УДК 004.056.53

МОДЕЛИ И ТЕХНОЛОГИИ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ

С. А. Лесько, к.т.н., доцент кафедры КБ-3 «Управление и моделирование систем» РТУ МИРЭА, Москва, Россия;
orcid.org/0000-0002-6641-1609, e-mail: sergey@testor.ru
Д. О. Жуков, д.т.н., кафедры КБ-8 «Информационное противоборство», РТУ МИРЭА, Москва, Россия;
orcid.org/0000-0002-1211-5214, e-mail: zhukovdm@yandex.ru
П. Ю. Пушкин, к.т.н., заведующий кафедрой КБ-3 «Управление и моделирование систем» РТУ МИРЭА, Москва, Россия;
orcid.org/0000-0003-3684-550X, e-mail: is-irk@mail.ru

Широкое распространение современных технологий Интернета вещей (Internet of Things, IoT) будет во многом базироваться на информационной безопасности, а также защите конфиденциальности данных. Это оказывается достаточно сложной проблемой в IoT из-за особенностей развертывания и мобильности. Так как IoT позволяет многие постоянные вещи отслеживать и связывать, при этом большое количество персональной информации может автоматически собираться и обрабатываться. Защита приватности в IoT становится более серьезной, чем в традиционной сети, так как количество векторов атак на устройства (вещи) IoT будет заведомо больше. Многие из существующих на данный момент технологий доступны для бытового применения и не подходят для промышленных приложений, в которых предъявляются повышенные требования по информационной безопасности. Рассматриваются механизмы реализации атак в IoT, требования по обеспечению безопасности, а также построение безопасной архитектуры и использование ключевых технологий обеспечения безопасности (механизмы шифрования, обеспечение безопасности связи и криптографические алгоритмы).

Ключевые слова: *Интернет вещей (IoT), угрозы безопасности IoT, требования безопасности, построение безопасной архитектуры, механизмы шифрования, обеспечение безопасности связи, криптографические алгоритмы.*

DOI: 10.21667/1995-4565-2020-72-25-34

Введение

Интернет вещей (англ. Internet of Things, IoT) – одна из парадигм, которая в ближайшем будущем будет иметь влияние на наше общество и уже сейчас отражается в развитии ИТ-индустрии.

Под термином «Интернет вещей» обычно подразумеваются объекты (вещи), которые могут быть взаимосвязаны и однозначно идентифицированы. В настоящее время устройства IoT могут быть идентифицированы с использованием нескольких технологий, таких как RFID, NFC, цифровой водяной знак, QR-код и других.

Интернет вещей – это взаимосвязь уникально идентифицируемых встроенных вычислительных устройств в существующей Интернет-инфраструктуре. Как правило, предполагается, что IoT предложит расширенные возможности подключения устройств, систем и сервисов, которые выходят за рамки взаимодействия между машинами (англ. Machine-to-Machine, M2M) и охватывают множество протоколов, доменов и приложений.

Вещи в IoT могут относиться к широкому спектру устройств, таких как имплантаты для мониторинга сердца, транспондеры биочипов на сельскохозяйственных животных, автомобили со встроенными датчиками или устройства для полевых операций, которые помогают спасателям при поиске и спасании.

В ближайшем будущем каждый человек будет оснащен набором умных устройств, которые будут обмениваться информацией друг с другом. Люди станут концептуально подобными кластеру данных, для которого разработчики должны быть способны обеспечить надлежащий уровень безопасности.

Проще говоря, Интернет вещей (IoT) – это любая сеть физических устройств, которые содержат встроенные технологии, обеспечивающие разную степень доступа в Интернет, связь, управление и контроль.

Подключенные физические устройства состоят как из традиционных устройств, таких как персональные компьютеры, ноутбуки и планшеты, но также включают в себя множество других нетрадиционных устройств, таких как транспортные средства, термостаты, наручные часы, производственное оборудование, медицинские устройства и многое другое.

Использование технологий для облегчения жизни дома или в офисе – огромный плюс. Однако необходимо учитывать, что с увеличением подключенных устройств также увеличивается риск возникновения угроз безопасности, что делает сети IoT более уязвимыми для различных кибер-атак и вторжений.

Обычно IoT имеет четыре основных компонента, включая считывание, обработку информации, гетерогенный доступ, приложения и услуги, а также дополнительные компоненты, обеспечивающие безопасность и конфиденциальность.

