Львівський державний університет безпеки життєдіяльності

Національний університет Львівська політехніка

Департамент кіберполіції Національна поліція України

Львівська міська рада

LVIV IT CLUSTER

softserve

UnderDefense

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

УДК: 004.7

КЕРУВАННЯ БЕЗПЕКОЮ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ ІНДЕКСУ ДОВІРИ

Уляна Пановик[1], Сергій Кутас [1], Тарас Брич [2]

[1]Української академії друкарства, м. Львів, Україна
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Анотація. *Пристрої IoT за допомогою хмарних технологій збирають величезну кількість цінних даних, значна частина яких зберігається в хмарі. Довіра між пристроями IoT та їхніми даними визнана основою створення системи IoT. Підключення до підозрілих пристроїв Інтернету речей може становити загрозу для послуг і роботи системи. Тому дуже важливо аналізувати та керувати інформацією про довіру для пристроїв, а також надавати інформацію про довіру іншим пристроям або користувачам, яким вона потрібна.*

Ключові слова: *Інтернет речей, безпека IoT, довіра; управління довірчою інформацією; індекс довіри.*

Abstract. *IoT devices use cloud technologies to collect a huge amount of valuable data, a large part of which is stored in the cloud. Trust between IoT devices and their data is recognized as the foundation of an IoT system. Connecting to suspicious IoT devices can pose a threat to services and system operation. Therefore, it is very important to analyze and manage trust information for devices, and to provide trust information to other devices or users that need it.*

Keywords: *Internet of things, IoT security, trust; trust information management; confidence index.*

Інтернет речей – одна з найбільш стрімких у розвитку технологій у світі. Пристрої інтернету речей вже використовуються у багатьох галузях діяльності людини, включаючи такі критичні галузі, як енергетика, охорона здоров'я та військова галузь. Глибока інтеграція цих пристроїв допомагає людям швидко та ефективно вирішувати багато проблем, полегшити виконання складних завдань, вивільнити людські ресурси для виконання більш важливих інтелектуальних завдань. В майбутньому планується подальший розвиток технологій інтернету речей, більш глибока інтеграція в усі сфери діяльності людини та виконання інтелектуальними пристроями все більш складних та важливих функцій.

Для бездротової передачі даних особливо важливу роль в побудові Інтернету речей відіграють такі характеристики, як ефективність, відмовостійкість, адаптивність, можливість самоорганізації. Основне зацікавлення в цьому сенсі представляє стандарт IEEE 802.15.4, що управляє доступом

для організації енергоефективних персональних мереж, і є основою для таких протоколів, як ZigBee, WiFi, Bluetooth, 6LoWPAN.

Проте, незважаючи на всі переваги, які інтернет речей приносить у побут людини, він також несе у собі серйозні загрози. Через велику розповсюдженість інтернету речей та важливість функцій, які виконують пристрої IoT, сфера інтернету речей приваблює все більше уваги зловмисників. Втручання у роботу інтелектуальних пристроїв може призвести до фінансових збитків, які нараховують мільярди доларів США, або навіть нести безпосередню загрозу для життя людей.

Встановлено, що за допомогою пристроїв інтернету речей вже відбулося багато інцидентів інформаційної безпеки з отриманням несанкціонованого доступу зловмисників до персональних даних. Через високий ступінь інтеграції в життя та побут людей, ці пристрої мають доступ до великого обсягу персональної інформації. А через низький рівень захищеності пристроїв IoT, ця інформація може потрапити до зловмисників чи компаній, які можуть використовувати цю інформацію для власних потреб.

Спеціалісти OWASP визначили 10 основних проблем інформаційної безпеки, пов'язаних з IoT, до яких відноситься: незахищений вебінтерфейс, недостатній механізм автентифікації/авторизації, незахищені сервіси мережі, відсутність шифрування при передачі даних, порушення конфіденційності, незахищений хмарний інтерфейс, незахищений мобільний інтерфейс, недостатня конфігурація безпеки, ненадійне програмне забезпечення, слабка фізична безпека. Кожна з цих проблем містить додаткові вразливості, які зрештою можуть призвести до модифікації або витоку даних [1].

