УДК 004.054

ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕСТИРОВАНИЯ ИНТЕРНЕТА ВЕЩЕЙ

[1–3]Ананченко И.В., [2]Распопа Е.А., [2]Хаджиев И.В.

[1]ФГБОУ ВО «Санкт-Петербургский государственный технологический институт (технический университет)», Санкт-Петербург;
[2]ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Санкт-Петербург, e-mail: elizaveta.raspopa.yandex.ru, ilya.khadzhiev@gmail.com;
[3]ФГБОУ ВО «Российский государственный гидрометеорологический университет», Санкт-Петербург, e-mail: igor@anantchenko.ru

Настоящая статья посвящена исследованию процесса тестирования интернета вещей, рассмотрены характерные особенности систем: динамическая среда, зависимости от качества аппаратного обеспечения, повышенная нагрузка на сеть, интеграция с облачными сервисами, обработка больших объемов данных, использование устройств разных поколений от различных производителей и разработчиков программного обеспечения и другое. Выполнен обзор перспектив развития и сдерживающих факторов роста сегмента интернета вещей. На примере рассмотрены основные процессы, влияющие на выбор методологии тестирования IoT-системы. Классические методы функционального и нефункционального тестирования находят применение и в контексте интернета вещей, однако на первый план выходят проблемы обеспечения информационной безопасности и совместимости. Приведены основные направления развития тестирования интернета вещей: тестирование безопасности, совместимости, обновлений, соответствия отраслевым стандартам, тестирование на этапе поддержки.

Ключевые слова: интернет вещей, тестирование, информационная безопасность, стандартизация

THE PROSPECTS OF TESTING THE INTERNET OF THINGS

[1–3]Ananchenko I.V., [2]Raspopa E.A., [2]Khadzhiev I.V.

[1]Saint-Petersburg State Technological Institute (Technical University), Saint-Petersburg;
[2]Federal State Autonomous Educational Institution of Higher Professional Education «Saint-Petersburg National Research University Of Information Technologies, Mechanics and Optics», Saint-Petersburg, e-mail: elizaveta.raspopa.yandex.ru, ilya.khadzhiev@gmail.com;
[3]Federal State Budgetary Educational Institution of Higher Professional Education «Russian State Hydrometeorological University», Saint-Petersburg, e-mail: igor@anantchenko.ru

This article is devoted to the study of the process of testing the Internet of things discussed the characteristic features of the system: dynamic environment, based on quality of hardware, increased network load, integration with cloud services, handling large amounts of data, use of devices of different generations from different manufacturers and software developers, and more. Produced the review of development prospects and constraints for the growth of IOT. For example, consider the main processes influencing the choice of testing methodology IoT system. Classical methods of functional and non-functional testing applications in the Internet of things context, however, to the fore issues of information security and compatibility. The article presents the main directions of development testing the Internet of things: security testing, compatibility, updates, compliance with industry standards, testing phase support.

Keywords: Internet of things, testing, information security, standardization

Активное развитие сегмента интернета вещей направлено на автоматизацию процессов в различных сферах деятельности, в том числе и в повседневной жизни: «умный дом», «умный транспорт», финансовые услуги, сфера здравоохранения. Также интернет вещей находит широкое применение в производственных процессах, например использование систем мониторинга позволяет узнать о проблемных местах системы до выхода ее из строя. В России в 2017 г. по объему enterprise-рынка интернета вещей лидирует транспортная отрасль, далее идут промышленность и финансовая сфера, в сфере сельского хозяйства отмечается самый низкий уровень внедрения IoT-систем. На развитие интернета вещей в России влияют несколько сдерживающих факторов: в основном это устаревшие требования стандартизации и относительно низкий уровень информатизации некоторых отраслей экономики, сложность изменения производственных процессов и внедрения IoT-продуктов в существующую информационную среду.

Появление на рынке новых технологий оказывает существенное влияние на процессы тестирования программного обеспечения. Так, с появлением смартфонов и мобильных приложений возникли новые условия, требующие применения нового подхода к тестированию: специфиче-

ские операционные системы, обмен данными с помощью портов USB, Bluetooth, Wi-Fi, устройства различных производителей, конфигурации комплектующих, touch-интерфейс, проблемы организации памяти, адаптация приложения к портретной и альбомной ориентациям устройства и т.д. В процессе тестирования мобильных устройств и приложений особое внимание уделяется проведению испытаний в условиях, приближенных к реальным сценариям эксплуатации, в том числе стрессовых: со слабым подключением к сети, неточным определением местоположения, в условиях входящих звонков, нахождения в режиме ожидания и др.

