УДК 004.832

Михайленко Є. О.
Войтович О. П.

МАЛОРЕСУРСНА АВТЕНТИФІКАЦІЯ ДЛЯ СИСТЕМ IOT

Вінницький національний технічний університет

Анотація
Спроектовано систему, яка спрямована на підвищення стану захищеності інформації в системах IoT шляхом розробки та реалізації методу автентифікації.
Ключові слова: кібербезпека, автентифікація, інтернет речей, малоресурсна автентифікація.

Abstract
The system is designed to improve the state of information security in IoT systems, the way to develop and implement the authentication method.
Keywords: cybersecurity, authentication, Internet of Things, low-res authentication.

Вступ

Стрімкий розвиток інформаційних технологій сприяє швидкій появі все нових і нових систем та концепцій. Система IoT (інтернет речей) не виняток. Але разом з новими системами, в геометричній прогресії постають проблеми, в тому числі і проблеми кібербезпеки. Одним із важливих параметрів кібербезпеки є конфіденційність, яку не можливо забезпечити без належної автентифікації, що і забезпечує актуальність цього дослідження. Системи IoT відіграють важливу роль у житті суспільства, вони інтегруються як у промисловість, так і в побут звичайних людей, що тягне за собою проблему, яка полягає в обмеженні доступу до тієї чи іншої інформації[1].

Метою роботи є підвищення стану захищеності інформації в системах IoT, шляхом розробки та реалізації методу автентифікації в системах IoT.

Результати дослідження

Після проведення аналізу відомих методів захисту інформації[2]-[4], які можна використати в межах теми дослідження, було обрано реалізувати метод автентифікації, який буде доцільний для використання в системах IoT, та буде забезпечувати не високу трудомісткість обчислень, так як елементи систем IoT не мають великих обчислювальних потужностей.

Основними вимогами є такі аспекти:

- забезпечення стійкої до атак системи автентифікації;
- відносно мала важкість обчислень;
- інтегрованість в системи IoT;
- використання декількох підходів щодо захисту передаваної інформації для автентифікації;
- забезпечення оптимальної швидкодії.

Нехай є модель системи, в якій «речі» (T_n) об’єднанні в систему (F_n) та передають данні по мережі на сервер (*Cloud server*). Користувачі (FU_n) подають запити на різні операції: обрахування чогось, проведення якогось процесу, обмін інформацією та інше. Ці запити обробляють «речі» які об’єднані в мережу, сервер отримує дані, обробляє їх та обмінюється даними з «речами» та користувачами.

Пропонується метод малоресурсної автентифікації, який є двостороннім, використовує механізм запит-відповідь, ідентифікатори, а також є прив’язка до проміжних результатів в ході автентифікації.

Метод включає в себе багато операцій, які запобігають реалізації різних атак. У методі використовуються:

- мітки часу (послідовності символів, які показують в який момент часу проводиться певна подія);
- псевдовипадкові числа (числові послідовності, які обраховуються за не випадковим алгоритмом, але мають подібні властивості до випадкових чисел);

– геш-функції (функції, які дозволяють перетворювати інформацію різної довжини, в інформацію фіксованої довжини);
– непримітивні математичні/бітові операції (у методі використовуються такі операції як логічне або, та додавання за модулем два);
– зберігання інформації на сторонах в зашифрованому вигляді.

Симбіоз таких операцій, методів, функцій дозволяє підвищити стійкість процесу автентифікації, забезпечити захист від відомих атак, та реалізувати оптимальну швидкодію, зменшити трудомісткість обчислень. Таким чином, хоча фаза легкої аутентифікації виконується у відкритому каналі, інформаційна безпека забезпечена за рахунок обчислень, які проводяться між сторонами.

Аналіз швидкодії, у порівнянні з існуючими методами (таблиця 1) показав, що метод використовує менше обчислювальних потужностей системи.

Таблиця 1 - Порівняння методів малоресурсної автентифікації

Chuang[5]	Shi[6]	Запропонований метод
$8\ T_h + 5\ T_{xor}$	$12\ T_h + 6\ T_{sm}$	$7\ T_h + 3\ T_{xor}$

Використано такі позначення: - (порожнє значення), T_h (Геш функція), T_{xor} (операція Xor), T_{sm} (скалярний добуток).

Висновки

Отже, забезпечено підвищення стану захищеності інформації в системах IoT шляхом розробки та реалізації методу малоресурсної автентифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.
2. Р. Э. Смит Аутентификация: от паролей до открытых ключей. Издательский дом “Вильямс” 2002. – 432 ст.
3. Лужецький В.А., Войтович О. П., Шулятицька О. О. Метод автентифікації у бездротових мережах на основі моделі довіри // Наукоемкие технологии в инфокоммуникициях: обработка информации, кибербезопасность, информационная борьба : монография / под общей редакцией В. М. Безрука, В. В. Баранника. - Х. : Издательство "Лидер", 2017. - С. 500-515.
4. O. Voitovych, L. Kupershtein, O. Shulyatitska and V. Malyushytskyy, "The authentication method in wireless sensor network based on trust model" 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kyiv, Ukraine, 2017, pp. 993-997.
5. Chuang MC, Lee JFTEAM (2011) Trust-extended authentication mechanism for vehicular ad hoc networks[C]//. International Conference on Consumer Electronics, Communications and Networks. International Conference on Consumer Electronics, Communications and Networks (CECNet):1758–1761
6. Shi W, Gong P. A new user authentication protocol for wireless sensor networks using elliptic curves cryptography[J]. International Journal of Distributed Sensor Networks (IJDSN), 2013, (2013–4–11), 2013, 2013(730831):51–59

Михайленко Євген Олегович — студент групи 1БС-19м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 1bs15b.mykhailenko@gmail.com

Войтович Олеся Петрівна — кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Mykhailenko Eugen O.— Student of 1BS-19m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: 1bs15b.mykhailenko@gmail.com

Voytovich Olesia P. — Candidate of Technical Sciences, Docent of the Information Security department, Vinnytsia National Technical University, Vinnytsia.