УДК 004.492.2

Бочаров М.В., студент магистратуры
Сивец Н.С., студент магистратуры
1 курс, факультет «Институт магистратуры»
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Россия, г. Санкт-Петербург
Научный руководитель: Кушнир Д.В.

ТЕКУЩИЕ ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация: *Изучение проблем безопасности Интернета вещей имеет огромное значение. Основная цель обеспечения безопасности применительно к Интернету вещей - сохранение конфиденциальности, обеспечение безопасности пользователей, инфраструктуры, данных и устройств, а также гарантирование доступности услуг, предлагаемых экосистемой Интернета вещей. Таким образом, исследования в области безопасности Интернета вещей в последнее время становятся как никогда актуальны. В этой статье представлен анализ последних исследований в области безопасности Интернета вещей.*

Ключевые слова: *Интернет вещей, IoT, безопасность.*

Annotation: *Learning about IoT security issues is essential. The primary goal of IoT security is to preserve privacy, keep users, infrastructure, data and IoT devices safe, and ensure the availability of services offered by the IoT ecosystem. As such, research into IoT security has been gaining momentum lately. This article provides an analysis of the latest research on IoT security.*

Key words: *Internet of things, IoT, security.*

Введение

Архитектура Интернета вещей (Internet of Things, IoT) основана на трехуровневой системе, которая состоит из уровня оборудования, уровня сети и уровня интерфейсов. Элементами, составляющими систему IoT, являются оборудование, протоколы связи и службы.

Такое оборудование, как датчики и исполнительные механизмы, включает в себя самые важные элементы в IoT. Типичный микропроцессор, который используется на аппаратном уровне, обычно основан на архитектурах ARM, MIPS или X86. В идеале разработчики также должны включать оборудование безопасности, которое содержит в себе криптопроцессор или микросхему безопасности.

В качестве аппаратной операционной системы (ОС) устройства IoT обычно используют ОС реального времени (Real-time operating system, RTOS), которая включает в себя микроядро, уровень абстракции оборудования, коммуникационные драйверы и следующие функции безопасности: изоляцию процессов, безопасную загрузку и песочницу исполнения приложений. Для уровня прикладного программного обеспечения существуют пользовательские приложения, криптографические протоколы, а также сторонние библиотеки и драйверы.

В частности, выбор оборудования имеет решающее значение для защиты устройств IoT. Аппаратные средства Интернета вещей вызывают заинтересованность в сфере безопасности в связи с возможностями аутентификации, сквозным шифрованием трафика, безопасным процессом загрузки, принудительным использованием цифровых подписей во время обновлений прошивки и прозрачными транзакциями.

Следующий важный компонент системы IoT включает протоколы связи и обмена сообщениями. Сеть интеллектуальных объектов может напрямую связываться с «облаком» через такие «облачные» сервисы, как Amazon Kinesis. Однако важной концепцией в IoT является реализация беспроводной сенсорной сети (wireless sensor network, WSN) в качестве основной коммуникационной технологии в IoT. WSN имеет облегченные протоколы, позволяющие устройствам взаимодействовать друг с другом и со шлюзом на границе. Более того, WSN поддерживает динамическую связь, которая обычно всегда основана на стандарте 802.15.4. Среди протоколов IEEE 802.15.4 предназначен для низкоскоростных WPAN (wireless private area network), что соответствует требованиям системы IoT. Некоторыми преимуществами этого протокола являются его масштабируемость и тот факт, что он может быть автономным, потребляет мало энергии и имеет низкие эксплуатационные расходы. Тем не менее, Bluetooth, ZigBee, PLC, WiFi, 4G и 5G также могут быть выбраны в качестве протоколов связи, чтобы удовлетворить потребности процессов IoT.

Еще одним важным компонентом Интернета вещей является агрегатор, используемый в качестве шлюза для архитектуры Интернета вещей. Например, им может быть маршрутизатор WiFi. Шлюзы обеспечивают нисходящее подключение к множеству IoT устройств. «Облако» - еще один ключевой элемент системы Интернета вещей. Наиболее популярными поставщиками облачных услуг (cloud service provider, CSP) являются Amazon Web Services, Microsoft Azure, Google Cloud Platform и IBM Cloud. «Облако» предоставляет услуги для Интернета вещей, включая обмен сообщениями, хранение, обработку данных и аналитику. Кроме того, CSP предлагают новые функции, поддерживающие транспортную телеметрию очереди сообщений (MQTT), которая обычно используется в межмашинной связи (M2M), и протоколы передачи репрезентативного состояния (REST).

