УДК 004.056

Троценко В. В. ,
Остапченко К. Б.

ЗАХОДИ БЕЗПЕКИ В СИСТЕМАХ З ІНТЕРНЕТУ РЕЧЕЙ

У даній роботі розглядається проблема безпеки даних, якими оперують пристрої в IoT-системах, а також пропонуються базові принципи щодо проектування, розробки та інтеграції IoT-продуктів для розробників, вендорів та кінцевих користувачів таких продуктів.

Ключові слова: інтернет речей, багатофакторна аутентифікація, шифрування даних, динамічне тестування.

Бібл.: 3.

The article describes the problem of data security used by devices in IoT systems and offers the basic principles for designing, development and integrating IoT-products for developers, vendors and end-users of such products.

Key words: Internet of things, multifactor authentication, data encryption, dynamic testing.

Bibl.: 3.

Актуальність теми дослідження. Останнім часом все більше систем Інтернету речей інтегрується в середовище нашого побуту, що передбачає обмін даними через пристрої цих систем. З ростом обсягу даних, що передаються та обробляються в таких системах постає питання безпеки доступу до них. Метою даного дослідження є представлення набору правил розробки систем Інтернету речей для досягнення високого рівня безпеки таких розробок, які можуть використовуватися як основи майбутніх стандартів та сертифікатів. Більшість з цих правил можуть бути застосованими до будь-якого пристрою з інтернет-з'єднанням; однак, дана робота зосереджена на безпеці та заходах конфіденційності для IoT [1].

Постановка проблеми. Деякі виробники випускають та продають пристрої IoT, які не містять достатнього набору функцій безпеки. Це призводить до серйозних збитків, як економічних, так іморальних, конкретним особам та організаціям, що використовують IoT системи. Останній приклад цього - відеореєстратори та IP-камери, які зараз виготовляються компанією XiongMai Technologies. Оскільки пристрої IoT набувають великої популярності, якщо не вжити певних заходів для захисту цих пристроїв, то масштаб завданих збитків в майбутньому може бути ще більшим [3].

Аналіз останніх досліджень і публікацій. Стрімкий розвиток та розповсюдження IoT-технологій та систем, розроблених на їх базі, спричинив багато запитань до безпеки функціонування таких систем. В зв’язку з цим, останнім часом організації, що розробляють світові стандарти якості програмного та апаратного забезпечень, зокрема IEEE, проводять багато досліджень у цій галузі та публікують їх результати.

Виділення недосліджених частин загальної проблеми. В даній роботі пропонуються загальні принципи до проектування та розробки IoT-систем та пристроїв з високим рівнем безпеки і захищеності даних, обмін якими відбувається в таких системах.

Постановка завдання. На даний час, оскільки різні запобіжні заходи безпеки є обумовленими специфікою області застосування та визначаються в різних умовах по-різному, неможливо визначити набір універсальних правил для безпеки IoT. Однак важливо сформулювати набір загальних принципів для заходів безпеки та конфіденційності при розробці та інтеграції IoT систем.

Викладення основного матеріалу. В рамках даної роботи пропонується набір рекомендацій щодо забезпечення високого рівня безпеки IoT систем, згрупованих за призначенням:

- Безпека пристроїв;
- Безпека мереж;
- Безпека IoT-систем в цілому.

Безпека пристроїв.

1. Своєчасне встановлення оновлень прошивки

На сьогоднішній день постачальники пристроїв та виробники не мають достатніх фінансових стимулів для забезпечення IoT-пристроїв постійними оновленнями, на відміну від розробників програмного забезпечення, оскільки дохід надходить виключно від продажу пристрою, а не від технічного обслуговування. Проте, такі оновлення мають місце у разі виявлення того чи іншого недоліку в програмному забезпеченні пристрою, тому що вони є закріпленими в гарантійному документі на законодавчому рівні. Саме тому будь-яке оновлення прошивки пристроїв має бути обов'язково встановленим.