В настоящее время данная парадигма становится более известной, и благодаря этому начинают появляться различные приложения, связанные с IoT, например кибер-транспортные системы (англ. Cyber-Transportation Systems, CTS), кибер-физические системы (англ. Cyber-Physical System, CPS) и т.д.

Что касается безопасности, то IoT будет сталкиваться с более серьезными проблемами. Для этого существуют следующие причины:

1) IoT расширяет инфраструктуру передачи информации через традиционную сеть Интернет, мобильную сеть и сенсорную сеть и так далее;

2) все «вещи» IoT будут связаны Интернетом;

3) данные «вещи» будут общаться друг с другом. Поэтому возникнут новые проблемы безопасности и конфиденциальности.

При этом стоит уделять больше внимания вопросам исследований для обеспечения конфиденциальности, достоверности и целостности данных в IoT. В данном разделе будут рассмотрены различные атаки и уязвимости, связанные с парадигмой Интернета вещей, а также будут приведены рекомендации по устранению данных проблем.

Механизмы реализации атак

Первое с чего стоит начать обзор – это тип злоумышленника, который может быть заинтересован в использовании устройств IoT. Следует отметить, что данной парадигме угрожает множество участников, от киберпреступников до правительственных структур.

Причина проста: устройства IoT работают с огромным количеством информации, они распределены в каждой отрасли и, к сожалению, их текущий уровень безопасности по-прежнему остается низким.

Кибер-преступники могут быть заинтересованы в краже конфиденциальной информации путем взлома устройств IoT или могут быть заинтересованы в том, чтобы скомпрометировать их для запуска кибер-атак против, например, сторонней организации. В работе [1] авторы привели примеры злоумышленников и предоставили список наиболее актуальных угроз для Интернета вещей.

К злоумышленникам, например, можно отнести преступную команду, которая заражает миллионы маршрутизаторов или SOHO-сетей (англ. Small Office/Home Office), SmartTV и другие умные устройства по всему миру для проведения атаки с целью вымогательства или кражи данных.

Подобным же образом разведывательные управления и спецслужбы могут использовать интеллектуальные устройства, чтобы шпионить за лицами, представляющими для них некий интерес или проводить широкомасштабные кибер-атаки.

Основываясь на данных экспертов «Symantec», можно привести список основных киберугроз, связанных с Интернетом вещей, к ним относят:

Отказ в обслуживании (англ. Denial of Service, DoS) – атаки типа DDoS могут ориентироваться на все конечные точки рабочего сценария, вызывая серьезную проблему с сетью интеллектуальных устройств и парализуя предоставляемые ими услуги.

Ботнеты (англ. Botnet) и **вредоносные программы** (англ. malware) – это, вероятно, одни из наиболее распространенных и опасных сценариев. Автор вредоносного ПО специально проектирует свои коды, чтобы компрометировать архитектуры, используемые устройствами IoT. Вредоносный код может использоваться для заражения компьютеров, используемых для управления сетью умных устройств, или для компрометации программного обеспечения, запущенного на них.

Во втором случае (вредоносные программы) злоумышленники могут использовать наличие недостатков в прошивке, запущенной на устройствах, и выполнять произвольный код для незапланированного использования компонентов IoT.

В ноябре 2013 года специалисты Symantec обнаружили новый червь «Linux.Darlloz», который был специально разработан и предназначен для Интернета вещей, заражая Linux-устройства на базе Intel x86. Нападавшие скомпрометировали устройства IoT, чтобы построить бот-сеть, которая использовалась для незаконных действий, включая отправку спама, создание дорогостоящих SMS-сообщений или запуск DDoS-атаки.

Нарушения данных представляют собой еще один серьезный риск для Интернета вещей и устройств. Все организации должны знать о потенциальных непредвиденных последствиях использования IoT.

Атакующие могут следить за сообщениями между одноранговыми узлами в сети IoT и собирать информацию об услугах, которые они реализуют. Доступ к данным, доступным через Интернет, может быть использован для целей кибер-шпионажа со стороны злоумышленников или частной компании в коммерческих целях. Нарушения данных представляют собой серьезную угрозу для конфиденциальности организаций и частных лиц, которые используют умные устройства. К таким угрозам можно отнести атаки SQL-инъекций и XSS, описанные в разделах выше.

Непреднамеренные нарушения – управление данными в архитектуре, которая включает в себя устройства Интернета вещей, является критическим аспектом.

Конфиденциальная информация может быть раскрыта не только благодаря какой-либо атаке, но и может быть также случайно потеряна или открыта. В качестве примера можно представить автомобиль, умные датчики которого передают его координаты местоположения.

