УДК 004.7

А. І. Горбовський
О. П. Войтович

ДОСЛІДЖЕННЯ БЕЗПЕКИ У ІНТЕРНЕТІ РЕЧЕЙ

Вінницький національний технічний університет

Анотація

Досліджено засоби передавання в мережі, основні поняття Інтернету речей, їх розробка та проблеми впровадження. Проаналізовано проблеми безпеки та методи їх усунення. Проаналізована основна концепція Інтернету речей та його взаємодія з людиною.

Ключові слова: мережа, інтернет, інтернет речей, безпека, інформація, інформаційні технології.

Abstract

The means of transmission in the network, the basic concepts of Internet of things, their development and introduction problems are researched. The problems of security and troubleshooting are analyzed. The basic concept of the Internet of things and its interaction with man is investigated.

Keywords: network, internet, internet of things, security, information, information technology.

Вступ

Інтернет речей — це мережа, що складається із взаємозв'язаних фізичних об'єктів (речей) або пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Крім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові і бездротові мережі. Ці взаємопов'язані об'єкти (речі) мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів[1].

Основною концепцією IoT є можливість підключення всіляких об’єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки. Всі ці об'єкти (речі) повинні бути оснащені вбудованими датчиками або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої концепції є система «розумний будинок» або «розумна ферма»[3].

Результати дослідження

Для практичної реалізації всі навколишні предмети і пристрої (домашні прилади і посуд, одяг, продукти, автомобілі, промислове обладнання та ін.) повинні бути забезпечені мініатюрними ідентифікаційними і сенсорними (чутливими) пристроями[1]. Тоді при наявності необхідних каналів зв'язку з ними можна не тільки відслідковувати ці об'єкти і їх параметри в просторі і в часі, але і керувати ними, а також впроваджувати інформацію про них в загальну «розумну планету». У загальному вигляді з інформаційно-комунікаційної точки зору Інтернет речей можна записати у вигляді такої символічної формули:

IoT = Сенсори (датчики) + Дані + Мережі + Послуги.

Інтернет речей - це глобальна мережа комп'ютерів, датчиків (сенсорів) і виконавчих пристроїв (актуаторів), що зв'язуються між собою з використанням інтернет протоколу IP (Internet Protocol)[1].

При впровадженні Інтернету речей усе наше повсякденне життя кардинально зміниться. Підуть в минуле пошуки потрібних речей, дефіцити товарів або їх перевиробництво, крадіжки автомобілів і мобільних телефонів, оскільки буде точно відомо, що, в якому місці і в якій кількості знаходиться, виробляється і споживається.

Останнім часом для передачі даних від пристрою до обробника подій використовуються такі технолоігії:

- GSM/GPRS/CDMA;
- Bluetooth;

- радіочастотна ідентифікація RFID (Radio Frequency IDentification);
- бездротова сенсорна мережа WSN (Wireless Sensor Network);
- комунікація малого радіусу дії NFC (Near Field Communication);
- міжмашинна комунікація M2M (Machine-to-Machine).

Їх інтеграція з інтернет дозволяє забезпечити простий зв'язок різних технічних пристроїв, число яких обчислюється міліардами. За розрахунками консалтингового підрозділу Cisco IBSG в проміжку між 2008 і 2009 роками кількість підключених до інтернету пристроїв перевищило кількість людей, у 2015 року кількість підключених пристроїв сягнула 20 мільярд[2].

Таким чином, відбувається еволюційний перехід від «Інтернету людей» до « Інтернету речей », IoT (Internet of Things).

Атаки на Інтернет речей

Проблеми IoT на рівні сприйняття. Основна проблема безпеки на рівні сприйняття полягає у фізичній безпеці приладів і безпеки збору інформації. Проблеми безпеки на цьому рівні включають фізичне захоплення сенсорних вузлів, захоплення вузла шлюзу, витік інформації сенсора, загрози цілісності даних, виснаження енергозабезпечення, загрози перевантаження, атаки типу DoS (відмова в обслуговуванні), загрози маршрутизації встановлених в мережу нелегітимних сенсорів, і загрози копіювання вузла.

