УДК 004.7

А. І. Горбовський
О. П. Войтович

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СМАРТ-РОЗЕТКИ

Вінницький національний технічний університет

Анотація

В роботі виконано дослідження засобів передавання в мережі, основні поняття Інтернету речей, їх розробка та проблеми впровадження. Проведено аналіз проблеми безпеки та методи їх усунення. Проведено аналіз основної концепції Інтернету речей та його взаємодія з людиною. Аналіз роботи смарт-розетки та дослідження вразливостей за допомогою тесту на проникнення.

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

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. An analysis of the work of a smart outlet and the study of vulnerabilities with Penetration Test.

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

Вступ

Інтернет речей є інформаційно-комунікаційною системою, яка складається із взаємозв'язаних пристроїв, якщо мають вбудовані датчики, а також програмне забезпечення та дозволяють здійснювати передачу і обмін даними в комп'ютерних системах. Система може мати виконавчі пристрої, які вбудовуються у фізичні об'єкти і пов'язані між собою через дротові і бездротові мережі. Ці взаємопов'язані об'єкти мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити участь людини при використанні інтелектуальних інтерфейсів [1].

Для дослідження передавання даних в мережі, аналізу проблем передачі інформації буде використовуватись так звана смарт-розетка моделі TSR100. TSR100 - «розумна» розетка. Вона належить до серії пристроїв, які можуть контролювати домашню техніку. Тобто, за допомогою TSR100 можна регулювати роботу телевізора, праски, кондиціонера, обігрівача, аудіосистеми та іншизх пристроїв, які підключені до смарт-розетки. При цьому управління приладами здійснюється віддалено, за допомогою Wi-Fi. TSR100 сумісна тільки з набором «Розумний будинок»[6].

При дослідженні загальних концепцій та конкретного пристрою постає питання безпеки. Яким чином та якими шляхами зловмисник зможе зламати пристрій або отримати доступ до конкретної мережі та управляти нею. Для оцінки захищеності може використовуватись технологія PenTest, тобто тестування на проникнення. Тест на проникнення є методом оцінювання захищеності інформаційно-комунікаційної системи шляхом часткового моделювання дій з атаки на неї зовнішніх і внутрішніх зловмисників. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей. Ефективний тест на проникнення поєднає цю інформацію з точною оцінкою потенційного впливу на організацію і окреслить межі технічних і процедурних контрзаходів для зменшення ризиків.

Аналіз літературних джерел

Основною задачею при аналізі IoT є визначення основних проблем технології та визначення прогнозів на майбутнє[1]. 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.

До факторів, що уповільнює розвиток Інтернету речей, слід віднести складність переходу існуючого Інтернету до нової, 6-й версії мережевого протоколу IP, перш за все необхідність великих фінансових витрат з боку телекомунікаційних операторів і провайдерів послуг на модернізацію свого мережевого обладнання.

Якщо технологічні платформи для Інтернету речей вже практично створені, то, наприклад, юридичні та психологічні ще знаходяться тільки в стадії розробки, так само як і проблеми взаємодії користувачів, даних, пристроїв. Одна з проблем - захист даних в таких глобальних мережах. Існує також серйозна проблема, пов'язана з вторгненням Інтернету речей в приватне життя. Можливість відстежувати місцезнаходження людей і їх власності ставить питання про те, в чиєму розпорядженні опиняться ці відомості. [1].

Різноманітні «розумні» речі – холодильники, мікрохвильовки, вуличні стовпи тощо – стають дедалі популярнішими. І ними починають цікавитися кіберзлочинці, адже подібні гаджети не захищені від них. Нещодавно, наприклад, зловмисники зламали більше 5 тис. таких пристроїв в одному з американських університетів, об’єднавши їх у ботнет. А наприкінці 2016 року армія кавоварок та пральних машин здійснила найбільшу інтернет-атаку в історії [4].

Особливо вразливими сьогодні є пристрої інтернету речей, оскільки виробники техніки поки не приділяють уваги безпеці цих девайсів. Пристрої інтернету речей сьогодні часто захоплюються підбиранням встановлених або зовсім відсутніх паролів. Як зазначив керівник підрозділу Verizon Лоуренс Дін, яке займається розслідуваннями інцидентів у сфері кібербезпеки, DDoS-атаки на пристрої інтернету речей найближчим часом можуть стати серйозною небезпекою, буде з’являтися все більше і більше пристроїв, доступ до яких хакери можуть отримати дуже легко. DDoS-атаки на пристрої інтернету речей будуть усе більш і більш актуальними до того часу, поки не буде зрозуміло, як від них захищатися [5].

