ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТ ВЕЩЕЙ: ОБЗОР

Соколов М.Н.[1], Смолянинова К.А.[2], Якушева Н.А.[3]

Одной из сложных задач в развитии концепции Интернет вещей (IoT) во многих приложениях являются сложные проблемы обеспечения информационной безопасности в широком спектре защиты от угроз злоумышленника. Эти проблемы являются особенно актуальными, поскольку прогнозируется рост потребности пользователей в IoT. Для анализа поставленной в работе задачи принята одна из наиболее распространенных архитектур IoT, состоящая из трех уровней – уровень восприятии (per-ception), сетевой уровень и прикладной уровень. Для каждого из этих уровней приведены основные проблемы обеспечения ИБ. Отмечаются основные причины сложности обеспечения ИБ на сетевом уровне – гетерогенный характер структуры (многообразие вещей, разные технологии сетей) и большое число объектов. IoT принимает информацию от большого числа устройств, собирает большие данные различных форматов от множества источников с неоднородными характеристиками. Результатом являются отказы DoS из-за перегрузок в сети, программные ошибки из-за сложности отладки в реальном масштабе времени с помощью имитатора внешней нагрузки.

***Ключевые слова**: сенсорные сети, информационная безопасность, безопасность на уровне восприятия, безопасность на сетевом уровне, безопасность на прикладном уровне, уязвимости программного обеспечения*

Введение.

Благодаря широкому распространению беспроводных технологий и межмашинного обмена, возникновению технологии облачных вычислений и началу перехода на IPv6 в последние 2-3 года получила развитие концепция Интернет вещей IoT (Internet of Things). IoT является новым шагом в технологическом прогрессе. Интернет вещей позволяет людям и «вещам» соединиться в любое время и в любом месте, используя различные сети связи. В документах вместо термина «вещь» («things») применяют такие термины – объект («objects»), узел («node»), прибор («device») и др. Основными компонентами IoT являются всепроникающие сенсорные сети USN (Ubiquitious Sensor Networks) и радиочастотная идентификация RFID (Radio Frequency IDentification) [1]. Вещью в RFID является RFID-метка (RFID-тег), а в USN - сенсорный датчик или группа датчиков. Сетевые структуры сетей USN построены на базе протокола IPv.6 – 6LoWPAN (Low energy IPv6 based Wireless Personal Area Networks protocol). По данным работы [2] к 2020 году прогнозируется 50-100 миллиардов приборов, подсоединенных к Интернет. Возможность протокола 6LoWPAN присвоить всем сенсорным датчикам и RFID-меткам IP-адресации позволяет реализовать IoT. Уже сегодня можно наблюдать, как через Интернет между собой связаны различные устройства, работающие без участия человека – системы управления освещением, системы управления, автоматические системы полива, датчики пожарной и охраной сигнализации, светофоры и др. [3]. Одной из главных проблем IoT является обеспечение информационной безопасности (ИБ). В настоящей работе рассматриваются проблемы безопасности Интернет вещей только для одной из ее компонент – сенсорных сетей. Ежегодный прирост рынка сенсорных сетей порядка 7,8% и по прогнозам на 2016 год в мире будет составлять 91,5 млд. долларов. Покажем различие сенсорных сетей и IoT. Сенсорные сети используются для конкретных приложений, а IoT должен поддерживать различные виды приложений и может рассматриваться как сенсорная сеть общего назначения. Примерами приложений сенсорных сетей в РФ могут быть выполненные работы институтом точной механики и вычислительной техники им. С.А. Лебедева РАН – система аварийной связи для горноспасателей, система для решения комплекса задач по обеспечению безопасности про-

1 Соколов Михаил Николаевич, МГТУ им. Н.Э. Баумана, Москва, wetal91@gmail.com.
2 Смолянинова Кристина Александровна, МГТУ им. Н.Э. Баумана, Москва, kriszzztina@yandex.ru.
3 Якушева Надежда Александровна, University of Udine, Udine (Italy), nadejdaya2011@yandex.ru.

мышленных объектов и сооружений г. Москвы и др. [4] Все многочисленные приложения IoT можно объединить в три группы – индустриальный или промышленный (industry), окружающей среды (environment), общественный (society) [2]. Настоящая работа посвящена анализу проблем обеспечения информационной безопасности (ИБ) IoT. Для решения поставленной задачи анализу подлежат. 1. Многоуровневая структура IoT. 2. Проблемы обеспечения безопасности на каждом из уровней принятой структуры IoT. 3. Некоторые исследования обеспечения информационной безопасности IoT.

