CURRENT ISSUES OF COMPUTER SCIENCE AND CYBERNETICS

DOI https://doi.org/10.30525/978-9934-26-115-2-5

ІНТЕРНЕТ РЕЧЕЙ (IOT) В КОНТЕКСТІ КРИПТОГРАФІЇ: ДЕЯКІ АСПЕКТИ ПРОБЛЕМ ШИФРУВАННЯ

Слатвінська В. М.
лаборант кафедри кримінального права, процесу та криміналістики
Міжнародний гуманітарний університет
м. Одеса, Україна

Пристрої Інтернет речей (IoT) особливо вразливі для суб'єктів загрози, оскільки більшість, які зараз випускаються, не підтримують шифрування. Але ситуація виглядає ще гірше оскільки, пристрої IoT зазвичай вимагають певної форми бездротового зв'язку, яка спрощує перехоплення передач даних, якщо немає шифрування. Через характер та розмір пристроїв IoT вони, як правило, мають обмежений обсяг ресурсів. Наслідком цього є те, що більшість пристроїв IoT не мають потужності обробки або ресурсів, необхідних для більш надійних алгоритмів шифрування. Оскільки шифрування все ще є необхідним компонентом для їх функціональності, можна використовувати легкі алгоритми шифрування. Ці алгоритми можуть бути реалізовані в програмному забезпеченні або через інтегральну схему в апаратному забезпеченні. Кожен із цих методів збільшує вартість для виробника IoT, оскільки обидва методи потребують додаткових ресурсів. Наразі не

існує стандарту, і багато пристроїв IoT взагалі не підтримують шифрування [1, с. 126].

Серед наявних проблем в IoT щодо забезпечення захисту інформації можемо навести: аутентифікація датчиків/сенсорів/контролерів/шлюзів; аутентифікація запитів для доступу до датчиків/сенсорам/контролерам/ шлюзам і їх конфігурації; конфіденційність передаваних даних; забезпечення цілісності даних і команд; анонімність і приватність (для консьюмерського IoT) [2, с. 220].

Крім того, переважна більшість користувачів смарт гаджетів не має достатньо часу чи знань для забезпечення захисту для всіх своїх пристроїв, а найчастіше розраховує на далекоглядність їх виробників в аспекті створення надійного захисту [3, с. 9].

У зв'язку з обмеженими ресурсами для забезпечення процесу шифрування на якісному рівні, в IoT почали імплементувати алгоритми LW-криптографії. Як один із алгоритмів було обрано та реалізовано XTEA на мові JavaScript [4, с. 162]. Іншим варіантом забезпечення процесу шифрування на якісному рівні в IoT є використання потужностей Tor, але захищеність даних частково залежить від поведінки користувачів, що не гарантує конфіденційності шифрування.

Отже, розрізняють проблеми шифрування IoT, які спроможні вирішити розробники, і наявний низький рівень комп'ютерної грамотності користувачів IoT, що заважає втілювати нові спроби забезпечення цілісності даних криптографічними методами. У зв'язку з цим вважаємо, що необхідно прийняти державний стандарт шифрування IoT щоб забезпечити мінімальний рівень захищеності даних.

Література:

1. Черненко Р.М., Рябчун О.П., Ворохоб М.В., Аносов А.О., Козачок В.А. Підвищення рівня захищенності систем

мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка. № 3(11). 2021, С. 124–135. https://doi.org/10.28925/2663-4023.2021.11.124135

2. Праворська Н.І. Забезпечення безпечного обміну інформації в мережі елементів інтернету речей. Вісник Хмельницького національного університету, № 1, 2020 (281). С. 219-224. DOI 10.31891/2307-5732-2020-281-1-219-224

3. Гончаренко Н. Застосування механізмів Dark Web для забезпечення нового рівня захисту IoT. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповодідей та тез; м. Київ, 15-16 квітня 2021 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: О.К. Закусило. (голова) та ін.– К.: ВПЦ»Київський університет», 2021. С. 8-9.

4. Петренко А.І. Криптологія в інтернеті речей. Моделювання та інформаційні системи в економіці. 2019. № 97. С. 155–163. DOI: 10.33111/mise.97.16