УДК004.738

А. О. Гресько, Ю. М. Щебланін

ЗАГАЛЬНИЙ, КОМПЛЕКСНИЙ ОПИС ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В "ІНТЕРНЕТІ РЕЧЕЙ"

Розглянута проблема забезпечення безпеки інформації в Інтернеті речей. Запропонована декомпозиція проблеми за типом взаємодіючих пристроїв і характером взаємодії. Розглянуто серверні та вбудовані («embedded») кінцеві системи, їх специфіка і множина можливих загроз. Було проаналізовано характерні для мережевої взаємодії в Інтернеті речей вектори атак. Атаки за цим напрямом агреговано у дві категорії: прослуховування мережевих даних і вплив на мережеві ресурси. Визначено низку технічних, організаційний і нормативних проблем.

Ключові слова: Інтернет речей, IoT, забезпечення безпеки інформації, безпека серверних та вбудованих систем, технічні, організаційні та нормативні проблеми Інтернету речей.

Постановка проблеми

Енергоспоживання сучасних чіпів та вартість їх виробництва постійно знижується.Це стосується не тільки центральних процесорів, але, наприклад, і Wi-Fi-чіпів, вартість яких за останні роки значно знизилася. Як наслідок пристрої з доступом в інтернет стають все простіше і доступніше.

Згідно ITU-T Y.2060 [1], Інтернет речей *(InternetofThings, IoT)*- глобальна інфраструктура для інформаційного суспільства, яка включає передові рішення по об'єднанню фізичних і віртуальних речей на основі існуючих і розроблюванихінформаційних і комунікаційних технологій.

Згідно того ж документу, Річ (кінцевий пристрій) - об'єкт фізичного (реальний), або інформаційного світу (віртуальний), який може бути ідентифікований та інтегрований в комунікаційну мережу.Речі є незалежними системами з вбудованою електронікою, програмним забезпеченням (ПЗ) і сенсорами, здатні до мережевої взаємодії, збору та/або переробки інформації.

За інформацією TechNavio [2], Інтернет Речей буде складати все більше і більше число підключень, а загальна їх кількість зросте до 17 млрд. у найближчі 5 років.Процес складатиметься з трьох хвиль: спочатку, з'єднаються пристрої, які служать споживачам, далі IoT розшириться до підключених пристроїв на підприємствах, і нарешті його використання стане масовим завдяки впровадженню в державних органах та органах виконавчої влади.

IoT дозволить приватним і громадським організаціям оптимізувати управління, прискорити відгук системи виробництва на керуючі впливи, і розробити нові більш ефективні бізнес моделі.

Технологія IoT перетинається з багатьма іншими технологічними областями, включаючи телеметрію, телематику, M2M-комунікацію (міжмашинну взаємодію), інтелектуальні мережі, інтелектуальні системи транспортування та портативні комп'ютери.По суті вона є надзвичайно складним комплексом зібравшим в собі всі останні наукомісткі технології сучасності.

Взаємодія таких пристроїв буде ставати все більш складною в обслуговуванні, управлінні та моніторингу, що при дуже широкому їх розповсюдженні буде експоненціально збільшувати ризики їх використання.

Головною тенденцією притаманною IoT, так само як і його головною проблемою, є дуже швидке збільшення числа кінцевих пристроїв підключених до мережі.

При цьому, інтернет речей, зростаючий швидше ринку смартфонів, будується, функціонує і впроваджується в існуючу мережеву інфраструктуру без приділення уваги питанням безпеки. Щоб система була стійка необхідно закладати функції забезпечення її стійкості та безпечної експлуатації у фундамент технології.У свою чергу сучасний Інтернет речей зростає вибухово і без огляду навіть на елементарні сервіси безпеки, такі як шифрування трафіку або захищену авторизацію.

Аналіз останніх досліджень і публікацій

Кевін Ештон, що є співзасновником Auto-ID Center, першим ввів термін «Інтернет Речей», саме так він назвав свою доповідь дляProcter & Gamble в 1999 році [3].Це була спроба впровадити нову ідею радіочастотної ідентифікації (RFID) в ланцюг поставок виробничих товарів, а в результаті привернуло гарячу увагу до самої ідеї підключення до мережі нових типів пристроїв.

IoT як явище має глобальний характер, а отже, при створенні власної вітчизняної інфраструктури IoT, дуже важливо уніфікувати методи його взаємодії з іншим світом. Організацією з якою в першу чергу слід налагодити взаємодію в цьому питанні є IoT European Research Cluster. Її метою є розгляд потенціалу рішень на основі IoT, координації дослідницької діяльності та досягнення консенсусу щодо шляхів реалізації IoT в Європі.