Многоуровневая структура IoT. Для IoT определены три основные характеристики - комплексные знания (в результате получения информации об объекте, в любом месте и в любое время), надежная передача (с помощью протоколов связи, маршрутизации, шифрования, сетевой безопасности, с высокой точностью и реального времени), интеллектуальная обработка (с учетом множества вычислений, нечеткого опознания и других технологий для анализа и обработки Big Data и получения необходимых данных различными пользователями). В соответствии с этими характеристиками структура IoT может быть разделена на три уровня – уровень восприятии (perception), сетевой уровень и прикладной уровень [5, 6]. Задача уровня восприятия получить надежное считывание с сенсоров, RFID-меток. Сетевой уровень обеспечивает повсеместный доступ, передачу информации, обработку, хранение. Он состоит из уровня доступа (мобильные сети связи), и основного уровня обмена (Интернет, сети следующего поколения NGN, виртуальные частные сети). Большинство сенсорных сетей используют беспроводные сети связи: беспроводные персональные сети (WPAN) (например, Bluetooth), беспроводные локальные сети (WLAN) (например, Wi-Fi), беспроводные городские сети (WMAN) (например, WiMAX), беспроводные глобальные сети (WWAN) (например, 2G, 3G и 4G сети), спутниковую сеть (например, GPS). Сенсорные сети в IoT используют протоколы связи на основе IP (например, IPv6). Прикладной уровень анализирует и обрабатывает принятую информацию для принятия правильного решения и контроля за управлением, приложениями и услугами. На прикладном уровне выполняются функции по сбору и хранению данных, по обеспечению эффективности энергообеспечения и логистики и др.

Проблемы информационной безопасности на уровнях структуры IoT. Следует отметить, что в некоторых работах рассматривается более, чем трехуровневая архитектуре IoT. В работе [7] принята пятиуровневая архитектура IoT включающая, например, промежуточный уровень (Middleware) между сетевым и прикладным уровнем. Этот уровень выполняет функцию обработки сообщений информации взаимодействующих однотипных сенсорных датчиков.

В настоящей работе ограничимся анализом проблем информационной IoT на каждом из трех уровней – уровне восприятия, сетевом и прикладном уровнях.

Проблемы ИБ на уровне восприятия. Основная проблема безопасности на уровне восприятия состоит в физической безопасности приборов восприятия и безопасность сбора информации. Большинство узлов восприятия, для которых характерно развертывание в необслуживаемой людьми среде при отсутствии стандартов, разнообразие, простота, ограничение энергообеспечения и слабая способность к защите безопасности.

Поэтому IoT не может обеспечить унифицированную систему защиты безопасности и является уязвимой к угрозам злоумышленника. Так как беспроводная сенсорная сеть на уровне восприятия является источником информации, то ИБ на этом уровне важна.

Проблемы безопасности на этом уровне включает физической захват сенсорных узлов, захват узла шлюза, утечка информации сенсора, угрозы целостности данных, истощение энергообеспечения, угрозы перегрузки, атаки типа DoS (отказ в обслуживании), угрозы маршрутизации установлением в сеть нелегитимных сенсоров, и угрозы копирования узла.

Проблемы ИБ на сетевом уровне. Угрозы ИБ существующих сетей связи распространяются и на IoT, который построен на них. Это относится к несанкционированному доступу, перехвату данных, конфиденциальности, целостности, атаках типа человек посредине, Dos-атакам (отказ в обслуживании), вирусам, эксплойтам, сетевым червям, руткитам и др. Кроме того, существуют межсетевые проблемы аутентификации, которые могут быть причиной атак DoS.

В IoT стоят более сложные проблемы обеспечения безопасности по сравнению с теми, с которыми сталкивались ранее [8]. Это вызвано двумя причинами – гетерогенный характер структуры (многообразие вещей, разные технологии се-

тей в соединении) и большим числом объектов. IoT принимает информацию от большого числа устройств, собирает большой массив данных различных форматов от множества источников с неоднородными характеристиками. В результате этого на сетевом уровне имеют место более сложные проблемы безопасности. К ним относятся возможные проблемы масштабируемости сети, вызванные малопредсказуемым объемом передачи данных от большого числа узлов, и приводящие к возможности осуществления атак DoS, DDoS.

