www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.4.2

УДК 004.056.53
ББК 32.971.35

СИСТЕМА КОНТРОЛЯ ВЗАИМОДЕЙСТВИЯ В СЕТИ С ПОДКЛЮЧЕНИЕМ IoT-УСТРОЙСТВ

Глеб Дмитриевич Демьянов

Студент кафедры информационной безопасности,
Волгоградский государственный университет
005_gleb@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Наталья Петровна Садовникова

Доктор технических наук, профессор кафедры «Системы автоматизированного проектирования и поискового конструирования»,
Волгоградский государственный технический университет
npsn1@yandex.ru
просп. им. Ленина, 28, 400005 г. Волгоград, Российская Федерация

Аннотация. В статье рассматривается вопрос использования системы контроля взаимодействия в сети с подключением IoT-устройств. Выделяются основные угрозы информационной безопасности IoT-устройств и методы защиты представленных угроз. Посредством анализа выбирается приоритетный метод защиты и описывается как этот метод можно реализовать на практике.

Ключевые слова: интернет вещей, IoT-устройства, контроль взаимодействия в сети, информационная безопасность.

Интернет вещей (англ. internet of things, IoT) – концепция вычислительной сети физических предметов («вещей»), оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей, как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека [1].

Технология IoT оказала существенное влияние на развитие информационных технологий и других отраслей. Согласно Forbes, ожидается, что рынок интернет вещей в 2021 году достигнет 520 млрд долларов по сравнению с 235 млрд долларов в 2017 году, что свидетельствует о непрерывном росте потребности в таких устройствах в будущем [5]. Также, по оценкам Gartner Research, количество устройств, подключенных к Интернету, к 2021 году достигнет 25 миллиардов по сравнению с 8,4 миллиарда в 2017 году [4].

С каждым годом будет расти как количество устройств IoT, так и количество злоумышленников. Лаборатория Касперского представила следующую статистику за 2016–2018 годы [2] (см. рис. 1).

К основным типам угроз можно отнести (см. табл. 1):

На основе анализа угроз можно выделить основные методы защиты устройств IoT [3]:

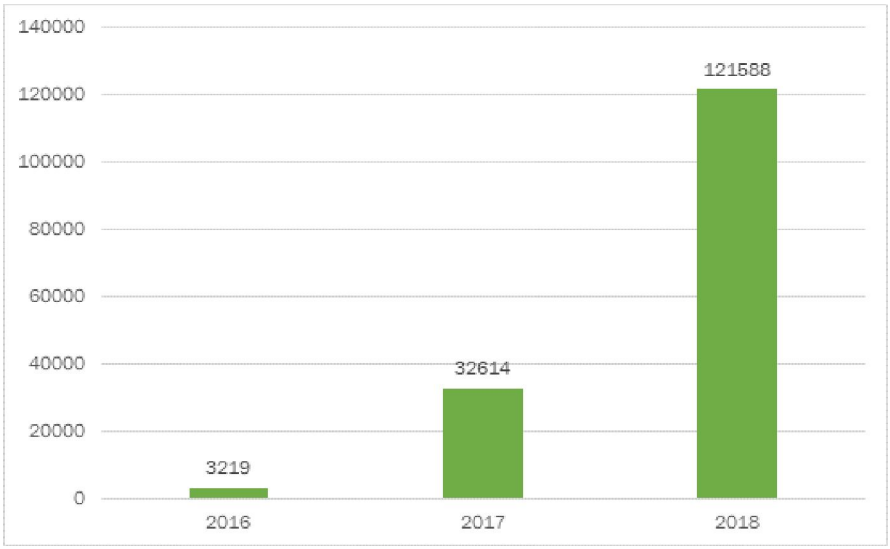

Рис. 1. Количество образцов вредоносного ПО для IoT-устройств в коллекции «Лаборатории Касперского», 2016–2018 гг.

Таблица 1

Анализ основных угроз, связанных с подключением устройств IoT

Субъект угрозы	Объект угрозы
Ботнеты и атаки DDoS	Сетевые ресурсы
Удаленная запись данных, передаваемых устройством	Конфиденциальные данные пользователя
Ransomware	Пользователь, имущество пользователя
Реальные кражи (взлом умных замков, автомобилей, гаражных дверей)	Пользователь, имущество пользователя

1. Безопасность связи – использование технологий шифрования, проверки подлинности.

