МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(национальный исследовательский университет)»

Факультет (институт, филиал) Институт № 4 «Радиоэлектроника, инфокоммуникации и информационная безопасность» **Кафедра 410**

Направление подготовки Радиотехника **Группа М4В-301Б-18**

Квалификация (степень) Бакалавр

РЕФЕРАТ

На тему: 4 Безопасность Интернета вещей -IoT

Реферат сдал Данилушкин Е.К. (_____)
(фамилия, имя, отчество)

Реферат принял Терехин А.Г. (_____)
(фамилия, имя, отчество)

Москва 2020

Введение

В быту, когда разговор идет про IoT, как правило, имеют в виду лампочки, обогреватели, холодильники и прочую технику для дома, которой можно управлять через интернет. На самом деле, тема IoT намного шире. Под интернетом вещей мы в первую очередь понимаем подключенные к вычислительной сети автомобили, телевизоры, камеры наблюдения, роботизированное производство, умное медицинское оборудование, сеть электроснабжения и бесчисленные промышленные системы управления (турбины, клапаны, сервоприводы и т. д.).

Чем больше вещей подключены к Сети, тем больше возможностей у хакеров поставить под угрозу вашу безопасность. Это не значит, что вы должны срочно заменить свой рабочий планшет на ручку и бумагу. Это значит, что вы должны серьезно относиться к безопасности технологии интернета вещей.

К счастью, безопасность интернета вещей можно построить на фундаменте из четырех краеугольных камней:

- безопасность связи
- защита устройств,
- контроль устройств
- контроль 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.

Безопасность связи

Усиленная модель доверия для IoT Шифрование, проверка подлинности и управляемость неизменно являются основой устойчивой безопасности. Есть отличные библиотеки с открытым исходным кодом, которые выполняют шифрование даже в устройствах IoT с ограниченными вычислительными ресурсами. Но, к сожалению, большинство компаний по-прежнему подвергаются опасным рискам, допуская ошибки при управлении ключами для IoT.

Транзакции на 4 млрд долларов в день электронной торговли защищены простой и надежной моделью доверия, обслуживающей миллиарды пользователей и более миллиона компаний по всему миру. Эта модель доверия помогает системам безопасно проводить проверку подлинности систем других компаний и взаимодействовать с ними по зашифрованным каналам связи.

Модель доверия сегодня является критичным фактором безопасного взаимодействия в компьютерных средах и основывается на очень кратком списке надежных центров сертификации (CA). Эти же CA устанавливают сертификаты в миллиарды устройств каждый год. Сертификаты устройств позволяют, например, проверять подлинность мобильных телефонов для безопасного подключения к базовым станциям, проверять подлинность интеллектуальных счетчиков для электроэнергетики, а также приставок в индустрии кабельного телевидения.

Надежные CA позволяют легко и безопасно генерировать, выдавать, регистрировать, контролировать и отзывать сертификаты, ключи и учетные данные, которые имеют решающее значение для надежной проверки подлинности. Учитывая реализуемые объемы сертификатов безопасности для IoT, большинство сертификатов устройств продаются большими партиями за весьма скромную сумму денег за единицу (в долларовом выражении речь идет о десятках центов за сертификат). Почему проверка подлинности имеет значение? Опасно принимать данные от непроверенных устройств или непроверенных сервисов. Такие данные могут повредить или скомпрометировать систему, передать контроль над оборудованием злоумышленникам. Использование надежной проверки подлинности для ограничения нежелательных подключений помогает уберечь системы IoT от подобных опасностей и сохранить контроль над вашими устройствами и сервисами. Независимо от того, соединяется ли устройство с каким-то другим устройством или происходит обмен данными с удаленным сервисом,

например, облачным, связь всегда должна быть защищена. Все взаимодействия требуют надежной проверки подлинности и взаимного доверия. Исходя из этих соображений, экономия на сертификатах устройств представляется спорной. К счастью, множество стандартов было разработано для упрощения нам с вами развертывания надежной проверки подлинности всех звеньев цепи обмена данными

Благодаря надежному центру сертификации, который предоставляет возможность обрабатывать сертификаты, ключи и учетные данные, фактическую проверку подлинности можно делать с помощью мощных стандартов TransportLayerSecurity (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. Однако когда конфиденциальность не является обязательным требованием, подлинность передаваемых данных может проверяться любой стороной, если они были подписаны во время их появления на датчике — такой подход не отягощает канал шифрованием, что предпочтительно в архитектурах multi-hop.

