IoT. **Эталонная архитектура защиты**

2017

Интернет вещей - IoT

Под Интернетом вещей мы понимаем в первую очередь 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.)

Интернет Вещей (IoT) уже плотно вошел в нашу жизнь и миллиардов людей по всему миру. Умные подключаемые устройства открыли новые возможности и сократили затраты на миллиарды в долларовом выражении. Однако, рост количества подключенных устройств ведет к увеличению рисков безопасности столь богатого и уязвимого ландшафта: от причинения физического вреда для людей до простоев и повреждения оборудования, которым может оказаться и трубопроводы, и доменные печи и установки для выработки электроэнергии. Поскольку ряд таких объектов и систем IoT уже подвергались нападению, и был причинен внушительный ущерб, обеспечение защиты выходит на первый план для тех, кто создает или эксплуатирует системы и устройства IoT, в особенности для промышленного Интернета.

Безопасность IoT можно построить на фундаменте из четырех краеугольных камней:

- **безопасность связи**;
- **защита устройств**;
- **контроль устройств;**
- **контроль взаимодействий в сети**.

Как можно защитить IoT? Системы IoT бывают очень сложными, им требуются комплексные меры защиты, покрывающие уровни облаков и подключений, также необходима поддержка устройств IoT с ограниченными вычислительными ресурсами, которых недостаточно для поддержки традиционных решений безопасности.

Простого универсального решения не существует и для обеспечения безопасности не достаточно запереть двери, оставив окна открытыми. Безопасность должна быть всесторонней, иначе атакующие просто воспользуются самым слабым звеном. Конечно, традиционные IT-системы как правило передают и обрабатывают данные из систем IoT, но сами системы IoT обладают своими уникальными потребностями в защите.

Безопасность связи

Канал связи должен быть защищен, для этого применяются технологии шифрования и проверки подлинности, чтобы устройства знали, могут ли они доверять удаленной системе

Шифрование, проверка подлинности и управляемость неизменно являются основой устойчивой безопасности

Канал связи должен быть защищен, для этого применяются технологии шифрования и проверки подлинности, чтобы устройства знали, могут ли они доверять удаленной системе.

Здорово, что новые криптографические технологии, такие как ECC (Elliptic Curve Cryptography), работают в десять раз лучше предшественников в слабомощных чипах IoT 8-bit 8MHz.

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 IoT, предоставив возможность выполнять проверку подлинности широкого спектра устройств, включая сотовые базовые станции, телевизоры и многое другое.

Защита устройств

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. Здесь 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 адаптированы для IoT и теперь хорошо проработаны и отлажены, не требуют доступа к облаку и бережно расходуют вычислительные ресурсы IoT-устройств.

Защита устройств – это в первую очередь обеспечение безопасности и целостности программного кода.

- Защита программного кода IoT
- Эффективная хостовая защита для IoT

Контроль устройств

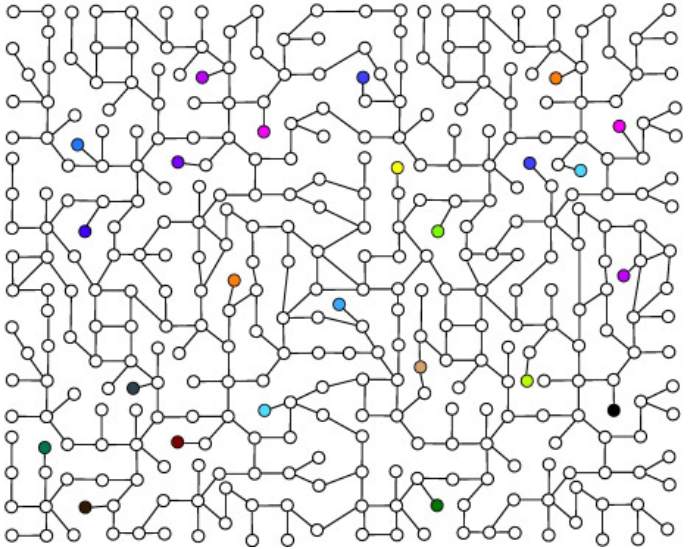
Механизм OTA может использоваться для многих целей, не только для исправлений программного обеспечения и функциональных обновлений, но также:

- 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 и множества других задач

Печально, но уязвимости в устройствах IoT все равно будут, их нужно будет патчить и это может происходить в течение длительного времени после передачи оборудования потребителю. Даже код с применением обфускации в критичных системах в конце концов реконструируется, и злоумышленники находят в нем уязвимости. Никто не хочет, а зачастую и не может отправлять своих сотрудников для очного визита к каждому устройству IoT для обновления прошивки, особенно, если речь идет, например, о парке грузовиков или о сети датчиков контроля, распределенных на сотни километров. По этой причине “управляемость по-воздуху” (over-the air, OTA), должна быть встроена в устройства до того, как они попадут к покупателям.

Контроль взаимодействий в сети

Некоторые угрозы смогут преодолеть любые предпринятые меры, независимо от того, насколько хорошо все защищено. Системы для аналитики безопасности помогут вам лучше понять вашу сеть, заметить аномалии.



Мониторинг и аналитика могут быть развернуты в качестве временного решения в средах, где развертывание других средств защиты займет несколько лет или в случаях, когда модификация систем IoT не возможна.

