Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Направление подготовки: 10.03.01 Информационная безопасность

Образовательная программа: "Технологии защиты информации"

Дисциплина:

«Основы теории надежности»

РЕФЕРАТ

«Оценка безопасности в контексте интернета вещей (IoT)»

Выполнили:

Чу Ван Доан, студент группы номер группы

(подпись)

Проверил:

Мухамеджанов Санжар, преподаватель ФБИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Введение

В последние несколько лет термин «Интернет вещей» (IoT) получил широкое распространение и вызвал значительный интерес у технологического сообщества. IoT — это система, в которой каждому объекту присваивается уникальный идентификатор и обеспечивается возможность передачи и обмена информацией и данными через единую сеть. Взрывной рост Интернета, расширение рынка мобильных технологий, программного обеспечения и встроенных систем стали мощным драйвером развития IoT. По прогнозам Statista, к 2025 году количество устройств, подключённых к Интернету по всему миру, достигнет 75,44 миллиарда. Рост в основном обусловлен развитием Интернета вещей, включающего такие устройства, как датчики, умная бытовая техника, транспортные средства и промышленное оборудование. При этом IoT-устройства занимают значительную долю от общего числа подключённых устройств. Очевидно, что IoT уже играет и будет играть важную роль в формировании информационного общества настоящего и будущего.

Тем не менее, сложная экосистема IoT содержит множество уязвимостей в безопасности, которые могут быть использованы злоумышленниками и непосредственно повлиять на личные данные пользователей. Недавнее исследование OWASP (Open Web Application Security Project) показало, что 75% IoT-устройств, включая интегрированные в автономный транспорт, системы видеонаблюдения и «умные» дома, подвержены риску атак хакеров и взлома. Традиционные методы защиты, такие как IPSec, PKI и механизм обмена ключами Диффи-Хеллмана, требуют больших вычислительных ресурсов и не подходят для интеграции в IoT-устройства, ограниченные по производительности, энергопотреблению и объёму памяти. Кроме того, неоднородность стандартов протоколов и инфраструктуры между производителями создаёт значительные трудности при построении комплексных решений безопасности для современных IoT-сетей.

Целью данной работы является предоставление наиболее полного обзора IoT, рассмотрение вопросов безопасности, связанных с компонентами системы, включая конечные устройства, маршрутизацию, коммутацию и облачные вычисления, а также анализ вызовов, которые предстоит решить в будущем, с целью повышения осведомлённости технологического сообщества.

Ход работы

1. Обзор Интернета вещей (IoT)

На сегодняшний день Интернет вещей (IoT) утвердил свои позиции благодаря слиянию множества технологий, включая плотное распространение беспроводной передачи данных, анализ данных в реальном времени, машинное обучение, сенсоры для отслеживания объектов и встроенные системы. Это означает, что все формы классических встроенных систем, такие как беспроводные сенсорные сети, системы управления, автоматизация (включая умный дом и автоматизацию зданий) и прочее, вносят свой вклад в функционирование IoT.

1.1. Архитектура системы IoT

Общая архитектура IoT включает четыре основных компонента, как показано на Рисунке 1. Объекты, подключённые к Интернету (Things), — это устройства, способные подключаться, передавать информацию и выполнять заданные функции, такие как часы, смартфоны, бытовая техника, осветительные приборы, измерители энергии или сенсоры для сбора различных данных. Шлюзы (Gateway) играют роль промежуточной станции, обеспечивая защищённое и удобное управление соединением между объектами и облачными вычислениями. Другими словами, шлюз — это окно внутренней IoT-системы во внешний мир. Для передачи данных используются технологии GSM, GPRS, оптоволокно и другие интернет-технологии.

Сетевая инфраструктура и облачные вычисления (Network and Cloud): сетевая инфраструктура включает маршрутизаторы (Router), коммутаторы (Switch), ретрансляторы (Repeater) и другие устройства для управления потоками данных, которые подключены к телекоммуникационным сетям и развернуты провайдерами услуг. Центры обработки данных и облачная инфраструктура состоят из большого количества серверов, систем хранения данных и виртуальных сетей. Беспроводные технологии, такие как Bluetooth, Smart, Zigbee, subGhz и Wi-Fi, обеспечивают связь между устройствами или между устройствами и Интернетом.