Ослабление периметров – устройства IoT обычно не разрабатываются с учетом безопасности. Несмотря на то, что они являются подключенными к сети Интернет, большинство из данных устройств не имеют механизмов сетевой безопасности.

Рассмотрим, например, интеллектуальные счетчики. Если злоумышленник сможет скомпрометировать данный тип устройств, то он может также получить доступ ко всей внутренней сети, шпионить за клиентом или нанести физический ущерб внутренней среде. Проблема одинаково важна, если рассматривать использование устройств IoT в любой отрасли.

Построение безопасной архитектуры

Безопасность информации и сети должна быть обеспечена такими свойствами, как идентификация, конфиденциальность, целостность и неоспоримость. В отличие от классической сети Интернет IoT будет применяться в важнейших областях народного хозяйства, таких как медицинское обслуживание и здравоохранение, интеллектуальная транспортировка, таким образом, необходимость в безопасности IoT будет выше в доступности и надежности.

В статье [2] авторами была представлена наиболее общая архитектура Интернета вещей со стороны безопасности данных и устройств. В общем, IoT можно разделить на четыре ключевых уровня. На рисунке 1 изображены уровни архитектуры IoT.

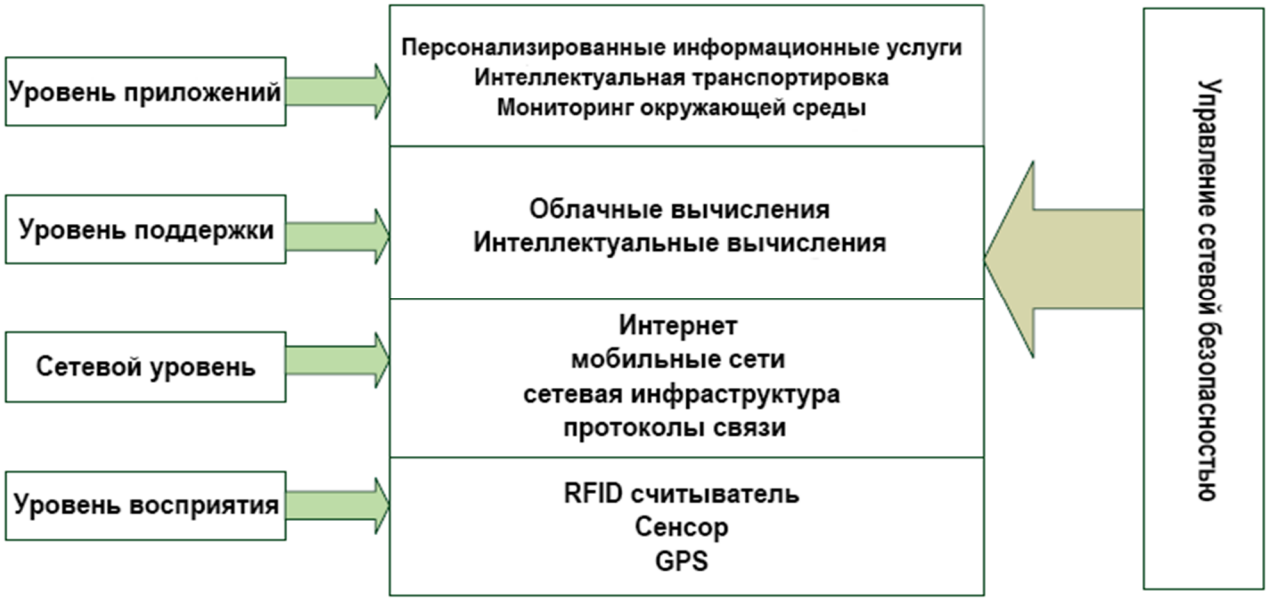

Рисунок 1 – Безопасная архитектура
Figure 1 – Secure architecture

Самый базовый уровень – это **уровень восприятия** (уровень распознавания), который собирает все виды информации через физическое оборудование и идентифицирует физический мир, информация включает в себя свойства объекта, состояние окружающей среды и т. д., физическое оборудование может включать в себя считыватель RFID, все виды датчиков, GPS и другое оборудование. Основным компонентом этого уровня являются датчики для захвата и представления информации физического мира в цифровом мире [3].

