Карен Кроули, Роберт Андрес

Безопасность в мире IoT

В статье рассмотрены вопросы обеспечения безопасности и противодействия киберугрозам в сетях IoT в свете бурного и бесконтрольного развития Интернета вещей. Приводятся основные требования к организации безопасных систем IoT, а также продемонстрирован комплексный подход к решению проблемы на примере концепции компании Eurotech.

Автомобили без водителей, фитнес-трекеры, умные промышленность и сельское хозяйство, умная одежда, умные приборы и сенсоры для контроля всего на свете, медицинское оборудование, помогающее людям, где бы они ни находились, – всё это Интернет вещей.

Интернет вещей изменяет принципы ведения бизнеса, общественных связей и отношений, сам уклад нашей жизни (рис. 1). По мере лавинообразного роста подключаемых к Интернету устройств и совершенствования технологий мы приближаемся к практическим результатам, предсказываемым ведущими экспертами:

- Gartener, Inc. прогнозирует, что к 2020 году в единой сети будет уже 20,8 млрд устройств;
- По мнению IDC, рынок Интернета вещей к тому же 2020 году вырастет до $1,7 трлн;
- Business Insider считает, что порядка $6 трлн будет потрачено во всём мире только в ближайшие пять лет;
- А вот European Commission полагает, что только европейский рынок IoT в 2020 году составит около 1 трлн евро.

Одной из проблем, с которыми мы сталкиваемся в процессе внедрения технологий IoT, является ограничение скоростей связи устройств между собой, а также их слабая защищённость и вообще отсутствие единых стандартов сетевой безопасности. IoT сегодня – поистине лакомый кусочек для хакеров и террористов всех мастей. И если ситуация не изменится, то техническая революция может привести рано или поздно к техногенной катастрофе. Факты таковы, что в настоящее время около 66% сетей имеют серьёзные уязвимости, а к 2020 году до 10% хакерских атак будет нацелено именно на устройства IoT, что также немало. Далее мы постараемся показать вам, как компания **Eurotech** предлагает бороться с этими угрозами.

Рис. 1. Интернет вещей меняет уклад нашей жизни

Сегодняшняя ситуация с киберугрозами

Нынешняя ситуация с киберугрозами по-настоящему серьёзна. По мере увеличения числа подключённых к сети устройств, разрастания облачных сервисов и внедрения технологий Big Data кибератаки становятся всё более масштабными и многочисленными. В результате мы наблюдаем ослабление защиты. И заметьте, речь уже не идёт о «если вас взломают» – речь идёт о «когда». Организации используют распределённые сети, которые гораздо сложнее защитить, нежели локальные. Для всех, кто пытается защитить свои активы, огромный объём незащищённых данных и устройств, который добавляется к этой проблеме безопасности благодаря IoT, весьма существенен. Кроме того, IoT привносит и новые направления кибератак, к которым мы не готовы. В рамках данной темы очень важно то, что речь идёт не об атаках на сетевую инфраструктуру, таких как DDoS-атаки, требующие глубоких знаний технологий и уязвимых мест сетевых протоколов, а об атаках на отдельные устройства, нарушающих их сетевую идентификацию и коммуникации между ними. Мы уже видели некоторые примеры атак такого рода и их плачевные результаты. Никто в настоящее время не защищён, и IoT-

ориентированные компании должны проявлять особую осторожность.

Автомобильная промышленность

Печально известная атака Jeep, по сообщениям Wired, заставила Chrysler отозвать 1,4 млн автомобилей для исправления уязвимости ПО, позволяющей хакерам дистанционно получать доступ к автомобилям и управлять их жизненно важными функциями.

Медицина

В Университете Южной Алабамы студенты могли попрактиковаться в «убийстве» виртуального пациента посредством получения доступа и дистанционного отключения его кардиостимулятора. Исследователь вопросов безопасности Билли Риос произвёл глубокий анализ механизма действия автоматизированной системы введения лекарственных препаратов производства фирмы Hospira и выяснил, что вполне реально дистанционно изменять дозы вводимых пациентам препаратов, что может привести к летальному исходу.

Жильё

В дополнение к множеству историй о взломе умных лампочек мы уже имеем сведения об авариях вследствие нарушений взаимосвязей устройств, потенциально приводящих к неработоспособности систем безопасности жилища. Chamberlain Group, Inc. и Ooma Inc. зафиксировали аварии, вызванные нарушением в подключении IoT-устройств к соответствующим сервисам и приводившие к проблемам с безопасностью людей.

Умная сетевая инфраструктура

Пока ещё не рассмотренная в этой статье умная сетевая инфраструктура, называемая также Smart Grid, также является потенциальной мишенью злоумышленников в рамках атак на IoT. Современные тенденции к распределённым системам контроля и мониторинга, глубоко внедряющиеся в нашу жизнь, также делают нас уязвимыми.

Безопасность – основной критерий при внедрении IoT

Пока ваша сеть IoT остаётся локальной, вы не будете испытывать существенных проблем с безопасностью. Но беда в том, что в реальной жизни сети уже давно выросли до глобальных размеров, объединив инфраструктуры различных бизнесов и вобрав в себя множество устройств. Беда ещё и в том, что идея IoT эксплуатирует имеющиеся ресурсы Интернета, в силу многих причин являющиеся весьма уязвимыми и изначально не приспособленными для этих целей, поэтому безопасность IoT по своей природе является гораздо более сложной задачей, чем, например, безопасность в приложениях M2M.

Поскольку индустрия активно развивается и обновляется, мы наблюдаем бум подключения различных продуктов. Проблемой первых IoT-продуктов «из коробки» была их слабая защищённость. Такие устройства, к примеру, всегда поставляются с паролем по умолчанию вида «1234», они имеют открытые сервисы для подключения к ним извне (типа Telnet), легко взламываемое ПО, основанное на HTTP-запросах, а также миллионы других врождённых пороков. Из-за несовершенства стандартов защиты и отсутствия хороших практических примеров IoT имеет все шансы стать основной частью IT-бюджета департаментов безопасности, подрывая все остальные полезные инвестиции. Более того, проблемы безопасности IoT отвращают от этих технологий значительную часть потенциальных пользователей. Если государственные органы, владельцы бизнеса и рядовые пользователи не могут поверить в сохранность своих данных, они делают выбор в пользу более примитивных (но более надёжных в плане безопасности) технологий, а созданный прецедент существенно замедляет развитие IoT в будущем. В 2015 году на конференции IoT Security глава службы информационной безопасности ФБР Арлетт Харт предупредила, что угрозы IoT могут быть гораздо опаснее, чем это принято считать. По её словам, когда злоумышленники крадут коммерческую информацию организаций, это становится лишь новостями. Но когда они крадут персональные данные и идентификаторы, это уже угроза для жизни конкретных людей. Люди чувствуют свою незащищённость, а этого нельзя допустить.

Botnet of Things

Один из опасных сценариев, появляющихся в последнее время, – IoT-Botnet-сети (Ботнет вещей). Они представляют собой группы взломанных компьютеров, а также умных IoT-устройств, объединённых злоумышленниками в криминальных целях. Бот, созданный из взломанного IoT-устройства, может рассылать спам или ссылки на хост с вредоносным контентом, и всё это без ведома владельца устройства. В 2013 году исследователь из компании Proofpoint, специализирующейся на вопросах секретности, обнаружил, что через шлюзы безопасности проходили сотни и тысячи спамовых писем. Proofpoint идентифицировала Botnet-атаки, в результате которых было скомпрометировано до ста тысяч устройств. Компания кибернетических исследований IID проанализировала миллионы фрагментов данных, распространяемых по сети, и сделала вывод, что огромное число IoT-устройств является частью вредоносной сети Botnet. IID предсказала, что к концу 2017 года владельцы сетей Botnet благодаря расширению границ произведут полномасштабное вторжение скомпрометированных устройств Интернета вещей, таких как носимые устройства и устройства умных домов, в нашу жизнь. Например, камеры CCTV уже сейчас идентифицируются в качестве источников DDoS-атак против банков и других целей.

Расширение возможностей устройств IoT, таких как автономные дроны, а также прочих умных приложений, тоже не добавляет уверенности в достаточности требований безопасности. Вице-президент IID по противостоянию киберугрозам Шон Тирни отмечает, что, так как эти устройства используются для первичных и ответных атак на другие сети, они могут стать родоначальниками «войны Ботнетов» за господство в среде IoT.

С появлением вредоносного кода Mirai сообщество Интернет испытало первые серьёзные последствия атак IoT-Botnet. Mirai – это программа, заражающая компьютерные системы на базе ОС Linux и превращающая их в дистанционно управляемые боты, которые затем можно было объединять и использовать для сетевых атак. После того как исходный код Mirai был открыто опубликован на одном из хакерских форумов, тут же появились его разнообразные клоны. Типичная мишень их – удалённые камеры и сетевые роутеры. Заражённые устройства непрерывно сканируют Интернет с целью поиска IP-адресов других подключённых устройств. Затем вирус пытается идентифицировать устройство и подключиться к нему, применяя стандартные заводские настройки логина и пароля. Если это удаётся сделать, устройство также заражается. Впервые Mirai был обнаружен в августе 2016 года и с тех пор стал основой самых разрушительных DDoS-атак. Примеры атак Mirai-BotNet – это и атака на DNS-

сервисы Dyn в октябре 2016 года, и атака на инфраструктуру Интернет Либерии в ноябре 2016 года, и, конечно, ситуация в том же ноябре 2016 года с выходом из строя благодаря клону Mirai миллиона роутеров Deutsche Telekom.

Ещё один пример вредоносного ПО, действующего в среде IoT, – Stuxnet. Это имя компьютерного червя, заражающего системы под управлением Windows и SCADA-системы Siemens, управляющие контроллерами этого производителя. Впервые червь проявил себя в 2010 году в компьютерной атаке, затормозившей работу ПО на иранском предприятии по обогащению урана. Это вполне могло привести к плачевным последствиям. Stuxnet атаковал систему Windows, используя как вновь обнаруженные, так и известные уязвимости этой ОС. Обычно червь распространялся посредством инфицированных съёмных USB-носителей данных, то есть «добровольными» разносчиками выступали сами сотрудники предприятия. С 2010 года выявлено уже несколько клонов червя Stuxnet. Анализируя качество написания вредоносного кода и объём требуемых для его разработки ресурсов, можно прийти к выводу, что тут дело не обошлось без государственных органов. Конечно, были разработаны соответствующие «заплатки» для ОС, препятствующие распространению Stuxnet, но ведь это лишь первая ласточка!

Вызов IoT брошен

В одном из интервью Евгений Касперский назвал Интернет вещей Интернетом уязвимостей. И в этом высказывании, как мы уже заметили, заключён большой смысл. Чтобы обеспечить достаточный уровень доверия и исключить риски при подключении IoT-устройств, такие как кража приложений, требуется идентификация, аутентификация, авторизация, обеспечение конфиденциальности и целостности данных. Безопасность IoT – не то же самое, что безопасность Интернет-сетей и примеры новых рисков должны обострить наше отношение к проблеме. Данные должны быть защищены при обработке в системе, при передаче и хранении, а для этого требуется существенный пересмотр принципов идентификации, аутентификации и авторизации, как устройств, так и людей. Именно так считает Робин Дак-Вулли, директор компании Beecham Research. По его словам, мы должны также учитывать, что некоторые полевые устройства могут быть скомпрометированы или выйти из строя, таким образом, нам требуются эффективные процедуры восстановления – это ещё один вызов эры IoT.

Технологический директор Beecham Research профессор Джон Хаус также полагает, что нам требуется высокая степень доверия, и это ещё более критично в условиях экосистемы IoT. Доверие должно начинаться с устройств уровня сенсоров и микроконтроллеров и распространяться по всей инфраструктуре до самого верха. Это огромная головоломка, в которой каждый кусочек должен вносить свою лепту в общий положительный результат.

