УДК 681.518.3

Проблематика использования интернета вещей на примере смарт-холодильников

Е. В. Смирнова[1]✉, А. О. Смирнов[2], О. В. Ольшевская[3], В. Б. Владимирова[4]
[1,3,4] Одесская национальная академия пищевых технологий, ул. Канатная,112, г. Одесса, 65039, Украина
ORCID: [1] 0000-0002✉-3818-8083, [2] 0000-0002-9459-6292, [3] 0000-0002-4512-3915, [4] 0000-0002-6092-7946
✉ e-mail: smirnova.kathrin@gmail.com

Одной из главных проблематик в развитии концепции интернета вещей (IoT, Industrial Internet of Things) в большинстве приложений является обеспечение информационной безопасности. Эти проблемы становятся все более актуальными из-за роста спроса на IoT и их относительной доступности. Встроить систему безопасности в каждое устройство практически невозможно. А так как IoT могут принимать информацию от большого количества устройств, собирают данные различных форматов от источников с неоднородными характеристиками, вопрос информационной безопасности затрагивает не только конкретное устройство, а всю сеть сообщающихся устройств. В статье рассматривается проблематика использования IoT на примере смарт-холодильников. Акцентируется внимание на вопросах информационной безопасности, не решенных к настоящему моменту, а также тенденции развития в области IoT.

Ключевые слова: *интернет вещей; интеллектуальна техника; умный дом; информационная безопасность; уязвимости программного обеспечения.*

Проблематика використання інтернету речей на прикладі смарт-холодильників

Е. В. Смірнова[1], А. О. Смірнов[2], О. В. Ольшевская[3], В. Б. Владімірова[4]
[1,3,4] Одеська національна академія харчових технологій, вул. Канатна, 112, г. Одеса, 65039, Україна
ORCID: [1] 0000-0002✉-3818-8083, [2] 0000-0002-9459-6292, [3] 0000-0002-4512-3915, [4] 0000-0002-6092-7946

За останнє десятиліття зростання розвитку різних технологій породило занепокоєння, щодо безпеки та конфіденційності їх використання. На відміну від інфраструктури звичної мережі Інтернет, Інтернет речей базується на величезній кількості датчиків, вбудованих в найрізноманітніші пристрої (на 2017 рік кількість пристроїв становить трохи більше 20 мільярдів [1]). Багато з цих пристроїв досить примітивні і їх функції обмежуються відправкою на сервер будь-якої інформації, наприклад, вимірювання температури. Але всі ці пристрої, в цілому, формують величезні потоки інформації і на такій інфраструктурі будується "мережа мереж", що складається з підключених пристроїв, більшість з яких можуть самостійно приймати певні рішення. Вбудувати систему безпеки абсолютно в усі пристрої практично неможливо. Ринок IoT-пристроїв вже неодноразово стикався з низкою серйозних порушень інформаційної безпеки. Так, восени 2016 року було зареєстровано першу DDoS-атаку з боку ботнету Mirai, що повністю складається з "розумних" речей - понад півмільйона камер, термостатів, відеореєстраторів та безліч інших пристроїв. У лютому 2017 року було проведено атаку на один з навчальних закладів. У цій атаці брали участь близько 10 тисяч "розумних" пристроїв, включаючи камери, роутери, термостати. Тобто протягом майже 5 місяців виробники IoT-пристроїв не виправили вразливості, які спричинили можливість повторного створення ботнету. Станом на квітень 2017 року Mirai включав в себе 30 можливих емуляцій браузерів, на відміну від 5 до первісної версії. А це означає, що бот може обходити більшість заходів захисту, що вживаються фахівцями з інформаційної безпеки. Створення функціональних інтерфейсів і засобів управління робить пристрої набагато зручнішими для потенційного споживача, однак, це робить пристрої більш уразливими. І якщо можливості керувати пристроєм у користувача немає, наявність несправності стане помітною лише за фактом, коли існуюча проблема або наслідки зламу пристрою не виявляться самі, заподіявши, в ряді випадків, чималої шкоди. Звичайно, участь в DDoS атаках смарт-пристроїв не може заподіяти видимого збитку власнику. Однак, починаючи з 2011 року неодноразово демонструвалися реальні наслідки зламу подібних пристроїв: дистанційний злам інсулінової помпи, дистанційний злам кардіостимулятора, який по команді видавав смертельний розряд в 830В, повне захоплення управлінням смарт-автомобілів і т.д. Смарт-холодильники, як складова концепції "розумного будинку", масово ще не увійшли в життя звичайного споживача через досить високу, у порівнянні зі звичайними холодильниками, ціною. Однак, за прогнозами аналітиків в найближчі 7-10 років ці пристрої будуть мати комерційний успіх. На даний момент основні тренди в смарт-холодильниках – це: управління через Інтернет, розуміння голосових команд, можливість замовлення та розпізнавання продуктів, наявність вбудованої камери. У статті розглядаються питання інформаційної безпеки речей, зокрема питання безпеки смарт-холодильників. Виходячи з