2. Динамічне тестування

Важливо, щоб пристрої IoT пройшли ретельне тестування та встановили мінімальну базу метрик, що відображають достатній рівень безпеки. Статичне тестування IoT пристроїв не призначене та не використовується для виявлення вразливостей, які існують в компонентах, що не входять до складу апаратної частини, що була інтегрована в пристрій, таких як процесори та пам'ять. Тобто, за допомогою статичного тестування перевіряються тільки апаратні компоненти пристрою, що відповідають за передачу даних, а не ефективність їх обробки [2].

В той же час, динамічне тестування здатне виявляти як слабкі сторони коду, так і будь-які дефекти чи уразливості, що виникають внаслідок апаратного забезпечення, і які можуть бути невидимими для статичного аналізу. Динамічне тестування може виявити вразливості, які створюються, коли новий код використовується на старих процесорах. Саме тому, рекомендується виробникам, які купують апаратне і програмне забезпечення від інших, здійснювати динамічне тестування, щоб забезпечити безпеку елементів.

3. Розробка процедури для безпечного захисту даних при утилізації пристроїв

Врешті-решт, коли пристрої стають застарілими, користувачі відмовляються від подальшого їх використання з огляду на техніку безпеки. В такому випадку слід провести процес безпечного видалення особистих даних. Це питання конфіденційності, оскільки, якщо пристрій залишається в експлуатації або використовується неправильно, він може слугувати для крадіжки особистої інформації про користувача в екосистемі IoT. Така ж проблема існує і для пристроїв IoT, які продаються другим власникам або стають стандартним обладнанням у будинках та передаються після продажу будинку. Для мінімізації

ризиків, пов'язаних з такою проблемою, виробникам необхідно підготувати рекомендаціїдля користувачів, які описують процедуру безпечного видалення даних з застарілих пристроїв IoT. Промислова практика в корпоративних системах передбачає політику "скинути, переробити або знищити" (DRD) з періодичним переглядом плану, щоб визначити, які пристрої потребують утилізації та як розпоряджатися ними. Деякі виробники закликають користувачів проводити такі процедури безпосередньо через службу підтримки виробника [1].

Безпека мережі.

1. Використання складного процесу аутентифікації

У пристроях IoT не слід використовувати прості значення для імені користувача та пароля, такі як admin / admin. Пристрої не повинні використовувати облікові дані за замовчанням, які є інваріантними на кількох пристроях, і не повинні надавати змогу переходити до налагоджувального режиму, оскільки в такому випадку є можливість отримання доступу до інших пристроїв системи, через інтерфейси інших .

Рекомендується використовувати двофакторну аутентифікацію (2FA), яка вимагає від користувача вживати як пароль, так і іншу форму аутентифікації, яка не залежить від знань користувача, наприклад, випадковий код, що генерується за допомогою SMS-повідомлень. Для IoT-додатків особливо рекомендується використання контекстної аутентифікації (CAA), також відомої як адаптивна аутентифікація, в якій контекстна інформація та алгоритми машинного навчання постійно оцінюють ризик зламування. Якщо ризик є високим, то система не дозволить вхід без багатофакторного токену [1].

2. Використання складного шифрування та безпечних протоколів

Навіть якщо паролі пристроїв є безпечними, зв'язок між пристроями може бути вразливою. У IoT існує багато протоколів, включаючи Bluetooth, Zigbee, Z Wave, 6LoWPAN, Thread, Wi-Fi, мобільний зв'язок, NFC, Sigfox, Neul і LoRaWAN. Залежно від протоколу та доступних обчислювальних ресурсів, пристрій може бути більш-менш здатним використовувати високорівневе шифрування. При розробці сучасних IoT систем рекомендується застосовувати найсильніші методи та алгоритми шифрування, переважно IPsec та / або TLS / SSL [2].

Проте, бувають випадки, коли шифрування не є бажаним, наприклад, в SAE J2735 Основні повідомлення про безпеку (BSM), автомобілі бездротового зв'язку можуть комунікувати один з одним, щоб уникнути зіткнень. У цих випадках повідомлення можуть бути відправлені відкритими, тобто, без шифрування, та перевірені за допомогою цифрових підписів. Проте слід враховувати наслідки пропуску шифрування. Якщо дані передаються незашифрованими та непідписаними, слід дотримуватись запобіжних заходів фільтрації отриманих даних, щоб переконатись, що помилково отримані дані не можуть нанести шкоди.