Отдельное внимание уделяется уязвимостям программного обеспечения (software vulnerabilities), приводящим к нарушению ИБ после внедрения. Причинами программной уязвимости могут являться неизбежные ошибки разработчиков сложного многослойного программного обеспечения (ПО), ошибки ядра программы, неполнота обработки исключений, применение незащищенного кода. необработанных массивов с возможностью их переполнения злоумышленником, ошибки в обработке Big Data, ошибки БД, отсутствие должной индексации или закрепления запросов БД, web-уязвимости, недостаточная производительность или масштабируемость ПО, ошибки распределенной работы приложений, а также виртуальных платформ и облаков. Следует отметить сложность ПО в IoT, вызванную большим разнообразием используемых аппаратных платформ и операционных систем. Для проектирования ПО необходимо эмулировать поведение приборов IoT, т.е. создать имитатор внешней среды для серверов. По причине ограничений в приборах (энергообеспечение, производительность процессора, память) в IoT стоит сложная задача избежать сильного расхождения между эмулятором и прибором. Также для отгрузки отлаженного рабочего релизоа IoT приложения, необходимо провести полноценное тестирование, включая нагрузочное тестирование, тестирование производительности, комплексное тестирование взаимодействия модулей. Другой причиной программной уязвимости могут являться бэкдоры (backdoor, back door - черный ход) - это участки кода, внесенные разработчиком, для последующей возможности использования для просмотра данных, а в случае ОС удаленного управления компьютером. Бэкдором могут быть как бы случайные ошибки в коде, которые при определенном подборе констант или сочетании клавиш, или действиях в приложении могут давать доступ к каким-либо данным. Бэкдоры также устанавливаются и на оборудование производителями с целью управления или тестирования. Однако этот «черный ход» может быть обнаружен злоумышленником и использован им.

Проблемы ИБ на прикладном уровне. Широкое применение IoT является результатом интеграции компьютерной технологии, технологии связи и различных областей промышленной отрасли. Кроме нарушение информационной безопасности традиционных сетей связи (в результате угроз повтора, подслушивания, искажения информации, раскрытия информации и др.) приложения IoT сталкиваются с дополнительными проблемами безопасности на прикладном уровне - при использовании облачных вычислениях, обработке информации, обеспечении прав на интеллектуальную собственность, защите приватности и др.

Некоторые исследования обеспечения информационной безопасности IoT. Зарубежные специалисты уделяют большое внимание научным и экспериментальным исследованиям в обеспечении информационной безопасности IoT. Например, в работе [6] показано, что наибольший риск безопасности возможен на нижнем уровне архитектуры - на уровне восприятия. При этом отмечается, что некоторым угрозам безопасности на других уровнях архитектуры IoT так же характерен высокий уровень риска. В работе [9] приводятся результаты исследований обеспечения безопасности приватных данных на примере «умного дома» в IoT.

Выводы.

1. Стремительное развитие за последние 2-3 года в практическом плане концепции Интернета вещей вызвано широким распространением беспроводных технологий и межмашинного обмена, развитием технологии облачных вычислений и началом перехода на IPv6. Однако использование IoT во многих областях ограничено сложными проблемами в части обеспечения ИБ.

2. Необходимо продолжить эти работы в плане анализа предложений специалистов по решению проблем безопасности в IoT для использования в РФ.

Рецензент: Бельфер Рувим Абрамович, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, с.н.с., к.т.н., a.belfer@yandex.ru

Литература:

