Лекция 10 . Решения для обеспечения конфиденциальности, безопасности и устранения уязвимостей IoT

Цель лекции – ознакомить магистрантов с основными процессами и действиями по обеспечению безопасности и конфиденциальности в сетях, системах и устройстах IoT.

Введение

Международные организации прилагают ряд усилий для того, чтобы гарантировать, что проектирование IoT будет гарантировать доверие, безопасность данных и конфиденциальность.

- ***Доверие.*** Например, рассмотрим сообщения и видеоклипы операций от банкоматов до сервера. Пользователь доверяет банку, что конфиденциальная информация не будет раскрыта, что может навредить пользователю. Когда вещи общаются аналогичным образом, то существует доверие к безопасному использованию данных. Доверие в контексте IoT означает надежность, точность, качество данных из нескольких источников для предполагаемых приложений и услуг. Организация Open Trust Alliance создала IoT Trustworthy Group (ITWG) для признания приоритета (обязательного в дизайне для безопасности и конфиденциальности) с самого начала разработки продукта и решения проблемы в целом. Организация «I am the Cavalry» предписала клятву для подключенных медицинских устройств по принципу, аналогичному клятве Гиппократа, которая представляет собой подтверждение врачами предоставления медицинской помощи в наилучших интересах пациентов. Медицинские устройства должны иметь обязательства по возможностям, которые сохраняют безопасность пациентов, а также доверие к самому процессу предоставления медицинской помощи.
- ***Безопасность.*** Например, рассмотрим сообщения банкомата. Они должны безопасно передаваться по Интернету. Нарушения безопасности могут привести к серьезным последствиям. Безопасность умного города также важна. Город развертывает умное здравоохранение, общественную безопасность, транспорт и развертывает приложения и сервисы IoT и умного дома. Организация взяла на себя инициативу по решению проблем кибербезопасности в умных городах.
- ***Конфиденциальность.*** Видеоклипы передаются по Интернету в приложении безопасности умного дома. Если клипы попадут к не связанным с ними лицам, это может привести к серьезному нарушению безопасности дома.

Industrial Internet Consortium (IIC) был сформирован Intel, IBM, CISCO, GE и AT&T (2014) для координации усилий и инициатив по подключению и интеграции объектов. Другая организация, AllSeen Alliance, созданная Linux Foundation, является совместным проектом межотраслевого консорциума, который призван обеспечить взаимодействие миллиардов устройств и приложений/сервисов IoT.

Ниже приведены термины, значения которых необходимо понимать перед изучением тем, рассматриваемых в этой лекции.

Сообщение – это строка, представляющая данные, клиентский запрос или ответ сервера, которые обмениваются данными между объектами отправителя и получателя.

Хэш относится к коллекции или связке, которая дает необратимый результат после многих операций с данными, и операции являются только односторонними. Например, когда урожай пшеницы созрел и срезан, процесс хеширования отделяет зерна, которые используются для потребления, а полученные отходы выбрасываются. Когда данные, такие как идентификатор пользователя и пароль, требуют секретной связи для целей аутентификации, то они передаются после набора стандартных операций с использованием алгоритма, называемого алгоритмом безопасного хеширования. Алгоритм генерирует фиксированный размер, скажем, 128 или 256 бит, используя секретный ключ. Передается только значение хеширования. Получатель-конец извлекает значение хеширования и

сравнивает его с сохраненным значением хеширования. Если оба равны, то сообщение отправителя аутентифицируется.

Дайджест – это процесс, который дает необратимый результат, включающий множество операций. Для дайджеста также используется стандартный алгоритм MD5 (Message Digest 5), аналогичный значению хэша. Получатель сохраняет значение дайджеста, которое, как ожидается, будет получено после операций MD5, и сравнивает его с полученным значением. Если оба значения равны, то сообщение отправителя аутентифицируется.

Шифрование – это процесс генерации новых данных с использованием секретного ключа, известного только получателю. Перед отправкой зашифрованных данных отправитель и получатель идентифицируют друг друга и знают ключ, который они будут использовать. Шифрование использует 128-, 192- или 256-битный ключ для шифрования данных.

Расшифровка – это процесс извлечения данных из зашифрованных данных.

Случай использования означает список шагов событий или действий, которые определяют взаимодействия между двумя концами, в которых один играет роль, а другой является системой. Шаги выполняют задачу, цель или миссию. Один конец называется актером в унифицированном языке моделирования (UML), в то время как другой конец является системой. Случай использования – это термин из области разработки программного обеспечения. Например, API играет роль получения входных данных (событий) и генерации выходных данных, которые взаимодействуют с системой, такой как веб-сервер или веб-API, служба, веб-приложение, используя функцию обратного вызова () в соответствии с выходными данными. Случаи использования определяют требуемое поведение разрабатываемого программного обеспечения. Случаи использования описывают детали использования программного обеспечения и его нормальное поведение. Случай неправильного использования можно понимать как обратный смысл варианта использования.

Случай неправильного использования определяет поведение, которое не требуется от разрабатываемого программного обеспечения. Случай неправильного использования определяет поведение, которое не должно происходить. Это, в свою очередь, также определяет угрозы. Случай неправильного использования предоставляет информацию и помогает в определении требований новых вариантов использования для предотвращения атак и выяснения того, что не должно происходить.

