DOI 10.37882/2223–2966.2022.10.39

АНАЛИЗ УЯЗВИМОСТЕЙ ИНТЕРНЕТ ВЕЩЕЙ

VULNERABILITY ANALYSIS OF THE INTERNET OF THINGS

V. Shutov
M. Sholeninov
I. Kotilevets
L. Kashurin
E. Bogadelshchikova
V. Shishov

Summary. This article focuses on the security aspects of the Internet of things. The Internet of Things (IoT — internet of things) is a relatively new technology that connects many "smart" devices into a network, allowing them to collect, analyze, process and transmit data to each other. This industry develops rapidly, but there are some difficulties: vulnerability to cyber attacks, lack of secure update mechanisms, use of insecure or outdated components and other vulnerabilities. This article examined and structured the current vulnerabilities of the Internet of things, leading to disruption of device performance, leakage, hacking and loss of important, confidential information due to the implementation of various types of threats. Also analysis of vulnerabilities and their sources was performed, methods for their prevention were described. A list of recommendations for security of smart devices was also compiled.

Keywords: information security, information technology, Internet of Things, vulnerability of the Internet of things.

Шутов Василий Александрович
Аспирант, ассистент
Российский технологический университет МИРЭА
shutov@mirea.ru]
Шоленинов Михаил Владимирович
Российский технологический университет МИРЭА
medvedsholeninov@gmail.com
Котилевец Игорь Денисович
Старший преподаватель
Российский технологический университет МИРЭА
ikotilevets@gmail.com
Кашурин Лев Вячеславович
Российский технологический университет МИРЭА
OtSpec17L10@outlook.com
Богадельщикова Евгения Владимировна
Российский технологический университет МИРЭА
bogadelshikova@list.ru
Шишов Валерий Дмитриевич
Российский технологический университет МИРЭА
shishov265@gmail.com]

Аннотация. Данная статья посвящена аспектам безопасности интернет вещей. Интернет вещи (IoT — internet of things) — относительно новая технология, объединяющая множество «умных» устройств в сеть, позволяющая им собирать, анализировать, обрабатывать и передавать друг другу данные. Эта отрасль стремительно развивается, однако на пути ее развития встречаются трудности: уязвимость к кибератакам, отсутствие безопасных механизмов обновления, использование небезопасных или устаревших компонентов и другие уязвимости. В данной статье были рассмотрены и структурированы актуальные уязвимости интернет вещей, приводящие к нарушению работоспособности устройств, утечки, взлому и потере важной, конфиденциальной информации вследствие реализаций различных видов угроз. Также был выполнен анализ уязвимостей и их источников и описаны методы их предотвращения. Также был составлен список рекомендаций по обеспечению безопасности умных устройств.

Ключевые слова: информационная безопасность, информационные технологии, Internet of Things, уязвимость интернет вещей.

Введение

В настоящее время большую популярность набирает тема интернет вещей и одной из приоритетных является тематика умного дома. С каждым годом рынок интернет вещей наполняется новыми предложениями со стороны производителей интернет вещей, например, умные колонки, лампочки, розетки, телевизоры.

Интернет вещи упрощают жизнь, ускоряя бытовые и рутинные процессы, тем самым позволяя грамотно распределять время. IoT позволяют людям автоматизировать и контролировать необходимые функции жилых площадей, транспорта, здравоохранения и сервисов для населения, такие как поддержка работы экстренных служб и мониторинг общественной безопасности. Согласно статье «АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ СИСТЕМЫ «УМНЫЙ ДОМ» В ИНДИВИДУАЛЬНОМ ЖИЛОМ ДОМЕ»,

благодаря вышеуказанной автоматизации популярность и актуальность умного дома будет расти [5].

Учитывая рост количества Интернет вещей в жизни, немаловажным становится обеспечение безопасности данных устройств. Несмотря на удобство, существуют риски утечки информации, взлома и кражи, хранящихся данных, так как технология умных вещей появилась совсем недавно.

Основная часть

По данным исследований Microsoft Security 35% участников столкнулись с реализацией угроз на их устройствах IoT [4]. Это связано с определенными уязвимостями. Первой из которых является использование устаревших или небезопасных программных компонентов или библиотек, которые могут позволить скомпрометировать устройство, например, небезопасная настройка платформ операционной системы и использование сторонних программных или аппаратных компонентов из небезопасной цепочки поставок. Чтобы избежать данной уязвимости, целесообразно выполнять следующее действие — необходимо следить за выходом программных средств, дополнений безопасности, иначе рекомендуется сменить производителя.