Для забезпечення загального рівня інформаційної безпеки при використанні об'єктів Інтернету речей будь-якого призначення можна виділити чотири основні складові:

− безпека зв'язку (за допомогою технологій шифрування і перевірки справжності);

− захист пристроїв (забезпечення цілісності програмного коду, наприклад шляхом криптографічного підписання);

− контроль пристроїв (необхідність встановлення патчів та передбачення "безпеки зсередини" – вбудованої функції оновлень "по повітрю" ("over-the-air") на пристроях);

− контроль взаємодії в мережі (періодичні моніторинг, сканування та аналітика мережі на предмет аномалій та загроз).

Унікальним для IoT є те, що пристрої (наприклад, вбудовані датчики) повинні розпізнати інші пристрої. Саме це зменшує ймовірність проникнення чужорідного тіла в системі. Для забезпечення інформаційної безпеки на почтакових етапах "спілкування" з чужорідним пристроєм можна ввести таке поняття як індекс довіри (trust index) для пристроїв IoT [2].

Індекс довіри прямо пропорційний достовірності джерела з точки зору схожості. Чим вищий показник довіри, тим більше шансів для системи, що дані надійдуть від авторизованого пристрою IoT або джерела. На малюнку представлений алгоритм перевірки для підключення в систему (рис. 1).

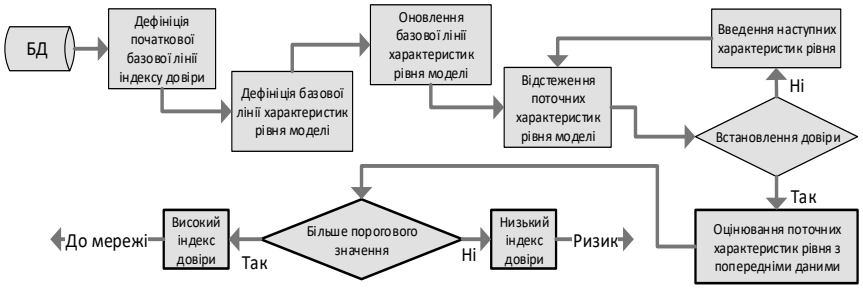

Рисунок 1 – Алгоритм перевірки безпеки

Якщо індекс довіри нижче порогового, то відповідно пристрій не зможе знаходитися в мережі. Система переспрямовує трафік з пристрою на сервіс, який аналізує відповідь і намагається зібрати більше даних про напад.

Ці дані надходять до підсистеми безпеки, і він оновлює параметри характеристик рівня для вивчення та аналізу атаки або зупиняє її на першому ж етапі. Відповідно, для зловмисників буде не легко копіювати дані. Це відбувається з тієї причини, що складність рівня збільшується, і стає важче влізти в систему або створити хибні характеристики. Наприклад, характеристики фізичного рівня, такі як направлення на абонента(angle of arrival) в бездротовому зв'язку. Приймач отримає дані, програмно визначити їх неможливо. Будь-який зловмисник не зможе придумати такі характеристики, доки він не використовуватиме таке ж обладнання чи місцезнаходження.

Такий алгоритм можна застосувати для зменшення ймовірності спуфінга. Система зможе проаналізувати мережу на наявність "чужих" пристроїв та вберегти її від злому, не дозволить зловмиснику проникнути в мережі та забезпечить інформаційну безпеку інформаційної системи IoT.

Інформаційні джерела

1. Um T-W, Lee E, Lee GM, Yoon Y. Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments. Sensors. 2019; 19(21):4707. https://doi.org/10.3390/s19214707

2. Warsun Najib, Selo Sulistyo, Widyawan. Survey on Trust Calculation Methods in Internet of Things. Procedia Computer Science 161 (2019) 1300–1307. 10.1016/j.procs.2019.11.245.