Принцип «обнаружение и реагирование» может дополнять технологии усиленной защиты

Эволюция парадигмы

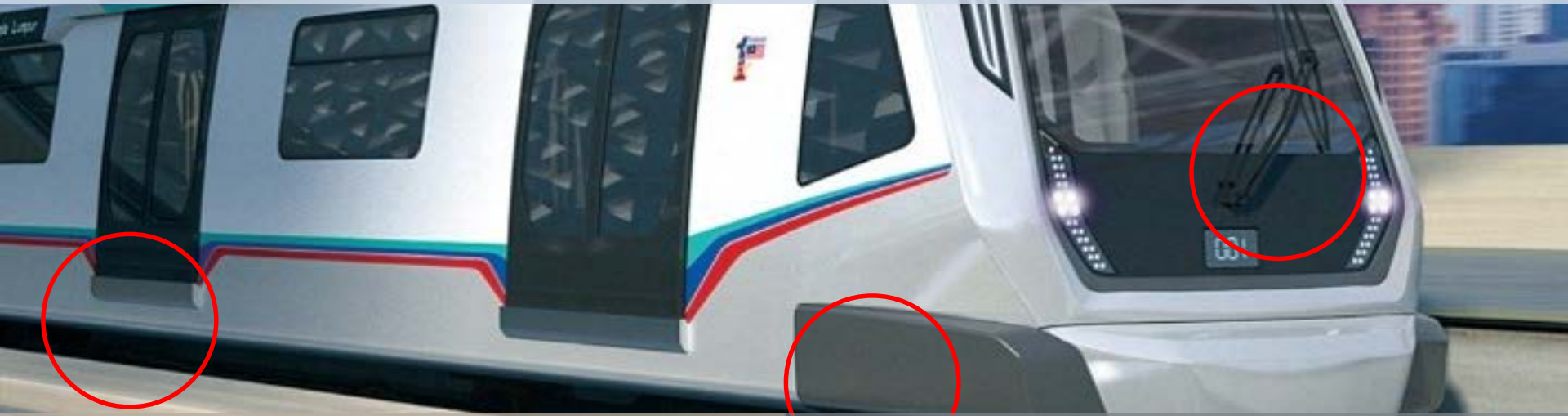
Защитные функции должны быть изначально встроены в устройства IoT, чтобы они были безопасными по своей архитектуре. Для большей части индустрии ИБ такая «безопасность внутри», то есть встроенная при изготовлении устройства на заводе – это новый способ обеспечения защиты.

webcontrol

Большинство устройств IoT представляют из себя «закрытые системы». Покупатели не смогут добавлять программное обеспечение безопасности после того, как устройства покинут завод. Такое вмешательство аннулирует гарантию, а зачастую попросту не представляется возможным. По этой причине, защитные функции должны быть изначально встроены в устройства IoT, чтобы они были безопасными по своей архитектуре. Для большей части индустрии ИБ такая «безопасность внутри», то есть встроенная при изготовлении устройства на заводе – это новый способ обеспечения защиты, это касается и к классических технологий безопасности, таких как шифрование, проверка подлинности, проверка целостности, предотвращение вторжений и возможности безопасного обновления. Учитывая тесную связь аппаратного и программного обеспечения в модели IoT, иногда проще, чтобы программы для защиты использовали расширение функций аппаратной части и создавали «внешние» уровни безопасности. Здорово, что многие производители чипов уже встроили функции безопасности в оборудование. Но аппаратный уровень - это всего лишь первый слой, необходимый для комплексной защиты связи и устройств. Комплексная защита требует интеграции функций управления ключами, защиты на основе хоста, инфраструктуры OTA и аналитики безопасности, о чем мы упоминали прежде. Отсутствие даже одного из краеугольных камней в фундаменте безопасности, оставит широкий простор действиям злоумышленников.

Пример – поезд

В поездах контроллеры электродвигателей зачастую контролируют не только ускорение, они еще контролируют и рекуперативное торможение. Если в качестве страховки от неконтролируемого ускорения можно подключить механические тормоза, то от экстренного торможения такой механической защиты нет. Могут пострадать люди, не говоря уже о поезде и транспортной инфраструктуре, если злоумышленники смогут перепрограммировать контроллер двигателя на внезапное торможение.



Поэтому очень важно, чтобы весь код, выполняемый в контроллерах, тормозах, переключателях и остальных элементах, был надлежащим образом подписан. Необходимо, чтобы все компоненты были правильно настроены и никогда не запускали неподписанный код. Аналогично, если нет проверки подлинности при взаимодействии компонентов поезда, а также при взаимодействии поезда с другой инфраструктурой, последствия могут быть серьезными.

Нетрудно представить себе что произойдет, если управляющие сигналы в поезде для ускорения и торможения будут сфальсифицированы, и что будет, если подделают разрешающие сигналы, когда впереди опасность. Кроме того, без хостовой защиты, сами контроллеры легче взломать, злоумышленники могут достичь своей цели без лишних усилий и без преодоления механизмов проверки подлинности и подписи кода.

Простая и эффективная эталонная архитектура защиты IoT, которую легко развернуть и масштабировать

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

• Архитектура снижения воздействия вредоносного кода гарантирует, что весь код криптографически подписан и авторизирован для устройства, неподписанный код не разрешен для запуска.

• 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.

• Эта архитектура дополнительно ослабляет вредоносное воздействие с помощью хостовой защиты и усиливает эффективность минимизацией рисков от всех остальных угроз с помощью аналитики безопасности.

• При обнаружении уязвимостей и угроз, риск их реализации можно снизить с помощью эффективного, надежного и защищенного динамического управления системой.

webcontrol

http://web-control.ru/

info@web-control.ru
+7 (495) 925-77-94