УДК 004.056.53

ИССЛЕДОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРИЛОЖЕНИЯХ IOT И МЕТОДОВ ЗАЩИТЫ ОТ ЭТИХ УГРОЗ

Тимофей Владимирович Таржанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся, тел. (953)881-23-25, e-mail: timofei1999.99@mail.ru

Сергей Николаевич Новиков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, профессор (совместитель), тел. (913)923-72-34, e-mail: snovikov@ngs.ru

Существующие технологии IoT не являются безопасными, и, если Интернет вещей функционирует в системе, где обрабатывается не только открытая информация, но и информация ограниченного доступа, то возникают риски утечки конфиденциальной информации. В Интернете вещей отсутствует единый стандарт и язык программирования, в связи с чем возникает необходимость анализа безопасности приложений IoT. Была поставлена цель исследовать угрозы информационной безопасности в приложениях IoT и методы защиты от этих угроз. Для достижения данной цели решаются следующие задачи:

– анализ беспроводных и проводных технологий IoT и их уязвимостей;
– разработка модели нарушителя;
– имитационное моделирование функционирования сети IoT в условиях внешних деструктивных воздействий;
– разработка рекомендаций по обеспечению целостности и доступности информации в сети IoT.

Ключевые слова: интернет вещей, виртуальная сеть, dos-атака, межсетевое экранирование, информационные технологии, кибербезопасность

INVESTIGATING THREATS OF INFORMATION SECURITY IN IOT APPS AND METHODS OF PROTECTION AGAINST THESE THREATS

Timofei V. Tarzhanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, phone: (953)881-23-25, e-mail: timofei1999.99@mail.ru

Sergei N. Novikov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor (part-time), phone: (913)923-72-34, e-mail: snovikov@ngs.ru

Existing IoT technologies are not secure, and if the Internet of Things operates in a system where not only open information is processed, but also information of limited access, then there are risks of leaks of confidential information. The Internet of Things lacks a single standard and programming language, which makes it necessary to analyze the security of IoT applications. The goal was to investigate information security threats in IoT applications and how to protect against these threats. To achieve this goal, the following tasks were being solved:

– analysis of wireless and wired IoT technologies and their vulnerabilities;
– development of a model of the intruder;

– simulation modeling of the functioning of the IoT network in conditions of external destructive influences;

– development of recommendations for ensuring the integrity and availability of information in the IoT network.

Keywords: internet of things, virtual network, dos-attack, firewalling, information technologies, cybersecurity

Введение

В настоящее время технологии IoT (от англ. Internet of Things – Интернет вещей) получают все большее распространение в промышленных предприятиях АСУ ТП и у физических лиц для бытового использования. Существующие технологии IoT не являются безопасными, и если IoT функционирует в системе, где обрабатывается не только открытая информация, но и информация ограниченного доступа, то возникают риски утечки конфиденциальной информации [2].

Были проанализированы наиболее распространенные в настоящее время технологии IoT [9], результаты сравнительного анализа [10] занесены в таблице.

Сравнительная характеристика технологий IoT

Технология	Стандарт	Тип сети	Рабочая частота	Дальность действия	Скорость передачи данных
Wi-fi	IEEE 802.11a,11b,11g,11n ,11ac,11ad	WLAN	2.4 ГГц	100 м	150–200 Мбит/с
Bluetooth	Bluetooth, Formerly, IEEE 802.15.1	Mesh	2.4 МГц	30 м	1024 кбит/с
ZigBee	IEEE 802.15.4	Mesh	868 МГц, 2.4 МГц	10 м	250 кбит/с
Z-Wave	Z-Wave	Mesh	до 1 ГГц	30 м	100 кбит/с
NFC	ISO/IEC 13157	Point to Point	13,56 МГц	0,1 м	100–400 кбит/с
LoRaWAN	LoRaWAN	Mesh	868 МГц	2–15 км	0,3–50 кбит/с
6LowPAN	RFC6282	Mesh	2.4 МГц	6 м	250 кбит/с
Thread	базируется на IEEE 802.15.4 и 6LowPAN	Mesh	2.4 МГц	11 м	250 кбит/с

Методы и материалы

В работе использовались следующие материалы:

– список литературы, рекомендованный научным руководителем;

– банк данных угроз безопасности ФСТЭК [1];

– основные технологии организации и реализации IoT (Wi-Fi, Bluetooth, ZigBee, Z-Wave, NFC, LoRaWAN, 6LowPAN, Thread, Ethernet, PLC, MoCa) [8].

