Моделювання кіберзагроз для Інтернет речей

Олександр Бєлов[1], *Максим Делембовський*[2], *Віталій Шкляр*[3]

[1, 2] Київський національний університет будівництва і архітектури
просп. Повітрофлотський, 31, Київ, Україна, 03037
[1]sanya100110@gmail.com,
[2]maksdel2@gmail.com, https://orcid.org/0000-0002-6543-0701
[3] Національний транспортний університет
вул. М. Омеляновича-Павленка 1, Київ, Україна, 01010
[3]parabellum199316@gmail.com

Отримано 29.04.2021, прийнято 19.05.2021
https://doi.org/10.32347/tit2141.0303

ВСТУП

Сучасний світ неможливо вже уявити без інформаційних технологій. В основі таких технологій лежить використання комп'ютерної техніки та засобів комунікацій. Як і в реальному світі, так і у віртуальному трапляються злочини, що отримали назву «кіберзлочини». Таким чином, об'єкти енергетичного забезпечення, транспортні системи, фінансові і банківські структури, військові відомства та правоохоронні органи, торговельні, медичні й наукові установи є потенційними жертвами комп'ютерної злочинності, зокрема кібертероризму.

Камери спостереження, датчики руху, біочіпи, розумні побутові прилади – всі ці речі спрощують наші повсякденні справи та роблять наше сучасне життя більш зручнішим. Із ростом кількості пристроїв, підключених до мережі, зростає і кількість кіберзагроз. Наприклад, розумний холодильник став частиною бот-мережі і почав розсилати спам, а розумна кавоварка виявилася причиною атаки на індустріальні мережі з подальшим зараженням комп'ютерів.

Інтернет речі, котрі в свою чергу мають простоту і складність реалізації, також володіють деякими проблемами, пов'язаними з інформаційною безпекою. Часом розробники, навмисно або ненавмисно, залишають недокументований канал, який не просто збирає інформацію про застосування пристрою, але і дозволяє проникати в особистий простір кінцевого користувача.

У разі вчинення витоку персональних даних, метою шахраїв зазвичай є особисті дані: імена, поштові адреси, адреси електронної пошти, дані кредитних карт або інформація про акаунт. Це дозволяє здійснювати замовлення товарів в Інтернеті під чужим іменем та оплачувати їх, використовуючи чужу дебетову картку або списання коштів з певного рахунку. З тією ж метою може використовуватися фішинг, котрий включає в себе використання фіктивних веб-сайтів, електронної пошти чи текстових повідомлень для доступу до персональних даних.

МЕТА

Метою дослідження являється оцінювання ризиків кіберзагроз, які поширюються через Інтернет речей.

ОСНОВНА ЧАСТИНА

Інтернет речей (Internet of Things – IoT) – одна з найвідоміших концепцій у науці прогнозування майбутнього, футурології, що складається із взаємопов'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу та обмін даними між фізичним світом і комп'ютерними системами через стандартні протоколи зв'язку. Ці мережеві протоколи представляють собою набори правил та дозволяють здійснювати зв'язок і обмін даними між двома або більше підключених до мережі пристроїв [1].

Сьогодні поняття «Інтернет речей» включає в себе відразу кілька явищ. Це і самі пристрої, які підключені до глобальної мережі і взаємодіють між собою. Це і спосіб підключення «M2M» – тобто машина-до-машина, без участі людини. Також це і великі об'єми даних, які тепер генерують ці пристрої [2].

Моделювання кіберзагроз для Інтернет речей можна поділити на два етапи. Перший етап показує технології порушення роботи пристроїв інтернет речей. Другий етап відображує моделювання існуючих вразливих місць і методів доступу до контролю пристроїв.

Основною концепцією Інтернету речей є взаємодія фізичних об'єктів та пристроїв. Пристрої мають вбудовані датчики і програмне забезпечення, що дає змогу здійснювати обмін даними між пристроєм та комп'ютерною системою за допомогою стандартних протоколів зв'язку. Найпримітивніша система Інтернету речей складається з пристрою, що включає в себе апаратну частину, програмне забезпечення, технологію передачі даних між пристроєм і системою, та саму систему, яка отримує дані.

Вразливість пристроїв Інтернет речей поділяється на два типи:

– апаратне ураження;
– взаємодія пристроїв через технології передачі даних.

На апаратному рівні дуже часто використовується радіочастотна ідентифікація «RFID-мітки». Ці мітки встановлюються на такі пристрої як перепустки, ключі, аудіо- та відеоконтроль, системи електронних платежів тощо. Особливістю та вразливістю цієї технології є:

– безконтактне спрацювання та передача інформації;
– зчитування та запис інформації за допомогою отриманням сигналів;
– спрацювання без джерела енергії;
– легкість у використанні та встановленні;
– велика ймовірність пошкодження;
– впровадження інформації на пристрій без попередньої перевірки;
– можливість впровадження нового пристрою у мережу з певними частотами;
– отримання даних про місцеположення за сигналом міток [3].