Розробками в сфері досліджень і стандартизації Інтернету речей займаються багато країн на рівні національних ініціатив, наприклад ANSI (США), BSI (Великобританія), ETSI (Європа),а також на рівні інтернаціональному: ITU, ISO, IEC.

У сфері бізнесу існує EPCglobal - ініціатива GS1з розвитку індустрії стандартів для електронного коду продукту (EPC), створена для підтримки використання RFID у виробництві, що дозволить у майбутньому об'єднати в мережу масову продукцію для постійного моніторингу та контролю якості споживчих товарів.

Питаннями опису та стандартизації IoT в академічній сфері займається Міжнародний консультаційний комітет по телефонії і телеграфії, що входить до складу Міжнародного союзу електрозв'язку.Він видав серію документів під загальним позначенням «Y», що описують глобальну інформаційну інфраструктуру, аспекти протоколізації інтернету і мереж наступного покоління.Безпосередньотемі IoT присвяченітакіпублікації: ITU-T Y.2060. (06/2012) «Overview of the Internet of things», ITU-T Y.2066 (06/2014) «Common requirements of the Internet of things», ITU-T Y.2069 (07/2012) «Terms and definitions for the Internet of things», і ITU-T Y.2068 (03/2015) «Functional framework and capabilities of the Internet of things».

Формулювання мети. Мета статті - сформувати загальний, комплексний опис проблем інформаційної безпеки в "Інтернеті речей" і розглянути найбільш ймовірні вектори атак.

Виклад основного матеріалу

Завдання забезпечення безпеки інформації в IoT можна розподілити на 2 підзадачі: забезпечення безпеки кінцевих систем та забезпечення безпеки їх мережевої взаємодії (рис.1).

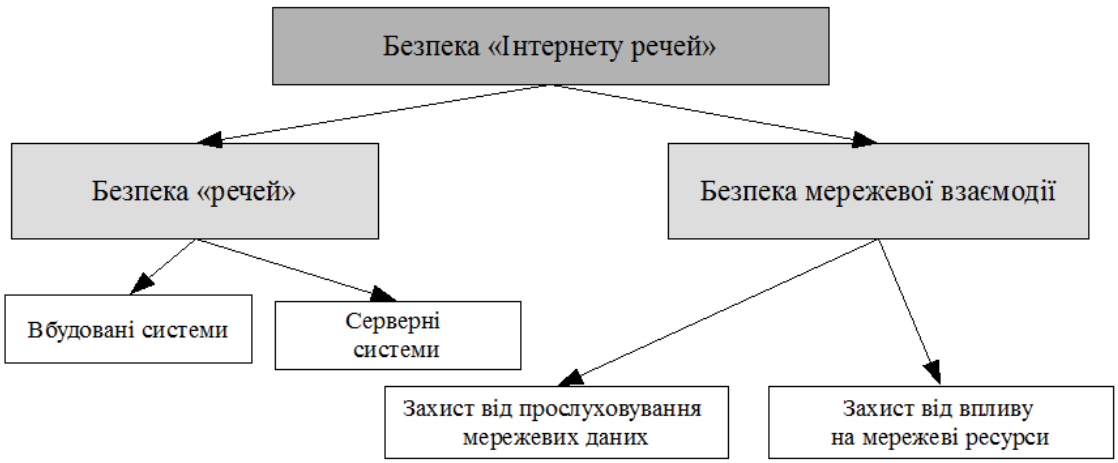

Рис. 1. Загальна структура забезпечення ІБ в IoT

Кінцеві системи зручно розділити на 2 категорії: серверні системи і так звані «embedded» системи.

ЗгідновизначеннюNCStateUniversity 'sElectricalandComputerEngineeringDepartment [4], «embedded» system або «вбудована система» - це система спеціального призначення, в якій комп'ютер повністю вбудований у пристрій, яким він керує.На відміну від комп'ютерів загального призначення, вбудовані системи виконують заздалегідь визначені завдання, як правило з дуже конкретними вимогами.

Вбудовані системи на базі 8- 16- або 32-х бітних мікроконтролерів широко поширені в автоматизованих системах управління технологічним процесом (АСУ ТП), побутовій техніці, автомобілях та інших транспортних засобах і можуть бути інтегровані в мережу інтернет по протоколу IEEE 802.3 Ethernet чи IEEE 802.11x Wi-Fi, а при наявності пам'яті можуть працювати зі стеком TCP/IP.

