УДК 004.7.056.53 Вестник УрФО № 3(29) / 2018, с. 38–42

Маслова М. А.

DOI: 10.14529/SECUR180306

ПРИНЦИПЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

В данной статье рассмотрены общие тенденции системы защиты интернет вещей и подробно рассмотрены четыре ее главных принципа: безопасность связи, защита устройств, контроль устройств и контроль взаимодействий в сети.

Ключевые слова: *интернет вещи, защита устройств, контроль устройств, сеть, безопасность связи.*

Maslova M. A.

PRINCIPY BEZOPASNOSTI INTERNETA VESHCHEJ

In this article we studied the general tendencies of the defence systems of the IoT (internet of things and reviewed (examined)) in detail four of its main principles: connection security, protection of the devices device protection), control of the devices and control of the interaction within the network.

Keywords: *Internet of Things, device protection, device monitoring, networking, communication security.*

При любом упоминании об интернет вещей, как правило, имеется в виду вещи для дома, которыми можно управлять через интернет, но если рассмотреть этот вопрос более глубже, то тема Internet of Things намного шире в своем применении. Под интернетом вещей в первую очередь понимается подключенные к вычислительной сети различные устройства: автомобили, телевизоры, камеры наблюдения, роботизированное производство, умное медицинское оборудование, сеть электроснабжения и бесчисленные промышленные системы управления. Все это современно и удобно, но необходимо помнить не только об удобстве в использовании, но и о ее безопасности и конфиденциальности. Безопасность интернета вещей можно построить на: безопасности связи, защите устройств, контроля устройств и контроля взаимодействий в сети. На этом фундаменте можно создать мощную и простую в развертывании систему безопасности, которая способна ослабить негативное воздействие большинства угроз безопасности для интернета вещей, включая целенаправленные атаки, что очень стало актуально в нынешнее время [1, 2].

Тема «Интернет вещей» очень актуальна в современном мире, т.к. «Интернет вещей» плотно вошел в нашу жизнь и миллиардов людей по всему миру. Однако рост количества подключенных устройств ведет к увеличению рисков безопасности: от причинения физического вреда людям до простоев и повреждения оборудования это могут быть даже трубопроводы, доменные печи и установки для выработки электроэнергии. Поскольку ряд таких объектов и систем интернета вещей уже подвергались нападению и был причинен внушительный ущерб, обеспечение их защиты выходит на первый план.

Необходимо рассмотреть, что же будет являться безопасностью связи и с помощью чего он будет реализован. Канал связи должен быть защищен, для этого применяются технологии шифрования и проверки подлинности, для того чтобы устройства знали, могут ли они доверять удаленной системе. Со-

временные криптографические технологии: Elliptic Curve Cryptography, работают в десять раз лучше предшественников в слабомощных чипах IoT 8-bit 8MHz.

Так же не менее важной задачей здесь является управление ключами для проверки подлинности данных и достоверности каналов их получения. Ведущие центры сертификации (CA) уже встроили «сертификаты устройств» в более чем миллиард устройств Internet of Things, предоставив возможность выполнять проверку подлинности широкого спектра устройств, включая сотовые базовые станции, телевизоры и многое другое [1].

Так же было разработано множество стандартов для упрощения развертывания надежной проверки подлинности всех звеньев цепи обмена данными. Существуют стандарты для форматов сертификатов, и надежные центры сертификации поддерживают как стандартные, так и кастомные форматы. С помощью стандартных протоколов, таких как Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) и Online Certificate Status Protocol (OCSP) во многих случаях сертификатами можно легко управлять удаленно.

Благодаря надежному центру сертификации, который предоставляет возможность обрабатывать сертификаты, ключи и учетные данные, фактическую проверку подлинности можно делать с помощью мощных стандартов Transport Layer Security (TLS) и Datagram TLS (DTLS) родственных SSL. Взаимная проверка подлинности, когда обе конечные точки проверяют друг друга, имеет решающее значение для качественной защиты систем IoT. В качестве дополнительного бонуса, однажды выполнив проверку подлинности по TLS или DTLS, две конечные точки могут обмениваться ключами шифрования или получать их для обмена данными, которые невозможно расшифровать подслушивающими устройствами. Для многих приложений IoT требуется абсолютная конфиденциальность данных, это требование легко выполняется использованием сертификатов и протоколов TLS/DTLS [1, 3].