2. Защита устройств – использование технологий обеспечения безопасности и целостности программного кода.

3. Контроль устройств – поддержка уже созданных устройств, выпуск обновлений прошивки, патчей, закрывающие бреши в защите прошлых патчей.

4. Контроль взаимодействия в сети – проанализировав все методы, приведенные выше, я пришел к выводу, что именно этот метод является самым надежным для обнаружения и предотвращения атаки на устройство. Контроль и защита устройств остается на стороне разработчика этих устройств, а безопасность связи и контроль взаимодействия в сети – на стороне предприятия использующего устройства IoT.

Наряду с эффективностью метода защиты так же можно выделить такой важный критерий выбора, как стоимость реализации метода защиты. В связи с этим самым перспективным направлением защиты является контроль взаимодействия в сети.

Было проанализировано несколько средств контроля взаимодействия в сети без использования IoT-технологий. Основой для этих программных средств является предупреждение пользователя о вероятном злоумышленнике, подключившимся к сети (см. табл. 2).

Для защиты устройств IoT необходимо выделять такие потенциально опасные подключения в отдельную группу и контролировать их деятельность в сети. Поэтому основными функциями системы контроля взаимодействия в сети должны быть анализ деятельности потенциально опасных устройств в сети и обнаружение новых потенциально опасных подключений.

Анализ действий в сети будет осуществляться посредством анализа заголовка каждого пакета в сети, основным сигналом к анализу передаваемых данных послужат поля заголовка «адрес получателя» и «адрес отправителя» (см. рис. 2).

Таблица 2

Методы контроля взаимодействия в сети

Наименование программы	Возможность автоматического сканирования устройств в сети	Информация об устройстве	Логирование	Обнаружение новых подключений
Wi-Fi Network Monitor	Есть	Показывает IP-адрес, MAC-адрес, имя устройства	Сохраняет отчет в форматах HTML/XML/CSV/TXT	Есть
SoftPerfect WiFi Guard	Есть	Показывает IP-адрес, MAC-адрес, имя, пинг устройства	Нет	Есть

Рис. 2. Структура пакета, передаваемого по сети

Обнаружение новых подключений будет осуществляться посредством мониторинга подключенных устройств в сети и ведения списков уже подключенных устройств.

Для получения пакетов отдельным устройством, на котором будет проходить анализ подключений и действий в сети, нужно будет использовать одну из представленных ниже технологий перехвата пакетов в сети (табл. 3).

Вне зависимости от выбора технологии зеркалирования пакетов, разрабатываемая система будет работать с этими пакетами. Проанализировав все три технологии, можно сделать вывод, что наиболее удобными будут технологии SPAN и RSPAN. Значительный минус технологии TAP – необходимость устанавливать в сеть специального оборудования и, в следствии чего, невозможность удаленной настройки.

Можно выделить следующие основные функции системы контроля взаимодействия в сети:

1. Сканирование подключенных к сети устройств.

2. Ведение списков доверенных устройств, устройств IoT и потенциально опасных устройств.

3. Перехват пакетов потенциально опасных устройств.

4. Анализ пакетов на наличие вредоносных действий в сторону IoT-устройств.

Таблица 3

Анализ популярных средств перехвата пакетов по сети

Название технологии	Потеря пакетов	Удобство настройки	Сложность установки
SPAN (port mirroring)	Потеря пакетов несущественна, но присутствует	Можно фильтровать зеркалируемые пакеты, уменьшая объем данных. Можно настроить отражаемую сеть VLAN	Необходимо наличие коммутатора, поддерживающего технологию SPAN
RSPAN	Потеря пакетов несущественна, но присутствует	Можно фильтровать зеркалируемые пакеты, уменьшая объем данных. Можно настраивать отражаемую сеть VLAN и принимающую сеть VLAN	Необходимо наличие коммутатора, поддерживающего технологию RSPAN
TAP (Test Access Point)	Практически без потери	TAP – аппаратное средство и его необходимо размещать непосредственно в сети, а не задать настройками коммутатора, нет возможности поменять настройки удаленно	Необходимо наличие, помимо коммутатора, специальных ответвителей трафика

5. Формирование отчета потенциально опасных действий в сторону IoT-устройств.

Основываясь на заданных функциях системы контроля взаимодействия в сети, можно выделить основные модули:

– модуль управления списками доверенных устройств;

– модуль управления списками IoT-устройств;

– модуль управления списками потенциально опасных устройств;

– модуль сбора пакетов, который должен реализовать прослушку IoT-устройства, чтобы принять от него потенциально опасный пакет;

– модуль логирования потенциально опасных действий в сети;

– модуль сканирования устройств в сети.

На рисунке 3 цифрами на стрелках обозначены передаваемые данные:

1. IP, MAC адреса устройств IoT и доверенных устройств.

2. IP, MAC адреса доверенных устройств.

3. IP, MAC адреса IoT-устройств.

4. IP, MAC адреса потенциально опасных устройств.

5. IP, MAC адреса потенциально опасных устройств и IP, MAC адреса прослушиваемого IoT-устройства.

6. Время потенциально опасного действия, IP, MAC адреса потенциально опасного устройства, подключенного к сети, либо IP, MAC адреса IoT-устройства и потенциально опасного устройства.

7. IP, MAC адрес IoT-устройства, которое получило пакет и IP, MAC адрес потенциально опасного устройства, с которого этот пакет был отправлен.

Модуль сканирования устройств в сети определяет все подключения в сети.

Модуль управления списками доверенных устройств позволяет заносить устройства в список доверенных.

Модуль управления списками IoT-устройств позволяет заносить устройства в список защищаемых IoT-устройств.

Модуль управления списками потенциально опасных устройств сам определяет, основываясь на работе предыдущих двух модулей, опасно новое подключившееся устройство или нет.

Модуль сбора пакетов получает все пакеты в сети, используя технологии зеркалирования трафика (см. табл. 3).

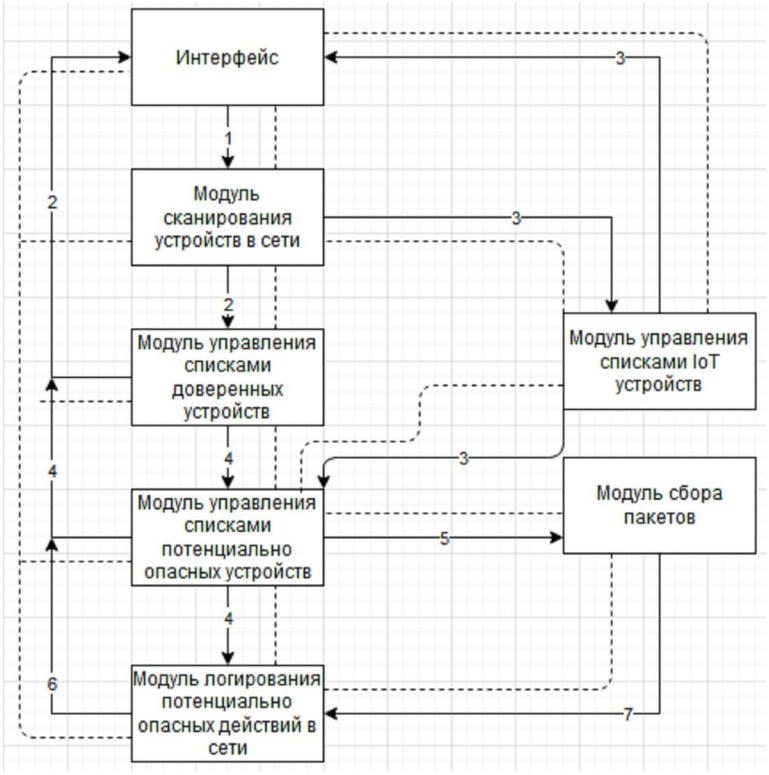

Рис. 3. Система контроля взаимодействия в сети

Модуль логирования потенциально опасных действий в сети формирует информацию о совершенных потенциально опасных действиях (подключение нового, потенциально опасного устройства в сети, передача потенциально опасного пакета устройству IoT), а так же дублирует эту информацию в файлы лога, с указанием времени потенциально опасного действия для повторного анализа.