Развитие технологий интернета вещей – развитие сети, объединяющей множество объектов: индивидуальные устройства, медицинское оборудование, транспортные средства и др., ставит новые задачи перед специалистами по обеспечению качества. Согласно модели Роба ван Кроненбурга, IoT включает в себя четыре слоя:

1. BAN (body area network) – индивидуальные устройства.

2. LAN (local area network) – устройства, объединенные в «умный дом».

3. WAN (wide area network) – «умное» городское пространство.

4. VWAN (very wide area network) – глобальная инфраструктура, повсеместная компьютеризация [1].

Таким образом, обеспечение непрерывности, устойчивости и безопасности в IoT-сетях выходит на первый план, а значит, процессы тестирования будут активно развиваться с появлением новых типов устройств и расширением сети. В качестве примера рассмотрим фитнес-трекер: на устройстве расположены датчики сердечного ритма и электропроводимости кожи, GPS-модуль, термометр, акселерометр. На тестирование устройства и программного обеспечения влияют следующие процессы:

1. Интеллектуальное устройство принимает полученные от датчиков данные и вычисляет другие параметры, такие как количество пройденных шагов, потраченных калорий, время активной деятельности.

2. Устройство синхронизируется с другим мобильным устройством и, возможно, с облачным сервисом для детального анализа данных.

3. Пользователь имеет возможность просматривать и вводить данные как на самом приборе, так и с помощью синхронизируемых приложений.

4. Пользователь может эксплуатировать устройство в стрессовых условиях, как физически воздействующих на прибор (механическое воздействие, прямой солнечный свет, повышенная влажность), так и связанных с работой программного обеспечения (слабый сигнал, неточное определение местоположения, проблемы синхронизации).

Таким образом, среди основных сложностей тестирования IoT-продуктов можно выделить:

1) IoT характеризуется динамической средой – взаимодействием множества различных устройств с интеллектуальным программным обеспечением;

2) точность и качество аппаратного обеспечения;

3) повышенная нагрузка на сеть;

4) выполнение трудоемких задач в режиме реального времени;

5) обработка больших объемов данных;

6) использование компонентов от сторонних разработчиков;

7) использование многофункциональных устройств;

8) сложность построения тестового окружения, отвечающего требованиям масштабируемости и надежности [2].

В общем случае интернет вещей включает в себя три компонента – аппаратное обеспечение, программное обеспечение и коммуникации. Процессы тестирования каждого компонента в отдельности налажены, однако в контексте IoT на первый план выходят проблемы совместимости систем и обработки больших объемов данных. Для эффективного тестирования IoT-систем необходима продуманная стратегия и формирование четких требований, так как дополнительной сложностью является отсутствие формализованных стандартов в данной области, что осложняет не только процесс тестирования и интеграцию IoT-систем, но и сдерживает рост данного сегмента рынка.

В контексте интернета вещей проблемы обеспечения информационной безопасности становятся особенно важными, так как к 2020 г. количество устройств, подключенных к сети Интернет, возрастет до 50–100 миллиардов [3]. Под потенциальной угрозой оказывается все большее количество устройств, и часто разработчики программного обеспечения пренебрегают тщательной защитой IoT-устройств. С распространением интернета вещей растут риски, связанные с обеспечением информационной безопасности: цена ошибки устройства на атомной электростанции значительно выше цены ошибки «умного дома». В безопасности информационных систем можно выделить три аспекта: конфиденциальность, целостность и доступность [4]. Рассмотрим тестирование безопасности IoT-систем в рамках каждого из этих трех направлений.

Первая угроза конфиденциальности в IoT-системах – незаконное наблюдение и вторжение в частную жизнь. Устройства из интернета вещей могут быть расположены повсеместно: камеры слежения на перекрестках, датчики на автомобилях, приборы в бытовой технике и так далее – все эти устройства могут предоставить злоумышленникам несанкционированный доступ к персональной информации людей. Например, может быть получена информация о времени нахождения или отсутствия жильцов в доме; может производиться трансляция с помощью веб-камеры без ведома ее владельцев и т.д. В 2013 г. Федеральная торговая комиссия подала жалобу на компанию производителя беспроводных камер TRENDnet Inc [5], на тот момент в интернете уже были распространены ссылки для несанкционированного доступа примерно к семи сотням камер. Следующая угроза конфиденциальности – профилирование данных. Сбор данных с многочисленных датчиков и устройств одного пользователя позволяет получать информацию о его образе жизни, предпочтениях и на основе этой информации, например, предоставлять целевую рекламу.