Слой означает этап в наборе действий, на котором действие выполняется в соответствии с определенным протоколом или методом, а затем результат переходит на следующий уровень, пока набор действий не будет завершен. Проектирование с использованием модели слоев позволяет представить набор систематических действий, которые выполняются последовательно для выполнения задачи.

Подслой – это слой, состоящий из различных подслоев в модели, обеспечивающий набор действий, последовательно происходящих на данном слое.

Брандмауэр – это программный интерфейс, который соединяет сети с различными уровнями доверия, невосприимчив к проникновению и обеспечивает защиту периметра. Он функционирует как контрольная точка для контроля и мониторинга. Он проводит аудит и обеспечивает контролируемый доступ. Он пропускает только авторизованный трафик и накладывает ограничения на сетевые службы. Он может подавать сигналы тревоги при ненормальном поведении.

Уязвимости, требования безопасности и анализ угроз

Конфиденциальность

Конфиденциальность сообщения означает, что сообщение не должно попасть в руки посторонних лиц. Когда данные или сообщения передаются от вещей (платформ

устройств), они предназначены только для приложений или служб и только для целевых целей.

Конфиденциальность также означает отсутствие помех или помех со стороны других. Рассмотрим пример сообщений от встроенных устройств в автомобиле, использующих Интернет, в автосервис. Конфиденциальность означает, что сообщения достигают только центра и используются только службами центра. Другая автомобильная компания, в чьи руки попадают данные, может столкнуться с серьезными деловыми последствиями.

IoT обязательно нуждается в политике конфиденциальности. Политика конфиденциальности должна определять, «какой объем данных устройств IoT и какие данные требуют абсолютной конфиденциальности, а какие – ограниченной конфиденциальности». Руководству компании нужна поддержка для доступа к данным, которые могут быть конфиденциальными для отдельных лиц. Руководству также необходимо уважать индивидуальные потребности клиентов в конфиденциальности и понимать, что конфиденциальность – это законная человеческая потребность. Поставщики политики конфиденциальности должны серьезно относиться к конфиденциальности. Они должны уважать своих клиентов настолько, чтобы понимать, что конфиденциальность – это законная человеческая потребность.

Национальный институт стандартов и технологий (NIST), США разрабатывает стандарты конфиденциальности. Система может быть безопасной, но может непреднамеренно нарушать конфиденциальность личности. Служба отслеживания может отслеживать транспортное средство, не желая, чтобы его/ее перемещения отслеживались. Органам безопасности и агентствам нужна поддержка для доступа к данным, которые могут быть конфиденциальными для отдельных лиц. Органы власти также должны уважать потребности отдельных лиц.

Уязвимости IoT

Уязвимость означает слабость без полной защиты, слабость защитить себя или легко поддается влиянию окружающих нежелательных вещей от себя. Статья о безопасности IoT описывает, что существует множество уязвимостей из-за участия ряда слоев, аппаратных подслоев и программного обеспечения в приложениях и сервисах. Природа IoT также различается. Например, датчики, машины, автомобили, носимые устройства и так далее. Каждый сталкивается с различными видами уязвимостей и имеет сложные проблемы безопасности и конфиденциальности.

Сеть IoT может быть уязвима для подслушивания. Подслушиватель создает проблемы безопасности. Подслушиватель, скажем E, прослушивает сообщения и команды в сети во время связи и получает конфиденциальные сообщения. Сервер в E отправляет поддельные команды, которые сервер S для данных устройств предполагает, что они исходят от устройств или приложений. S выдает ответы для операций устройства в ответ на запросы от E. E прослушивает эти ответы. Поддельное устройство в E может использоваться для отправки данных устройства, таких как данные датчиков, запросы и команды от E для нарушения работы системы управления. Использование шифрования с секретным ключом может защитить сообщения, отправляемые на устройство, сервер, приложение или службу и обратно.

Ключ – это строка, сгенерированная программным обеспечением устройства, которую можно взломать, перебрав большое количество комбинаций. Проблемы с уникальным идентификатором устройства и аутентификацией существуют в незначительном сценарии взаимодействия с пользователем.

Функции безопасности должны быть включены в стандартный формат, рекомендуемый для IoT. Например, стандарт для архитектуры электронных продуктов принадлежит развивающейся группе EPCglobal. Группа отвечает за создание и поддержку продуктов политики конфиденциальности.

Open Web Application Security Project (OWASP) взял на себя решение связанных с безопасностью вопросов IoT с целью оказания помощи разработчикам, производителям и потребителям. OWASP имеет открытый исходный код и политику лицензирования свободного использования. Проект представляет собой инициативу по разработке программного обеспечения на основе модели сообщества. Модель сообщества представляет собой коллективные усилия и инициативу университетов, организаций и учреждений в проекте с открытым исходным кодом. OWASP реализовал ряд подпроектов, связанных с безопасностью, например, по определению «Основных уязвимостей», «Поверхностных зон атак» и «Руководств по тестированию». OWASP определил десять основных уязвимостей в приложениях/сервисах IoT следующим образом:

- Небезопасный веб-интерфейс;
- Недостаточная аутентификация или авторизация;
- Небезопасные сетевые сервисы;
- Отсутствие транспортного шифрования/проверки целостности;
- Проблемы конфиденциальности;
- Небезопасный облачный интерфейс;
- Небезопасный мобильный интерфейс;
- Недостаточная настраиваемость безопасности;
- Небезопасное программное обеспечение или прошивка;
- Плохая физическая безопасность.