Для имитационного моделирования атаки и реализации защиты от неё использовалось следующее программное обеспечение:

– Oracle VirtualBox;
– Ubuntu Linux 20.04;
– Mininet;
– POX Controller;
– sFlow-RT.

Результаты

С помощью анализатора sFlow было зафиксировано состояние сети IoT во время воздействия атаки и после реализации защиты.

После моделирования DoS-атаки на IoT сеть мониторинг состояния сети показал, что она загружена и что работоспособность сильно упала (рис. 1).

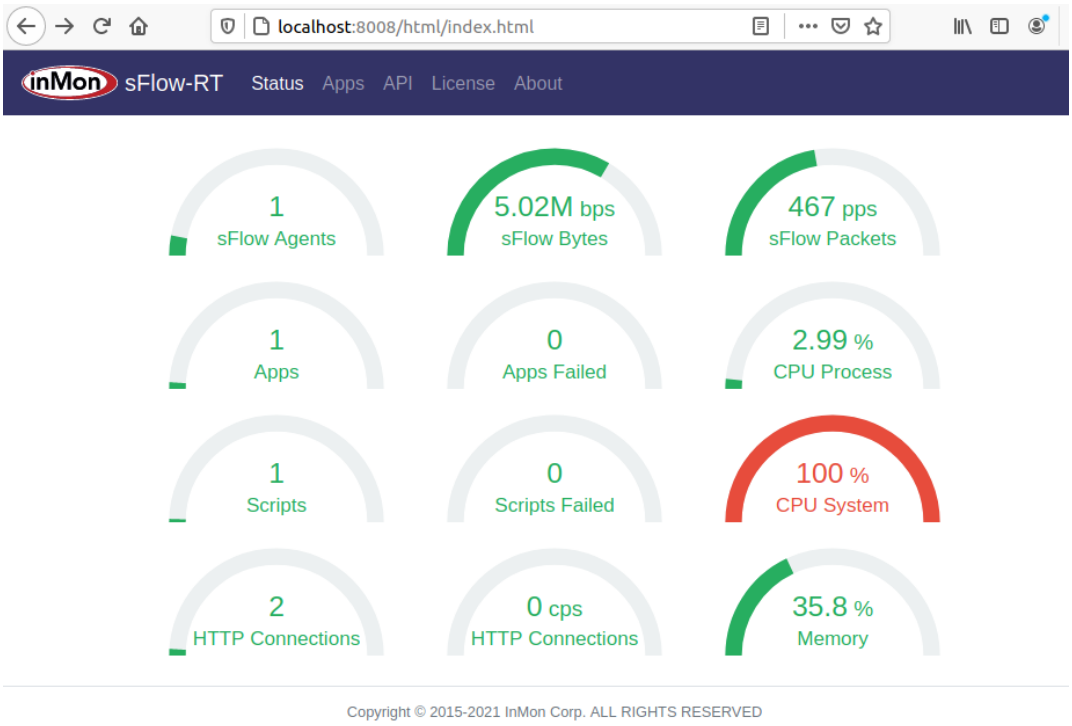

Рис. 1. Состояние IoT сети во время воздействия атаки

Затем была реализована защита от смоделированной атаки посредством межсетевого экранирования, проходящий сетевой трафик фильтровался контролером с новым правилом, которое было добавлено реализацией python-скрипта. При запуске сети с новыми параметрами была предпринята попытка ещё раз организовать DoS-атаку тем же способом, которая не увенчалась успехом. После реализации защиты пакеты атакующего хоста не достигали цели своего назначения, следовательно, сеть работоспособна и не нагружена (рис. 2).