особливостей даної галузі запропоновано можливі рішення організації інформаційного захисту складових "розумного" будинку.

Ключові слова: *інтернет речей; інтелектуальна техніка; розумний будинок; інформаційна безпека; уразливості програмного забезпечення.*

© The Author(s) 2017. This article is an open access publication
This work is licensed under the Creative Commons Attribution 4.0 International License (CC BY)
http://creativecommons.org/licenses/by/4.0/

Введение

Интернет вещей совмещает в себе как множество возможностей, так и множество рисков. Стремительный рост спроса на "умные" устройства и их разнообразие становится источником проблем их безопасности как для конечного пользователя, так и для компаний-разработчиков. Приобретая интересующее устройство, злоумышленники изучают как оно защищено и, соответственно, находят способ его взлома. Система защиты таких устройств не может быть обновлена достаточно оперативно, а значит дома, машины, бизнес становятся уязвимыми к угрозам технологических новинок.

Самой главной угрозой безопасности, и для IoT в частности, является человеческий фактор. Достаточно большие объемы информации, пересылаемые через сеть Интернет, притягивают внимание злоумышленников. И если взлом отдельной мелкой бытовой техники не несет в себе чаще всего значительного ущерба, то несанкционированный доступ к системе управления "умным" домом или предприятием может нести уже достаточно серьезные последствия.

Согласно исследованию ресурса Raconteur [2], к 2020 году 25% всех производимых кибератак будут приходиться на сферу Интернета вещей. При этом только 10% бюджета сферы информационных технологий будет направлено на улучшение кибербезопасности бизнес-структур и предприятий. Следует отметить, что по статистике люди гораздо больше беспокоятся о защите личных данных в сравнении с данными, связанными с их профессиональной деятельностью.

Рассматривая информационную безопасность Интернета вещей, можно выделить несколько основных проблем.

Ежедневно в сеть выходят порядка 7 миллионов новых IoT устройств, что влечет за собой появление новых уязвимостей. Уязвимость устройств обусловлена рядом факторов:

– Стандартные учетные записи от производителя, слабая аутентификация;

– Отсутствие поддержки со стороны производителей для устранения уязвимостей;

– Трудно или невозможно обновить программное обеспечение или операционную систему;

– Использование текстовых протоколов и ненужных открытых портов;

– Использование незащищенных мобильных технологий;

– Использование незащищенной облачной инфраструктуры;

– Использование небезопасного программного обеспечения.

Постоянно растущее количество легко взламываемых устройств массового потребления повышает вероятность, частоту и тяжесть атак, включая атаки на корпоративные данные, предприятия, оборудование. Используя слабость одного устройства, злоумышленнику легко попасть во всю цепь (использование слабого звена сети). Примером может быть атака на термостат NEST, проведенная в 2015 году инженерами компании TrapX Security. Они произвели подключение к miniUSB-порту термостата и провели MITM-атаку (man-in-the-middle), и при помощи специального приложение провели подмену адреса сетевого шлюза. Обретя контроль над IoT-сетью предприятия или дома, злоумышленники могут не только украсть личные данные, но и поставить под угрозу жизнь и здоровье владельцев.

Помимо этого можно выделить использование привычных паролей на всех устройствах, включая и корпоративные.

Аналитический раздел

Для встраиваемых устройств единственное решение, которое позволит исключить возможность эксплуатации уязвимостей, - это использование безопасных операционных систем.

Если рассматривать смарт-холодильники, то на рынке представлены в основном модели двух компаний - LG и Samsung. Компания LG для смарт-холодильников последних моделей использует операционную систему webOS. Это встраиваемая открытая операционная система, основанная на ядре Linux. Система оптимизирована для работы с устройствами, оснащенными сенсорными экранами. Включает стандартное программное обеспечение для организации работы с личной информацией. Компания Samsung свою линейку смарт-холодильников выпустила под управлением операционной системы Tizen, которая также является открытой и основана на ядре Linux.