Второй уровень – это **сетевой уровень**. Сетевой уровень отвечает за надежную передачу информации с распознавательного слоя, предварительную обработку информации, классификацию и полимеризацию. В этом слое передача информации основана на нескольких базовых сетях передачи данных, таких как: сеть Интернет, беспроводная сеть, спутниковые сети, сеть мобильной связи; сетевая инфраструктура а также протоколы связи, которые необходимы для обмена информацией между устройствами [3].

Третий уровень – это **уровень поддержки**. Уровень поддержки создаёт надежную платформу поддержки для прикладного уровня, на этом уровне все виды интеллектуальных вычислительных мощностей организованы через сетевые и облачные вычисления. Он играет роль интегратора уровня приложений [3] и сетевого уровня (рисунок 1).

Уровень приложения – это самый верхний уровень. Предоставляет персонализированные услуги в соответствии с потребностями пользователей. Пользователи могут получить доступ к Интернет через интерфейс прикладного уровня, используя телевизор, персональный компьютер или мобильные устройства.

Сетевая безопасность и управление играют важную роль на каждом уровне. Далее на основе предложенной архитектуры будут проанализированы основные требования безопасности.

Требования безопасности

Уровень распознавания

Обычно распознавательным узлам необходимы невысокие мощности компьютера и емкости хранилища, потому что они просты и предполагают работу на низких мощностях. Поэтому к ним нет возможности применять механизмы прыгающих частот и алгоритм шифро-

вания с открытым ключом для обеспечения безопасности и очень сложно настроить различные системы защиты.

Между тем атаки из внешней сети, такие как отказ в обслуживании (англ. denial-of-service-DoS), также приводят к новым проблемам безопасности. С другой стороны, данные датчика также нуждаются в защите целостности, конфиденциальности и подлинности. В статье [4] авторы описали некоторые аспекты безопасности устройств распознавания, из которых можно выделить следующее.

Первое: для аутентификации узла необходимо предотвратить незаконный доступ к самому узлу.

Второе: для защиты конфиденциальности передачи информации между узлами шифрование данных является абсолютной необходимостью.

Третье: чем сильнее меры безопасности, тем больше потребление ресурсов, для решения этой проблемы важна легкая технология шифрования, которая включает в себя легкий криптографический алгоритм и легкий криптографический протокол [3]. В то же время целостность и достоверность данных датчиков становятся предметом научных исследований, этот вопрос будет подробно рассмотрен в следующем разделе.

Сетевой уровень

Несмотря на то, что базовая сеть обладает относительно полной защитой, но атаки по типу «Человек посередине» (англ. Man in the middle, MITM) и поддельные атаки имеют место, между тем нежелательную почту и компьютерные вирусы также нельзя игнорировать, таким образом, большое количество передачи данных вызывает перегрузку. Поэтому механизм безопасности на данном уровне очень важен для IoT. В статье [5] авторы рассмотрели пути развития безопасности Интернета вещей на сетевом уровне.

На данном уровне трудно применять существующие механизмы обеспечения безопасности сети. Подлинность идентификации представляет собой своего рода механизм предотвращения подключения несанкционированных узлов, и это является предпосылкой для механизма безопасности.

Конфиденциальность и целостность имеют одинаковую важность, поэтому необходимо установить механизмы конфиденциальности данных и их целостность.

Кроме того, распределенная атака типа «отказ в обслуживании» (англ. DDoS) является распространенным методом атаки в сети и является наиболее серьезной в IoT, таким образом, для предотвращения атаки типа DDoS для уязвимого узла необходимо решить еще одну проблему на данном уровне.

Уровень поддержки

На данном уровне выполняются массовая обработка данных и интеллектуальные решения поведения сети. Интеллектуальная обработка ограничена для вредоносной информации, поэтому основная сложность заключается в улучшении возможности распознавания вредоносной информации [2, 6].

Данный уровень поддержки нуждается в большом количестве средств для защиты и безопасности приложений, таких как безопасные облачные вычисления и безопасные многосторонние вычисления, сильные алгоритмы шифрования и протоколы шифрования [3], более мощные системы и технологии безопасности и антивирусы.

Уровень приложения

На этом уровне потребности в безопасности для разных прикладных сред различны, а обмен данными – это одна из характеристик уровня приложения, которая создает проблемы конфиденциальности данных, контроля доступа и раскрытия информации. В статье [7] были рассмотрены решения для защиты IoT на уровне приложений.

Для решения проблемы безопасности прикладного уровня необходимы два аспекта. Один из них – это соглашение об аутентификации и ключах в гетерогенной сети, другое –

защита конфиденциальности пользователя. Кроме того, обучение и управление очень важны для информационной безопасности, особенно для управления паролями.