Системы управления используются для мониторинга IoT-сетей с помощью беспроводных технологий, это могут быть специализированные устройства, такие как пульты дистанционного управления (Remote), смартфоны (Smartphone) и планшеты (Tablet).

Слои создания и предоставления сервисов (Services-Creation and Solutions Layers) включают API (Application Programming Interface), которые поддерживают управление, анализ данных и эффективное быстрое использование имеющихся системных ресурсов.

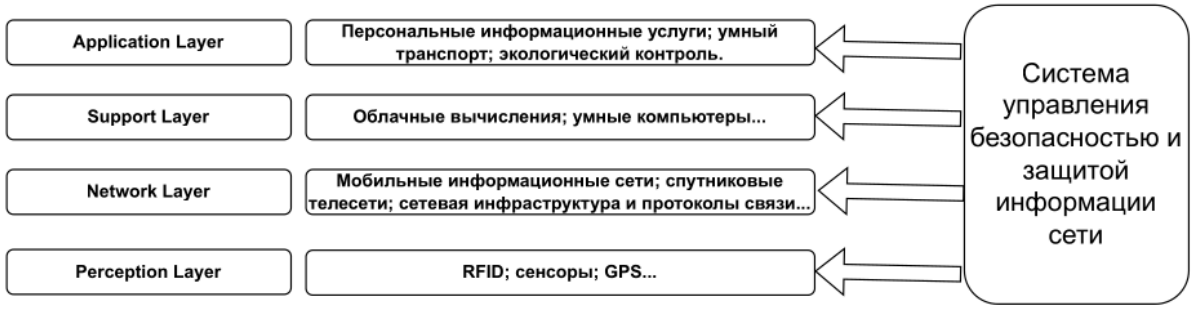

Рисунок 1 – Модель архитектуры безопасности в IoT

1.2. Архитектура безопасности в IoT

Как и в других традиционных системах, конечной целью безопасности в IoT является обеспечение конфиденциальности, целостности, доступности, аутентичности данных и информации. В этой системе архитектура безопасности IoT может быть разделена на четыре основных части с разными требованиями, как показано на модели на Рисунке 2, для поддержания безопасности и защиты информации пользователей.

Уровень восприятия собирает информацию о свойствах объектов и условиях окружающей среды с помощью сенсорных устройств. Требования безопасности на этом уровне включают аутентификацию (Authentication), которая предотвращает несанкционированный доступ к IoT-системе; шифрование (Encryption), обеспечивающее конфиденциальность при передаче информации; и согласование ключей (Key agreement), которое выполняется до шифрования для предоставления расширенных возможностей сетевой безопасности. Легковесные ключи могут использоваться для оптимизации использования ресурсов и повышения производительности системы.

Сетевой уровень передает информацию на основе базовой сетевой инфраструктуры, такой как Интернет, мобильные коммуникационные сети, спутниковая связь, беспроводные сети и коммуникационные протоколы. Текущие механизмы безопасности сложно применимы к этому уровню. Основная причина — IoT-устройства имеют низкое энергопотребление, подвержены деградации и обладают ограниченными вычислительными ресурсами, что затрудняет обработку алгоритмов с высокой сложностью.

Уровень поддержки организован по-разному в зависимости от предоставляемых услуг, таких как разгрузка и обработка данных. Уровень поддержки может включать промежуточное программное обеспечение (Middleware), M2M (Machine to Machine) или облачные платформы. Большинство криптографических протоколов, методов безопасности и анализа вредоносного ПО реализуются именно на этом уровне.

Уровень приложений формирует пользовательские приложения. Для решения вопросов безопасности на этом уровне необходимо уделять внимание двум аспектам: аутентификации и асимметричному согласованию ключей по сети; защите конфиденциальности пользователей. Кроме того, вопросы управления, такие как управление паролями, также требуют особого внимания.

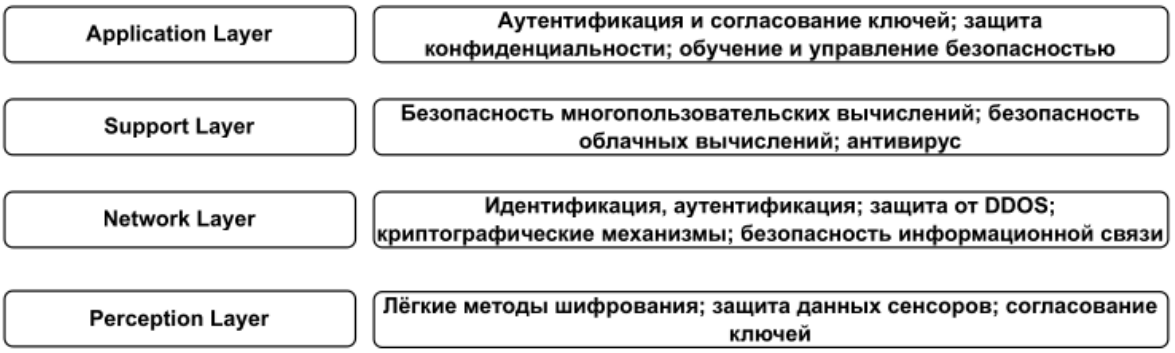

Рисунок 2 – Модель архитектуры безопасности в IoT

2. Механизмы безопасности и вызовы в области защиты информации в IoT

Наряду с активным развитием IoT, вопросы безопасности приобретают всё более важное значение для обеспечения защиты информации клиентов и предотвращения несанкционированного управления устройствами. Основываясь на архитектурной модели IoT, в этой части статьи представлены современные решения в области безопасности, а также выявлены существующие проблемы и вызовы, призванные повысить максимальную эффективность защиты и удобство как для производителей, так и для пользователей.

2.1. Методы шифрования

Основное требование к системе безопасности — обеспечить надёжное шифрование информации, которое сложно взломать. Для этого используются алгоритмы с высокой степенью сложности, при этом необходимо учитывать производительность устройств. Наиболее распространёнными являются симметричное и асимметричное шифрование.

Некоторые современные системы безопасности комбинируют оба метода, чтобы использовать их преимущества.

Симметричное шифрование (Symmetric Encryption), такое как AES (Advanced Encryption Standard), Triple DES (Triple Data Encryption Algorithm) или IDEA (International Data Encryption Algorithm), использует один общий секретный ключ. Его преимущество — меньшая вычислительная нагрузка, что подходит для устройств с низкими характеристиками. Однако уровень безопасности симметричного шифрования сравнительно невысок.

Асимметричное шифрование (Asymmetric Encryption) использует пару ключей — публичный и приватный. Публичный ключ применяется для шифрования, а приватный — для расшифровки. Асимметричные алгоритмы, например RSA, имеют значительно большую вычислительную сложность и нагрузку по сравнению с симметричными.

Алгоритм обмена ключами Диффи-Хеллмана позволяет установить общий секретный ключ для шифрования данных по незащищённому каналу связи.

Таблица 1. Сравнение симметричного и асимметричного шифрования

Характеристика ключа	Симметричное шифрование	Асимметричное шифрование
Особенности ключа	Используется один общий ключ для процесса шифрования и расшифровки.	Если для шифрования используется публичный ключ, то для расшифровки применяется приватный ключ и наоборот.
Преимущества	Быстрая скорость шифрования и расшифровки. Использование простого ключа.	Более высокая безопасность по сравнению с симметричным шифрованием.
Ограничения	Трудности с выбором, распределением и хранением доверенных ключей. Решение «согласования» секретного ключа небезопасно. Не подходит для аутентификации или предотвращения отказов.	Большая вычислительная нагрузка при шифровании и расшифровке. Медленная скорость шифрования, высокая стоимость. Уязвимость к атакам на публичный ключ.