Как и для любого другого IoT устройства, "сердцем" смарт-холодильников является программное обеспечение, а не компрессор. Эти устройства подключены ко всем устройствам сети, имеют постоянное Интернет-подключение.

Ошибки являются частью процесса разработки программного обеспечения. Ни одно программное обеспечение не защищено от ошибок и многие из этих ошибок могут привести к уязвимостям, которые могут быть использованы киберпреступниками.

С внедрением большого количества "умных" устройств в жизнь человека, часто нет необходимости взламывать ноутбук или персональный компьютер,

чтобы получить доступ к, например, денежному счету жертвы. При взломе одного из небезопасных IoT устройств, злоумышленники могут поставить под угрозу всю сеть. И смарт-холодильники из-за своей новизны на данный момент выступают одними из самых уязвимых в концепции "умного" дома.

Обратившись к странице гарантии смарт-холодильников компаний Samsung и LG, невозможно найти ни слова о программном обеспечении. То есть потенциальный пользователь при покупке данного устройства не получает сведений касательно того, как долго продукт будет получать обновления программного обеспечения. Запросы на предоставления такой информации в официальных группах социальных сетей компаний так же не дали ответов о поддержке программного обеспечения для выпускаемых смарт-холодильников.

Поскольку компании, выпускающие смарт-холодильники, не имеют прозрачной политики поддержки программного обеспечения, нет никакого подтверждения и гарантии получения своевременных обновлений для исправления брешей в безопасности.

В 2016 году киберпреступники собрали интеллектуальные устройства в огромный ботнет для запуска массовых DDoS-атак. Однако, смарт-холодильники могут служить для более серьезных правонарушений. И речь не только о том, чтобы использовать устройства для запуска атак на других людей/компании, но и о личной безопасности владельца устройства.

Рассмотрим основные возможности смарт-холодильник Samsung Family Hub и возможные угрозы информационной безопасности для аналогичных устройств.

Главным анонсированным достоинством данной модели является 21.5-дюймовый сенсорный экран и наличие трех камер. Камеры установлены внутри для того, чтобы каждый раз, когда закрывается дверь делать снимки продуктов в холодильнике. Полученные данные передаются на смартфон и позволяют узнать, что из продуктов нужно купить, а чего достаточно. Это можно увидеть и на экране самого холодильника. Помимо этого, в США и некоторых странах Европы Family Hub интегрируется с локальными магазинами продуктов и можно заказывать доставку продуктов как с панели на дверце холодильника, так и со смартфона. Оплата при этос производится с привязанной к приложению для удаленного управления холодильником карты.

Какие угрозы может нести данный функционал. Учитывая тот факт, что для смарт-устройств нет установленной политики безопасности, вопросы конфиденциальности личных данных остаются под вопросом. К тому же использование открытых wi-fi точек доступа, отсутствие проверки подлинности SSL-сертификатов (данная уязвимость была представлена на конференции Defcon и касалась линейки смарт-холодильников Samsung) делают конфиденциальные данные более доступными.

Десктопные системы, ноутбуки, рабочие станции и мобильные телефоны относительно давно находятся в зоне риска и интересах злоумышленников, которые внедряют вредоносное программное обеспечение с целью контроля и получения доступа к банковским счетам, электронным кошелькам и другим ценным ресурсам. Таким образом, как ответ на это, антивирусные системы выработали ряд определенных мер защиты, которые, пусть и в недостаточной мере, однако защищают пользователей от хищений средств. Со стороны злоумышленников атаки на такие системы с каждым днем становятся все дороже, чем разумнее становятся системы, и более тонко учатся отражать их атаки. В свою очередь, IoT техника, в которой предусмотрен функционал покупки (автоматической покупки) или любых других автоматизированных операций, является "голубым океаном" и не требует таких затрат (классический подход). Среди таких вещей следует выделить "умные" холодильники, которые уже сегодня дозаказывают недостающие продукты из магазинов, с которыми есть партнерская программа. Вектор для кражи средств может быть реализован через простую подмену адреса получателя при денежном переводе.

