявся питання безпеки IoT та склав список десяти найбільших слабкостей [2].

Першим кроком впевненість в правильній авторизації. Лише авторизовані особи повинні мати доступ до конфіденційних даних зібраних об'єктами IoT. Для цього потрібно чітко і ясно визначати важливість фізичної ідентифікації та управління доступом. Цим способом однаково задовільнять свої вимоги і автентифікація, і авторизація.

Криптографія є однією з головних технологій, яка бере участь в механізмах безпеки, що стосуються девайсів IoT. Це своєрідна гарантія того, що дані будуть в безпеці. Туди входить шифрування та дешифрування, генерація ключів, хешування та хеш-верифікація. В таблиці 1 наведені одні з часто використовуваних криптографічних алгоритмів для безпеки IoT.

Таблиця 1 – Криптографічні алгоритми

Тип	Алгоритм	Ціль
Симетричне шифрування	Advanced encryption standard (AES)	Конфіденційність
Асиметричне шифрування	Rivestshamir Adelman (RSA)/Elliptic curve cryptography (ECC)	Цифрові підписи, передача ключів
Асиметричне узгодження ключів	Diffie-hellman (DH)	Узгодження ключів
Хешування	SHA-1/SHA-256	Цілісність системи

Висновки

Було розглянуто потенційні загрози мереж IoT і запропоновано методи забезпечення надійного захисту від цих загроз. Приведені методи захисту при відповідній імплементації їх в механізми Інтернету речей мають змогу забезпечити належний, а найголовніше ефективний рівень захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Critical Analysis on the Security Concerns of Internet of Things (IoT) [Елетронний ресурс]. URL: https://research.ijcaonline.org/volume111/number7 /pxc3901280.pdf
2. OWASP internet of things top 10 [Електронний ресурс]. URL: https://owasp.org/www-project-internet-of-things-top-10/

Паламарчук Анастасія Олександрівна – студентка групи ТКТ-18б, факультет інформаційних електронних систем.

Науковий керівник:

Семенова Олена Олександрівна – кандидат технічних наук, доцент кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, Вінниця.

Palamarchuk Anastasia O. - student of the Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia.

Supervisor:

Semenova Olena O. - Candidate of Technical Sciences, Associate Professor at the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia.