УДК 004.056

Методы повышения уровня информационной безопасности при использовании интернета вещей

Хабибулин Александр Касимович
Российский экономический университет им. Г.В. Плеханова
студент

Холоденина Анна Викторовна
Российский экономический университет им. Г.В. Плеханова
студент

Аннотация
В данной работе приведено разъяснение понятия «Интернет вещей» и объяснена его актуальность. Далее проведен анализ существующих угроз с целью выявления методов их устранения. После разбираются сами методы, и делается вывод об их применении.
Ключевые слова: информационная безопасность, интернет вещей, угрозы информационной безопасности, уровень информационной безопасности

Methods of increasing the level of information security when using the Internet of things

Khabibulin Alexander Kasimovich
Plekhanov Russian University of Economics
student

Kholodenina Anna Vicktorovna
Plekhanov Russian University of Economics
student

Abstract
In this paper, we explain the concept of «Internet of things» and explain its relevance. Further, an analysis of existing threats is carried out to identify methods for their elimination. After the methods themselves are sorted out and concluded about their application.
Keywords: information security, Internet of things, threats to information security, level of information security

Интернет вещей (далее IoT – Internet of Things) подразумевает под собой множество гетерогенных устройств, плотно взаимосвязанных и сообщающихся с целью достижения широкого круга задач, часто совместного. Можно утверждать, что в относительно ближайшем будущем конструкция IoT будет охватывать промышленные предприятия,

инфраструктуру, жилье и другие системы, которые сегодня контролируются системами ICS и SCADA. Появление IoT будет сопровождаться рядом разработок: миниатюризация устройств и датчиков, повышение мобильности устройств, носимых устройств, вездесущая робототехника и растущая автоматизация всех функций IoT. Многие из этих устройств будут содержать интеллектуальные датчики, которые имеют микропроцессор, регулирующий сигналы перед передачей в управляющую сеть. Некоторые из устройств, вероятно, будут нанороботами с общим размером порядка нескольких микрометров или менее во всех пространственных направлениях и состоят из наноскопических компонентов.

Интернет вещей является одной из наиболее перспективных современных цифровых технологий, которая может обеспечить новый скачок производительности в бизнесе и промышленности. По оценкам аналитиков, к 2020 году число подключённых к Интернету вещей устройств достигнет от 20 до 50 млрд. единиц. Но несмотря на всю привлекательность и перспективность этой технологии, у неё есть и ряд недостатков. Одним из наиболее значимых таких недостатков является угроза кибербезопасности, возникающая при повсеместном внедрении IoT-устройств.

Как и каждая новая технология, IoT имеет помимо своих преимуществ новые для индустрии риски и проблемы. Поскольку IoT тесно связан с коммуникационными и информационными технологиями, очевидно, имеет смысл рассмотреть проблемы безопасности и конфиденциальности информации, уже известные в области информационной безопасности (далее - ИБ), и изучить, как эти проблемы проявляются в текущем и будущем состояние IoT. На первый взгляд, сходства кажутся настолько многочисленными, а различия настолько тонкими, что можно обмануться и решить, что проблемы информационной безопасности в IoT являются теми же проблемами, что и те, которые уже известны в индустрии ИБ, а значит, и те же меры, что применяются в ИБ достаточны для решения этих проблем. Однако некоторые характеристики делают проблемы безопасности и конфиденциальности в IoT настолько отличными, что требуется более тщательное их исследование.

- Количество подключенных к Интернету устройств уже превысило количество людей на планете, и это число продолжает резко увеличиваться. Этому способствует ряд факторов, в том числе внедрение Интернет-протокола версии 6 (IPv6), который позволяет каждому устройству иметь уникальный IP-адрес, что значительно облегчает обмен данными между устройствами. Тем не менее, проблемы безопасности и конфиденциальности данных для Интернета вещей не увеличиваются пропорционально количеству подключенных к Интернету устройств, а растут гораздо быстрее. Это связано с тем, что количество каналов связи в сети растёт гораздо быстрее количества узлов в ней.
- Компьютерные сети часто неоднородны по своему характеру, что может вызвать проблемы безопасности. Ожидается, что IoT будет гораздо

более разнородным, чем текущие компьютерные сети, интегрируя множество различных устройств от разных производителей, программных платформ и протоколов связи.

