УДК 004.056.53

Є. О. Михайленко

ЗАСІБ ДЛЯ АВТЕНТИФІКАЦІЇ В ІОТ

Вінницький національний технічний університет

Анотація

Запропоновано засіб для автентифікації в мережі інтернету речей, який дозволяє підвищити захищеність цієї технології, а також забезпечує три основні постулати захисту інформації, тобто, конфіденційність, цілісність та доступність.

Ключові слова: автентифікація, інтернет речей, протокол зв'язку.

Abstract

A means for authentication on the Internet of things is offered, which allows to increase the security of this technology, and provides three basic information security postulates, that is, confidentiality, integrity and availability.

Keywords: *authentication, Internet of things, communication protocol*.

Вступ

Інтернет речей (IoT) – це мережа, яка складається із взаємозв'язаних фізичних об'єктів (речей) або пристроїв, які здійснюють передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку [1]. Всі пристрої, які відносяться до IoT, будь це радіо-няня, інсулінова помпа, кардіостимулятор, чи пристрій контролю тиску у трубопроводі, всі вони потребують захисту, від тих чи інших атак. На сьогодні в технологіях IoT великою вразливістю, є або повна відсутність автентифікації, або не якісна її реалізація, через те що ресурсів для реалізації не достатньо[3]. Тому доцільним буде розробити, адекватну систему автентифікації, яка буде забезпечувати захищеність систем інтернету речей.

Метою роботи є розроблення методу та засобу для автентифікації систем IoT, для підвищення захищеності технології та забезпечення обмеження доступу до оброблюваних даних в системах такого роду, за для того щоб доступ мали лише привілейовані особи.

Результати дослідження

На початку розробки засобу автентифікації в IoT, потрібно дослідити вже відомі способи автентифікації та розмежування доступу в даній технології. На сьогоднішній день найрозповсюдженішими є такі принципи:

- базова автентифікація (найпростіший вид автентифікації за допомогою логіна та паролю які ніяк не захищаються, і передаються у відкритому вигляді)[5];
- дайджест-автентифікація (принцип аналогічний базовій автентифікації, але з однією відмінністю, вона полягає в тому що данні введені користувачем криптографічно захищені);
- автентифікація з пред'явленням сертифікату (базується на пред'явленні цифрових сертифікатів приклад – автентифікація за протоколом SSL)[2];
- децентралізована автентифікація (данні для автентифікації є універсальними і можуть бути використані для входу до багатьох систем, прикладом слугують такі технології як - OpenID, OpenAuth, Oauth та інші);
- автентифікація за допомогою смарт-карток та USB-ключів (дозволяють організувати автентифікацію з закритими ключами, які зберігаються на них);
- багатофакторна автентифікація (використовує декілька методів автентифікації одразу, наприклад логін-пароль + відбиток пальця, логін-пароль + електронна карта, та інше, головне щоб ці фактори були різної природи)

Для забезпечення захисту, обрано дотримання принципу багатофакторної автентифікації, так як вона може мінімізувати не санкціонований доступ, так як для автентифікації використовується декілька факторів, і навіть при зломі зловмисником одного, система буде залишатися захищеною. Вибираючи для системи той чи інший фактор або спосіб аутентифікації, необхідно, насамперед,

відштовхуватися від необхідної ступеня захищеності, вартості побудови системи, забезпечення мобільності суб'єкта. Тому обрано двохфакторну автентифікацію з допомогою логіну та паролю, а також з декілька значним кодом перевірки, який генерується випадково кожні декілька десятків секунд на стороні, і для доступу до цього коду користувач може використати наприклад свій телефон з встановленим ПЗ[4]. На рисунку 1 наведено схему, яка показує принцип роботи системи в якій задіяна двохфакторна автентифікація.