Надёжность IoT: кто будет отвечать?

IoT задаёт головоломные вопросы о кибератаках и авариях систем. Кто же будет отвечать за последствия таких событий: производитель и продавец устройства, Интернет-провайдер или, может быть, сам пользователь? Должен ли и производитель ПО быть добавлен в это уравнение? В цепочке IoT весьма много чувствительных звеньев, и в случае ава-

рии удобнее, конечно, указать в качестве виновника на производителя устройства, но в целом это неоднозначный вопрос. Например, в торговле или здравоохранении потеря данных в результате применения технологий IoT может привести к последствиям для частных лиц, за которые должны будут ответить продавцы, банки или медицинские учреждения. Производители датчиков как таковые, безусловно, несут большую ответственность, особенно в случае разработки критически важных устройств типа детекторов дыма, датчиков CO или систем автомобильных подушек безопасности. Но в производстве качественных продуктов крайне важно стратегическое партнёрство производителей «железа» и ПО для устройств IoT. В качестве примера приведём случай, озвученный сенатором США Эдвардом Марки, который показал, что хакеры могут получить доступ к некоторым популярным автомобилям, управляя их внезапным ускорением, поворотами, отключением тормозов, активацией гудка, включением аварийного стоп-сигнала, перенастройкой спидометра, считыванием показаний датчиков. Таким образом, в мире IoT производители ПО также не защищены от исков и должны понимать, что они несут ответственность за продукт, а также за возможные физические повреждения и имущественный ущерб, возникающие в результате его использования. Производители подключаемых устройств финансово ответственны за небрежное проектирование кода ПО и архитектуры.

Недостатки стандартизации

В традиционном мире IT существует огромное множество стандартов, и сегодня их пытаются адаптировать для мира IoT. Это означает, что пока мы имеем очень уязвимую экосистему, состоящую из устройств и ПО различных производителей, а также разрозненных сетевых сервисов. Чтобы добиться безопасности в этих условиях, мы должны выработать цельное решение для обеспечения идентификации устройств, их аутентификации и защищённых коммуникаций между ними.

Укажем на несколько практик, ведущих к нарушению безопасности в IoT:

- недостаточные возможности защиты, встроенные в базовые системы, такие как система на кристалле (SoC), что даёт хакеру лёгкую возможность получить права доступа администратора;
- передача незашифрованных данных позволяет любому злоумышленнику при помощи сетевого сниффинга перехватывать информацию;
- использование устройств с незакрытыми (без заплаток) уязвимостями в ПО – это приглашение для разного рода вирусов и червей, эксплуатирующих ошибки в системах;
- Web-сервисы и ОС с жёсткой логикой организации доступа позволяют хакерам легче получать доступ к данным;
- неразумная политика в сфере ПО без надлежащего контроля целостности прикладного ПО и ОС в устройствах и шлюзах;
- незашифрованные API-токены и вызовы в текстовом виде также ослабляют защищённость коммуникаций;
- низкая защищённость мобильных устройств в среде IoT усугубляет проблему растущего числа открытых беспроводных точек доступа;
- отсутствие должной аутентификации – путь к потенциально опасному доступу для хакерских атак.

Нарушение безопасности всего лишь на одном устройстве может привести к ситуации, когда множество других устройств, составляющих единую с ним сеть, окажутся под угрозой, поэтому для успешного обеспечения безопасности необходим контроль сверху донизу. Чтобы обеспечить пользователя целостной и надёжной платформой, производители устройств и ПО для них, в свою очередь, должны иметь единую концепцию, базирующуюся на испытанных открытых промышленных стандартах. Хорошая новость состоит в том, что пути реализации такого подхода по примеру мира IT найдены. Но они требуют понимания производителями разницы между классическими IT и IoT. Только тогда они смогут эффективно применить свои лучшие наработки в области IT к миру IoT.