Говорити про єдиний підхід до захисту вбудованих систем досить складно тому, що на відміну від настільних комп'ютерів і ноутбуків, для яких використовується досить обмежений набір процесорних архітектур (в основному x86), в процесорах для вбудованих систем використовуються численні, конкуруючі архітектури.Найбільш поширені ARM і x86 (Intel-сумісні), меншою мірою - PowerPC та MIPS.

При наявності у зловмисника доступу до таких систем може бути реалізованамодифікація схеми пристрою (плати/мікросхеми), тобто встановлення фізичних закладок в сам пристрій або в розрив кабелю (у разі Ethernet) здатних утворювати канали витоку інформації.

Причиною виникнення в кінцевих пристроях програмних закладок, здатних впливати на дані, що передаються до наступних пристроїв в мережі, є неправильні процеси оновлення версій прошивки, або використання сторонніх прошивок неліцензованих виробників.

Основним джерелом загроз залишається сам доступ таких пристроїв до мережі, при цьому першочергове завдання полягає в недопущенні несанкціонованого доступу до вбудованих систем, так як в залежності від сфери застосування вони можуть бути безпосередніми джерелами впливу на навколишнє середовище.

Найчастіше функції управління у вбудованих системах не виносяться в окремий пристрій і всі функціональні алгоритми виконуються безпосередньо в межах системи.Для цього на них встановлюється операційна система (ОС), що може бути дуже малою, спеціально розробленою для використання у вбудованих системах, або урізаною версією системи, яка зазвичай використовується на комп'ютерах загального призначення.

Багато вбудованих систем настільки спеціалізовані, що вся логіка може бути реалізована у вигляді програми на асемблері, що зберігається в пам'яті без необхідності встановлення операційної системи.

Найчастіше у вбудованих системах використовуються операційні системи на базі вільного програмного забезпечення (тобто, програмне забезпечення, яке доступне безкоштовно і може бути використане з будь-якою метою). В значній мірі це обумовлено, мінімізацією вартості кінцевої продукції, а також можливістю вільно модифікувати такі операційні системи відповідно до вимог конкретного кінцевого продукту.

Операційні системи на базі Linux найбільш широко використовуються у вбудованих системах, що розробляються в США і Європі. Безкоштовними операційними системами, які зазвичай використовуються у вбудованих систем є: Freertos, NetBSD і OpenBSD.

Для повноцінної комунікації в інтернеті речей буде мало об'єднання в мережу одних тільки вбудованих систем, вони цілком можуть виконувати дрібні функції автономно, наприклад в побутовій техніці, проте сервісне обслуговування тієї ж побутової техніки (первинне налаштування, оновлення прошивки, резервне копіювання конфігурації), вимагатиме підключення до таких систем зовні.Найімовірніше подібна взаємодія буде проводитися в рамках клієнт-серверної архітектури, а значить припускає наявність деяких

серверних систем, які є центрами обробки, координації та консолідації інформації від кінцевих систем.

Не менш гостро стоїть питання захистусерверних систем**,** які представляють собою програмно-апаратні комплекси, що виконують певні мережеві служби і реалізовують прийом запитів від клієнтів.Згідно звіту W3Techs [5, 6], 35.98% серверних систем працюють на базі ОС Linux (Debian, Ubuntu, CentOS, RHEL, Gentoo);31.52% на базі BSD та інших Unix-подібних системах (FreeBSD, HP-UX, Solaris);і 32.5% на базі Windows Server.

Проведений аналіз використання операційних систем дозволяє визначити загрози їх безпеки і згрупувати їх за наступними векторами [6]:

- Використання відомих (легальних) каналів отримання інформації (експлуатація помилок в конфігурації системи безпеки, несанкціоноване використання легальних облікових записів та ін.).
- Використання прихованих каналів отримання інформації (загроза використання зловмисником недокументованих можливостей ОС, вразливостей нульового дня та ін.).
- Створення нових каналів отримання інформації за допомогою вбудованого шкідливого коду (використання логічних бомб, троянських програм та ін.).

Важливої уваги заслуговують питання мережевої взаємодії в IoT. За цим напрямом можлива реалізація наступних векторів атак на інформаційну систему:

1. Прослуховування мережевих даних. Сюди відноситься мережева розвідка та аналіз мережевого трафіку, використання сніфферів на різних рівнях моделі OSI. Використання розумних пристроїв розмиває кордони локальних мереж, що належать окремим суб'єктам, і це може дозволити зловмиснику на основі відкритих даних отримати доступ до закритих мереж.