В дополнение к существующим услугам появление новых коммуникационных технологий, таких как 5G, сделает роль «облака» более значимой. Сотовая связь 4G и 5G обеспечивает беспроводную связь на большом расстоянии. Более того, возможность сделать все устройства IoT адресуемыми с помощью IPV6, позволяет устройствам IoT подключаться непосредственно к «облаку».

Введение в безопасность IoT систем

В настоящее время традиционные методы обеспечения безопасности не применимы к IoT, в котором используется большое число различных коммуникационных протоколов для предоставления различных сервисов. Сообществом Open Web Application Security Project (OWASP) выделено 3 уровня IoT, которые наиболее подвержены атакам злоумышленников: аппаратное обеспечение, канал связи, предоставляемая функциональность и услуги. Таким образом, при проектировании таких систем для обеспечения безопасности должны быть охвачены все вышеперечисленные уровни IoT. Типичная структура построения IoT приведена на рисунке 1.

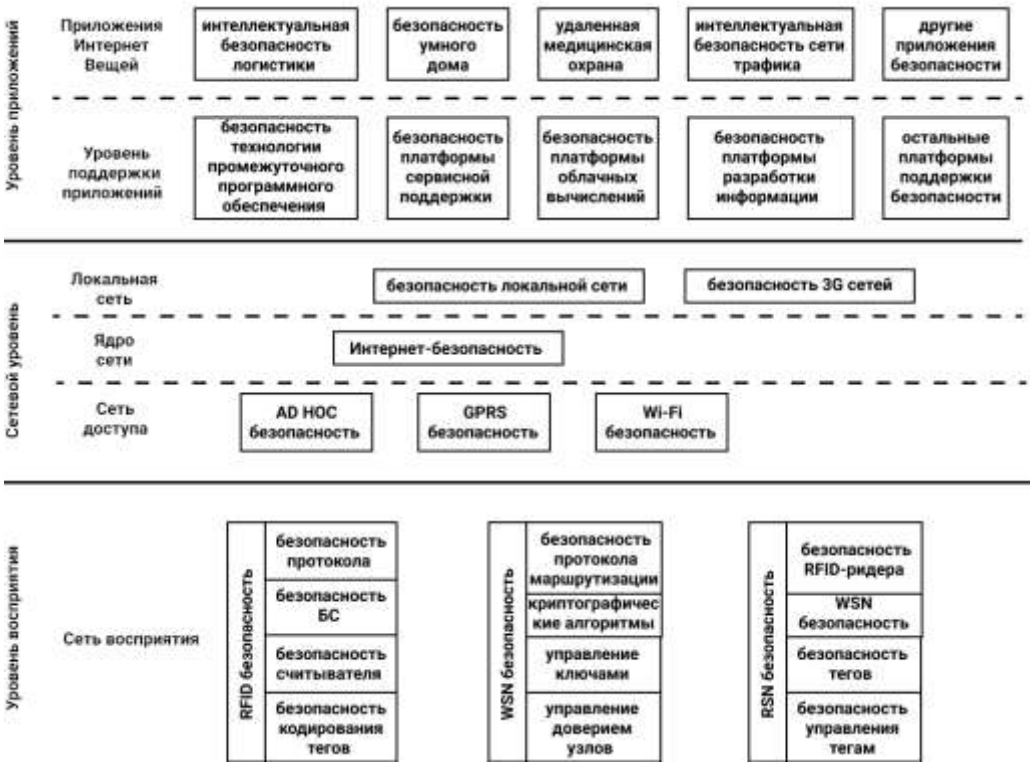

Рисунок 1. Обеспечение безопасности в архитектуре IoT

Кроме того, стоит учитывать, что беспроводные сенсорные сети и технология радиочастотной аутентификации (radio frequency identification, RFID) также рассматриваются, как часть сети Интернета вещей. В таблице 1 приведены основные векторы атак на RFID и сенсорные сети.

Таблица 1.