Основы безопасности IoT и передовая практика

Итак, по сравнению с бурным ростом IoT вопросы безопасности находятся лишь в начале пути. И сейчас самое время поговорить о лучшей практике в этой области. Согласно исследованиям Gartner, для успеха IoT будут иметь первостепенное значение принципы распознавания устройств, а также обеспечение безопасности новых и поддержание безопасности существующих устройств. Требуется целостный подход, когда идентификация, аутентификация и автоматическое распознавание применяются комплексно. Лучшая практика требует принимать во внимание специфику распределённых необслуживаемых мобильных систем и устройств. Необходима защищённая рабочая среда (AEP – Application Enablement Platform), интегрирующая все устройства IoT, а также безопасное обслуживание и распространение ПО.

В первую очередь, присоединённые устройства и платформы IoT должны получить подтверждённые уникальные идентификаторы. Для этого необходимо:

- строить решения на базе открытых промышленных стандартов;
- максимально использовать проверенные технологии защиты и партнёрских связей;
- закладывать потенциал обеспечения безопасности, масштабируемости и сопротивляемости на первых этапах проектирования устройств;
- встраивать в устройства идеологию сквозных комплексных решений безопасности;
- обеспечивать идентификацию каждого узла сети IoT на основе его уникального ID и полномочий;
- взаимно идентифицировать узлы в сети IoT;
- шифровать все коммуникации между узлами;
- обеспечить встраивание механизмов автоматического контроля легитимности сертификатов узлов и разрешения/запрета их работы на этой основе;
- подтверждать цифровой подписью все коммуникации в дополнение к шифрованию трафика;
- контролировать состояние ПО и конфигураций устройств с помощью цифровой подписи;
- внедрить контроль доступа, основанный на роли устройства;
- осуществить инвестиции в инструменты обслуживания и диагностики сетей, позволяющие выявлять опасные отклонения и сертифицировать построенные решения IoT.

RAYSTAR
OLED Display Provider

Лучшая замена ЖК-панелям

OLED-дисплеи Raystar

Специсполнение по ТЗ заказчика Прозрачные модели

АВТОМОБИЛЬНАЯ ЭЛЕКТРОНИКА • СИСТЕМЫ БЕЗОПАСНОСТИ • ИЗМЕРИТЕЛИ МОЩНОСТИ • БЫТОВАЯ ТЕХНИКА • МЕДИЦИНСКИЕ ПРИБОРЫ

Характеристики

- Яркость экрана до 150 кд/м² обеспечивает считывание изображения при ярком солнечном свете
- Высокая контрастность 2000:1
- Широкий угол обзора до ±175°
- Цвет свечения: жёлтый, зелёный, красный, белый, синий
- Формат изображения: 122×32, 128×64, 240×64, 256×64 и 96×64 точки
- Низкая потребляемая мощность 10 мА (схемы управления – токовые)
- Светоэмиссионная схема: не требуется система подсветки
- Короткое время отклика: 10 мкс при температуре +25°C
- Широкий диапазон рабочих температур от –40 до +80°C
- Малая толщина модуля дисплея, небольшой вес
- Срок службы: 50 000 ч для белого и синего цвета; 100 000 ч для жёлтого, зелёного, красного цветов

ProSoft® ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР (495) 234-0636 INFO@PROSOFT.RU WWW.PROSOFT.RU

Базовые элементы безопасности IoT

Безопасная платформа IoT должна:

- обеспечивать доверенную среду функционирования;
- быть спроектированной таким образом, чтобы минимизировать возможность атак (минимум открытых портов, надёжные межсетевые экраны, и т.п.);
- использовать лучшее из технических и функциональных наработок, защищающих устройства IoT от угроз извне;
- быть безопасным и естественно интегрированным компонентом IT-инфраструктуры в целом.