Проверка подлинности информации, устройств и происхождения информации могут иметь решающее значение, так как данные зачастую хранятся, кэшируются и обрабатываются несколькими узлами, а не просто передаются из из одной точки в другую. Поэтому необходимо придерживаться правила, что данные всегда должны быть подписаны в тот момент, когда они были впервые зафиксированы и сохранены, что поможет снизить риски любого вмешательства в информацию. Подписание объектов данных, как только они были зафиксированы, и ретрансляция подписи с данными даже после их дешифрации является все более распространенной и успешной практикой [4].

Если рассматривать защиту устройств, то это в первую очередь обеспечение безопасности и целостности программного кода. Тема безопасности кода выходит за рамки этой статьи, заострим внимание на целостности. Подписание кода требуется для подтверждения правомерности его запуска, также необходима защита во время выполнения кода, чтобы атакующие не перезаписали его во время загрузки. Подписание кода криптографически гарантирует, что он не был взломан после подписания и безопасен для устройства. Это может быть реализовано на уровнях application и firmware и даже на устройствах с монолитным образом прошивки. Все критически важные устройства, будь то датчики, контроллеры или что-то еще, должны быть настроены на запуск только подписанного кода. Устройства должны быть защищены и на последующих этапах, уже после запуска кода, тут поможет защита на основе хоста, которая обеспечивает харденинг, разграничение доступа к системным ресурсам и файлам, контроль подключений, песочницу, защиту от вторжений, защиту на основе поведения и репутации. Также в этот длинный список возможностей хостовой защиты входят блокирование, протоколирование и оповещение для различных операционных систем IoT. В последнее время многие средства хостовой защиты были улучшены и адаптированы для IoT и теперь хорошо проработаны и отлажены, они не требуют доступа к облаку и бережно расходуют вычислительные ресурсы IoT-устройств [5].

Возможности удаленного обновления (Over the air) имеют решающее значение и должны быть встроены в устройства до того, как они покинут завод. OTA-обновления software и firmware очень важны для поддержания высокого уровня защищенности устройства. Тем не менее, обфускация, сегментированное подписание кода и OTA-обновления в конечном счете должны быть плотно объединены между собой для эффективной работы. Сегментированное подписа-

ние кода использует модель доверия на основе сертификатов, которое было описано в предыдущем разделе «Безопасность связи», а использование ECC при подписании кода может обеспечить те же самые преимущества высокого уровня безопасности в сочетании с высокой производительностью и низким энергопотреблением. В этой ситуации предлагаются следующие рекомендации по длине ключа для подписи кода IoT, где безопасность имеет значение:

– минимум 224-bit ECC для сертификатов конечных объектов с предпочтительным 256-bit и 384bit;

– минимум 521-bit ECC для корневых сертификатов, поскольку, как правило, ожидается, что подписанный код будет использоваться годами или даже десятилетиями после подписания, а подписи должны быть достаточно сильными, чтобы оставаться надежными в течение столь длительного времени [6, 7].

Рассмотрим безопасное и эффективное управление IoT. Мы знаем, что реверс-инжиниринг устройств рано или поздно будет проведен, уязвимости будут обнаружены, а для устройств необходимо будет предоставлять обновления OTA. Конечно, механизмы обновления OTA добавляют сложность архитектуре устройства IoT, поэтому многие инженеры стараются избегать их на свой страх и риск [8]. К счастью, хороший механизм OTA может использоваться для многих целей, не только для исправлений программного обеспечения и функциональных обновлений, но также:

1. Обновления конфигурации
2. Управления телеметрией безопасности для аналитики защищенности
3. Управления телеметрией для контроля правильности функционирования устройства
4. Диагностики и восстановления
5. Управления учетными данными доступа к сети (NAC)
6. Управления правами/привилегиями и множества других задач.

Конечно, все вышеперечисленное должно исполняться безопасно и надежно, здесь потребуется наиболее тщательный подход к подписанию кода и организации передачи файлов. Необходимо использовать существующие стандарты управления окружением software и firmware на каждом устройстве, включая конфигурацию, так как многие производители, в частности, Open Mobile Alliance (OMA), поддерживают такие стандарты. Некоторые из решений масштабируются для управления миллиардами устройств [9, 10].