В целом технология безопасности в IoT очень важна и полна различных проблем. По данным приведенного выше анализа, можно просуммировать требования безопасности для каждого из уровней (см. рисунок 2).

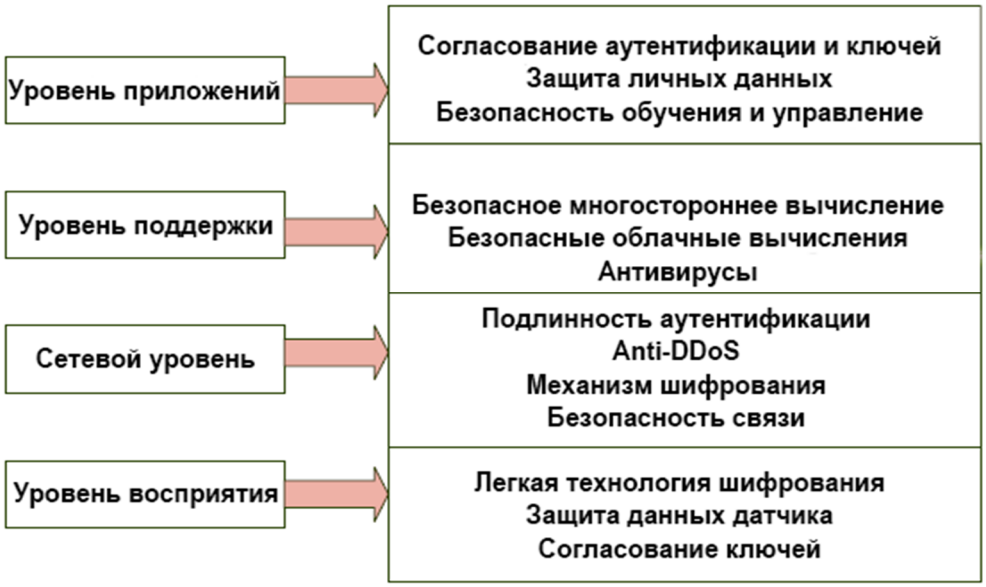

Рисунок 2 – Требования безопасности на каждом уровне
Figure 2 – Security requirements at each level

Состояние ключевых технологий обеспечения безопасности

Исходя из описанных ранее требований безопасности, рассмотрим состояние выявленных механизмов и технологий, приведём более подробную информацию о механизмах шифрования, безопасности связи, защите данных датчиков и криптографическом алгоритме.

Механизмы шифрования

В традиционном сетевом слое используется механизм шифрования «Hop-by-Hop (HbH)», таким образом, информация зашифровывается в процессе передачи, но она должна сохранять открытый текст в каждом узле посредством операций дешифрования и шифрования.

Между тем в традиционном алгоритме шифрования на уровне приложений есть шифрование «End-to-End» (E2EE), то есть информация доступна только для отправителя и получателя, а в процессе передачи и узлах пересылки она будет всегда зашифрована. В статье [8] авторы рассмотрели механизмы шифрования данных в IoT и описали их недостатки.

В IoT сетевой уровень и уровень приложений достаточно тесно связаны, поэтому необходимо выбирать между HbH и сквозным E2EE шифрованием. Если мы применим шифрование по Hop-by-Hop, мы можем зашифровать только те ссылки, которые нуждаются в защите. Таким образом, на сетевом уровне мы можем применить его ко всем бизнесам, которые обеспечивают безопасное внедрение различных приложений.

Механизм безопасности прозрачен для бизнес-приложений, что дает конечным пользователям удобство. В то же время это приводит к особенностям полноценной игры HbH, такой как низкая латентность, высокая эффективность, низкая стоимость и т. д.

Однако из-за операции расшифровки в узле передачи, используя шифрование «Hop-by-Hop», каждый узел может получить незашифрованное текстовое сообщение, поэтому шифрование «Hop-by-Hop» требует высокого доверия к узлам передачи.

Используя сквозное шифрование (E2EE), можно выбрать другую политику безопасности в соответствии с типом бизнеса. Таким образом, она может обеспечить защиту высокого уровня безопасности для требований высокой безопасности бизнеса.

Однако сквозное шифрование не может шифровать адрес назначения, поскольку каждый узел определяет, как передавать сообщения в соответствии с адресом получателя. Это приводит к тому, что он не может скрыть источник и место назначения передаваемого сообщения и при этом вызвать вредоносные атаки.

