УДК 621.392

ТЕХНІЧНІ ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ INTERNET OF THINGS І SMART HOME

Здоровець Ю. В., Галькевич О. О., Колесник І. М.

Національний аерокосмічний університет ім. М. Є. Жуковського "ХАІ"

В статті проаналізовані основні проблеми фізичної безпеки пристроїв, загрози цілісності даних, перехват даних та ін. Розглянуті технічні засоби для зниження рівня несанкціонованого доступу до IoT і Smart.

Постановка проблеми

Повсюдне використання портативної електроніки дає поштовх розвитку багатьох сфер індустрії в тому числі і Інтернету, як засобу комунікації не лише між людьми, але і між предметами. Для виробничих компаній наслідки розвитку Internet of Things (IoT) великі. Згідно зі звітом інституту McKinsey Global, IoT має потенціал росту щорічної глобально економічної цінності до 6,2 трильйона доларів до 2025 року та від 80 до 100 процентів всіх виробників будуть використовувати додаток IoT до того ж року, що призведе до потенціального економічного ефекту розміром 2,3 трлн. доларів лише для світового виробництва.

Поштовхом розвитку IoT стали інновації, що дозволили створювати відповідні технології. Відбувся розвиток від простих фізичних систем до складних, включаючи процесори, датчики, програмне забезпечення та цифрові інтерфейси користувача, які підключені до Інтернет та одне до одного. У зв'язку з цим, сьогодні, ми маємо великий спектр обчислювальних пристроїв, що працюють автономно без участі людини, виконуючі різні задачі такі як: моніторинг параметрів оточуючого середовища, управління побутовими пристроями, логістичними ланцюгами на підприємствах та ін.

В міру постійного збільшення числа пристроїв, підключених до Інтернет, виникають нові потенціальні уразливі місця. Недостатньо захищені пристрої можуть служити точками доступу для кібератак, дозволяючи зловмиснику перепрограмувати пристрій чи викликати його несправність. Пристрої недосконалої конструкції можуть піддавати дані користувачів небезпеці викрадання за рахунок недостатнього захисту потоків даних. Несправні чи дефектні пристрої також можуть створювати вразливі точки. Тому, існує необхість в забезпеченні безпеки пристроїв IoT за допомогою впровадження належних заходів щодо захисту об'єктів інформаційної інфраструктури та комп'ютерних систем і мереж від загроз кіберзлочинів

Мета статті

Проаналізувати основні проблеми безпеки пристроїв IoT і Smart Home та дослідити технічні засоби інформації, що відносяться до : запобігання витоку, викрадення, втрати, спотворення, підробки інформації та запобігання інших несанкціонованих негативних впливів та знизять до мінімуму можливість несанкціонованого доступу до IoT і Smart Home.

Основні матеріали дослідження

Аналіз основних проблем безпеки пристроїв IoT. Багато пристроїв, підключених до IoT, таких як датчики і предмети побутової техніки, призначені для масового розгортання, порівняного з числом традиційних пристроїв, підключених до Інтернет. В результаті потенційне число взаємних підключень між цими пристроями є безпрецедентним. Крім того, більшість з цих пристроїв можуть самостійно встановлювати зв'язок один з одним непередбаченим і динамічним способом.

Багато з систем IoT будуть складатися з ідентичних чи майже ідентичних груп. Така однорідність підсилює потенціальний вплив кожної уразливості, умножаючи його на кількість пристроїв, які мають ті ж характеристики.

Розгортання багатьох пристроїв IoT, буде здійснюватися з врахування терміну використання, що на багато років перевищує звичайні терміни для високотехнологічного обладнання. Розгортання цих пристроїв може здійснюватися в умовах, які ускладнять чи зроблять неможливою модернізацію чи зміну конфігурації пристрою; чи дані пристрої зможуть пережити свого виробника і залишиться без технічної підтримки в довготривалі перспективі. В результаті це може призвести до появи уразливостей, які будуть зберігатися протягом тривалого часу.

Багато пристроїв IoT, від самого початку, не припускають можливості оновлення або дана процедура занадто незручна і непрактична.

Багато пристроїв IoT працюють таким чином, що користувач майже немає уявлення про внутрішнє функціонування пристрою чи створюваними її потоком даних. Це створює вразливість в області безпеки, коли користувач вважає, що пристрій IoT виконує певні функції, коли насправді він може виконувати не бажані дії або збирати дані, які користувач не має наміру надавати. Функції пристрою також можуть змінюватися без попередження при оновлені, в результаті чого користувач піддається небезпеці в результаті будь – яких змін, що вноситься виробником.

Деякі пристрої IoT встановлюються в таких місцях, де важко або неможливо забезпечити їх фізичну безпеку.