В аспекте доступности устройства интернета вещей являются крайне опасным инструментом для атаки на другие инфраструктуры. В качестве примера можно привести атаку на сеть французского хостинг-провайдера OVH [6], которая была осуществленная посредством ботнета, включающего более ста пятидесяти тысяч IoT-устройств, мощность атаки составляла 1 Тб/с. Наиболее уязвимыми для взлома являются встраиваемые устройства, имеющие доступ к интернету, не содержащие надежных средств защиты от атак ввиду ограничений операционной системы. Пример такого устройства – встроенная в ноутбук веб-камера: после настройки устройства пользователь о нем забывает, редко обновляет программное обеспечение, оставляя уязвимости неустраненными. Часто на таких устройствах остаются неизмененными данные для процедуры аутентификации, выставляемые производителями устройств, что облегчает злоумышленнику получение доступа, например, к роутеру при помощи ввода логина и пароля по умолчанию [7]. Наиболее распространенные логины, использующиеся во вредоносных программах: «root», «admin», «DUP root», «ubnt», «access», «DUP admin», «test», «oracle», «postgres», «pi». Известные часто используемые пароли: «admin», «root», «123456», «12345», «ubnt», «password», «1234», «test», «qwerty», «raspberry» и др.

Для того, чтобы безопасно использовать устройство, конечный пользователя должен знать, что использование паролей, выставленных по умолчанию, недопустимо, а также то, что следует использовать достаточно сложные пароли. Наилучшее решение – использование сложных для подбора методом перебора паролей изначально. Целость данных, хранящихся на IoT-устройствах или передаваемых ими, учитывая сферы использования этих устройств, велика. Например, изменение содержимого сообщения от датчика на электростанции или заводе, может привести к аварии. Изменение целостности программного обеспечения устройств облегчает злоумышленнику получение доступа к огромным сетям IoT-устройств, а получив доступ, он может использовать их для атак на другие объекты инфраструктуры.

В настоящее время нет единого подхода к тестированию IoT-систем, однако для тестирования применяются классические методы с учетом характерных особенностей систем:

1. Тестирование взаимодействия протоколов и устройств различных стандартов и спецификаций.

2. Тестирование конфиденциальности и безопасности, включающее в себя такие аспекты, как защита данных, аутентификация устройств, шифрование данных. Проводится тестирование на проникновение, для выявления уязвимостей, которыми может воспользоваться злоумышленник для атаки. С помощью статических тестов анализируется программный код с целью нахождения возможных уязвимостей; динамические тесты проводятся в процессе нормальной работы приложения и анализируют сетевой трафик, использование памяти и т.д.

3. Тестирование сетевых подключений предполагает оценку количественных и качественных показателей производительности IoT-системы в реальных условиях, включая различную топологию сети, условия среды, мощность сигнала.

4. Нагрузочное тестирование направлено на проверку взаимодействия IoT-устройств с сетевой инфраструктурой – учитываются уязвимости устойчивости к IoT-трафику и поддержания соединения. В контексте IoT, при проведении тестирования, необходимо учитывать, как характеристики сети (пропускную способность, нагрузку, потери пакетов, джиттер), так и технические показатели устройства (использование памяти, потребление ресурсов, температура).

5. Функциональное и нефункциональное тестирование IoT-системы, включая usability-тестирование и возможности взаимодействия с пользователем [8].

6. Тестирование обновлений. IoT – это комбинация различных платформ, протоколов, аппаратного обеспечения и сетевых средств, поэтому требуется тщательное регрессионное тестирование. Общая стратегия должна включать пункты, учитывающие сложности, связанные с обновлениями, а именно: возвратом устройства в исходное состояние в случае неудачи в обновлении, нагрузки на сеть в процессе загрузки обновления, регистрация устройства в центре управления после рестарта, проверки целостности пакета обновлений, удалении старых файлов после обновления и т.д.

Рынок IoT активно развивается и предоставляет множество возможностей для внедрения не только новых продуктов для конечных пользователей, но также инструментов и услуг для разработчиков. Широкое применение информационных технологий в повседневной жизни оказало существенное влияние на процессы разработки: высокая конкуренция вынуждает производителей тщательно следить за качеством выпускаемых продуктов. Дальнейшее развитие как интернета вещей, так и других перспективных направлений, таких как Big Data и Data Fusion [9], системы логистики и телемедицины, облачных технологий, технологий виртуальной реальности, приведет к возникновению новых требований и стандартов, активное развитие рынка способствует возникновению новых продуктов и услуг. Отметим и то, что конечные потребители становятся все более требовательными к качеству продуктов и услуг, а значит, растет необходимость пересмотра существующих процессов технической поддержки. Таким образом, можно выделить следующие направления развития практик тестирования в контексте интернета вещей:

1. Тестирование безопасности, в частности необходимо учитывать специфические уязвимости интернета вещей: слабая аутентификация пользователей, использование стандартных учетных записей; отсутствие технической поддержки со стороны производителей для устранения уязвимостей; сложность обновления программного обеспечения и операционной системы; использование текстовых протоколов и ненужных открытых портов; уязвимость одного устройства становится уязвимостью всей сети; использование незащищённых мобильных технологий, облачной инфраструктуры, небезопасного стороннего программного обеспечения.