Проблеми IoT на мережевому рівні. Загрози IoT існуючих мереж зв'язку поширюються і на IoT, які побудовані на них. Це відноситься до несанкціонованого доступу, перехоплення даних, конфіденційності, цілісності, атаках типу людина всередині, Dos-атак (відмова в обслуговуванні). Крім того, існують між мережеві проблеми автентифікації, які можуть бути причиною атак DoS.

Проблеми IoT на прикладному рівні. Широке застосування IoT є результатом інтеграції комп'ютерної технології, технології зв'язку і різних областей промислових галузей. Крім порушення інформаційної безпеки традиційних мереж зв'язку (в результаті загроз повтору, підслуховування, спотворення інформації, розкриття інформації та ін.) додатки IoT стикаються з додатковими проблемами безпеки на прикладному рівні - при використанні обчислень, обробці інформації, забезпеченні прав на інтелектуальну власність, захисту приватності та ін.

Починаючи з 16 вересня 2016 року, невідомими зловмисниками було скоєно кілька найсильніших в історії DDoS-атак. Сумарна потужність двох з них досягала рекордних 1Тбіт / с.

Все почалося з атаки на ресурс відомого в IT-середовищі журналіста Брайана Кребса, який в одному зі своїх розслідувань розкрив діяльність хакерської групи V-Dos, що спеціалізується на організації замовних DDoS-атак. Невдовзі зловмисників було заарештовано, а на Кребса посипалися погрози і шквал рекордних за потужністю DDoS-атак.

Проаналізувавши інциденти, фахівці прийшли до висновку, що основною ударною силою атак були IoT-пристрої: роутери, IP-камери, DVR і інші. Всі вони були об'єднані в різні ботнети. Всього ж за вересень 2016 року було зафіксовано вже 14 DDoS-атак потужністю понад 200 Mbps.

Згідно з дослідженням експертів, по всій планеті близько 1 млн. IoT-пристроїв об'єднані в різні ботнети, здатні проводити безпрецедентні за своїми масштабами DDoS-атаки.

У своєму аналізі дослідники говорять про ботнети, в які входило близько 150 тис. IoT-пристроїв. Примітно, що головна мета хакерів - це IP-відеокамери. У мережі був виявлений ботнет, який складається з 25 тис. відеокамер. Такі пристрої мають велику смугу пропускання, тому цілком можуть бути застосовані в організації атак та досягати сотні гігабіт [4].

Висновки

Інтернет речей - це мережа, що складається із взаємозв'язаних фізичних об'єктів (речей) або пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку.

Широкому впровадженню Інтернету речей перешкоджають складні технічні та організаційні проблеми, зокрема, пов'язані зі стандартизацією. Єдиних стандартів для Інтернету речей поки немає, що ускладнює можливість інтеграції пропонованих на ринку рішень і багато в чому стримує появу

нових. Найсильніше глобальному впровадженню перешкоджає розпливчастість формулювань концепції Інтернету речей і велике число регуляторів і їх нормативних актів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Интернет вещей. Учебное пособие. [Текст]/ Росляков А. В., Ваняшин С. В., Гребешков А. Ю. – Книга, 2015 – 136 с.
2. Wireless challenges in the Ageing in Place Environment [Book]/ Jan Poesse, Philips Research, 2015 – 37 с.
3. Справочник модуля «Умный дом»[Текст]/ Палагута К. А., Шубникова И. С., Сафонов А.Л. – Книга, 2014 – 184 с.
4. Атака «розумних» речей [Електронний ресурс]: - Режим доступу: http://nag.ru/articles/article/30371/ataka-umnyih-veschey.html.

Горбовський Артем Ігорович — студент групи 1БС-16мс, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Войтович Олеся Петрівна*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Gorbovsky Artem I. — Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Voitovych Olesya P.*** — candidate, Sc., assistant professor of information security, Vinnytsia National Technical University, Vinnytsia