Технічні канали витоку інформації. Майже всі технічні засоби створюють технічні канали витоку інформації за рахунок побічних і ненавмисних випромінювань. Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення, технічні канали витоку інформації можна розділити на: електромагні-

тні, індукційні; гальванічні; параметричні; апаратні закладки. Технічні канали витоку інформації частіше розглядають в сукупності з джерелами перешкод. Для традиційних систем зв'язку такі перешкоди є негативним явищем, в значній мірі ускладнюють прийом. Джерелами випромінювань в технічних каналах є різноманітні технічні засоби, в яких знаходиться інформація з обмеженим доступом.

Технічні засоби захисту інформації. Технічними називаються такі засоби захисту інформації, в яких основна захисна функція реалізується технічним пристроєм (комплексом або системою). Всі основні засоби захисту інформації за функціональним призначенням можна умовно розділити на наступні групи: інженерні засоби, що представляють собою різні пристрої і споруди, які протидіють фізичній проникненню зловмисників на об'єкти захисту; апаратні засоби (вимірювальні прилади, пристрої, програмно-апаратні комплекси та ін.), призначені для виявлення каналів витоку інформації, оцінки їх характеристик і захисту інформації; програмні засоби, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і в основних засобах обробки даних; криптографічні засоби, спеціальні математичні і алгоритмічні засоби захисту комп'ютерної інформації, переданої з відкритими системами передачі даних і мереж зв'язку.

Залежно від схеми і способу використання енергії спецзасоби негласного отримання інформації можна поділити на пасивні і активні. Пасивний технічний засіб захисту - пристрій, що забезпечує приховування об'єкта захисту від технічних способів розвідки шляхом поглинання, відбиття або розсіювання його випромінювань. До пасивних технічних засобів захисту відносяться екранують пристрої і споруди, маски різного призначення, розділові пристрої в мережах електропостачання, захисні фільтри і т. д.

Мета пасивного способу - максимально послабити акустичний сигнал від джерела звуку, наприклад, за рахунок обробки стін звукопоглинальними матеріалами. Активний технічний засіб захисту - пристрій, що забезпечує створення маскувальних активних перешкод (або імітують їх) для засобів технічної розвідки або порушують нормальне функціонування засобів негласного знімання інформації. Активні способи попередження витоку інформації можна поділити на виявлення і нейтралізацію цих пристроїв. До активних технічних засобів захисту відносяться також різні імітатори, кошти постановки аерозольних і димових завіс, пристрої електромагнітного і акустичного зашумлення і інші засоби постановки активних перешкод. Активний спосіб попередження витоку інформації по акустичним каналам зводиться до створення в "небезпечному" середовищі сильного сигналу з перешкодами, який складно відфільтрувати від корисного.

Для підвищення рівня захисту необхідно забезпечити системний підхід при формуванні системи захисту інформації, тобто використовувати як програмні так і технічні засоби захисту інформації.

Висновки

Оскільки кількість і природа технічних каналів витоку інформації велика і, безперервно зростає необхідно знизити до мінімуму можливість кіберзлому. Для цього необхідно: встановлювати сучасні контролери, що відрізняються від простих ПК; використовувати вузькопрофільні утиліти і операційні системи, адже в них хакерам складніше забратися; закривати будь-яку значиму інформацію про систему від по сторонніх осіб; система віддаленого управління за допомогою Інтернету повинна мати функцію відключення; захистити обмін інформацією між пристроями секретним цифровим ключем

Список використаних джерел

1. Хорев А. А. Способы и средства защиты информации / А. А. Хорев. М.: МО РФ, 2000. — 316 с.

2. Интернет вещей: особенности, проблемы и уязвимости [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://json.tv/tech_trend_find/internet-veschey-osobennosti-problemy-i-uyazvimosti-20160321115428.3

3. Vish Pai. An end-to-end approach is needed for IoT device security [Електронний ресурс] / Vish Pai. – 2015. – Режим доступу до ресурсу: http://blog. aylanetworks.com/author/vish-pai.

Аннотация

ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ INTERNET OF THINGS И SMART HOME

Здоровец Ю. В., Галькевич А. А., Колесник И. Н.

В статье проанализированы основные проблемы физической безопасности устройств, угрозы целостности данных, перехват данных и др. Рассмотрены технические средства для снижения уровня несанкционированного доступа к IoT и Smart Home.

Abstract

TECHNICAL SAFETY EQUIPMENT INTERNET OF THINGS AND SMART HOME

Yu. Zdorovets, O. Galkevich, I. Kolesnyk

In the article the basic problems of physical security devices threat to data integrity, data interception, etc .. Considered the technical means to reduce unauthorized access to IoT and Smart Home.