2. Тестирование совместимости – на первый план выходят проблемы совместимости в гетерогенных сетях, с использованием устройств разных производителей и поколений, многофункциональных устройств, интеграция облачных сервисов.

3. Новые задачи стандартизации интернета вещей: в настоящее время вопросами стандартизации интернета вещей занимаются международные группы Ассоциации специалистов в области разработки стандартов по радиоэлектронике и электротехнике и группа Международного союза электросвязи [10]. На текущий момент разработаны базовые стандарты, а также ведется работа по адаптации существующих стандартов в сфере инфокоммуникаций в контексте интернета вещей. Однако переход к глобальной инфокоммуникационной среде предполагает возникновение не только новых технологий и продуктов, но также концепций, бизнес-моделей и путей их внедрения в существующую инфраструктуру. Существующие процессы стандартизации выступают сдерживающим фактором на пути развития интернета вещей и нуждаются в реструктуризации, а следовательно, будут меняться подходы тестирования на соответствие отраслевым стандартам.

4. Тестирование обновлений: интернет вещей представляет собой комбинацию различных устройств, программного обеспечения, протоколов, а значит, при обновлении одного компонента может произойти сбой в любом участке сети – главной задачей является оптимизация регрессионного тестирования.

5. Техническая поддержка: одна из важнейших проблем в настоящее время – трудность или даже невозможность обновления некоторых программных продуктов; в связи с потенциальными проблемами совместимости пользователи часто с недоверием относятся к установке обновлений и игнорируют его. Необходимо уделять больше внимания процессам тестирования на этапе поддержки, резервировать время на установление причин неполадок, на тщательное регрессионное тестирование после внесения изменений. Также немаловажен контакт с потребителем. Налаженные процессы коммуникации с пользователями позволят производить поиск и устранение неполадок, а также обновление системы с наименьшими издержками. С развитием интернета вещей техническая поддержка будет осуществлять не только мониторинг функциональных проблем, но и сопровождать процессы необходимых обновлений для исключения уязвимостей системы.

Список литературы

1. Роб ван Краненбург: Что такое IoT? [Электронный ресурс]. – Режим доступа: http://internetofthings.ru/78-

blog/21-rob-van-kranenburg-chto-takoe-iot (дата обращения: 28.08.2017).

2. Testing IoT Applications – A Perspective [Электронный ресурс]. – Режим доступа: https://www.infosys.com/IT-services/validation-solutions/Documents/testing-iot-applications.pdf (дата обращения: 28.08.2017).

3. Perera C. Context Aware Computing for The Internet of Things: A Survey/ C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos // IEEE Communications Surveys & Tutorials. – 2014. – №1. – С. 414-454.

4. CIA Triad [Электронный ресурс]. – Режим доступа: http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/the-security-cia-triad (дата обращения: 28.08.2017).

5. Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy [Электронный ресурс]. – Режим доступа: https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles (дата обращения: 28.08.2017).

6. Более 150 000 IoT-устройств были задействованы в ходе DDoS-атаки мощностью 1 Тб/с [Электронный ресурс]. – Режим доступа: https://xakep.ru/2016/09/30/ovh-ddos (дата обращения: 28.08.2017).

7. IoT devices being increasingly used for DDoS attacks [Электронный ресурс]. – Режим доступа: https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks (дата обращения: 28.08.2017).

8. Долгушев Р.А. Обзор возможных видов и методов тестирования интернета вещей / Р.А. Долгушев, Р.В. Киричек, А.Е. Кучерявый // Информационные технологии и телекоммуникации. – 2016. – № 2. – С. 1–11.

9. Технологии слияния гетерогенной информации из разнородных источников (Data Fusion) / И.В. Ананченко, А.В. Гайков, А.А. Мусаев // Известия Санкт-Петербургского государственного технологического института (технического университета). – 2013. – № 19 (45). – С. 98–105.

10. Сарьян В.К. Прошлое, настоящее и будущее стандартизации Интернета вещей // Труды НИИР. – 2014. – № 1 [Электронный ресурс]. – URL: http://niir.ru/news/zhurnal-trudy-niir/articles/proshloe-nastoyashhee-i-budushhee-standartizacii-interneta-veshhej/ (дата обращения: 27.09.2017).