Следующая уязвимость связана с отсутствием возможности безопасного обновления устройства. Данная уязвимость включает в себя недостаток валидации встроенного программного обеспечения на устройстве, безопасной доставки. Которая должна быть реализована согласно ГОСТу Р 51898–2002 «Аспекты безопасности. Руководящие указания по включению их в стандарты», без шифрования при передаче, механизмов предотвращения отката и отсутствие уведомлений об изменениях безопасности из-за обновлений [3]. Отсутствие возможности обновления устройства само по себе является слабым местом безопасности. Невозможность установить обновление означает, что устройства в течение неопределенного времени остаются уязвимыми. Решение данной проблемы на стороне производителя. Также возможно самостоятельно проверить, способно ли ваше устройство обновляться. Необходимо убедится, что файлы обновления загружаются с проверенного сервера по зашифрованному каналу и что устройство использует безопасную архитектуру установки обновления.

К одному из вариантов решения проблемы данной уязвимости можно отнести использование сетевого устройства. Через него все IoT имеют доступ к интернету, с помощью которого поддерживаются безопасные протоколы передачи данных, для того чтобы через него получать обновления.

Устройства или системы IoT поставляются с небезопасными настройками по умолчанию или не имеют возможности сделать систему более безопасной, ограничивая пользователей в изменении конфигурации. Чтобы избежать данной проблемы следует изменять настройки «по умолчанию» при возможности. Если отсутствует такая возможность, рекомендуется отказаться от производителя устройств Io T.

Немаловажной уязвимостью интернет вещей является недостаточная защита конфиденциальности. К недостаточной защите конфиденциальности относится личная информация пользователя, хранящаяся на устройстве или в экосистеме, которая используется небезопасно, ненадлежащим образом или без разрешения. IoT- устройства собирают информацию об окружающей среде и пользователях. Украденные или неправильно обработанные данные о пользователе могут ненамеренно дискредитировать человека. Чтобы избежать последствий данной незащищенности интернет вещей необходимо знать, какие данные собираются устройством IoT, мобильным приложением и облачными интерфейсами. Следует убедиться, что собираются только необходимые для функционирования устройства данные, проверить, есть ли разрешение на хранение персональных данных и защищены ли они, а также прописаны ли политики хранения данных. Иначе, при несоблюдении этих условий, у пользователя могут возникнуть проблемы с законодательными органами.

Существуют и другие проблемы уязвимости интернет вещей, связанные с оборудованием и программным обеспечением. Одна из наиболее распространенных — это ограниченность памяти. Поскольку в IoT устройствах используется оперативная память и жесткий диск, устройства IoT имеют ограниченную память. Данные устройства используют операционную систему реального времени (RTOS) или операционную систему общего назначения (GPOS) облегченной версии. Следовательно, схемы безопасности IoT также должны быть эффективными с точки зрения памяти. Поэтому необходимо выбирать продукции надежного производителя, который учел данный недостаток.

Немаловажной уязвимостью также является недостаточная физическая безопасность и наличие бэкдоров. Первая проблема безопасности экосистемы IoT заключается в том, что ее компоненты распределены в пространстве и часто устанавливаются в публичных или незащищенных местах. Это дает возможность злоумышленникам получить доступ к устройству и взять его под контроль локально или использовать для доступа к остальной сети. Данный недостаток исправляется усложнением физического доступа к устройствам. Их можно устанавливать на защищенных площадках,

на высоте или использовать антивандальные защищенные шкафы.

Следующая уязвимость — это ограниченность встроенного программного обеспечения. Устройства IoT используют операционные системы реального времени, которые встроены в эти устройства, поэтому IoT имеют очень маленький стек сетевых протоколов, что приводит к отсутствию большего количества модулей безопасности. Как меру предотвращения используют надежный и отказоустойчивый модуль безопасности с небольшим стеком протоколов.