Контроль взаимодействия в сети. Сегодня бесчисленные технологии и системы IoT представляют из себя не более чем «интернета вещей». Однако поскольку все больше систем должны будут связываться друг с другом, все важнее становится знать, «чему доверять». Сертификаты устройств могут содержать информацию о происхождении и типе устройства. Тем не менее на вопросы о том, нужно ли доверять этому устройству, в конечном итоге должны будут отвечать другие службы, например, основанные на репутации, или «Справочник вещей» (Directory of Things) [11]. Такой каталог способен не только отслеживать информацию о безопасности для каждого устройства и систем IoT, но еще отслеживать и управлять привилегиями и полномочиями, которыми устройства и системы наделяют друг друга. Фактически каждый из нас оказывается окруженным все большим количеством устройств IoT, а такие справочники могут помочь разобраться с устройствами с интересующими функциями в интересующих областях. Модель справочника делает возможным быстрый поиск удаленного устройства через каталог и, может быть, будет содействовать ускорению принятия решения об использовании данных с чужого устройства. Даже если пользователь никогда не видел устройство раньше, информация об устройстве, включая его возможности и репутацию, могут быть указаны в таком каталоге. Если предположить, что устройство захочет узнать, может ли оно доверять пользователю, то «Справочника вещей», возможно, будет недостаточно, и в этом случае скорее потребуется «Справочник всего», который будет включать устройства, системы и пользователей. Конечно, у многих людей нет умных чайников или умных холодильников, но это все временно, так как технологии развиваются стремительным ростом [12]. Но все же, у многих из нас уже есть автомобиль, который получает информацию для навигатора через интернет, фитнес-браслеты, Smart TV или проигрыватели Blu-ray, которые транслируют видео через интернет, а еще мы используем банкоматы и вендинговые аппараты. Наше взаимодействие с IoT на самом деле чаще, чем мы замечаем. В этой ситуации возможно захочется иметь свой собственный «Справочник вещей». Защищая устройства и связь,

управляя программными обновлениями и выполняя аналитику безопасности для стратегической защиты от угроз, становится понятно, что все эти меры абсолютно необходимы для защиты IoT. Концепция каталогов «чему доверять» весьма перспективна, но не является сегодня ни основополагающей технологией, ни ключевым ингредиентом в «контроле взаимодействий в сети» для большинства участников. Поэтому будем использовать эту перспективную концепцию каталогов только для того, чтобы дать предварительный обзор стоящих перед многими компаниями вызовов, и приводим пример, как можно справиться со сложными масштабными задачами.

Некоторые компании уже столкнулись с подобного рода проблемами, поскольку они несут ответственность за защиту более чем миллиарда устройств. Для них это «будущее» уже наступило, и они не одиноки [13, 15].

Можно сделать вывод, что сегодня уже очевидно, что реализовать все возможности, которые может предоставить пользователям концепция IoT без решения проблем с безопасностью и конфиденциальностью будет сложно. Указанные выше способы защиты IoT, конечно же, не являются исчерпывающими, над решением проблемы работают множество групп, компаний и энтузиастов. Но прежде всего высокий уровень безопасности устройств «Интернета вещей» должен быть основной задачей их производителей. Надежная защита должна изначально входить как часть функций изделия и стать новым конкурентным преимуществом, как для производителей, так и поставщиков комплексных IoT-решений.

В данной статье была предложена простая и эффективная эталонная архитектура защиты «Интернета вещей», которую легко развернуть и масштабировать с помощью: снижения воздействия вредоносного кода, который гарантирует, что весь код криптографически подписан и авторизирован для устройства, неподписанный код не разрешен для запуска; защиты устройств, которое гарантирует симметричное шифрование и сертификат x.509; защищена связь посредством взаимной проверки подлинности и шифрования. Применяются проверенные временем центры сертификации и модели доверия, которые уже защищают более миллиарда IoT-устройств. Используются новые алгоритмы ECC для обеспечения высокого уровня безопасности в устройствах IoT с ограниченными вычислительными ресурсами; связь между устройством и интернетом, должна быть защищена современными протоколами шифрования (TSL 1.3); ослабления вредоносного воздействия с помощью хостовой защиты и усиления эффективности минимизации рисков от всех остальных угроз с помощью аналитики безопасности; веб – приложения управления устройством, которое должно быть включено device identity registry (реестр удостоверений устройств) police -based authorization of security keys (авторизация ключей безопасности); обнаружения уязвимостей и угроз можно снизить риск их реализации с помощью эффективного, надежного и защищенного динамического управления системой.

Необходимо помнить, что успешное обеспечение безопасности систем начинается с моделирования рисков. Без понимания, как злоумышленники могут скомпрометировать систему, маловероятно надежно защитить любую IT-систему.

Литература

1. Маслова М. А., Кималидинов Э. Л. IOT (Интернет Вещей) : Материалы Студенческой Науч.-Техн. Конф., Г. Севастополь, 2018 / Севастополь. Гос. Ун-Т; Науч. Ред. А. Н. Дегтярев., Севастополь, 2018, с. 8-11.

2. Соколов М.Н., Смолянинова К.А., Якушева Н.А. Проблемы Безопасности Интернет Вещей: Обзор // Вопросы Кибербезопасности: Журнал, 2015, № 5(13), с. 34.