С помощью приведённого выше анализа механизмов шифрования можно сделать вывод: когда требования к безопасности какого-либо бизнеса не очень высоки, можно использовать шифрование «Hop-by-Hop»;

Когда бизнес нуждается в высокой безопасности, тогда «End-to-End» шифрование является основным решением.

Таким образом, в соответствии с различными требованиями производится выбор альтернативного механизма шифрования. В настоящее время IoT развивается и находится только на начальном этапе, исследование механизма безопасности требует проверки эффективности на практике, поэтому предстоит пройти долгий путь для исследования этой области.

Обеспечение безопасности связи

Сначала в протоколах связи устанавливаются некоторые решения, которые могут обеспечить целостность, достоверность и конфиденциальность связи, например TLS/SSL или IPSec.

TLS/SSL предназначен для шифрования связи на транспортном уровне, а IPSec предназначен для защиты безопасности сетевого уровня, они могут обеспечить целостность и конфиденциальность на каждом уровне [9].

Механизмы безопасности связи достаточно редко применяются в настоящее время. Поскольку на небольших устройствах IoT меньше вычислительной мощности, это приводит к тому, что безопасность связи часто слабая.

Между тем в IoT основная сеть всегда является текущим или следующим поколением Интернета, при этом большая часть информации будет передаваться через каналы сети Интернет.

Таким образом, DDoS все еще существует и представляет собой очень серьезную проблему. Различные бот-сети и DDoS атаки будут уничтожать доступность связи [10]. Когда происходят организованные атаки DDoS, создать метод аварийного восстановления очень важно, поэтому необходимо уделять больше внимания поиску более эффективных предупредительных мер и механизмов аварийного восстановления.

Криптографические алгоритмы

В современных сетях существует известный и достаточно доверенный набор криптографических алгоритмов, применяемых к протоколам безопасности сети Интернет, самые известные представлены в таблице 1. Данный набор может с успехом использоваться и для обеспечения безопасности в Интернете вещей.

• Обычно для шифрования данных используется симметричный алгоритм шифрования, чтобы обеспечить конфиденциальность, например, такой как расширенный стандарт шифрования блочного шифрования AES.

• Для цифровой подписи и передачи ключей часто применяется асимметричный алгоритм, например, такой как алгоритм RSA.

• Для согласования ключей используется алгоритм соглашения с асимметричным ключом DH.

• Для целостности будут применены алгоритмы безопасного хэша SHA-1 и SHA-256.

Набор криптографических алгоритмов
Set of cryptographic algorithms

Алгоритм	Назначение
Advanced Encryption Standard (AES)	Конфиденциальность
RSA/Elliptic-curve cryptography (ECC)	Передача ключей цифровых подписей
Diffie-hellman (DH)	Согласование ключей
SHA-1/SHA-256	Целостность

Другой важный асимметричный алгоритм, также известный как эллиптическая криптография (ECC), может обеспечить одинаковую безопасность с использованием ключа меньшей длины [11]. Криптография на эллиптических кривых применяется в современных Web технологиях, таких как в TLS, PGP и SSH, поэтому использование ECC может стать хорошей заменой DH и RSA.

Для реализации всех описанных криптографических алгоритмов необходимы доступные ресурсы, такие как скорость процессора и память. Так как применение этих криптографических методов для IoT до конца не ясно, исследователи должны прилагать больше усилий для дальнейшего развития, чтобы убедиться, что алгоритмы могут быть успешно реализованы с использованием ограниченной памяти и низкой скорости процессора в IoT.

Выводы

Большое распространение современных технологий Интернета вещей будет во многих аспектах базироваться на информационной безопасности, а также защите конфиденциальности данных. Это оказывается достаточно сложной проблемой в IoT из-за особенностей развертывания и мобильности.

Многие из существующих на данный момент технологий могут быть применены для бытового использования, но не подходят для коммерческих приложений, в которых предъявляются повышенные требования по информационной безопасности.

Существующие технологии шифрования, заимствованные из WSN (беспроводной сенсорной сети) и других сетей, должны быть тщательно проанализированы перед тем, как их применять для защиты информации в Интернете вещей. В статье [12] авторы привели некоторые примеры IoT систем, рассматривая которые, можно выделить некоторые важные аспекты.

Так как IoT позволяет многие вещи отслеживать и связывать, при этом большое количество персональной информации может автоматически собираться и обрабатываться.