Защита устройств

Защита программного кода IoT При включении каждое устройство загружается и запускает определенный исполняемый код. Нам крайне важно быть уверенными в том, что устройства будут делать только то, на что мы их запрограммировали, а посторонние не смогут перепрограммировать на злонамеренное поведение. То есть первым шагом в защите устройств является защита кода, чтобы гарантированно загружался и запускался только нужный нам код. К счастью, многие производители уже встроили возможности безопасной загрузки в свои чипы. Похожим образом дела обстоят и с высокоуровневым кодом — различные проверенные временем клиентские библиотеки с открытым исходным кодом, вроде OpenSSL, могут использоваться для проверки подписи и разрешения кода только из авторизованного источника. Вследствие этого все большее распространение

получают подписанные прошивки, загрузочные образы и более высокоуровневый встроенный код, в том числе подписанные базовые программные компоненты, куда входят любые операционные системы.

Все чаще встречаются не просто подписанные прикладные программы, а вообще весь код на устройстве. Такой подход гарантирует, что все критичные компоненты систем IoT: датчики, механизмы, контроллеры и реле сконфигурированы правильно — на запуск только подписанного кода и никогда не запустят неподписанный код. Хорошей манерой было бы придерживаться принципа «никогда не доверять неподписанному коду». Логичным продолжением было бы «никогда не доверять неподписанным данным и, тем более, неподписанным конфигурационным данным».

Использование современных средств проверки подписи и распространение аппаратной реализации безопасной загрузки, ставят серьезную задачу перед многими компаниями — управление ключами и контроль доступа к ключам для подписи кода и защиты встроенного программного обеспечения. К счастью, некоторые центры сертификации предлагают облачные сервисы, которые делают проще, безопаснее и надежнее администрирование программ для подписывания кода и гарантируют строгий контроль, кто может подписывать код, отзывать подписи, и как ключи для подписания и отзыва защищены. Возникают ситуации, когда программное обеспечение нужно обновить, например, в целях безопасности, но при этом необходимо учесть влияние обновлений на заряд батареи.

Операции перезаписи данных увеличивают потребление энергии и сокращают период автономной работы устройства. Появляется необходимость подписать и обновить отдельные блоки или фрагменты таких обновлений, а не монолитные образы целиком или бинарные файлы. Тогда программное обеспечение, подписанное на уровне блоков или фрагментов, можно обновлять с гораздо более тонкой детализацией, не жертвуя безопасностью или зарядом батареи. Для этого не нужна обязательно аппаратная поддержка, такую гибкость можно достичь от предзагрузочной среды, которая может работать на множестве embedded-устройств. Если время автономной работы настолько важно, почему бы просто не сконфигурировать устройство с неизменяемой прошивкой, которую никто не может изменить или обновить? К сожалению, мы вынуждены предположить, что устройства в полевых условиях подвержены реверс-инжинирингу для вредоносных целей. После его проведения обнаруживаются и

эксплуатируются уязвимости, которые необходимо патчить как можно скорее. Обфускация и шифрование кода могут существенно замедлить процесс реверс-инжиниринга и отбить охоту продолжать атаковать у большинства злоумышленников. Но враждебные спецслужбы или межнациональные деструктивные организации все-таки способны это сделать даже для программ, защищенных с помощью обфускации и шифрования, прежде всего потому, код должен быть дешифрован для запуска. Такие организации найдут и воспользуются уязвимостями, которые не были своевременно пропатчены. В связи с этим возможности удаленного обновления (OTA) 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.