- В то время как серверы и рабочие станции защищены в серверных комнатах и офисах, а персональные компьютеры, ноутбуки и портативные устройства защищены присутствием владельца, в случае IoT-датчики и другие устройства расположены повсюду и более подвержены краже, злонамеренному повреждению и т.д. Злоумышленники могут использовать повышенную физическую доступность устройств для обнаружения дополнительных уязвимостей в системах Интернета вещей.
- Ожидается, что Интернет вещей будет повсеместным и очень распространённым. Подключенные к нему устройства используются повсюду или легко встраиваются в другие привычные нам устройства (в том числе, в бытовую технику и городскую инфраструктуру). Они могут собирать данные, общаться и взаимодействовать с другими устройствами без нашего разрешения или даже нашего ведома просто потому, что они не находятся в нашем личном владении (например, камеры видеонаблюдения в торговом центре или подключенные транспортные средства, которые мы используем в качестве пассажиров).
- По мере увеличения количества подключенных устройств количество собранной и накопленной информации о нас в различных базах данных постоянно увеличивается. Несмотря на то, что конфиденциальные данные могут быть удалены или защищены с помощью анонимизации, непредсказуемое сочетание, казалось бы, не конфиденциальных данных из разных источников может создать уникальный идентификатор конкретного человека, что может привести к нарушению неприкосновенности его частной жизни.
- В то время как в последние годы кибератаки в основном угрожали информационным системам, компьютерным сетям и персональным компьютерам, в случае с IoT кибератаки будут повышать риски до более высокого уровня. В эпоху интернета вещей, когда датчики и управляющие информационные системы будут связаны со множеством других информационных систем, злоумышленники будут иметь возможность достигать таким образом любые подключенные к сети устройства и добиваться их, в том числе, физического уничтожения - например, оборудования и инфраструктуры, беспилотных автомобилей и умных домов, электрических сетей, транспортных систем, АЭС и так далее. Stuxnet был первым вредоносным кодом, который атаковал систему управления ядерным объектом; однако, с ускоряющимися темпами развития IoT, он не будет последним, а значит риски для таких систем будут только расти.
- Интернет вещей по своей сути является динамической структурой. Её всепроникающий характер обеспечивает возможность девайсов, таких как носимые устройства, присоединяться к сети IoT и выходить из нее в любое время. Это, в сочетании с многопротокольными

характеристиками связи, делает традиционные меры информационной безопасности недостаточными для IoT.

Система обеспечения информационной безопасности в сетях Интернета вещей должна быть комплексной и всеобъемлющей. Она должна состоять из следующих взаимосвязанных этапов:

1. Контроль безопасности каналов связи.

Каналы связи должен быть защищены, для этого используются технологии шифрования и аутентификации, чтобы устройства знали, могут ли они доверять удаленной системе. Ведущие сертификационные центры (CA) уже встроили «сертификаты устройств» на более чем миллиарде IoT-устройств, предоставляя возможность аутентифицировать широкий спектр устройств, включая сотовые базовые станции, телевизоры и многое другое.

2. Защита ПО устройств.

Защита устройства в первую очередь заключается в обеспечении безопасности и целостности программного кода - все критически важные устройства, будь то датчики, контроллеры или что-ибо ещё, должны быть настроены на запуск только подписанного кода.

3. Контроль ПО устройств.

К сожалению, уязвимости в IoT-устройствах никуда не денутся, а значит, компаниям производителям придётся на протяжении длительного времени после продажи устройства осуществлять его поддержку и вовремя обновлять прошивку. Over-the air programming (OTA) – это технология, позволяющая проделывать это без очного присутствия сотрудника компании-производителя, которая избавит от необходимости отправлять к каждому такому устройству сотрудника компании.

4. Контроль взаимодействия в сети.

Некоторые угрозы способны справляться с любыми предпринимаемыми мерами безопасности. Хакеры постоянно находят лазейки в программном обеспечении устройств, получая доступ к управлению ими. Поэтому чрезвычайно важно иметь возможности проведения аналитики безопасности в системах IoT. Системы для анализа безопасности помогут лучше понять IoT-сеть, заметить подозрительные, опасные или злонамеренные аномалии.

Безопасность должна быть всеобъемлющей, иначе злоумышленники просто воспользуются самым слабым звеном в системе её обеспечения. Конечно, непосредственно традиционные ИТ-системы обычно передают и обрабатывают данные из систем Интернета вещей, но системы IoT имеют свои собственные уникальные потребности в безопасности.

Для защиты потребителей и общественности, технических специалистов, законодателей и других лиц, определяющих политику, необходимо вести и поощрять надлежащую практику безопасности и конфиденциальности. В настоящее время, в связи с разнообразием условий невозможно указать набор универсальных правил безопасности IoT. Защита должна быть индивидуальной и комплексной во избежание возможности использования слабых мест для атаки.

Библиографический список

1. Интернет вещей» (IoT) в России. Технология будущего, доступная уже сейчас // PricewaterhouseCoopers URL: https://www.pwc.ru/ru/publications/iot/IoT-inRussia-research_rus.pdf
2. Хабибулин А. К., Попов А. А. Технологии M2M для городской транспортной инфраструктуры // Студенческий. 2018. № 2-3 (22). С. 26-28.
3. 9 ways to improve IoT device security // Hewlett Packard Enterprise. Available at: https://www.hpe.com/us/en/insights/articles/9-ways-to-make-iot-devices-more-secure-1701.html (accessed: 22 May 2018).
4. Internet of things (IoT) security best practices // IEEE Internet Technology Policy Community White Paper. https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf (accessed: 05 May 2018).
5. The Future Internet of Things and Security of its Control Systems // Cornell University Library. Available at: https://arxiv.org/ftp/arxiv/papers/1610/1610.01953.pdf (accessed: 22 May 2018).