Соответствующие изменения должны затронуть все устройства группы потенциального риска. Аутентификация и шифрование данных требуют масштабируемых решений, обеспечивающих взаимную идентификацию с высокой степенью стандартизации, что позволит разнообразным устройствам, включённым в инфраструктуру, беспрепятственно и безопасно обмениваться данными между собой. Для этого разработано немало методов, среди которых идентификация с доверенным ID, API-ключи, самозаверенные сертификаты, биометрия, связки пароль/логин, решения на базе платформ Trusted Platform Module (TPM), динамические пароли, а также решения с многофакторной аутентификацией.

Несмотря на обилие перечисленных методов, нельзя сказать, что все они легко применимы к среде IoT с учётом функциональности, безопасности и масштабируемости и могут использоваться для необслуживаемых устройств. API-ключи, например, обычно слабы в плане криптостойкости, а ненадёжные связки пароль/логин могут быть подобраны.

Однако многие эксперты сходятся во мнении, что один из лучших на сегодняшний день методов аутентификации и защиты данных – интегрированный сертификат x.509 с PKI (Public Key Infrastructure – инфраструктура открытых ключей). Технология PKI даёт уверенность в подлинности идентификации узла на другой стороне обмена данными. Являясь широко распространённой и хорошо отработанной технологией, PKI уже встроена в самые надёжные промышленные стандарты. PKI поддерживает подписание сообщений и документов, вход в систему и аутентификацию, сертификаты и ключи в виде файлов и токенов и является ядром самозаверенных сертификатов.

Подход к безопасности IoT от начала до конца

В качестве яркого примера системного подхода к решению описанных проблем можно привести концепцию компании Eurotech. Она создаёт технологические блоки, из которых можно строить распределённые системы устройств и сенсоров, интегрированные в IT-инфраструктуру. Для этого компания предоставляет решения, состоящие из аппаратных платформ, ПО низкого и высокого уровня, операционных систем, инструментов программирования, а также обеспечивает профессиональную поддержку разработчиков, резко сокращающую время и стоимость разработок (рис. 2). Итак, предложение Eurotech для IoT состоит из четырёх основных компонентов:

- облачная платформа интеграции IoT Everyware Cloud (EC);
- платформа разработки Everyware Software Framework (ESF), компью-

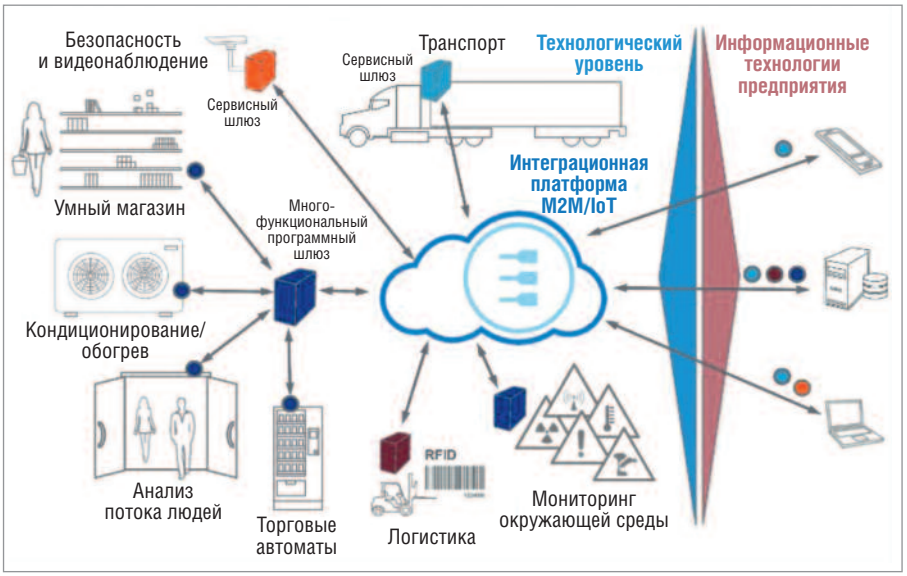

Рис. 2. Eurotech создаёт безопасную концепцию IoT

терная платформа и Application Development Framework;

- многофункциональные IoT-шлюзы, спроектированные специально для различных вертикальных рынков;
- профессиональная поддержка разработок IoT.