Отдельным аспектом следует отметить и то, что с такой техникой обход верификации банков плательщика по фотографии также легко осуществим в силу того, что смарт-холодильники оснащаются, в том числе, и внешними камерами.

Также следует отметить, что смарт-холодильники оснащаются не только камерами, но и микрофонами для голосовых команд, разнообразными датчиками освещенности, приближения, что позволит на базе такого устройства создавать прекрасный инструмент для различного рода шпионажа.

Еще одним пунктом следует отметить, что богатый функционал, заложенный в холодильнике и доступный пользователю (и, несомненно, может быть доступен злоумышленнику), который находится непосредственно на операционной системе холодильника, может влиять (менять) на сроки годности продуктов, сочетая это с повышениями температур в то время суток, в которое человек холодильником не пользуется. Таким образом доводя определенные продукты до состояния токсичности, что, в определенных случаях, может заканчиваться летальным исходом в силу того, что определенный вид продуктов может не менять (или менять незначительно) свои вкусовые качества, но быть при этом уже крайне токсичным. Этот фактор не так критичен для стран Европы, но является серьезной угрозой для пользователей из Азии, которые в большом количестве употребляют морепродукты некоторые из которых требуют особого температурного режима не только для хранения, но и для приготовления.

Обеспечение безопасности в киберпространстве IoT

Потенциальными вопросами при определении потенциально возможно вреда от IoT устройств являются следующие:

– Есть ли возможность удаленного подключения к устройству и какие действия возможно произвести при наличии доступа?

– Каковы функциональные возможности устройства и какой вред они могут нанести, если устройство будет скомпрометировано?

– Какова "анатомия" устройства (работает ли устройство с полной операционной системой, имеет ли

она файловую систему и настройки конфигурации?

Если говорить о корпоративном секторе с отдельным штатом специалистов по информационной безопасности, то рекомендации по обеспечению безопасности можно выделить следующие:

– Выделение отдельного сегмента сети;
– Контроль целостности системных файлов;
– Контроль изменения конфигурации;
– Управление обновлениями;
– Резервное копирование;
– Жесткие парольные политики.

Однако, для рядового пользователя, использующего IoT устройства дома, эти правила малоприменимы. Соответственно, поскольку такой пользователь самостоятельно в большинстве случаев не сможет обеспечить безопасность IoT устройств, это задача должна ложиться на плечи вендоров.

Если рассматривать IoT устройства в целом, то на уровне производителя могут быть произведены следующие шаги:

– Донести до пользователя о рисках подключения устройства к сети Интернет и необходимых действиях со стороны пользователя для обеспечения минимального уровня безопасности;
– Обеспечить безопасную конфигурацию используемых сервисов и отключение неиспользуемых;
– Принудительная смена паролей по умолчанию, ввод парольных политик, исключающих использование простых паролей;
– Внедрение контроля безопасности кода программного обеспечения;
– Своевременное обновление программного обеспечения;
– Автоматическая проверка критических обновлений касающихся безопасности.

Касательно таких крупных устройств как смарт-холодильник, целесообразно не повышать уровень «интеллектуальности» устройства там, где это опасно. Если вернуться к примеру с достаточно опасным удаленным изменением температуры внутри смарт-холодильников, то это может быть возможность блокировки удаленного изменения температуры внутри камер.

Выводы

Классическими клише мира IoT являются интеллектуальный тостер и холодильник. Хотя эти примеры и представляют небольшую угрозу по сравнению с теми, которые используются в критически важной инфраструктуре.

Если сравнить сравнить смартфон, который используют повсеместно, со смарт-холодильником, то смартфон потенциально может наносить гораздо больший вред: он обрабатывает конфиденциальные данные, банковские счета, пароли, у него есть микрофон и камера, которыми можно злоупотреблять, обеспечивает идеальную промежуточную связь для взлома других устройств и он практически всегда рядом с владельцем. Однако смартфон с самого начала известен как потенциально уязвимый и меры безопасности встроены в устройство, обновления для защиты от новых уязвимостей применяются автоматически, а защита дополняется шифрованием данных и криптографически подписанным программным обеспечением.

Смарт-холодильники же просто распаковываются и включаются в сеть и проблематика безопасности крайне мало или вообще не учитывается в процессе его разработки, что делает это устройство крайне небезопасным.