3. Зменшення пропускної здатності пристрою

Останнім часом в системах, які функціонують на базі IoT-пристроїв атаки DDoS стали досить частими прецедентами. Більшість пристроїв IoT складаються з товарних компонентів, які значно перевищують можливості мережі для функції, яку вони повинні виконувати, що спричиняє затори з запитів в домашніх мережах і потенційно може призвести до величезних втрат даних. Для прикладу припустимо, що кожен IoT-пристрій здатний генерувати трафік на рівні ліній, еквівалент-

ний Gigabit Ethernet (81,274 - 1,488,096 кадра в секунду), наприклад, система ARM9 на одному чіпі (SoC) має два таких вбудованих з'єднання. Таким чином, встановивши понад 10 IoT-пристроїв в систему та ввімкнувши їх в роботу на повну потужність, ми отримаємо 80% вірогідність створення DDoS-атаки всередині самої системи.

Не виключаються також і DDoS-атаки, спричинені зловмисниками. Враховуючи значну пропускну здатність IoT-пристроїв, вони легко можуть пропускати таку кількість трафіку, серед якого шкідливий в режимі реального часу виявити є дуже складним завданням.

Розробникам рекомендується обмежувати кількість мережевого трафіку, що можуть пропускати пристрої IoT на програмному рівні. Незважаючи на високи запас потужності обробки пакетів даних, якими комунікують IoT-пристрої в системах, доцільно знижувати та регулювати його з метою забезпечення ефективної та стабільної їх роботи. Також розробникам рекомендується використовувати обмеження пропускної здатності на апаратному рівні та рівні ядра процесору, щоб збільшити швидкість передачі мережі до стабільного рівня. Такі обмеження ускладнюють для зловмисників використання пристрою під час атаки DDoS, навіть якщо він повністю скомпрометував це. Окрім того, пристрої слід запрограмувати для самоконтролю при незвичній поведінці та відновлювати себе до заводських налаштувань при виявленні тривожної поведінки. Якщо перезавантаження пристроїв до заводських налаштувань неможливо, пристрої потрібно принаймні перезавантажити, щоб потенційно очистити код, який зловмисник запускає в пам'яті [3].

Безпека IoT-системи в цілому.

1. Захист конфіденційної інформації

Основна ідея IoT полягає в тому, щоб з'єднувати побутові об'єкти через Інтернет або спеціальну внутрішню мережу. Пристрої IoT надають інтерфейси для комунікації, які можуть бути виявленими іншими пристроями IoT. Більшість протоколів є вразливими та можуть призвести до витоку особистої інформації, такої як ім'я власника або інші персональні дані. Не виключено, що дані, що були викрадені можуть бути пов'язані з іншими джерелами інформації для цільових атак. Рекомендується використовувати сервісні механізми та захищені протоколи аутентифікації й передачі даних, щоб пристрій могли виявити виключно авторизовані клієнти [1].

2. Інститут сертифікації IoT

Через поширені проблеми з безпекою та конфіденційністю, які вже спричинені пристроями IoT, поступово створюється технічна база, на основі якої розробники беруть на себе відповідальність за свої розробки. IEEE або деяка міжнародна організація надають професійну програму сертифікації для проектувальників, розробників та провайдерів нових технологій IoT, які зобов'язуються дотримуватися визнаних правил створення нових пристроїв.

Проте, на сьогоднішній день цих заходів недостатньо і орган сертифікації повинен перевіряти принаймні наступні елементи продукту постачальника:

- Використовувані або рекомендовані протоколи, за якими було розроблено продукт, не мають містити інформації про користувачів, окрім необхідних для функціонування пристрою;
- Коли виникають проблеми з конфіденційністю, сертифікований постачальник має негайно реагувати на проблеми;

- Аутентифікація має бути достатньо комплексною та відповідати перевіреним протоколам;
- Пристрої не мають перевантажуватись та повинні бути захищеними відповідно до нормативних документів;
- Пристрої повинні мати ідентифікаційну мітку, яку неможливо легко підробити, і яка містить веб-посилання, на якому клієнти можуть шукати статус сертифікації пристрою разом із описом пристрою (модель та серійний номер тощо).