Everyware Cloud

Программная платформа Everyware Cloud (EC) разработана специально для поддержки приложений IoT. Она обеспечивает все необходимые сервисы для управления полевыми IoT-устройствами, включая их конфигурацию, сопровождение на всём протяжении жизни и удалённый доступ. Она также даёт возможность сбора данных с полевых устройств и предоставляет эти данные для использования другими приложениями, бизнес-процессами, формирования отчётов и т.п. Согласно концепции Eurotech безопасность заложена в Everyware Cloud с самого начала её разработки и является интегрированной составляющей всех компонентов. В EC использован опыт лучших IT- и Интернет-разработок в области безопасности, изначально заложены механизмы масштабируемости, а также возможности технологий PKI, MQTT on SSL, двухфакторной аутентификации пользователь/администратор.

Everyware Software Framework

Everyware Software Framework (ESF) обеспечивает высокоэффективную, гибкую и IT-ориентированную компьютерную платформу и среду разработки приложений для построения нового поколения присоединяемых к сети умных устройств и приложений на единой технологической основе с использованием Java и OSGi. ESF позволяет разработчику сконцентрироваться на собственном приложении, избавляя его от рутинной работы благодаря целому ряду функциональных библиотек.

Программируемые многофункциональные шлюзы (Multi-service IoT Gateways) разработаны для применения на устройствах, функционирующих в жёстких условиях высоких температур, повышенной влажности и пыли (рис. 3). Благодаря оптимизированному и сертифицированному IoT-стеку, включающему ОС Linux, Java, OSGi и ESF IoT Edge Framework, обеспечивается максимально безопасное выполнение программ и среды программирования для шлюзов и устройств IoT. В зависимости от требований приложения могут быть задействованы дополнительные возможности для обеспечения безопасности, такие как безопасная загрузка, аппаратное хранение ключей, криптографическая акселерация. Комбинирование продвинутых мер защиты создаёт многоуровневую надёжную систему охраны IoT от угроз.

Сервисы IoT Professional Services гарантируют, что конечный продукт будет соответствовать заданным требованиям системной интеграции и пользовательским спецификациям. Они предлагают ряд программ по сопровождению разработчиков аппаратных и программных средств на всём протяжении проекта.

Для разработчиков доступно также целое семейство тестовых комплектов IoT Development Kit (рис. 4). Они представляют собой полноценные аппаратные платформы с предустановленным программным обеспечением, позволяющие резко сократить трудозатраты по изучению архитектуры системы и адаптации решения к собственным нуждам, а также по прототипированию.

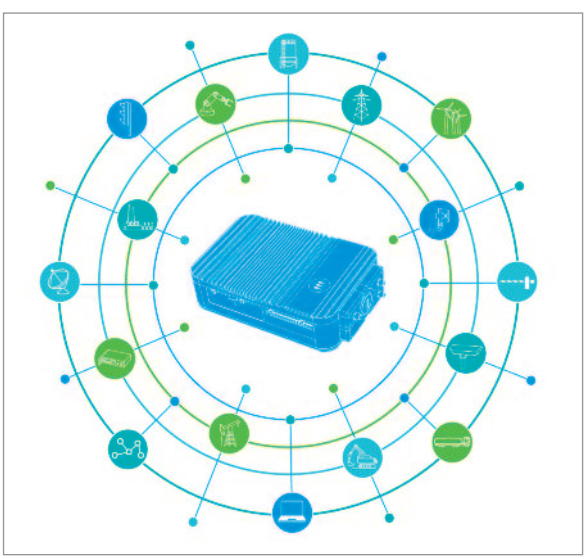

Рис. 3. Универсальные многофункциональные шлюзы Eurotech

Рис. 4. Набор разработчика IoT

Архитектура Eurotech IoT Security была разработана на базе концепции сквозной безопасности и безопасности каждого элемента системы. Вот некоторые её принципы.