Конечно, потенциальный вред от холодильника иногда кажется фантастическим. Однако, интеллектуальные приборы уже очень плотно входят в сферу медицины, например, где неправильное хранение препаратов может нанести непоправимый вред

Література

1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). [Electronic source] Date of Access: 06 June 2017. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
2. IoT cyber security [Electronic source] Available at: https://www.raconteur.net/infographics/infographic-iot-cyber-security
3. **Zhang, Z. K. et al.** (2014) IoT security: ongoing challenges and research opportunities. *Service-Oriented Computing and Applications* (SOCA), 2014 IEEE 7th International Conference, pp. 230-234.
4. **Xu, T., Wendt, J. B., Potkonjak, M.** (2014) Security of IoT systems: Design challenges and opportunities. *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, pp. 417-423.

Отримана в редакції 04.07.2017, прийнята до друку 08.09.2017

The problem of using the Internet of things on the example of smart refrigerators

K. Smirnova[1], A. Smirnov[2], O. Olshevska[3], V. Vladimirova [4]
[1,3,4] Odessa National Academy of food Technologies, 112 Kanatnaya str., Odessa, Ukraine, 65082, Ukraine
ORCID: [1]0000-0002-3818-8083, [2]0000-0002-9459-6292, [3]0000-0002-4512-3915, [4] 0000-0002-6092-7946

Over the past decade, the growth in the development of various technologies has given rise to growing concerns about the security and confidentiality of their use. Unlike the infrastructure of the usual Internet network, the Internet of things is based on a huge number of sensors built into a wide variety of devices (in 2017 the number of devices is just over 20 billion [1]). Many of these devices are quite primitive and their functions are limited to sending to the server of

some information, for example, temperature measurement. But all these devices, in general, form huge streams of information and on the basis of such infrastructure a "network of networks" is built, consisting of connected devices, many of which can independently make certain decisions. It is almost impossible to integrate the security system into absolutely all devices. The market of IoT-devices has repeatedly faced with a number of serious violations of information security. So, in the fall of 2016, the first DDoS attack from the Mirai botnet, consisting entirely of "smart" things - more than half a million cameras, thermostats, DVRs and many other devices, was registered. In February 2017, an attack was carried out on one of the educational institutions. In this attack were involved about 10 thousand "smart" devices, including cameras, routers, thermostats. That is, for almost 5 months the manufacturers of Iot-devices did not fix the vulnerabilities that entailed the possibility of re-creating the botnet. As of April 2017, Mirai included 30 possible browser emulations, as opposed to 5 in the original version. And this means that the bot can bypass most of the security measures taken by information security specialists. Creating of functional interfaces and controls makes devices much more convenient for the potential consumer, however, this makes the devices more vulnerable. And if the user does not have the ability to control the device, the malfunction will only become apparent when the existing problem or the consequences of hacking the device do not manifest themselves, causing, in some cases, considerable damage. Of course, participation in DDoS attacks of smart devices can not cause visible damage to the owner. However, starting in 2011, the real consequences of hacking of similar devices were repeatedly demonstrated: remote cracking of an insulin pump, remote pacing of a pacemaker, which commanded a deadly discharge in 830V, complete capture of smart cars, etc. Smart refrigerators, as a component of the "smart home" concept, have not yet massively entered the life of the ordinary consumer because of the high price, compared to conventional refrigerators. However, according to analysts' forecasts in the next 7-10 years, these devices will have commercial success. At the moment, the main trends in smart refrigerators are: Internet management, understanding of voice commands, the possibility of ordering and recognizing products, the presence of a built-in camera. The article deals with the issues of information security of things in particular the safety issues of smart refrigerators. Based on the features of the area under consideration, possible solutions for organizing information protection of the components of the "smart" house are suggested.

Keywords: *internet of things; intellectual technique; smart house; information security.*

References

1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). [Electronic source] Date of Access: 06 June 2017. Available at: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

2. IoT cyber security [Electronic source] Available at: https://www.raconteur.net/infographics/infographic-iot-cyber-security

3. **Zhang, Z. K. et al.** (2014) IoT security: ongoing challenges and research opportunities. *Service-Oriented Computing and Applications* (SOCA), 2014 IEEE 7th International Conference, pp. 230-234.

4. **Xu, T., Wendt, J. B., Potkonjak, M.** (2014) Security of IoT systems: Design challenges and opportunities. *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, pp. 417-423.

Received 04 July 2017
Approved 08 September 2017
Available in Internet 30 October 2017