Висновки. В даній роботі було розглянуто набір загальних принципів, на основі яких мають будуватись сучасні IoT-пристрої та системи. Наведено загальні рекомендацію для розробки та експлуатації таких пристроїв та систем як на апаратному, так і на програмному рівнях. Дотримуючись даних рекомендацій, розробники та постачальники IoT-продуктів, мінімізують як економічні, так і репутаційні ризики, пов'язані із безпекою своїх продуктів.

Список використаних джерел

1. Stankovic J. A. Research Directions for the Internet of Things [Електронний ресурс] / IEEE INTERNET OF THINGS JOURNAL. – 2014. – №1. – С.1–7. – Режимдоступудожурн. : https://ru.scribd.com/document/354442742/IEEE-Research-Directions-for-the-Internet-of-Things.

2. Hua-Dong Ma. Internet of Things: Objectives and Scientific Challenges [Електронний ресурс] / Journal of Computer Science and Technology. – 2011. – №26. – С.919–920. – Режим доступу до журн. : https://link.springer.com/article/10.1007%2Fs11390-011-1189-5.

3. Baker F. Broadband Internet Technical Advisory Group. [Електронний ресурс] : Internet of Things (IoT) Security and Privacy Recommendations. – 2016. – №1. – С.17–41. – Режим доступу до журн. : https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

ДОВІДКА ПРО АВТОРІВ

Остапченко Костянтин Борисович – к.т.н., доцент, кафедра технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Ostapchenko Konstantin – doctor of technical sciences, associate professor, Department of Tehnical Cybernetics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: okb2003@ukr.net

Троценко Владислав Вікторович – студент, кафедра технічної кібернетики, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Trotsenko Vladyslav – student, Department of Tehnical Cybernetics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: vtrotsenko1@gmail.com

Trotsenko Vladyslav, Ostapchenko Konstantin

SECURITY MEASURES IN IOT SYSTEMS

Relevance of research topic. Recently, more and more systems of the Internet are integrated into the environment of our everyday life, which involves the exchange of data through the devices of these systems. With the increase in the amount of data transmitted and processed in such a system raises the issue of security access to them. The purpose of this study is to present a set of Internet safety principles (IoT), rules for developing Internet things to achieve a high level of security and best practices for such developments that can be used as the basis for future standards and certificates. Most of these rules can be applied to any device with an Internet connection; However, this article focuses on security and privacy practices for IT.

Formulation of the problem. Some manufacturers produce and sell IoT devices that do not have a sufficient set of security features. This leads to serious damage, both economic and moral, to specific individuals and organizations that use the IoT system. The latest example is video recorders and IP cameras now mentioned by XiongMai Technologies. Because IoT devices are becoming popular, if you do not take certain measures to protect these devices, the scale of the damage done in the future may be even greater.

Analysis of recent research and publications. The rapid development and spread of IoT technologies and systems developed on their basis has raised many questions about the security of the functioning of such systems. In this regard, organizations that develop world-class standards for the quality of software and hardware, such as IEEE, have been conducting a lot of research in this area and publishing them.

Selection of unexplored parts of the general problem. This article provides general principles for the design and development of IoT systems and devices with a high level of security and security of data exchange that occurs in such systems.

Setting objectives. At the moment, since various precautionary measures are due to the specifics of the scope and are defined in different conditions in different ways, it is impossible to define a set of universal rules for the security of the IoT. However, it is important to describe a set of general principles and best practices for security and privacy measures in the development and integration of IoT systems.

Presentation of the main material. Within the framework of this article a set of recommendations for ensuring a high level of safety of IoT systems grouped by appointment is proposed.

Conclusions. In this paper, a set of general principles on which modern IoT devices and systems should be built are considered.. Following these recommendations, developers and vendors of IoT products minimize both the economic and reputational risks associated with the safety of their products.

Key words: Internet of things, multifactor authentication, data encryption, dynamic testing.