- **Идентификация и контроль доступа.** Конфиденциальность и интегрированность достигаются благодаря модели доступа, основанной на роли узла. Модель контроля доступа и лист контроля доступа следуют принципу наименьшей привилегии и пронизывают все слои архитектуры. Каждый аккаунт управляет списком пользователей и контролирует их полномочия. Everyware Cloud имеет конфигурируемую политику блокировки, привязанную к аккаунту. Она может запретить регистрацию пользователя после заданного числа неудачных попыток входа. Вход в консоль Everyware оснащён защитой в виде двухфакторной аутентификации (2FA). Everyware Cloud поддерживает индивидуальную аутентификацию устройств на базе сертификата x.509 с интегрированным PKI, а также пользовательские приложения с функциональностью PKI.
- **Безопасный обмен данными.** Весь трафик MQTT шифруется посредством SSL-соединения. Доступ к консоли возможен только через HTTPS-соединение. Весь доступ к REST API (Representational State Transfer – передача состояния представления) также происходит только через HTTPS-соединения.
- **Физическое хранение данных.** Облако Eurotech поддерживается дата-центрами, организованными по последнему слову техники, использующими современную архитектуру и инженерные наработки.
- **Логический доступ к данным.** Все базы данных защищены стойкими межсетевыми экранами с жёсткими правилами доступа извне и доступны напрямую только для компьютеров среднего уровня. В базах данных все записи имеют привязку к аккаунту посредством специального идентификатора. В брокере MQTT данные и трафик между разными аккаунтами связываются посредством виртуальной машины.
- **Безопасность устройств и управление встроенными приложениями.** Для оконечных устройств крайне важны безопасность, чёткая аутентификация, отсутствие необоснованно открытых портов, настройка межсетевых экранов, качество встроенного ПО, развитая диагностика и логирование событий, применение стойкой криптографической техники для передачи данных. Безопасность может быть ещё усилена благодаря безопасной загрузке, аппаратно реализованным функциям, а также применению VPN.
- **Управление уязвимостями.** Независимые компании по сертификации безопасности проводят оценку уязвимостей, включая сети, компьютеры и приложения. Eurotech гарантирует, что анализ внутренних и внешних уязвимостей проводится периодически и после всех значимых изменений в оборудовании. Компания исправляет все выявленные критические проблемы с безопасностью в кратчайшие сроки.

Все компоненты Eurotech IoT-архитектуры изначально спроектированы для создания безопасных масштабируемых и надёжных систем и базируются на наиболее успешных и современных стандартах M2M и IoT, поэтому они готовы защитить инвестиции пользователей, как сегодня, так и в отдалённом будущем.

Заключение

Текущее состояние кибербезопасности и возможность взлома IoT-устройств и инфраструктуры заставляет нас присвоить этой проблеме приоритет номер один.

Безопасность должна стать главным ориентиром для разработчиков устройств IoT, программного обеспечения и инфраструктурного окружения. Если усилия в этой области будут недостаточными, мы рискуем разочароваться в самой концепции IoT. Конфиденциальность, целостность и доступность данных пользователей, а также IoT-инфраструктуры – самые важные задачи для Eurotech, и поэтому безопасность является главной заботой специалистов компании.

Если вы захотели узнать больше о решениях Eurotech для рынка IoT, обратитесь к специалистам компании ПРОСОФТ – официального дилера Eurotech в России. ●

Авторизованный перевод
Юрия Широкова
E-mail: textoed@gmail.com

ПРОМЫШЛЕННЫЕ ИЗМЕРЕНИЯ И АВТОМАТИЗАЦИЯ

Надежные контрольно-измерительные системы с длительным сроком доступности

ADDI-DATA®

- Помехоустойчивые платы аналогового и цифрового ввода/вывода PCI, PCI Express, CompactPCI, ISA
- Модули управления движением
- Коммуникационные платы для локальных сетей с интерфейсами RS-232, RS-422, RS-485
- Интеллектуальные измерительные Ethernet-системы со степенью защиты IP65

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636 ▪ INFO@PROSOFT.RU ▪ WWW.PROSOFT.RU

Реклама