ЗАХИСТ ДАНИХ В ІНТЕРНЕТІ РЕЧЕЙ

Трохименко Д. В.; Курдеча В. В., доцент, к.т.н.
Національний технічний інститут України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

Концепції, засновані на Інтернеті речей, такі як розумні пристрої, розумні автомобілі, розумні міста та розумні будинки, охоплюють як статичні, так і динамічні об'єкти фізичного світу та світу формування, які можна ідентифікувати та інтегрувати в комунікаційні мережі. Важливо виділити той факт, що дані, які надаються речами, часто є конфіденційними. Вони можуть містити стан нашого довкілля, стан наших будинків і міст або стан особистого здоров’я та діяльності. Ось чому механізми забезпечення та гарантії безпеки та конфіденційності даних є вирішальними питаннями в IoT. Завдяки своїй природі захист Інтернету речей є комплексним і складним завданням. Далі наведені основні загрози безпеці мережі та запропоновано протидії, які допоможуть їм запобігти чи знизити вплив на мережу.

Завдяки своїй природі як різнорідної мережі, потенційні загрози для даних IoT мають майже нескінченні можливі вектори атак [1]. Ці вектори можна приблизно розділити за початковою ціллю атаки:

Атаки проти IoT-пристроїв: в першу чергу експлуатуються вразливості обладнання.

Атаки проти комунікацій: в основному експлуатується вразливості, пов’язані з перевіркою цілісності даних.

Атаки на рівень сприйняття: в основному використання вразливості безпеки в сенсорних мережах, як цілісність служб та доступність мережі.

Атаки на фізичний рівень: експлуатуються вразливості, пов'язані з фізичними каналами.

Атаки на мережевий рівень: експлуатуються вразливості каналів передачі.

Такі складні системи, як IoT та Cloud, не можуть бути захищені одним загальним протоколом. Кожен шар мережі пред'являє власні вимоги [2]. Один із підходів зазначає, що взаємодія між користувачем та пристроєм має бути обмежена підключенням до віртуального об'єкта, використовуючи відповідний захист. Кожен користувач у хмарі може навіть мати своє особисте уявлення про послуги пристрою та параметри, таким чином обмежуючи шанс витоку даних та крадіжки привілеїв. Відсутність доступу до фізичних пристроїв зменшить вимоги до архітектури безпеки і таким чином зменшить складність самої системи.

Приклад такої системи захисту даних IoT розглянемо oneM2M. OAuth 2.0 використовується в oneM2M для забезпечення аутентифікації та авторизації, як показано на рисунку 1. Mobius, платформа сервера відкритого коду IoT забезпечує загальні сервісні функції як проміжне програмне забезпечення для IoT-додатків різних областей обслуговування. Будь-який пристрій IoT підключений через спеціальне програмне забезпечення TAS (Thing Adaptation Software) та спеціальну платформу пристроїв IoT (& Cube), а додаток IoT може контролювати речі через API [3]. Архітектура безпеки oneM2M поділяється на: Security Functions Layer - забезпечує шість функцій захисту. Secure Environment Abstraction Layer, Secure Environments Layer - містять декілька захищених середовищ, які реалізують різні служби безпеки.