Требования безопасности

Эталонная архитектура IoT означает руководство для одного или нескольких конкретных архитекторов. Эталонная архитектура IoT представляет собой набор из трех архитектурных представлений – функционального, информационного и развертывания и эксплуатации. Безопасность – одна из функциональных групп функционального представления. Функциональная группа для безопасности состоит из функций безопасности между приложением и устройством.

Функциональная группа безопасности функциональных групп содержит пять наборов функций, необходимых для обеспечения безопасности и конфиденциальности. Большое количество устройств, приложений и сервисов взаимодействуют в IoT. Пять функциональных компонентов безопасности определены в эталонной архитектуре IoT.

Ниже приведены пять функциональных компонентов:

1. Управление идентификацией;
2. Аутентификации;
3. Авторизация;
4. Обмен ключами и управление ими;
5. Доверие и репутация.

Случаи использования и неправильного использования

Диаграммы вариантов использования нотации UML требуются для функциональных компонентов функциональных групп безопасности. Анализ вариантов использования позволяет проводить анализ требований. Варианты использования являются ключевыми функциями многих моделей и фреймворков для разработки процессов. Oracle Unified Method (OUM) и IBM Rational Unified Process (RUP) являются примерами фреймворков для моделей процессов разработки программного обеспечения и анализа требований.

Модели безопасности, профили и протоколы для IoT

Рекомендованный проект IETF рекомендует следующие модели безопасности для пяти профилей безопасности. Таблица 10.1 содержит подробную информацию.

Таблица 10.1. Модель безопасности для различных профилей безопасности

Профиль безопасности	Использование	Описание	Модель безопасности
SecProf_0	6НизкийPAN/CoAP	Нет безопасности	Не устойчив к закалке (нет положений, предотвращающих закалку)
SecProf_1	Домашнее использование	Операции между вещами без центрального устройства	1. Не устойчив к закалке 2. Распределение ключей между слоями
SecProf_2	Управляемое домашнее использование	Возможно взаимодействие между вещами и локальным устройством и центральным устройством	1. Не устойчив к закалке 2. Распределение ключей между слоями
SecProf_4	Расширенное промышленное использование	Специальные операции между включенными вещами и полагаются на центральное устройство или набор устройств управления для обеспечения безопасности. Распределенная и централизованная (локальная и/или внутренняя) архитектура безопасности	1. (Нет) устойчив к закалке 2. Совместное использование ключей между слоями/ключами и разделением процессов в песочнице

Некоторые приложения нацелены на мощные устройства, предназначенные для более уязвимых приложений, и нуждаются в параметрах безопасности, таких как материалы ключей, а сертификаты должны быть защищены в вещах. Например, с помощью оборудования, устойчивого к взлому.

Совместное использование ключей имеет следующие особенности:

● Требуется для всего сетевого стека устройств.

● Обеспечивает аутентичность и конфиденциальность на каждом сетевом уровне, минимизирует количество ключевых установлений/согласований, требует меньших

накладных расходов для ограниченных вещей, например, приложений с ограничениями ресурсов (например, датчик температуры и влажности)

Разделение ключей на разных сетевых уровнях:

● Необходимо в сложных приложениях

● Также возможно использование разделения процессов и «песочницы» для изоляции одного приложения от другого.

В инфраструктуре безопасной среды CISCO IoT предусмотрено четыре FC:

1. Аутентификация
2. Разрешение
3. Политика, применяемая в сети
4. Безопасная аналитика: видимость и контроль

Протоколы безопасности

Open Trust Protocol (OTrP) – это протокол, который управляет конфигурацией безопасности в доверенной среде выполнения (TEE) и используется для установки, обновления и удаления приложений и служб.

● Протокол DTLS (Datagram Transport Layer Security) предназначен для сохранения конфиденциальности во время передачи датаграммы при использовании клиентов и серверов CoAP или L2M2M. Он обеспечивает защиту от подслушивания, взлома или подделки сообщений. Основой протокола DTLS является протокол Transport Layer Security (TLS) для передачи сегментов данных с использованием транспортного уровня.

● Протокол X.509 относится к выпуску цифрового сертификата с доверием на основе уполномоченного центра сертификации TTP. Он развертывает инфраструктуру открытых ключей (PKI). PKI управляет цифровыми сертификатами и шифрованием с открытым ключом. Это подблок протокола TLS, используемый для защиты связи с вебом.

Контрольные вопросы:

1. Какие требования должна выполняться в системах-IoT?
2. Что такое дайджест?
3. Что означает уязвимость?
4. Какие протоколы безопасности существуют?
5. Назование типы функционаьльных компонентов.