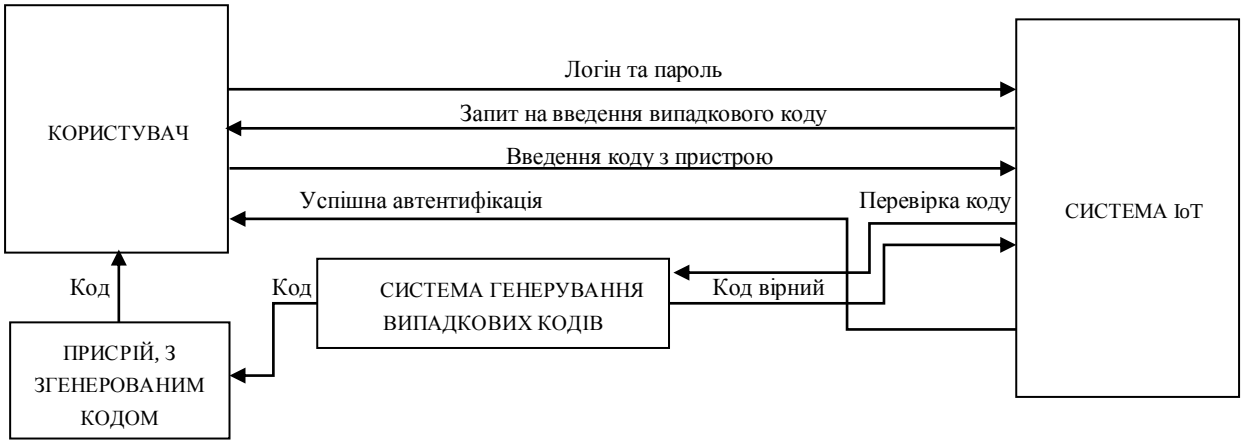

Рис. 1. Схема двоетапної автентифікації

Схема показує принцип принцип роботи системи, він такий:

- Користувач вводить свій логін та пароль;
- При введенні правильних даних, система IoT їх обробляє, та посилає запит на введення випадкового коду;
- Випадковий код генерується в системі генерування, та відправляється на пристрій з якого користувач може його отримати, та відіслати до системи IoT;
- Після отримання випадкового коду система IoT звіряється з системою генерування кодів, чи код вірний;
- Якщо код вірний, автентифікація пройшла успішно.

Висновки

Запропоновано засіб для автентифікації в мережі інтернету речей, який дозволяє підвищити захищеність цієї технології, а також забезпечує три основні постулати захисту інформації, тобто, конфіденційність, цілісність та доступність. Досліджено та проаналізовано розповсюдженні методи автентифікації в IoT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Интернет вещей. Учебное пособие. [Текст]/ Росляков А. В., Ваняшин С. В., Гребешков А. Ю. – Книга, 2015 – 136 с

2. Internet Of Things 101 – IoT Device Authentication Explained [Електронний ресурс]: - https://blog.ipswitch.com/internet-of-things-101-iot-device-authentication-explained

3. Войтович О.П. Дослідженння безпеки системи розумного будинку / Войтович О.П., Вишньовський В.В., Савченко К.В //Тези доповідей Шостої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації» м. Вінниця, 24-25 жовтня 2017 року. – Вінниця: ВНТУ, 2017. – С. 67-70.

4. Евсеев С.П. Исследование методов двухфакторной аутентификации / С.П. Евсеев, О.Г. Король // Системи обробки інформації. – 2014. – Вип. 2(118). – С. 81– 87

5. Баришев Ю. В., Каплун В. А. Метод автентифікації віддалених користувачів для мережевих сервісів Інформаційні технології та комп'ютерна інженерія. - 2014. - № 2. - С. 13-17.

Михайленко Євген Олегович — студент групи 1БС-15б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 1bs15b.mykhailenko@gmail.com

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Mykhailenko Eugen O. — Department of information technologies and computing engineering, Vinnytsia National Technical University, Vinnytsia, email : 1bs15b.mykhailenko@gmail.com

Supervisor: ***Voitovich Olesia P.*** — Cand. Sc. (Eng), Assistant Professor of information protection, Vinnytsia National Technical University, Vinnytsia