9. Жуков А. Фингерпринтинг браузера. Как отслеживают пользователей в Сети [Электронный ресурс]. URL: https://xakep.ru/2015/01/30/user-web-tracking-howto/ (дата обращения: 10.10.2017).

10. Бессонова Е.Е. Метод идентификации пользователей в сети Интернет с использованием компонентного профиля, дисс. на соиск. степ. к-та. техн. наук [Электронный ресурс]. URL: https://isu.ifmo.ru/index/B996F9609F0750E3BBDF52445A22C FC1 (дата обращения: 14.10.2017).

11. Cao Y., Li S., Wijmans E. (Cross-)Browser Fingerprinting via OS and Hardware Level Features Conference: Network and Distributed System Security Symposium, 2017 [Electronic resource]. URL: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf (access date: 14.10.2017).

12. Fleishman G. How to kill the evercookie and supercookie, the cockroaches of tracking, 2017 [Electronic resource] URL: https://www.macworld.com/article/3152056/privacy/ how-to-kill-the-evercookie-and-supercookie-the-cockroaches-of-tracking.html (access date: 14.10.2017).

13. Методы идентификации пользователя в Интернете, 2017 [Электронный ресурс]. URL: https://serfmoney.ru/cpa/metody-identifikatsii-polzovatelya-v-internete/ (дата обращения: 15.10.2017).

АНАЛИЗ УЯЗВИМОСТЕЙ В ЭНЕРГОЭФФЕКТИВНЫХ СЕТЯХ ДАЛЬНЕГО РАДИУСА ДЕЙСТВИЯ НА ПРИМЕРЕ LORAWAN

С.Ю. Исхаков, А.А. Исхакова, Р.В. Мещеряков
(г. Томск, Томский государственный университет систем управления и радиоэлектроники)
e-mail: iskhakov.sy@gmail.com

ANALYSIS OF VULNERABILITIES IN LOW-POWER WIDE-AREA NETWORKS BY EXAMPLE OF THE LORAWAN

Sergey Iskhakov, Anastasia Iskhakova, Roman Meshcheryakov
(Tomsk, Tomsk State University of Control Systems and Radioelectronics)

Abstract. The increasing number of automated systems using the global network for management has led to the need to search for new technologies for transmitting data from various sensors over long distances with minimal energy consumption. Today, there are several similar technologies on the market that claim to be the world standard in the concept of the Internet of things, but none of them has yet been studied in detail from the point of view of security. This article is devoted to the analysis of one of the most common protocols in order to identify potential vulnerabilities.

Keywords: Internet of Things; modulation; network; vulnerability; replay attack; spoofing.

Введение. В последнее время наблюдается интенсивное распространение концепции Интернета вещей (IoT) [1,2], которую можно определить как глобальную динамическую сетевую инфраструктуру, где физические и виртуальные «вещи» имеют идентификаторы и физические атрибуты, и интегрируются в информационную сеть, используя различные интерфейсы. Все большее внимание привлекают технологии, позволяющие создавать энергоэффективные сети дальнего радиуса действия (Low-Power Wide-area Network, LPWAN) [4]. Представим жилой многоквартирный дом, где системы водоснабжения и электрификации подключены к IoT и передают показания в автоматическом режиме на станцию мониторинга. Во-первых, если для электросчетчика легко обеспечить постоянное питание, то прокладка кабелей к счетчикам воды сводит на нет всю концепцию использования беспроводных технологий. Поэтому радиомодуль счетчика должен работать от локального источника энергии (батарейки). Энергопотребление современных модулей Wi-Fi [1] и LTE [4] обуславливает

ограничение работы батарей несколькими сутками, что в условиях большого количества датчиков приведет к нецелесообразности их использования. Во-вторых, в случае многоквартирного дома количество датчиков будет измеряться сотнями. Несмотря на малые объемы создаваемого ими траффика, практически все ресурсы ближайших станций сотовой связи будут задействованы на поддержание связи с таким множеством «абонентов».

Одной важнейших составляющих IoT является обеспечение защиты устройств, поскольку ими генерируется и обрабатывается огромное количество конфиденциальной информации. Кроме того, важным моментом является обеспечение безопасности IoT устройств от использования в DDoS-атаках [5-7] и ботнетах. Решение таких проблем возможно только при комбинировании многих технологий и протоколов, а также сотрудничества производителей, но для этого необходимо выявлять общие проблемы и уязвимости в различных технологиях. В данной статье предпринята попытка обобщить методологические наработки в области обеспечения безопасности LPWAN-решений.