Таким образом система контроля взаимодействия в сети может обнаружить и пресечь потенциально опасные действия в сторону устройств IoT (посредством блокировки злоумышленника по MAC адресу и др.). Система контроля взаимодействия в сети может использоваться как на предприятии (умные электростанции, торговые и транспортные сети), так и у частных лиц (система умного дома).

Все устройства IoT заведомо содержат уязвимости, так как они находятся не в изолированной системе, а с доступом в интернет. Это подтверждает активный рост вредоносного ПО. Необходимо уделять должное внимание безопасности IoT-устройств. При своевременном анализе сетевого трафика возможно предотвратить угрозу устройству.

СПИСОК ЛИТЕРАТУРЫ

1. Интернет-энциклопедия. – Электрон. текстовые дан. – Режим доступа: https://ru.wikipedia.org/wiki (дата обращения: 14.09.2020). – Загл. с экрана.

2. Лаборатория касперского. – Электрон. текстовые дан. – Режим доступа: https://www.kaspersky.ru (дата обращения: 26.09.2020). – Загл. с экрана.

3. Эталонная архитектура безопасности интернета вещей (IoT). Часть 1. – Электрон. текстовые дан. – Режим доступа: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (дата обращения: 14.09.2020). – Загл. с экрана.

4. Gartner представил список стратегических IoT-трендов до 2023 года. – Электрон. текстовые дан. – Режим доступа: https://iot.ru/promyshlennost/gartner-predstavil-spisok-strategicheskikh-iot-trendov-do-2023-goda (дата обращения: 26.09.2020). – Загл. с экрана.

5. Juniper Research. IoT Connections to Grow 140% to Hit 50 Billion By 2022, As Edge Computing Accelerates ROI. – Электрон. текстовые дан. – Режим доступа: https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion (дата обращения: 12.09.2020). – Загл. с экрана.

REFERENCES

1. *Internet entsiklopediya* [Wikipedia]. URL: https://ru.wikipedia.org/wiki/ (accessed 14 September 2020).

2. *Laboratoriya Kasperskogo* [Kasperky Lab]. URL: https://www.kaspersky.ru (accessed 26 September 2020).

3. *Etalonnaya arkhitektura bezopasnosti interneta veshchey (IoT). Chast 1* [Internet of Things (IoT) Reference Security Architecture. Part 1]. URL: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1 (accessed 14 September 2020).

4. *Gartner Has Presented a List of Strategic IoT Trends Until 2023*. URL: https://iot.ru/promyshlennost/gartner-predstavil-spisok-strategicheskikh-iot-trendov-do-2023-goda (accessed 26 September 2020).

5. *Juniper Research. IoT Connections to Grow 140% to Hit 50 Billion By 2022, As Edge Computing Accelerates ROI.* URL: https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion (accessed 12 September 2020).

NETWORK INTERACTION MONITORING SYSTEM WITH IoT DEVICES CONNECTED

Gleb D. Demyanov

Student, Department of Information Security,
Volgograd State University
005_gleb@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Natalya P. Sadovnikova

Doctor of Sciences (Engineering), Professor,
Department of Computer-Aided Design and Search Engineering,
Volgograd State Technical University
npsn1@yandex.ru
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Abstract. The Internet of Things is a concept of a computer network of physical objects equipped with built-in technologies for interacting with each other or with the external environment, considering the organization of such networks as a phenomenon that can restructure economic and social processes, eliminating the need for human participation from part of actions and operations. IoT technology has had a significant impact on the development of information technology and other industries. According to Forbes, the Internet of Things market is expected to reach $520 billion in 2021, up from $235 billion in 2017, indicating a continued growth in demand for such devices in the future. Gartner Research also estimates that the number of devices connected to the Internet will reach 25 billion by 2021, up from 8.4 billion in 2017. Network with IoT devices connected is an indispensable prey for intruders. There are many ways to attack IoT devices. In this article, the authors have identified several methods of protection. Among them, network interaction monitoring through the analysis is highlighted. The paper also describes how to apply this method in practice.

Key words: Internet of Things, IoT devices, network interaction monitoring, information security.