УДК 004.738.5:004.722]:004.056

ПРОБЛЕМИ ПІДВИЩЕННЯ БЕЗПЕКИ В IoT

Чорний Р.В.
Науковий керівник – к.т.н., доцент Сердюк Н.М.
Харківський національний університет радіоелектроніки, каф. КІТС
м. Харків, Україна
тел. +38(066) 104-75-20

To reduce risks to users and companies using IoT, security measures such as regular software updates, authentication and authorization, data encryption, and the use of known and trusted standards should be taken. This work discusses modern security methods in IoT. Vulnerabilities of the main protocols: WPA2, TLS, Zigbee have been identified.

Інтернет речей (IoT) пропонує величезні переваги для користувачів та компаній, але з ним також пов'язані різні ризики та небезпеки. Основні з них: небезпека злому, проблеми з конфіденційністю, недостатня безпека, відмова у роботі, ризик від ботнетів, несумісність стандартів, застарівання програмного забезпечення, неавторизований доступ, проблеми з надійністю а також етичні та правові питання.

Для зменшення цих ризиків користувачам та компаніям, які використовують IoT, слід вживати заходів щодо підвищення безпеки, таких як регулярне оновлення програмного забезпечення, забезпечення аутентифікації та авторизації, шифрування даних та використання відомих та надійних стандартів.

Безпечної екосистеми IoT немає. Експерти наполегливо заявляють, що постачальники послуг та пристроїв ринку IoT порушують принцип наскрізної інформаційної безпеки (ІБ), який рекомендований для всіх ІКТ-продуктів та послуг. Відповідно до цього принципу, ІБ повинна закладатися на початковій стадії проектування продукту чи послуги та підтримуватись аж до завершення їх життєвого циклу. Наведено деякі дані досліджень корпорації HP, метою яких було не виявити якісь конкретні небезпечні інтернет-пристрої та викрити їх виробників, але визначити проблему ІБ-ризиків у світі IoT в цілому.

Дослідники HPE звертають увагу на проблеми, як на стороні власників пристроїв, так і на проблеми, над якими повинні подумати розробники. Оскільки не всі прилади мають вбудовані засоби ІБ-захисту, власникам також слід подбати про встановлення зовнішнього захисту, призначеного для домашнього використання, щоб інтернет-пристрої не стали відкритими шлюзами в домашню мережу або прямими інструментами заподіяння шкоди. Доступ до пристрою можна отримати через вразливості в протоколоах, котрі використовуються майже кожною людиною кожен день, наприклад:

- WPA2 (Wi-Fi Protected Access II): це протокол, який забезпечує захищене з'єднання Wi-Fi. Вразливості WPA2 можуть включати атаки на паролі і DoS-атаки.

- Zigbee: протокол бездротового зв'язку, який використовується в багатьох пристроях IoT. Вразливості Zigbee можуть включати атаки на слабкі ключі і MITM-атаки.

- TLS (Transport Layer Security): це криптографічний протокол, який забезпечує захищений зв'язок між пристроями. Деякі з вразливостей TLS включають атаки типу "людина посередині" (Man-in-the-Middle, MITM), атаки на слабкі ключі і відмова в обслуговуванні (DoS) атаки.

У ході проведеного HP дослідження виявлено, що приблизно 70% проаналізованих пристроїв не шифрується бездротовий трафік. Веб-інтерфейс 60% пристроїв експерти HP вважали небезпечним через небезпечну організацію доступу і високі ризики міжсайтового скриптингу. У більшості пристроїв передбачено паролі недостатньої стійкості. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома. Усього ж фахівці HP нарахували близько 25 різних уразливостей у кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток тощо) та їх мобільних та хмарних компонентах.

Висновок експертів HP невтішний: безпечної екосистеми IoT на сьогоднішній день не існує. Особливу небезпеку речі Інтернету ховають у контексті поширення цільових атак (APT). Варто лише зловмисникам виявити інтерес до будь-якої такої системи, то вона стає відкритою для них.

Слабкі місця IoT:

- Перехід на IPv6;
- живлення датчиків;
- стандартизація архітектури та протоколів, сертифікація пристроїв;
- інформаційна безпека;
- стандартні облікові записи від виробника, слабка автентифікація;
- відсутність підтримки з боку виробника для усунення вразливостей;
- важко чи неможливо оновити ПЗ та ОС;
- використання текстових протоколів та непотрібних відкритих портів;
- використовуючи слабкість одного гаджета, хакер легко потрапити на всю мережу;
- Використання незахищеної хмарної інфраструктури;
- Використання небезпечного ПЗ тощо.

Таким чином було з’ясовано, які саме небезпеки чекають користувачів та компанії, котрі використовують IoT. Виявлення проблеми є першим кроком для її вирішення. Хоча сучасні методи вирішення цих проблем ще не можуть вирішити всі проблеми безпеки разом, але на даний час потрібно використовувати не тільки програмні методи захисту, а й апаратні гібридним чином.

Список використаних джерел:

1. “Learning IoT with Particle Photon and Electron” (2016, Packt Publishing Limited). Rashid Khan, Kajari Ghoshdastidar, Ajith Vasudevan.