Стандарты LPWAN. На сегодняшний день в области LPWAN сетей существует два основных направления развития беспроводной связи: технологии, работающие в лицензируемом диапазоне частот и технологии, развертывание которых не требует лицензирования.

NB-IoT – это стандарт сотовой связи для устройств телеметрии с низкими объемами обмена данными. Разработан консорциумом 3GPP на базе существующих стандартов мобильной связи и опубликован в 2016 г [8]. Так как сеть NB-IoT относится к сотовой связи, то устройства, работающие в ней, должны «просыпаться» и синхронизироваться с сетью. В противном случае получить или отправить сообщение не удастся.

LoRaWAN – это протокол канального уровня, основанный на запатентованной технологии модуляции LoRa [9-10], представленной в 2015г. компаниями Semtech и IBM Research. LoRa не является стандартом мобильной связи. Для работы LoRaWAN не требуется получение лицензий на использование частот. В сети LoRaWAN асинхронная отправка данных подразумевает передачу данных только тогда, когда эти данные есть. Пока устройству нечего передавать, оно «спит», экономя энергию. Специалисты могут задать отправку данных по расписанию или вне зависимости от времени. При этом синхронизация с сетью не требуется. В данной статье большее внимание уделено обеспечению безопасности решений, использующих технологию LoRa.

Lorawan. Когда говорят о технологии LoRa, обычно имеют ввиду метод модуляции LoRa и открытый протокол LoRaWAN. Модуляция LoRa это проприеритарный механизм, в основе которого лежит техника расширения спектра, а именно вариация линейной частотной модуляции (Chirp Spread Spectrum modulation, CSS) [9,10], который позволяет обеспечить передачу данных на дальние расстояния и низкое энергопотребление. В свою очередь, LoRaWAN это протокол канального уровня для сетей с множеством узлов с большим радиусом действия и низким собственным потреблением мощности. Сеть LoRaWAN имеет архитектуру типа “многоуровневая звезда” без ретрансляторов и mesh-связей, имеет конечные узлы, которые через шлюзы, образующие прозрачные мосты, общаются с центральным сервером сети. Типичная сеть LoRaWAN состоит из следующих элементов: конечные узлы, шлюзы, сетевой сервер и сервер приложений.

Поскольку LoRaWAN является относительно новым протоколом, уровень его безопасности развит недостаточно и требует анализа и доработок. Несмотря на то, что технология LoRa предусматривает некоторые механизмы безопасности, такие как шифрования и цифровая подпись, уровень безопасности проработан недостаточно. Далее будут рассмотрены возможные атаки на протокол LoRaWAN.

Анализ уязвимостей. Одним из самых уязвимых мест в работе IoT инфраструктуры является этап добавления в сети новых устройств. Для обеспечения безопасности сети в целом, необходимо обеспечить безопасность на данном этапе, внедрив так называемую «процедуру активации»: перед тем как оконечные устройства получат возможность взаимодействовать с сетевым сервером, они должны быть активированы посредством процедуры

присоединения. Этот механизм предназначен для контроля доступа неопознанных устройств в сеть и предотвращения их взаимодействия с другими объектами сети. В случае с протоколом LoRaWAN предусмотрено два возможных метода активации – Активация ABP (Activation by Personalisation) и Аутентификация «по воздуху» (Over-theAir Activation, OTAA).

Атака повторного воспроизведения при ABP активации

Метод активации ABP имеет определенные уязвимости. Для оконечных устройств, активированных данным способом, используются статические ключи, что в свою очередь означает, что после перезагрузки ключи не будут изменены и останутся теми же самыми. Кроме того, в отличие от аутентификации «по воздуху» (OTAA), в данном случае отсутствует процедура присоединения.

Стоит отметить, что подход к использованию счетчиков также небезопасен, поскольку в спецификации к протоколу сказано, что после обмена сообщениями JoinReq–JoinAccept или перезагрузки уже активированного оконечного устройства счетчики кадров на конечном устройстве и счетчики кадров на сетевом сервере для данного оконечного устройства сбрасываются на 0. Таким образом, активированное методом ABP оконечное устройство после перезагрузки, будет повторно использовать значение счетчика кадров от 0 с теми же ключами. В этом случае злоумышленник может перехватить сообщения на последней сессии с большими значениями счетчика и использовать его в текущей сессии. При этом, атака повторного воспроизведения возможна независимо от того каким способом было активировано устройство – ABP или OTAA. Помимо этого существует возможность сброса счетчика путем его переполнения: после того, как счетчик достигнет своего максимального значения, он будет сброшен и перезапустится с 0.