Другие уязвимости связаны с проблемами сети и их данных, например, небезопасная передача и хранение данных, и отсутствие возможности управлять устройством. К данным недостаткам интернет вещей можно отнести отсутствие поддержки безопасности на устройствах, развернутых в производстве, включая управление активами, обновлениями, безопасный вывод из эксплуатации, мониторинг систем и реагирование, также недостаток шифрования или контроля доступа к конфиденциальным данным в любом месте экосистемы, в том числе при хранении, передаче или во время обработки. Устройства интернет вещей собирают и хранят данные об окружающей среде, в том числе различную персональную информацию. Чтобы избежать приведенные выше уязвимости обычно используют специализированное ПО для управления устройствами интернет вещей, например, облачные решения AWS, Google, IBM, помимо этого пользователю рекомендуется использовать безопасные каналы связи для передачи данных, а шифрованием хранимых паролей, биометрических и других важных данных должен заниматься производитель устройств.

Рекомендации по безопасности Io T

Согласно ГОСТу Р 50922–2006 и ГОСТ Р 51275–2006 можно выделить некоторые рекомендации по обеспечению безопасности IoT:

1. одной из основных задач безопасности, является устранение неоднородности IoT, вариантов решения может быть несколько вот некоторые из них: использование устройств только от одного производителя, использование защищенного приложения для контроля и настройки устройств. Данные действия помогают контролировать все IoT и также позволят следить за их состоянием;
2. немаловажным также является планирование сети IoT, то как устройства соединены и как в ней действуют. И чтобы избежать проблем, связанных с тем что устройство при взломе будет узлом для атаки персональных вещей. Крайне рекомендуется использовать для интернет вещей отдельную сеть, чтобы персональные данные были всегда в безопасности;
3. необходимо использовать устройства, которые вышли недавно, так как поддержка их ПО только началась, то есть, новое программное обеспечение создавалось с учетом существующих ошибок, или же покупать устройства, которые до сих пор получают поддержку от производителя в виде обновлений ПО. Таким образом можно будет избежать реализации угрозы использования уязвимостей старых обновлений;
4. активация двухфакторной аутентификации или использование возможностей биометрической аутентификации. Данная система значительно усложняет доступ к конфиденциальным данным пользователя и устраняет недостатки парольной системы. Также аутентификацию можно усложнить с помощью голосовой идентификации, SecureID, USB-ключей, а также генераторов кодов [1], [2].
5. Усложнение физического доступа к устройствам.
6. Использование шифрования хранимых паролей.

Заключение

В настоящее время IoT является довольно молодой технологией, которая стремится сделать те или иные задачи более доступными для человека, и вследствие чего имеет недостатки, связанные с информационной безопасностью.

Для их устранения необходимо подробно ознакомиться с соответствующими рекомендациями; необходимо обращать особое внимание на стадии проектирования сети интернет вещей. По этой причине одной из главных задач при применении IoT технологий является обеспечение защиты информации, путем применения комплексов средств защиты.

В данной статье были рассмотрены теоретические и практически установленные недостатки и уязвимости IoT устройств, свойственные продукции различных производителей. На их основании было проведено исследование возможных способов решения, которые, в соответствии с государственными стандартами, приводятся в тексте статьи.

Как уже было сказано выше, технологии интернета вещей еще довольно молоды. По этой причине еще не удается в полной мере охватить возможные проблемы, которые могут возникнуть в ходе эксплуатации. Однако, опираясь на уже имеющиеся данные и знания в области информационной безопасности, в ходе написания статьи был получен набор правил и рекомендаций, который уже готовы к применению.

ЛИТЕРАТУРА

1. ГОСТ Р 50922–2006 «Основные термины и определения»
2. ГОСТ Р 51275–2006 — «Объект информатизации. Факторы, воздействующие на информацию»
3. ГОСТ Р 51898–2002 — «Аспекты безопасности»
4. Chris Hallum Senior Product Marketing Manager "New research shows IoT and OT innovation is critical to business but comes with significant risks" URL: https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/ (дата обращения: 17.04.2022).
5. Полищук Е.И. АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ СИСТЕМЫ «УМНЫЙ ДОМ» В ИНДИВИДУАЛЬНОМ ЖИЛОМ ДОМЕ // Материалы XI Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2019/article/2018015646 (дата обращения: 17.04.2022).

© Шутов Василий Александрович (shutov@mirea.ru), Шоленинов Михаил Владимирович (medvedsholeninov@gmail.com),
Котилевец Игорь Денисович (ikotilevets@gmail.com), Кашурин Лев Вячеславович (OtSpec17L10@outlook.com),
Богадельщикова Евгения Владимировна (bogadelshikova@list.ru), Шишов Валерий Дмитриевич (shishov265@gmail.com]).
Журнал «Современная наука: актуальные проблемы теории и практики»

МИРЭА — Российский технологический университет