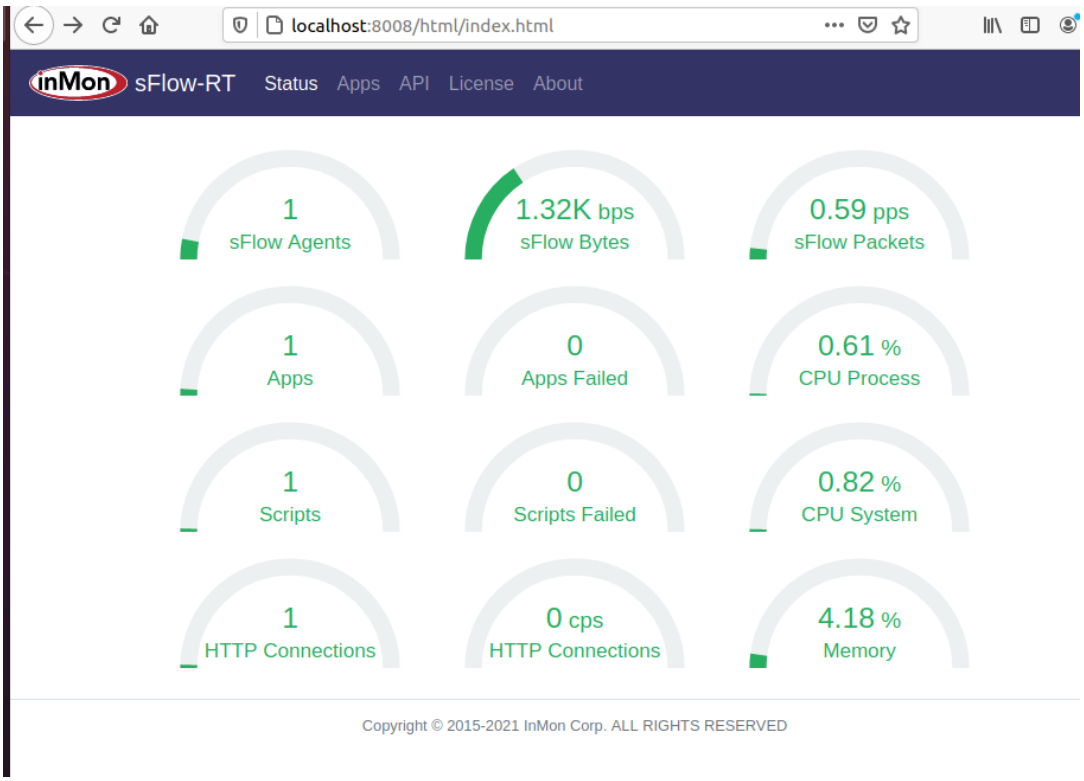

Рис. 2. Состояние IoT сети после реализации защиты

Обсуждение

Большое количество уязвимостей в IoT-устройствах обусловлено несколькими факторами, а именно: отсутствием у производителей достаточного опыта по обеспечению надёжной защиты своей продукции, скромные вычислительные и дисковые мощности устройств IoT, ограничивающие спектр доступных механизмов безопасности, непростые процедуры обновления ПО, а также отсутствие пользовательского внимания к угрозам, провоцируемым IoT-устройствами. Следует также учесть тот факт, что элементы Интернета вещей способны обмениваться данными по сети без какого-либо участия человека, и такое превращение умных устройств в самостоятельные интернет-узлы приводит к значительному снижению безопасности всей сети, где они функционируют [4].

Применение традиционных методов защиты устройств, таких как шифрование, идентификация/аутентификация и внедрение физических мер обеспечения безопасности, не подходит для Интернета вещей, так как требует их существенного реинжиниринга и адаптации, поскольку IoT устройства имеют множество ограничений. Например, хранение вредоносных сигнатур для обнаружения атак и «черных списков» требует большого объема памяти на диске, что является не всегда возможным. Интернет вещей, как правило, состоит из портативных устройств с низким электропотреблением, малым форм-фактором и ограниченными возможностями. Также, чаще всего, устройства являются неуправляемыми, т. е. работают без участия оператора, который мог бы ввести учетные дан-

ные или принять решение о том, насколько команда или приложение являются доверенными, поэтому устройства должны самостоятельно принимать подобные решения [7].

Также в свою очередь, устройства Интернета вещей за счет своей портативности и мобильности доступны злоумышленникам физически и могут быть украдены для получения доступа к конфиденциальным данным и установления связи с другими устройствами сети. Уязвимым является и программное обеспечение этих устройств за счет того, что на них не так часто выходят обновления и не все пользователи их своевременно обновляют. К тому же злоумышленник может взломать не только само устройство, но и сеть, в которой оно функционирует.