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.[4].

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 [4].

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.

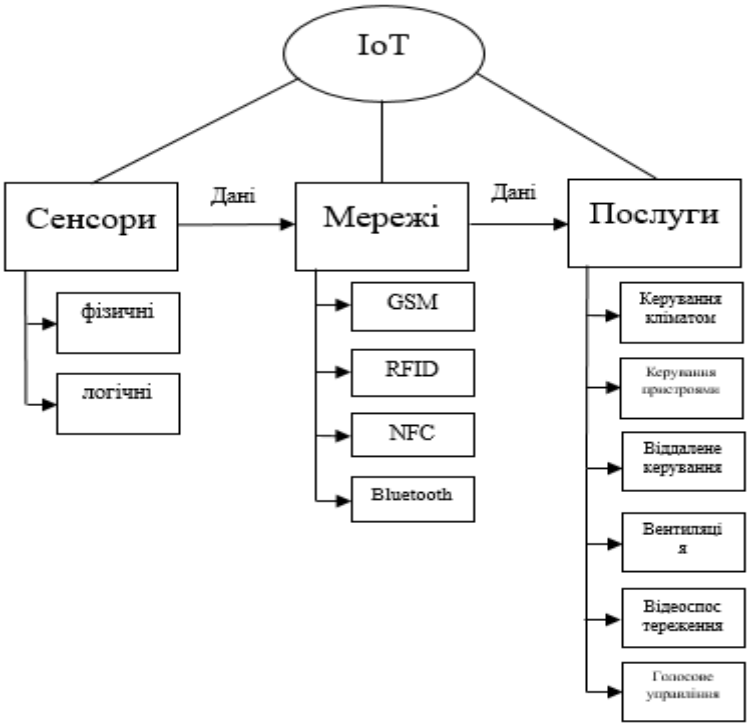

Рисунок 1 – Загальна структура IoT

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) [5].

Проблеми IoT на фізичному рівні. 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. 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.

Метою тесту на проникнення є виявлення слабких місць в захисті ІС і, якщо це можливо, і відповідає бажанню замовника, здійснити показовий злам.

Основна задача тесту на проникнення: повністю імітуючи дії зловмисника, здійснити атаку на веб-сервер, сервер застосувань або баз даних, персонал, корпоративну мережу.

Використовуючи смарт-розетку, першим та головним шляхом зловмисника буде злам через Wi-Fi. Тому основною задачею тестування буде виявлення слабких місць підключення по Wi-Fi, а також тестування різних технологій передачі даних, таких як Bluetooth, GSM і т.п.

Висновки

Інтернет речей є системою, яка складається із взаємозв'язаних пристроїв, ящо мають вбудовані датчики, а також програмне забезпечення та дозволяють здійснювати передачу і обмін даними в комп'ютерних системах. Система може мати виконавчі пристрої, які вбудовуються у фізичні об'єкти і пов'язані між собою через дротові і бездротові мережі. Ці взаємопов'язані об'єкти мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити участь людини при використанні інтелектуальних інтерфейсів. Проаналізувавши IoT виявлено певні недоліки, на сьогоднішній день ця система являється недостатньо захищеною і може бути використана хакерами з ціллю зламу та крадіжки інформації. Виявлено недоліки беспосередньо самої смарт-розетки та визначено можливі шляхи усунення. Тестування на проникнення може бути безцінним методом для програми інформаційної безпеки будь-якої організації.

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. IoT: вразливості та безпека [Електронний ресурс]: - Режим доступу: https://www.kaspersky.ru/blog/internet-of-things-insecurity/14857/
5. Обзор безопасности протокола передачи данных Bluetooth [Електронний ресурс]. – Режим доступу:http://cyberleninka.ru/article/n/obzor – bezopasnosti – protokola – peredachi – dannyh – Bluetooth
6. Войтович О.П. Дослідженння безпеки системи розумного будинку / Войтович О.П., Вишньовський В.В., Савченко К.В //Тези доповідей Шостої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації» м. Вінниця, 24-25 жовтня 2017 року. – Вінниця: ВНТУ, 2017.
7. Інтернет речей: цивільне і військове застосування [Електронний ресурс]: - Режим доступу: https://defence-ua.com/index.php/statti/4250-internet-rechey-tsyvilne-i-viyskove-zastosuvannya

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