1. Гольдштейн Б.С., Кучерявый А.Е. Сети связи пост-NGN. СПб.: БХВ-Петербург, 2013, 160 С.
2. Perera, C. and etc. Context Aware Computing for The Internet of Things: A Survey. Communications Surveys & Tutorials, IEEE, 2014, V.16, Issue 1, pp. 414-454.
3. Алексеев В. Модули Bluetooth, Wi-Fi и NFC производства u-blox- connectBlue для «Интернета вещей», часть 1. Модули с поддержкой Bluetooth // Беспроводные технологии. 2015. Т. 2. № 39. С. 27-32.
4. Беспроводной промышленный мониторинг. М.: ИТМиВТ, URL: http://www.ipmce.ru.img/release/is_sensor.pdf.
5. Quandeng Gou (and others). Construction and Strategies in IoT Security System, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 1129-1132. DOI = 10.1109/GreenCom-iThings-CPSCom.2013.195.
6. Zhang Baoquan, Zou Zongfeng, Liu Mingzheng, Evaluation on security system of internet of things based on Fuzzy-AHP method, E -Business and E -Government (ICEE), 2011 International Conference on 2011, pp. 1 – 5. DOI = 10.1109/ICEBEG.2011.5881939.
7. Zhi-Kai Zhang (and others). IoT Security: Ongoing Challenges and Research Opportunities, Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, 2014, pp. 230 – 234. DOI = http://doi.ieeecomputersociety.org/10.1109/SOCA.2014.58.
8. Khan, R. [and others], Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, Frontiers of Information Technology (FIT), 2012 10th International Conference on, 2012, pp. 257 - 260.
9. Schurgot, M.R.; Shinberg, D.A.; Greenwald, L.G., Experiments with security and privacy in IoT networks, World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on, 2015, pp. 1-6.

SECURITY PROBLEMS INTERNET OF THINGS: SURVEY

Sokolov M.N.[4], Smolyaninova K.A.[5], Yakusheva N.A.[6]

One of the challenges in the development of the concept of the Internet of Things (IoT) in many applications is a complex problem of information security in a wide range of threat protection attacker. These issues are particularly relevant, as in the coming years is projected to increase in the needs of users in the IoT. To analyze the problem posed adopted one of the most common IoT architectures, which consists of three levels – the level of perception, the network layer and application layer. The main information security challenges for each of level are considered in the article. The main reasons for the complexity of information security at the network level are specified – the heterogeneous nature of the structure (the variety of things, different network technologies in a compound), and a large number of objects. IoT receives information from a lot of devices and collect a Big Data massive in various formats from multiple sources with heterogeneous characteristics. The result is a security breach DoS failures due to network congestion, software errors due to the difficulty in debugging real–time simulator of the external load.

***Keywords**: Sensor Network, information security, security in perception layer, security in network layer, security in application layer, software vulnerabilities*

References:

1. Gol'dshteyn B.S., Kucheryavyy A.E. Seti svyazi post-NGN. SPb.: BKhV-Peterburg, 2013, 160 P.
2. Perera, C. and etc. Context Aware Computing for The Internet of Things: A Survey. Communications Surveys & Tutorials, IEEE, 2014, V.16, Issue 1, pp. 414-454.
3. Alekseev V. Moduli Bluetooth, Wi-Fi i NFC proizvodstva u-blox- connectBlue dlya «Interneta veshchey», chast' 1. Moduli s podderzhkoy Bluetooth, Besprovodnye tekhnologii. 2015. T. 2. № 39, pp. 27-32.
4. Besprovodnoy promyshlennyy monitoring. M.: ITMiVT, URL: http://www.ipmce.ru.img/release/is_sensor.pdf.
5. Quandeng Gou (and others). Construction and Strategies in IoT Security System, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 1129-1132. DOI = 10.1109/GreenCom-iThings-CPSCom.2013.195.
6. Zhang Baoquan, Zou Zongfeng, Liu Mingzheng, Evaluation on security system of internet of things based on Fuzzy-AHP method, E -Business and E -Government (ICEE), 2011 International Conference on 2011, pp. 1 – 5. DOI = 10.1109/ICEBEG.2011.5881939.
7. Zhi-Kai Zhang (and others). IoT Security: Ongoing Challenges and Research Opportunities, Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on, 2014, pp. 230 – 234. DOI = http://doi.ieeecomputersociety.org/10.1109/SOCA.2014.58.
8. Khan, R. [and others], Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, Frontiers of Information Technology (FIT), 2012 10th International Conference on, 2012, pp. 257 – 260.
9. Schurgot, M.R.; Shinberg, D.A.; Greenwald, L.G., Experiments with security and privacy in IoT networks, World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on, 2015, pp. 1-6.

4 Mikhail Sokolov, Bauman Moscow State Technical University, Moscow, wetal91@gmail.com.

5 Christine Smolyaninova, Bauman Moscow State Technical University, Moscow, kriszzztina@yandex.ru.

6 Nadezhda Yakusheva, University of Udine, Udine (Italy), nadejdaya2011@yandex.ru.