Зная значения счетчика предыдущей сессии и ключи текущего сеанса, злоумышленник может воспроизводить предыдущие сообщения, чтобы нарушить связь между оконечным устройством и сервером. Основной целью атаки повторного воспроизведения является достижение повторения значения счетчика. Поэтому, в сетях с OTAA активацией злоумышленнику для достижения цели необходимо дождаться, когда значение счетчика оконечного устройства достигнет максимума и сбросится на 0. Для устройств, активированных по методу ABP, злоумышленник может также дождаться переполнения счетчика либо перезагрузить оконечное устройство и тогда значение счетчика сбросится на 0. В случаях активации по методу ABP подобная атака займет намного меньше времени, чем при использовании OTAA активации, если у злоумышленника есть возможность перезагрузить оконечные устройства.

Для реализации этой атаки злоумышленник может использовать сниффер [4,7] для перехвата трафика, и передатчик LORA для повторного воспроизведения сообщений. Подобная атака может быть чрезвычайно опасна для оконечных устройств, активированных методом ABP в большой сети LORAWAN. В случае небольших размеров сети с малым количеством устройств злоумышленнику может потребоваться значительное количество времени для переполнения счетчика. Однако, в большой сети с множеством конечных устройств, время ожидания для любого из перезагруженных конечных устройств сильно уменьшается. Как только атакующий получает наибольшее возможное значение счетчика для одного конечного устройства, он может периодически повторять это сообщение, чтобы принудительно перезагружать атакуемое устройство. Если ключи сессии для конечного устройства изменены, то оно не сможет функционировать после перезагрузки. Кроме того, если злоумышленник найдет способ перезагрузки устройства (например, отключение питания), то ему не нужно будет ждать переполнения счетчика. В случае перезагрузки устройства и повторного воспроизведения сообщения с максимальным значением счетчика сообщения от устройства-жертвы будут отклонены сервером.

ACK Spoofing

В большинстве случаев в LorAWAN сетях шлюз одним из интерфейсов подключен к сети Интернет, что обуславливает повышение количества потенциальных уязвимостей.

Например, возможно создание вредоносного шлюза, который может быть добавлен в сеть с помощью таких атак как UDP-спуфинг. Потенциальная уязвимость протокола заключается в том, что сообщение ACK при установлении связи не содержит информации о том, какое сообщение оно действительно подтверждает, оно лишь только подтверждает последнее полученное сообщение. Поэтому возможно, что взломанный вредоносный шлюз может сохранить подтверждение и поддерживать его для будущих сообщений, поступивших от конечных устройств.

Целью атаки типа ACK спуфинг является получение злоумышленником возможности перехвата и повторной отправки одного и того ACK сообщения для подтверждения различных сообщений от конечного устройства. Для реализации подобной атаки злоумышленник должен обладать:

- возможностью получения контроля над шлюзом
- возможностью распознавания ACK сообщений и встраивания в процесс передачи их между шлюзом и конечным устройством
- возможностью чтения и выбора необходимых ACK сообщений
- возможностью отправки выбранных ACK сообщений от шлюза конечному устройству.

Возможность осуществления данной атаки основана на предположении, что шлюз уже заражен и является вредоносным либо злоумышленник провел атаку по спуфингу самого шлюза, т.е. он полностью контролирует шлюз и может добиться возможности спуфинга ACK сообщений. Теоретически, в LORAWAN сети шлюз используется для передачи сообщений. Если злоумышленник контролирует шлюз, то он может нанести вред только на физическом уровне. Однако, с учетом вышеуказанного недостатка в конструкции ACK сообщений, шлюзы становятся серьезной уязвимой точкой в LORAWAN сети.

Заключение. Стремительное распространение рынка устройств и услуг в сфере IoT повлекло за собой необходимость разработки новых стандартов и технологий передачи данных, поскольку использование существующей инфраструктуры, например сетей сотовой связи или сетей WiFi, не позволяет обеспечить достижение целей и задач, стоящих перед интернетом вещей. Одним из наиболее ярких примеров является широкое распространение решений на базе протокола LORAWAN, который имеет все шансы, чтобы стать мировым стандартом в IoT. Однако, тот факт, что от IoT работы устройств нередко может зависеть жизнь и здоровье человека, потребители данного рынка диктуют требования к гарантиям безопасности и конфиденциальности данных, обрабатываемых такими устройствами.