Контроль устройств

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

- Обновления конфигурации

- Управления телеметрией безопасности для аналитики защищенности

- Управления телеметрией для контроля правильности функционирования устройства

- Диагностики и восстановления

- Управления учетными данными доступа к сети (NAC)

- Управления правами/привилегиями

Конечно, все вышеперечисленное должно исполняться безопасно и надежно, здесь потребуется наиболее тщательный подход к подписанию кода и организации передачи файлов. Здорово, что существуют стандарты управления окружением software и firmware на каждом устройстве, включая

конфигурацию, и многие производители, в частности, OpenMobileAlliance (OMA), поддерживают такие стандарты. Некоторые из решений масштабируются для управления миллиардами устройств. Естественно, некоторые технологии безопасности предусматривают обновления OTA для контента безопасности, например, черные и белые списки, эвристика, сигнатуры IPS и данные о репутации. Также существуют технологии безопасности, основанные на политиках, которым обновления нужны только при переустановке на устройстве программного обеспечения для каких-то целей, например, для добавления функциональных возможностей.

Тем не менее оба типа технологий могут генерировать телеметрию безопасности, которая имеет большое значение при столкновении с целенаправленными атаками. Поэтому телеметрические данные безопасности всегда должны собираться от этих host-based (device-based) технологий для централизованного анализа. Разумеется, компоненты безопасности не единственные в устройстве IoT, которыми необходимо управлять безопасно и надежно. Большинство устройств генерируют телеметрию или данные с датчиков, которые нужно также безопасно и надежно собирать и передавать в места хранения и анализа. Многие устройства уже содержат в себе функции контроля, которыми нужно аккуратно управлять через конфигурационные параметры, а те в свою очередь безопасно и надежно хранить и обновлять. К счастью, инфраструктуры управления устройствами, которые используют общепринятые безопасные протоколы, могут применяться и для защищенного управления основными функциями устройства, контентом безопасности и телеметрией устройства. Фактически подобные модели адаптируются для OTA-управления автомобилями и используются для безопасного и надежного управления торговыми автоматами. Некоторые из инфраструктур управления комбинируют агентские и безагентские протоколы управления IoT, тогда как устройства выпускаются с поддержкой стандартизированного управления для упрощения функций контроля. А отдельные инфраструктуры управления могут дополнительно сочетать все эти методы управления с понимаем информации, полученной от сетевыхснифферов.

В сложившейся ситуации системы IoT должны изначально иметь встроенные возможности обновления OTA. Отсутствие этих возможностей оставит устройства подверженными угрозам и уязвимостям в течение всего срока их службы. Разумеется, обновление OTA может применяться еще для управления конфигурациями устройств, контентом безопасности, учетными

данными, а также для расширения функциональных возможностей устройств, сбора телеметрии и данных программного окружения, для доставки патчей безопасности и многого другого. Однако с дополнительной функциональностью или без нее базовые возможности обновления и управления защищенностью должны быть предусмотрены еще на этапе проектирования устройств IoT.

Контроль взаимодействий в сети

Чему доверять Давайте заглянем немного вперед, в будущее. Сегодня бесчисленные технологии и системы IoTпредставляют из себя не более чем «интернет 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» (DirectoryofThings). 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 вы никогда не видели 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» (DirectoryofEverything), который будет включать устройства, системы и пользователей. Конечно, у многих людей нет умных чайников или умных холодильников… пока нет... Но у многих из нас уже есть автомобиль, который получает информацию для навигатора через интернет, Smart TV или проигрыватели Blu-ray, которые транслируют видео через интернет, фитнес-браслеты, а еще мы используем банкоматы и вендинговые аппараты. Наше

взаимодействие с IoT на самом деле чаще, чем мы замечаем. В этой ситуации мы, возможно, захотим иметь наш собственный «Справочник вещей». Защищая устройства и связь, управляя программными обновлениями и выполняя аналитику безопасности для стратегической защиты от угроз, мы понимаем, 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. Мы включаем 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.

Выводы

IoT становится все более распространенным явлением и все чаще появляется в системах, от которых зависит жизнь людей, например, автомобилях, самолетах и промышленном оборудовании, поэтому безопасность должна правильным образом встраиваться в эти системы, чтобы они были «безопасны по архитектуре» с защитой, встроенной изначально. В большинстве случаев ставки слишком высоки для ошибок.

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