Векторы атак на RFID и сенсорные сети

Уровень OSI	**Атаки на сенсорные сети**	**Атаки на RFID**
	Типы атак	
Физический	Устройства для глушения сигнала, атака повторного воспроизведения, Атака	Активное глушение сигнала или частичное отключение функций устройств, Атака

	Сивиллы, Атака выборочной пересылки, Атаки синхронизации времени	Сивиллы, атака повторного воспроизведения, уничтожение считывателей RFID
Сетевой, Транспортный	Атака на выделенный узел, man in the middle, сниффинг, разновидности ddos	Атаки на метки: клонирование, спуффинг. Атаки на считыватели: обезличивание, сниффинг Атаки на протоколы
Прикладной	Инъекции, переполнение буффера	Инъекции, переполнение буффера, несанкционированное чтение и модификация заголовков пакетов
Многоуровневые атаки	Атаки по побочным каналам, криптографические атаки	

Согласно архитектуре IoT, предложенной OWASP, все основные уровни IoT подвержены атакам. Наиболее популярный вектор атак связан с процедурами аутентификации и авторизации устройств IoT. На данный момент распространены следующие протоколы IoT систем, поддерживающие аутентификацию: DDS, ZigBee, MQTT, Zwave. Однако не все устройства IoT в данный момент используют вышеуказанные протоколы. Одной из немаловажных

проблем является недостаточная возможность настройки безопасности из-за жестко заданного пароля, устанавливаемого производителями IoT устройств.

Недостаточная физическая безопасность устройств из-за уязвимостей в аппаратном обеспечении является еще одним вектором атак на IoT системы. Например, для таких простых устройств, как сенсоры невозможно применить шифрование. При реализации шифрования существует проблема удобства использования таких устройств из-за требуемого изменения их габаритов, однако выходом в такой ситуации может быть применения простейших криптографических методов шифрования без модификации устройств.

Другим вектором атак могут служить уязвимости в программном обеспечении для управления IoT устройствами: небезопасные web и облачные интерфейсы управления. Существуют также и другие методы атак, характерные для традиционных компьютерных сетей.

Разработка текущих механизмов безопасности IoT

Основная цель применения мер безопасности - сохранить конфиденциальность, обеспечить безопасность пользователей, инфраструктуры, данных и IoT устройств и гарантировать доступность услуг, предлагаемых экосистемой Интернета вещей. Таким образом, меры по смягчению и противодействию обычно применяются в соответствии с классическими векторами угроз.

1. Аутентификация

Аутентификация - процесс идентификации пользователей и устройств в сети и предоставления доступа авторизованным лицам и устройствам, которыми они управляют. Аутентификация это один из способов борьбы с атаками на IoT системы. Примерами таких атак являются: атака повторного воспроизведения, атака Man-in-the-Middle, атака олицетворения и атака Сивиллы. В настоящее время аутентификация по-прежнему является наиболее популярным методом для

предоставления доступа пользователю на уровне приложения, а также предоставления доступа к устройству в сети IoT.

Безопасность транспортного уровня (протокол TLS) широко используется для аутентификации и шифрования связи. Специально для устройств с ограничениями TLS предлагает механизм TLS-PSK, который использует предварительный обмен общими ключами и метод аутентификации TLS-DHE-RSA, который использует обмен ключами RSA (RSA handshake) и Диффи-Хеллмана (DH). RSA и DH представляют собой открытый ключ и криптографические протоколы. В этой схеме два объекта, которые должны выполнять взаимную аутентификацию, должны доказать друг другу свою легитимность, заранее поделившись секретной информацией (предварительно совместно используемыми ключами). Поскольку в процессе аутентификации используется только шифрование с симметричным ключом, схема подходит для ограниченных устройств, таких как датчики [1]. В настоящее время существует три типа протоколов аутентификации, разработанных для IoT: протоколы на основе асимметричной криптографии, на основе симметричной криптографии и гибридные протоколы [2]. Пользователи и устройства в среде IoT создают двустороннюю связь, т.к. существует взаимодействие между устройством IoT и серверами. Устройство будет отправлять данные на сервер, а также получать данные управления, передаваемые сервером. Таким образом, взаимная аутентификация имеет решающее значение в системе IoT для проверки активности как устройства, так и сервера. В последнее время появилась огромная потребность в облегченной аутентификации и шифровании, о чем будет сказано далее.