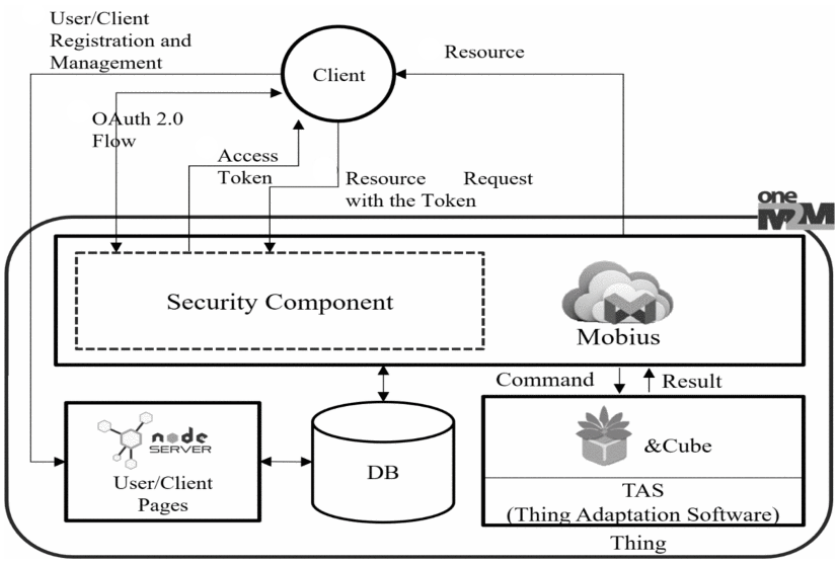

Рисунок 1. Структура підключення для компонента безпеки OneM2M

Часто дані IoT не є надійно засвідченими, а служби репутації даних не доступні [4]. Застосування Blockchain вирішує проблему з довірою, надаючи вузлам спосіб перевірити дані, що поширюються всередині мережі, щоб переконатися, що вони не були жодним чином підроблені. Однак сам по собі Blockchain не дає гарантії, що дані не будуть підроблені ще до того, як дані з нього потраплять у мережу, цю задачу має вирішувати система моніторингу. Необхідність зберігання історії транзакцій може бути принаймні частково вирішена з частково розподіленим блок-ланцюгом, коли кожен вузол містить лише відповідні йому дані.

В інтересах вирішення проблем управління та моніторингу системи інформаційної безпеки пропонується використання Artificial Immune System (AIS) [5]. Підхід, заснований на AIS, сканує дані у IoT та аналізує їх, щоб визначити, чи містять вони загрози чи порушення. AIS дозволяє виявляти мутовані загрози безпеці. AIS складається з таких частин: моделювання антигену, моделювання детектора, механізм еволюції та самотолерантності. В імунній системі антигеном називають вихідні дані. Детектори використовуються для розпізнавання аномальних антигенів. Механізм самотолерантності використовується для запобігання реакції на власні антигени. При цьому,

розпізнавати власні антигени можуть спеціальні детектори, однак такі детектори не повинні використовуватися для безпосереднього виявлення загроз. Потім AIS проводить оцінку та вибирає дії відповідно до політик реагування, що можуть бути встановлені на основі прогнозованих системних потреб та вартості мережевих ресурсів, або вони можуть бути динамічно змінені, реагуючи на зміни в мережі.

IoT інтегрує передові технології комунікацій, мереж, хмарних обчислень, зондування та спрацьовування, а також прокладе шлях для новаторських додатків у різних областях, що вплине на багато аспектів життя людей та принесе багато зручностей. Тим не менше, враховуючи величезну кількість підключених пристроїв, у питаннях безпеки, конфіденційності та управління в IoT виникають дуже значні ризики. Незважаючи на те, що жодне рішення "для всіх" неможливо створити найближчим часом, все ж є можливість значно підвищити безпеку мережі IoT за допомогою комбінації запропонованих способів та рішень.

Перелік посилань

1. Choudhury T. Privacy and Security of Cloud-Based Internet of Things (IoT) / T. Choudhury, A. Gupta, S. Pradhan, P. Kumar, Y. S. Rathore // *2017 3rd International Conference on Computational Intelligence and Networks (CINE),* 2017 – pp. 40-45

2. Kakanakov N. Adaptive models for security and data protection in IoT with Cloud technologies / N. Kakanakov, M. Shopov // *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2017, – pp. 1001-1004.

3. Oh S. Development of IoT security component for interoperability / S. Oh and Y. Kim // *2017 13th International Computer Engineering Conference (ICENCO)*, 2017, – pp. 41-44

4. Rodrigo R. On the features and challenges of security and privacy in distributed internet of things / R.Rodrigo, Z. Jianying, J. Lopez // Computer Networks 57.10, 2013 – pp. 2266-2279

5. Liu C. A Novel Approach to IoT Security Based on Immunology / C. Liu, Y. Zhang and H. Zhang // *2013 Ninth International Conference on Computational Intelligence and Security*, 2013, – pp. 771-775

Анотація

Представлено можливі вектори атаки зловмисників і запропоновано способи для запобігання і протидії цим атакам в контексті хмари та "речей" мережі Інтернету речей.

Ключові слова: захист даних, Інтернет речей, розподілені мережі.

Аннотация

Представлены возможные векторы атаки злоумышленников и предложены способы предотвращения и противодействия этим атакам в контексте облака и "вещей" сети Интернета вещей.

Ключевые слова: защита данных, Интернет вещей, распределенные сети.

Abstract

Possible attack vectors for attackers were presented. Proposed methods that can be used to to prevent and counter these attacks in the context of the cloud and "things" of the Internet of Things.

Keywords: data protection, Internet of Things, distributed networks.