2. Вплив на мережеві ресурси. Це дуже широка категорія до якої можна віднести різні види спуфінгу на різних рівнях моделі OSI, атаки типу Man in the middle, ін'єкції коду, підміна довірених суб'єктів (session hijacking), атаки типу відмова в обслуговуванні (DDoS), атаки типу brutforce, криптоаналіз алгоритмів передачі. При широкому поширенні IoT, і недостатньому забезпеченні безпеки включених до нього кінцевих систем, кількість можливих об'єктів для DDos-атак а також потенційний збиток від їх здійснення багаторазово зросте. Відмови розумних побутових приладів можуть призводити до неполадок в електромережі і пожеж. Відмова датчиків зворотного зв'язку в системі АСУ ТП може призвести не тільки до втрати прибутку через затримку виробництва, але й до різноманітних надзвичайних подій.

Крім того пристрої підключені до мережі, є потенційними агентами бот-мереж, і реалізації атак цього вектора призведуть до несанкціонованого використання обчислювальних ресурсів цих пристроїв для розсилання спаму або участі у DDoS-атаках.

Крім проблем чисто технічного характеру слід також згадати проблеми організаційні та нормативні:

- Масштаб створюваної інфраструктури. Підключені пристрої будуть генерувати дуже великий трафік і для його обслуговування необхідно буде забезпечити можливості розширюваності та масштабованості мережевої інфраструктури.
- Складнощі з документування методів і засобів обробки інформації в усіх кінцевих пристроях. Значна частина IoT буде підзвітна не корпоративним організаціям, з чіткими прописаними політиками безпеки, а простим користувачам, які подібними питаннями взагалі не переймаються. Що в свою чергу призведе до дуже швидкого зростання бот-мереж на основі розумних будинків, або розумних побутових приладів, а також масового порушення конфіденційності персональних даних.
- Відсутність єдиного підходу. Незважаючи на те, що існує безліч сучасних технологій за допомогою яких можна побудувати IoT, широко прийнятих уніфікованих стандартів для розробників все ще немає. Відсутність стандартизованого підходу до побудови IoT призведе до виникнення нових типів загроз і загальної вразливості системи.

Висновки і рекомендації

З точки зору технічної стандартизації, IoT можна розглядати як глобальну інфраструктуру для інформаційного суспільства, яка поєднує передові послуги на основі існуючих і розроблюваних інформаційних і комунікаційних технологій.

У найближчому майбутньому IoT буде безпосередньо причетний як до життя простих людей так і до бізнесу і державної діяльності. Отже таку складну структуру необхідно будувати з урахуванням сучасних вимог до інформаційної безпеки.

До питання забезпечення захищеності інформації в межах IoT необхідно підходити комплексно і особливо приділяти уваги таким аспектам як безпека кінцевих інформаційних систем і безпека їх взаємодії.

Кінцеві системи в цілях декомпозиції можна розділити на вбудовані і серверні системи, відповідно підходи до їхнього захисту будуть відрізнятися. Основним завданням цього напрямку є побудова захищених операційних систем, які зможуть ефективно протистояти інформаційним атакам, як по відкритим, так і закритим каналам передачі інформації.

З погляду мережевої взаємодії слід приділяти увагу захисту від прослуховування мережевих даних і впливу на мережеві ресурси.

Також окремо слід відзначити наявність організаційних і нормативних проблем IoT, таких як відсутність єдиного підходу до стандартизації взаємодії між окремими інформаційними системами, складності з організацією документованості інформаційних процесів, зокрема політик безпеки, і питання масштабованості.

Література

1. Overview of the Internet of things.// ITU-T Recommendation Y.2060. – 2012.

2. Global IoT Security Market 2015-2019 // TechNavio, 2015.

3. Kevin Ashton. That 'Internet of Things' Thing [Електронний ресурс] / Kevin Ashton // RFID Journal, 2009 // Режим доступу: http://www.rfidjournal.com/articles/view?4986 (22.02.2016 р.)

4. Embedded Computer Systems [Електроннийресурс] // NC State University's Electrical and Computer Engineering Department // Режим доступу: http://www.ece.ncsu.edu/research/cas/ecs (22.02.2016 р.)

5. Usage of operating systems for websites [Електроннийресурс] // W3Tech // Режим доступу: http://w3techs.com/technologies/overview/operating_system/all (22.02.2016 р.)

6. Usage statistics and market share of Unix for websites [Електроннийресурс] // W3Tech. // Режим доступу: http://w3techs.com/technologies/details/os-unix/all/all (22.02.2016 р.)

7. Шаньгин В. Защита информации в компьютерных системах и сетях / Владимир Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

Надійшла 29.01.2016 р. Рецензент: д.т.н., проф. Бурячок В.Л.