2. Шифрование

Для достижения сквозной безопасности все узлы сети должны иметь шифрование. Однако из-за неоднородности систем IoT некоторые устройства не

имеют возможность встраивания микропроцессоров общего назначения из-за своих габаритов. Устройства с ограниченными ресурсами могут включать только специализированные средства защиты [3]. Следовательно, обычные криптографические примитивы не подходят для интеллектуальных устройств с низким уровнем ресурсов из-за их низкой вычислительной мощности, ограниченного срока службы батареи, небольшого размера, небольшой памяти и ограниченного источника питания. Таким образом, облегченная криптография может быть эффективным средством решения проблемы использования шифрования для этих устройств.

3. Безопасное управление устройствами IoT

Увеличивается количество публикаций по безопасному управлению устройствами IoT. Целью такого управления является обнаружение и устранение вредоносных узлов сети и обеспечение безопасного контроля доступа. Автоматизированные и динамические расчеты доверия для проверки значений легитимности участвующих узлов в сети IoT являются одними из последних достижений в исследованиях безопасного управления устройствами IoT. Однако большая часть исследований сосредоточена на обнаружении вредоносных узлов. В частности, было предложено лишь несколько методов управления доступом на основе доверия. Действительно, из-за масштабируемости и огромного количества интеллектуальных устройств, которые хранят конфиденциальные данные, существует острая необходимость в автоматизированном, прозрачном и простом управлении контролем доступа, чтобы разным узлам можно было предоставить разный уровень доступа [4]. Несмотря на то, что только 20% методов контроля доступа в настоящее время используют оценку доверия, это все же многообещающий механизм безопасности. Причина эффективности этого механизма связана с его способностью рассчитывать динамическую оценку доверия узла [5], что позволяет постепенно оценивать значение доверия каждого

узла. Более того, такой ученый, как Caminha в работе [6] предложил интеллектуальную оценку доверия с помощью машинного обучения. Это может помочь сделать менее опасной атаку включения-выключения, которая может повлиять на расчет доверительного значению узла сети. Кроме того, безопасное управление устройствами IoT могло бы устранить такую очевидную слабость аутентификации, как действенность атак, направленных на повреждение узлов. Группа ученых под руководством Zhang [7] утверждает, что доверительные вычисления для контроля доступа в сети IoT, Trust-Based Access Control (TBAC), все еще относительно новы, но успешно реализованы в коммерческих приложениях. Bernal и ряд др. ученых предложили в [8] систему управления с учетом доверия для Интернета вещей, которая продвигает многомерные математические свойства для оценки доверия. Однако из-за ограниченности ресурсов устройств выполнение оценки доверия централизовано, как и во многих предложениях, что также требует дальнейших исследований в этом направлении.

Выводы

Цель этого исследования была достигнута путем предоставления обзора тенденций исследований в области безопасности Интернета вещей. Будущие направления этого исследования включают разработку комплексного моделирования угроз Интернета вещей с последующим проектированием алгоритма нулевого доверия для уменьшения влияния известных и неизвестных кибератак на систему Интернета вещей.

Использованные источники:

1. Shinzaki T. et al. IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data //Fujitsu Sci. Tech. J. – 2016. – Т. 52. – №. 4. – С. 52-60.

2. Ferrag M.A. et al. Authentication protocols for internet of things: a comprehensive survey //Security and Communication Networks. – 2017. – Т. 2017.
3. Katagi M. et al. Lightweight cryptography for the internet of things //Sony Corporation. – 2008. – Т. 2008. – С. 7-10.
4. Ishaq I. et al. IETF standardization in the field of the internet of things (IoT): a survey //Journal of Sensor and Actuator Networks. – 2013. – Т. 2. – №. 2. – С. 235-287.
5. Gong B., Zhang Y., Wang Y. A remote attestation mechanism for the sensing layer nodes of the Internet of Things //Future Generation Computer Systems. – 2018. – Т. 78. – С. 867-886.
6. Caminha J., Perkusich A., Perkusich M. A smart trust management method to detect on-off attacks in the internet of things //Security and Communication Networks. – 2018. – Т. 2018.
7. Zhang Y. History and Future of the National College Entrance Exam (NCEE) in China //National College Entrance Exam in China. – Springer, Singapore, 2016. – С. 1-15.
8. Bernabe J. B., Ramos J. L. H., Gomez A. F. S. TACIoT: multidimensional trust-aware access control system for the Internet of Things //Soft Computing. – 2016. – Т. 20. – №. 5. – С. 1763-1779.