УДК 004.62:004.031.2:004.031.43

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

Бушинський Д.А., Курдеча В.В.
Навчально-науковий Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: dbushynskyi2002@gmail.com

CHALLENGES OF INFORMATION SECURITY IN THE INTERNET OF THINGS NETWORK

Suggestions for improving the effectiveness of protection and integrity of confidential data by modifying the architecture of the Internet of Things network.

Конфіденційність є дуже широким і різноманітним поняттям, для якого в літературі пропонується безліч визначень і точок зору. Інформаційну конфіденційність прийнято розуміти як право та можливість обирати, яка особиста інформація буде відома і кому саме. Таке визначення конфіденційності, охоплює ідею інформаційного самовизначення, дозволяючи користувачеві оцінити ризики, вжити відповідних заходів для захисту своєї інформації та бути впевненим, що вона не виконується за межами сфери його безпосереднього контролю.

Поняття особистої інформації є нечітким, оскільки конфіденційність є глибоко соціальною концепцією, що підлягає дуже різноманітним індивідуальним сприйняттям і вимогам. Тож, при розробці нових систем і послуг необхідно ретельно оцінити чутливість залученої інформації та відповідних вимог користувачів.

З вдосконаленням пристроїв, збільшенням обчислювальної потужності та зменшенням споживання енергії тенденція впровадження IoT продовжиться. Однією з найскладніших тем у такому взаємопов’язаному світі мініатюрних систем і датчиків є аспекти безпеки та конфіденційності: без упевненості, що гарантується безпека приватної інформації та належний захист, користувачі не за хочуть прийняти цю нову технологію, яка непомітно інтегрується в життя. Щоб широко запровадити IoT, цю проблему слід вирішити, щоб забезпечити впевненість користувачів щодо конфіденційності та контролю особистої інформації.

Ця публікація присвячена проблемам безпеки, конфіденційності та методам їх вирішення в мережі IoT. Уразливі місця, як правило, відносяться до мало захищених місць системи, якими можуть зацікавитися зловмисниками для виконання корисливих дій. В Інтернеті речей хакери можуть використовувати цілісність, конфіденційність і доступність послуг для законних користувачів, користуючись перевагами таких проблем, що проростають. Тому розуміння такої делікатності в системі стає обов'язковим до розробки відповідних захисних механізмів.

Для початку потрібно вказати зображені на рис. 1 основні вразливості IoT:

1. Безпека пристроїв.

Цей аспект безпеки в першу чергу включає фізичне пошкодження пристроїв IoT, головним чином спричинене несанкціонованим доступом до них.

2. Незахищене впровадження.

Відсутність належної перевірки перед впровадженням пристрою.

3. Мережеві вразливості.

Зазвичай вони включають незахищені служби в самих пристроях, відсутність належної автентифікації та шифрування, тобто використання стандартних або слабких паролів, а також застосування методів шифрування, які не відповідають стандартам полегшеної криптографії в IoT

4. Уразливості програмного забезпечення.

Невиконання відповідних оновлень програмного забезпечення, використання застарілих бібліотек або компонентів програмного забезпечення.

5. Недостатня конфіденційність.

Це означає компрометацію особистої інформації користувача без запиту його дозволу.

6. Недосконалий механізм аудиту.

Відсутність достатнього механізму журналювання.