Защита приватности в IoT становиться более серьезной, чем в традиционной сети, так как количество векторов атак на устройства (вещи) IoT, будет заведомо больше.

К примеру, датчик мониторинга здоровья собирающий данные пациента, например частоту сердечных сокращений и уровень сахара в крови, после отправляет информацию непосредственно на устройство врача по сети. При этом она может быть похищена и использована в целях злоумышленника.

Другим примером можно считать биодатчик, используемый в пищевой промышленности. Он может применяться для мониторинга каких-либо характеристик продуктов питания (температура, влажность, бактериальный состав и т.д), хранящихся в холодильнике. Когда что-то портится, данные об этом отправляются в компанию через сеть.

Таким образом, подобная информация должна быть строго конфиденциальной, чтобы защитить репутацию компании. Стоит отметить, что некоторые вопросы, такие как определение конфиденциальности в IoT, по-прежнему однозначно не определены. Несмотря на то, что уже существуют сетевые технологии безопасности, для обеспечения конфиденциальности и безопасности в IoT предстоит проделать еще много работы.

В частности, необходимо исследовать следующие аспекты:

1) определение безопасности и конфиденциальности с социальной, правовой и культурной точек зрения;

2) защита сервисов и приложений;

3) механизм доверия и репутации;

4) конфиденциальность переписки и данных пользователя;

5) безопасность связи – в том числе сквозное шифрование (end-to-end).

Библиографический список

1. **Ammar M., Russello G., Crispo B.** Internet of Things: A survey on the security of IoT frameworks. (2018) Journal of Information Security and Applications, vol. 38, pp. 8-27. DOI: 10.1016/j.jisa.2017.11.002.

2. **Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F.** Internet of Things security: A survey. (2017) Journal of Network and Computer Applications, vol. 88, pp. 10-28. DOI: 10.1016/j.jnca.2017.04.002.

3. **Taha M. Alfaqih, Jalal Al-Muhtadi**. Internet of Things Security based on Devices Architecture: International Journal of Computer Applications (0975 – 8887), vol. 133, no.15, January 2016.

4. **Khan M. A., Salah K.** IoT security: Review, blockchain solutions, and open challenges. (2017) Future Generation Computer Systems, In Press, pp. 1-36. DOI: 10.1016/j.future.2017.11.022.

5. **Zhou B., Zhang Q., Shi Q., Yang Q., Yang P., Yu Y.** Measuring web service security in the era of Internet of Things. (2017) Computers and Electrical Engineering, In Press, pp. 1-11. DOI: 10.1016/j.compeleceng.2017.06.020.

6. **Stergiou C., Psannis K. E., Kim B. -G., Gupta B.** Secure integration of IoT and Cloud Computing. (2018) Future Generation Computer Systems, vol. 78, part 3, pp. 964-975. DOI: 10.1016/j.future.2016.11.031.

7. **Zarpelão B. B., Miani R. S., Kawakani C. T., de Alvarenga S. C.** A survey of intrusion detection in Internet of Things. (2017) Journal of Network and Computer Applications, vol. 84, pp. 25-37. DOI: 10.1016/j.jnca.2017.02.009.

8. **Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A.** Security, privacy and trust in Internet of things: The road ahead. (2015) Computer Networks, vol. 76, pp. 146-164. DOI: 10.1016/j.comnet.2014.11.008

9. **Conti M., Dehghantanha A., Franke K., Watson S.** Internet of Things security and forensics: Challenges and opportunities. (2018) Future Generation Computer Systems, vol. 78, part 2, pp. 544-546. DOI: 10.1016/j.future.2017.07.060.

10. **Sahmim S., Gharsellaoui H.** Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: A review. (2017) Procedia Computer Science, vol. 112, pp. 1516-1522. DOI: 10.1016/j.procs.2017.08.050.

11. **Weber R. H., Studer E.** Cybersecurity in the Internet of Things: Legal aspects. (2016) Computer Law and Security Review, vol. 32, no. 5, pp. 715-728. DOI: 10.1016/j.clsr.2016.07.002

12. **Liu C.** Securing networks in the internet of things era. (2015) Computer Fraud & Security, vol. 2015, no. 4, pp. 13-16. DOI: 10.1016/S1361-3723(15)30028-2.