3. Алексей Лукацкий. Криптография в "Интернете Вещей" // www.slideshare.net, сайт, 2016.

4. Сети http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html, http://stfw.ru/page.php?id=19016/.

5. Laurence Cruz. Интернет Вещей и Информационная Безопасность // www.cisco.com.

6. Зеленин Д. В., Логинов Е. Л. Новая Парадигма Управления Экономикой: Переход к "Умным Сетям" Различного Управленческого Назначения // Экономические Науки, 2010, Т. 70, №. 9, с. 156-161.

7. Интернет Протокол IPv6 http://ru.wikipedia.org/wiki/IPv.

8. Tsvetkov V. Ya. Information interaction// European Researcher. Series A, 2013, № 11-1 (62), pp. 2573-2577.

9. Майечак Интернет. Майечак, Беате, М.: Интерэксперт, 2002, с. 345.

10. Эштон К. That "Internet of Things" Thing // RFID Journal: Электронный Журнал, 2009.

11. International Telecommunication Union, Overview of the Internet of Things, Recommendation ITU-T Y.2060, June 2012. Nordrum, Amy (18 Aug 2016).»Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated». IEEE.

12. Грингард, Сэмюэл Интернет Вещей. Будущее уже Здесь / Сэмюэл Грингард, М.: Альпина Паблишер, 2016, 188 с.

13. Грингард, Сэмюэл Интернет вещей: Будущее уже здесь / Сэмюэл Грингард. - М.: Альпина Диджитал, 2015. - 261 с.

14. Зараменских Е. П. Интернет Вещей. Исследования И Область Применения / Е.П. Зараменских, И.Е. Артемьев, М., ИНФРА, М, 2016, 188 с.

15. Дмитрий Подкопаев. Как Работают OTA-Обновления. //xakep.ru./.

Refereces

1. Maslova M. A._ Kimalidinov E. L. The Problems of Information Security .Materials of Student Science-Technical Conference. Sevastopol, 2018, pp. 8-11.

2. Sokolov M.N., Smolyaninova K.A., Yakusheva N.A. Problemy-Bezopasnosti Internet Seshchej Obzor Vopros Kiberbezopasnosti, Zhurnal, 2015, № 5(13), pp.34.

3. Aleksej Lukackij Kriptografiya v Internete Veshchej www.Slideshare.net, Sajt , 2016.

4. Seti http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html, http://stfw.ru/page.php?id=19016/.

5. Laurence Cruz. InternetVeshchej i Information Security, www.cisco.com.

6. Zelenin D.V, Loginov E L. Novaya Paradigma Upravleniya Ehkonomikoj Perekhod k Umnym Setyam Razlichnogo Upravlencheskogo Naznacheniya Ehkonomicheskie Nauki, 2010, T. 70, №. 9, pp. 156-161.

7. Internet Protokol IPv6 http://ru.wikipedia.org/wiki/IPv.

8. Tsvetkov V. Ya. Information interaction// European Researcher. Series A, 2013, № 11-1 (62), pp. 2573-2577.

9. Majechak Internet/ Majechak, Beate,M: Interehkspert, 2002, pp. 345.

10. Ehshton K. That "Internet of Things" Thing // RFID Journal, Ehlektronnyj Zhurnal, 2009.

11. International Telecommunication Union, Overview of the Internet of Things, Recommendation ITU-T Y.2060, June 2012. Nordrum, Amy (18 Aug 2016).»Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated». IEEE.

12. Gringard Sehmyuehl. Internet Veshchej. Budushchee Uzhe Zdes Seh-myuehl Gringard, M., Alpina Pablisher, 2016, pp. 188.

13. Gringard Sehmyuehl. Internet Veshchej. Budushchee Uzhe Zdes Seh-myuehl Gringard¬M.: Alpina Pablisher, 2015, pp. 261.

14. Zaramenskih E.P. Internet Veshchej. Issledovaniya i Oblast Primeneniya/ E.P. Zaramenskih, I.E. Artemev, M., Infra, M, 2016, pp. 188.

15. Dmitrij Podkopaev kak Rabotayut OTA-Obnovleniya, //xakep.ru./.

МАСЛОВА Мария Александровна, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности, ФГАОУ ВО «Севастопольский государственный университет», Россия, 299053, г. Севастополь, ул. Университетская, 33. . E-mail: mashechka¬81@mail.ru

MASLOVA Maria, senior lecturer, Department of Information security, Institute of radio electronics and information security, Sevastopol State University, Russia, 299053, Sevastopol, Universitetskaya str., 33. E-mail: mashechka-81@mail.ru