В данной статье авторами представлены результаты анализа спецификаций на данный протокол с целью выявления потенциальных уязвимостей. Полученные результаты свидетельствуют о том, несмотря на серьезный подход разработчиков к обеспечению защиты устройств в сети, уровень безопасности протокола LoRaWAN развит недостаточно и требует анализа и доработок. Выявленные уязвимости могут быть использованы для дальнейших исследований, а также для снижения риска компрометации оконечных устройств при их разработке.

Данная работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках проектной части государственного задания ТУСУР на 2017–2019 гг. (проект № 2.3583.2017/4.6).

ЛИТЕРАТУРА

1. Jerkins J. Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code // IEEE 7th Ann. Comp. and Comm. Workshop and Conf. (CCWC), Las Vegas, NV. – 2017. – Pp. 1-5.

2. Zhao Y. Research on data security technology in internet of things // 2nd Int. Conf. on Mechatronics and Control Engineering (ICMCE), Dalian, China. – 2013. – Pp. 1752–1755.

3. Howser G., McMillin B. A Modal Model of Stuxnet Attacks on Cyber-physical Systems: A Matter of Trust // Eighth Int. Conf. on Soft. Sec.and Reliability (SERE), San Francisco, CA. – 2014. – Pp. 225-234.

4. Margelis G., Piechocki R., Kaleshi D., Thomas P. Low throughput networks for the iot: Lessons learned from industrial implementations. In Internet of Things (WF-IoT) // 2015 IEEE 2nd World Forum. – 2015. Pp. 181-186.

5. Detken K., Rix T., Kleiner C., Hellmann B., Renners L. SIEM approach for a higher level of IT security in enterprise networks // IEEE 8th Int. Conf. on Intelligent Data Acquisition and Adv. Comp. Systems: Techn. and App. (IDAACS), Warsaw. – 2015. – Pp. 322-327.

6. Evsutin O., Kokurina A., Meshcheryakov R., Shumskaya O. An adaptive algorithm for the steganographic embedding information into the discrete fourier transform phase spectrum // Advances in Intelligent Systems and Computing. – 2016.

7. Iskhakov S., Shelupanov A., Meshcheryakov R. Simulation modelling as a tool to diagnose the complex networks of security systems // J. of Phys.: Conf. Series. – 2017. – Vol. 803. – Pp. 12-57.

8. Abomhara M., Kien G.M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks // Journal of Cyber Security. – 2015. – Vol. 4. – Pp. 65–88.

9. LoRa Alliance [Electronic resource]. URL: https://www.lora-alliance.org/.(access date: 01.10.2017).

10. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A. Security, Privacy & Trust in Internet of Things: the road ahead // Computer Networks (Elsevier). – 2015. – Vol. 76. – Pp. 146–164.

АНАЛИЗ УЯЗВИМОСТЕЙ ВСТРОЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ IOT-УСТРОЙСТВ ПОСРЕДСТВОМ ВНЕДРЕНИЯ СЕТИ HONEYPOT

А.О. Исхакова, А.Ю. Исхаков, Р.В. Мещеряков
Томск (Томский государственный университет систем управления и радиоэлектроники)
shumskaya.ao@gmail.com

ANALYSIS OF THE VULNERABILITIES OF THE EMBEDDED INFORMATION SYSTEMS OF IOT-DEVICES THROUGH THE HONEYPOT NETWORK IMPLEMENTATION

A.O. Iskhakova, A.Yu. Iskhakov, R.V. Meshcheryakov
Tomsk (Tomsk State University of Control Systems and Radioelectronics)

Abstract. The Internet of Things is now an essential tool in many areas of human life. Researches related to the security of IoT-devices and IoT-networks are extremely relevant over the past ten years. The violation of the confidentiality, integrity of the transmitted data and the availability of smart objects and control devices can lead to major risks and various negative consequences. The article details the conduct of the research experiment on the introduction of a honeypot trap into a smart house IoT-network. The results allow to make a conclusion about the ways of attacks on smart objects, the protocols and services use, the influence of the devices placement in the network on their security level.

Keywords: Internet of Things; IoT-device; smart device; information security; honeypot, IoT-network; attack; trap; unauthorized access

Введение. Переход к Интернету вещей, согласно исследованию Cisco [1], произошел примерно в 2008-2009 годах. С этих пор количество устройств, подключенных к глобальной сети Интернет, превысило численность населения Земли. Число инноваций в этой области непрерывно растет, что говорит об активном развитии Интернета вещей.

Интернет-вещи могут образовывать локальные сети, объединенные какой-либо одной зоной обслуживания или функцией. По данным [2] на май 2017 года в коллекции «Лаборато-