UDC 004.056.53

MODELS AND TECHNOLOGIES OF INTERNET OF THINGS SECURE NETWORK CONSTRUCTION

S. A. Lesko, Ph.D. (Tech.), associate professor of KB-3 department «System Control and Modeling» RTU MIREA, Moscow, Russia;
orcid.org/0000-0002-6641-1609, e-mail: sergey@testor.ru
D. O. Zhukov, Dr. Sc. (Tech.), KB-8 «Information Confrontation» Department, RTU MIREA, Moscow, Russia;
orcid.org/0000-0002-1211-5214, e-mail: zhukovdm@yandex.ru
P. Yu. Pushkin, Ph.D. (Tech.), Head of KB-3 «System Control and Modeling» Department, RTU MIREA, Moscow, Russia;
orcid.org/0000-0003-3684-550X, e-mail: is-irk@mail.ru

The widespread adoption of modern Internet of Things (IoT) technologies will largely be based on information security, as well as protecting data privacy. This turns out to be a rather complicated problem in IoT due to the deployment and mobility features. Since IoT allows many persistent things to be tracked and linked, a large amount of personal information can be automatically collected and processed. Protection of privacy in IoT will become more serious than in a traditional network, since the number of vectors of attacks on IoT devices (things) will be knowingly greater. Many of the existing technologies at the moment are available for domestic use, and are not suitable for industrial applications, in which high demands are placed on information security.

The article discusses the mechanisms for implementing attacks in IoT, security requirements, as well as the construction of a secure architecture and the use of key security technologies (encryption mechanisms, communication security and cryptographic algorithms).

Keywords: *Internet of Things (IoT), IoT security threats, security requirements, building a secure architecture, encryption mechanisms, ensuring communication security, cryptographic algorithms.*

DOI: 10.21667/1995-4565-2020-72-25-34

References

1. **Ammar M., Russello G., Crispo B.** Internet of Things: A survey on the security of IoT frameworks. (2018) *Journal of Information Security and Applications*, vol. 38, pp. 8-27. DOI: 10.1016/j.jisa.2017.11.002.

2. **Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F.** Internet of Things security: A survey. (2017) *Journal of Network and Computer Applications*, vol. 88, pp. 10-28. DOI: 10.1016/j.jnca.2017.04.002.

3. **Taha M. Alfaqih, Jalal Al-Muhtadi**. Internet of Things Security based on Devices Architecture: *International Journal of Computer Applications* (0975 – 8887), vol. 133, no.15, January 2016.

4. **Khan M. A., Salah K.** IoT security: Review, blockchain solutions, and open challenges. (2017) *Future Generation Computer Systems, In Press*, pp. 1-36. DOI: 10.1016/j.future.2017.11.022.

5. **Zhou B., Zhang Q., Shi Q., Yang Q., Yang P., Yu Y.** Measuring web service security in the era of Internet of Things. (2017) *Computers and Electrical Engineering, In Press*, pp. 1-11. DOI: 10.1016/j.compeleceng.2017.06.020.

6. **Stergiou C., Psannis K. E., Kim B. -G., Gupta B.** Secure integration of IoT and Cloud Computing. (2018) *Future Generation Computer Systems*, vol. 78, part 3, pp. 964-975. DOI: 10.1016/j.future.2016.11.031.

7. **Zarpelão B. B., Miani R. S., Kawakani C. T., de Alvarenga S. C.** A survey of intrusion detection in Internet of Things. (2017) *Journal of Network and Computer Applications*, vol. 84, pp. 25-37. DOI: 10.1016/j.jnca.2017.02.009.

8. **Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A.** Security, privacy and trust in Internet of things: The road ahead. (2015) *Computer Networks*, vol. 76, pp. 146-164. DOI: 10.1016/j.comnet.2014.11.008

9. **Conti M., Dehghantanha A., Franke K., Watson S.** Internet of Things security and forensics: Challenges and opportunities. (2018) *Future Generation Computer Systems*, vol. 78, part 2, pp. 544-546. DOI: 10.1016/j.future.2017.07.060.

10. **Sahmim S., Gharsellaoui H.** Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: A review. (2017) *Procedia Computer Science*, vol. 112, pp. 1516-1522. DOI: 10.1016/j.procs.2017.08.050.

11. **Weber R. H., Studer E.** Cybersecurity in the Internet of Things: Legal aspects. (2016) *Computer Law and Security Review*, vol. 32, no. 5, pp. 715-728. DOI: 10.1016/j.clsr.2016.07.002

12. **Liu C.** Securing networks in the internet of things era. (2015) *Computer Fraud & Security*, vol. 2015, no. 4, pp. 13-16. DOI: 10.1016/S1361-3723(15)30028-2.