Технологія NFC, яка в свою чергу принесла дуже зручний спосіб розрахування картками і телефонами, має ті самі вразливості, що й RFID-мітки. NFC – це безконтактна технологія обміну інформацією на відстані не більше 10 см. Попри зручність даної технології, існує велика можливість отримати вірус на пристрій і втратити персональну інформацію, паролі чи сам доступ.

QR – це технологія штрих-кодів, їх ще називають фізичними гіперпосиланнями, тобто підпис, за котрим можна легко отримати контакти, перейти на сайт в інтернет магазині чи завантажити вірус на пристрій через посилання. Попри зручність, без спеціального програмного забезпечення, людина ніяким чином не може визначити правдивість даної "картинки-адреси", яка також може бути і набором певних команд для зміни налаштувань скануємого пристрою.

Самою найрозповсюдженішим способом отримання доступу через механізми передачі даних є втручання у бездротову мережу. Всі бездротові мережі в будь-якому випадку з'єднуються з дротовою мережею. Відповідно, при проникненні у дротову мережу, ураження розповсюджується по всім пристроям. Ураження може проходити через програмно-апаратні методи захисту локальних мереж:

– мережеві екрани;
– криптографічний захист;
– антивірусні програми;
– біометричні технології ідентифікації та аутентифікації;
– віртуальні захищені канали.

Для технологій бездротової передачі даних особливо важливу роль в побудові Інтернету речей відіграють такі характеристики, як:

– ефективність
– відмовостійкість;
– адаптивність;
– самоорганізація.

Типи атак які виконуються у бездротовому інтерфейсі IEEE 802.11:

– імперсонація та Identity Theft;
– мережевий сніффинг;
– IP- та MAC-spoofing;

– парольні атаки;
– атаки типу "Man-in-the-Middle";
– переадресація портів;
– віруси і додатки типу "троянський кінь";
– відмова в обслуговуванні (Denial of Service – DoS);
– атаки на рівні додатків;
– атаки з деаутентифікацією [4…6].

Системи захисту потрібно комбінувати між собою для більшої ефективності, бо стандарт IEEE 802.11 надає вкрай слабкі засоби забезпечення безпеки, які схильні до численних мережевих атак.

Найефективнішими методами захисту від атак на Інтернет речей будуть:

– планова перевірка апаратного функціоналу пристроїв;
– перевірка та використання систем захисту і антивірусів;
– шифрування даних найсучаснішими стандартами і технологіями;
– резервне копіювання.

Варто зазначити, що будь-який пристрій Інтернет речей не може бути повністю захищений від будь-яких вразливостей. Деякими характеристиками завжди потрібно було жертвувати для того, щоб система відповідала іншим вимогам. Як приклад, деякі пристрої володіють простотою у використанні та мобільністю. Для отримання таких параметрів нехтують захистом.

ВИСНОВКИ

Наразі, більшість компаній розроблюють пристрої Інтернет речей, але не в кожній із них є стандарти та правила застосування технологій цих пристроїв. Звідси випливає, що відсутність певних протоколів стандартів безпеки збільшує ймовірність зараження пристроїв кожного дня, які зіштовхуються багато користувачів. Більшість Інтернет речей слугують дуже великою зручністю, але при цьому жертвують безпекою інформації. Стрімкий ріст пристроїв Інтернет речей показує таку тенденцію, що в майбутньому все більше цих технологій набиратимуть популярність у всіх сферах людської життєдіяльності. На даний час постає питання запобігання отримання несанкціонованого доступу до таких приладів.

Ключові слова: Інтернет речі, кібератака, стандарт протокол, захист пристроїв, інформаційна безпека.

ЛІТЕРАТУРА

1. Futurum [Електронний ресурс]: «Інтернет Речей: концепція IoT». – Режим доступу: https://futurum.today/internet-rechei-kontseptsiiaiot-shcho-chekaty-vid-maibutnoho/ (дата звернення: 19.04.2021).
2. AppTractor [Електронний ресурс]: «Интернет вещей». – Режим доступу: https://apptractor.ru/internet-veshhey (дата звернення: 19.04.2021).
3. Bill Glover, Himanshu Bhatt (2006) RFID essentials. O'Reilly Media, Inc., ISBN 0-596-00944- 5, 88-89.
4. UMD Department of Computer Science [Електронний ресурс]: «An Initial Security Analysis of the IEEE 802.1x Standard». – Режим доступу: http://www.cs.umd.edu/~waa/1x.pdf (дата звернення: 19.04.2021).
5. IEEE SA [Електронний ресурс]: «Official IEEE 802.11 Working Group Project Timelines». – Режим доступу: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm (дата звернення: 19.04.2021).
6. Cisco [Електронний ресурс]: «Cisco Wireless LAN Security Web site». – Режим доступу: http://www.cisco.com/go/aironet/security (дата звернення: 19.04.2021).