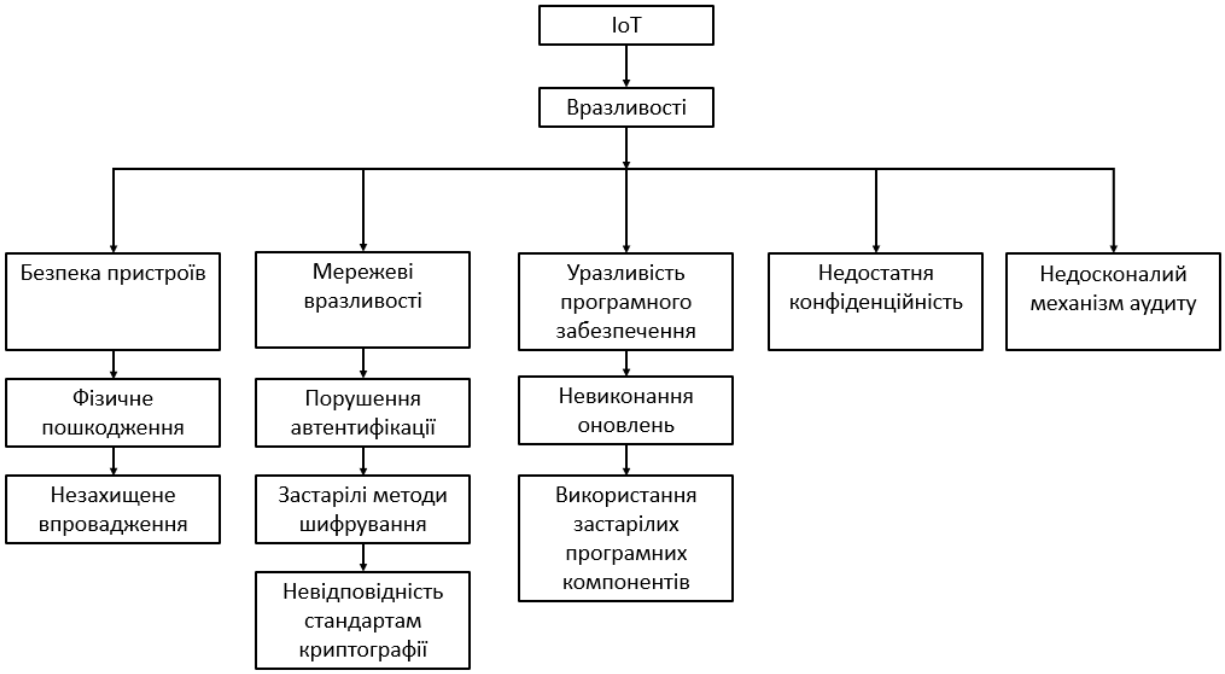

Рис. 1. Основні вразливості IoT.

Рішення на основі навчання для захисту IoT. Фахівці з machine learning (далі - ML) визначають підходи до навчання як продуктивний інструмент для вирішення проблем безпеки, що призводить до

об’єднання підходів ML і deep learning (далі - DL) з технологією intrusion detection system (далі – IDS).

Контрольоване навчання.

Процедура вивчення функціональних можливостей із навчального набору даних. Основною метою є оцінка функції відображення для прогнозування правильних вихідних міток для заданих нових даних.

Неконтрольоване навчання.

Для моделювання елементарної або прихованої структури даних через відсутність позначеного набору даних сприяє комплексній оцінці даних.

Навчання з підкріпленням.

Методика пов’язана із застосуванням відповідних дій програмних агентів у середовищі для максимізації роботи. Два основні методи навчання з підкріпленням включають пошук політики та апроксимацію функції цінності.

Федеративне навчання.

Ця передова техніка машинного навчання здатна тренувати моделі машинного навчання розподіленим способом. Традиційно під час передачі оновлень між централізовано керованим сервером і підключеними пристроями в мережі спостерігалися значні витрати на зв’язок. Накладні витрати на мережу призводять до компрометації швидкості передачі даних, надійності, конфіденційності та управління ресурсами. Проте з появою методів федеративного навчання (далі – FL) спостерігається значне покращення аспекту безпеки розумних систем. Моделі навчання під FL використовують переваги розподіленого характеру навчання та забезпечують передачу лише параметрів, які можна вивчати, замість цілих наборів даних.

Для прикладу, розглядаючи «розумне місто» де пристрої знаходяться на відкритій території, тобто, повністю залишені у розпорядженні природи та зловмисників, доцільно використати як доповнення захисту до вище згаданого ML та DL програмне забезпечення (далі - ПЗ) яке зможе моніторити стан кожного пристрою в мережі. Це у свою чергу завадить клонуванню пристроїв, несанкціонованому доступу до них. Забезпечення конфіденційності базуватиметься не лише на зібраній інформації від ПЗ про певні аномалії конкретного пристрою, а й на передачі цих даних для опрацювання ML для постійного вдосконалення захисту.

Література

1. Jan H. Z. Конфіденційність в Інтернеті речей: загрози та виклики [Електронний ресурс] / H. Z. Jan, G. M. Oscar, W. Klaus – Режим доступу до ресурсу: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.795.
2. Wei C. H. Інтернет речей: еволюція, проблеми та складнощі безпеки [Електронний ресурс] / C. H. Wei, M. Parushi, S. Yashwant – Режим доступу до ресурсу: https://www.mdpi.com/1424-8220/21/5/1809.
3. Fadele A. A. Безпека Інтернету речей: огляд [Електронний ресурс] / A. A. Fadele, O. Mazliza, A. T. brahim – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455.