Существуют следующие способы обеспечения безопасности IoT [6]:

– обновление системы. Рекомендуется регулярно обновлять до последней версии операционную систему и все драйверы устройств. С каждым обновлением разработчики закрывают найденные на текущий моменты уязвимости, и в безопасной ОС риск возникновения угроз значительно меньше;

– обеспечение безопасности сети, в которой функционирует IoT. Важно защищать сетевые передачи данных и вести контроль взаимодействий в сети, например, путем установки межсетевого экрана. Системы для просмотра и аналитики сетевого трафика помогут лучше понять сеть и то, что в ней происходит, заметить подозрительные, опасные или злонамеренные аномалии и своевременно на них отреагировать;

– защита от вредоносных действий. Добавление новейших антивирусных программ и сканеров в те операционные системы устройств, которые их поддерживают. Это помогает устранять внешние угрозы и вовремя обнаружить компьютерную атаку;

– частое проведение аудита. Для своевременного предупреждения и предотвращения атак рекомендуется выполнять аудит инфраструктуры Интернета вещей на наличие уязвимостей в системе. Большинство операционных систем обладает встроенными средствами ведения журнала событий. Их следует часто просматривать, чтобы убедиться в отсутствии брешей в системе безопасности. Данные аудита также можно отправлять в разные облачные службы для анализа;

– физическая защита инфраструктуры Интернета вещей. Наиболее простыми угрозами безопасности для инфраструктуры IoT можно воспользоваться всего лишь с помощью физического доступа к устройствам. Очень важно обеспечить защиту USB-портов и других физически доступных злоумышленнику компонентов устройства. Также сюда относятся линии передачи данных, к которым злоумышленник может получить доступ;

– защита облачных учетных данных. Учетные данные, которые находятся в облаке и используются для настройки и работы IoT, возможно, являются самым простым способом получить доступ к системе устройства. Чтобы защитить свои учетные данные, следует изменять стандартные пароли и не авторизовываться на общедоступных компьютерах или в общедоступных сетях.

Заключение

В данном исследовании были рассмотрены особенности обеспечения информационной безопасности сети Интернета вещей, а также основные угрозы приложений IoT. Одна из них, самая распространенная, была реализована в смоделированной виртуальной сети с IoT устройствами. Была произведена эмуляция DoS-атаки, которая является одной из наиболее опасных для Интернета вещей в силу их слабых вычислительных мощностей. Также помимо эмуляции атаки на сеть, был разработан и реализован метод защиты от этой атаки путём добавления правила межсетевого экранирования в контроллер сети.

Таким образом можно сделать вывод, что информационная безопасность IoT находится не на должном уровне и должна постоянно развиваться. В настоящее время происходит очень большой рост внедрения Интернета вещей в повседневную жизнь многих людей. Любые предпринимаемые меры по защите Интернета вещей рано или поздно теряют свою актуальность и надежность, поэтому необходимо постоянно анализировать безопасность всей системы IoT в целом и отдельных устройств. Системы аналитики должны понимать сеть, видеть ее особенности и своевременно замечать подозрительные и опасные события.

Учитывая, что IoT приложения имеют слабую защиту, пользователям нужно регулярно соблюдать рекомендации по безопасности во избежание нарушения конфиденциальности персональных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Банк данных угроз безопасности информации [Электронный ресурс]. URL: https://bdu.fstec.ru/vul (дата обращения: 15.04.2021).

2. Грингард С. Интернет вещей. Будущее уже здесь / С. Грингард // М.: Альпина Паблишер. – 2019. – 56 с.

3. Мачей К. Интернет вещей. Новая технологическая революция / К. Мачей // М.: Бомбора. – 2018. – 132 с.

4. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]. URL: https://fstec.ru/component/%20attachments/download/812 (дата обращения: 14.04.2021).

5. Развитие «Интернета вещей»: проблемы и их решения [Электронный ресурс]. URL: https://wireless-e.ru/iot/razvitie-iot/ (дата обращения: 15.04.2021)

6. Рекомендации по обеспечению безопасности "Интернета вещей" [Электронный ресурс]. URL: https://docs.microsoft.com/ru-ru/azure/iot-fundamentals/iot-security-best-practices (дата обращения: 15.04.2021).

7. Полегенько А.М. Особенности защиты информации в Интернете вещей / А.М. Полегенько // International Journal of Open Information Technologies, no. 10. – 2018. – 41 с.

8. Cirani S., Ferrari G., Picone M., Veltri L. Internet of Things: Architectures, Protocols and Standards / S. Cirani, G. Ferrari, M. Picone, L. Veltri // John Wiley & Sons. – 2018. – 143 с.

9. Eleven Internet of Things (IoT) Protocols You Need to Know About [Электронный ресурс]. URL: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about (дата обращения: 14.04.2021).

10. Key Wireless Technologies for IoT Explained [Электронный ресурс]. URL: http://blog.bliley.com/wireless-technologies-for-iot (дата обращения: 15.04.2021).