Таблица 2. Сравнение некоторых основных алгоритмов симметричного и асимметричного шифрования

Алгоритм	Преимущества	Ограничения
AES (Advanced Encryption Standard): AES — это блочный шифр с ключами длиной 128, 192 или 256 бит.	Высокая скорость выполнения, низкое потребление ресурсов. AES имеет чёткую математическую модель и структуру. Входит в группу стандартов информационной безопасности.	AES недостаточно защищён от атак через боковой канал (side channel attack). Математическая структура AES достаточно проста.
Triple DES (Triple Data Encryption Algorithm): DES — блочный симметричный шифр с блоком 64 бита и ключом 56 бит, 3DES использует три ключа DES.	Triple DES более широко используется благодаря тройному выполнению DES, что увеличивает сложность и длину ключа. Следовательно, размер ключа и безопасность выше.	Хотя считается надёжным на практике, с теоретической точки зрения алгоритм может быть взломан.
IDEA (International Data Encryption Algorithm): Симметричный блочный шифр с ключом 128 бит и блоком данных 64 бита.	IDEA удовлетворяет трём основным требованиям безопасности: (1) безопасность ключа; (2) длина ключа; (3) сложность алгоритма.	Алгоритм может быть теоретически взломан.
RSA (Rivest-Shamir-Adleman): Надёжный асимметричный алгоритм с публичным и приватным ключами.	В VPN соединениях RSA часто используется для шифрования "session key", что упрощает и защищает обмен секретными ключами и обеспечивает целостность данных.	Скорость шифрования и дешифрования низкая. Этот недостаток снижает безопасность ключей, если открытые ключи используются в изоляции.
Diffie-Hellman: Асимметричный алгоритм, устанавливающий общий секретный ключ для безопасного обмена данными по незащищённому каналу путём создания общего приватного ключа.	При правильном управлении ключами алгоритм защищает от атак, таких как раскрытие ключа; операции с публичными и приватными ключами ограничены.	Возможность найти секретный ключ существует. Связь между ключами и параметрами алгоритма позволяет расшифровывать без знания ключа.

В современных системах информационная безопасность реализуется на основе двух механизмов: End-to-End (E2E) и By-Hop. В механизме E2E (обычно применяется на уровне приложений) шифрование и расшифровка выполняются только отправителем и получателем. В механизме By-Hop (чаще используется на сетевом уровне) шифрование и

расшифровка происходят на каждом отдельном участке передачи данных. В среде IoT сетевой и прикладной уровни тесно связаны между собой. Обычно E2E применяется для задач с высокими требованиями к безопасности, а By-Hop может обеспечить безопасность на более низком уровне.

2.2. Безопасность информационной связи

Коммуникационный уровень обеспечивает безопасную передачу и приём данных независимо от того, на каком уровне происходит передача — физическом (Wi-Fi, 802.15.4 или Ethernet), сетевом (IPv6, Modbus или OPC-UA) или прикладном (MQTT, CoAP, веб-сокеты). Используемые решения безопасности на этом уровне включают:

1. Центрированные на данных (data-centric) методы защиты, обеспечивающие надёжное шифрование данных как при передаче, так и в состоянии покоя, так что даже в случае перехвата данные могут быть расшифрованы только обладателями корректных ключей;
2. Использование межсетевых экранов и систем предотвращения вторжений, предназначенных для проверки конкретных потоков трафика на конечных устройствах.

Некоторые вопросы безопасности, требующие внимания на этом уровне:

- Установка соединения с облаком: Открытие портов межсетевого экрана требуется только при подключении к определённому сервису. Устройства управляются удалённо через двунаправленный канал связи с облаком. Рассматривается возможность использования виртуальных частных сетей (VPN) для доступа к IoT-устройствам, что также предполагает разрешение для сервисов, пользователей или других сетей воздействовать на внутренние ресурсы сети.
- Безопасность сообщений: Низкоуровневые протоколы на основе сообщений хорошо подходят для IoT-устройств и предусматривают такие опции, как двойное шифрование (Double Encrypt), упорядочивание, фильтрация и даже совместное использование с третьими сторонами. Точное маркирование позволяет каждому сообщению обрабатываться в соответствующем режиме безопасности. Передача сообщений с контролем доступа и обеспечением безопасности сообщений является необходимым решением на коммуникационном уровне IoT.

Для противодействия вызовам безопасности IoT соблюдение этих основных принципов как на уровне сенсорных устройств, так и на коммуникационном уровне поможет снизить риски для базовой архитектуры систем безопасности IoT в будущем.

TLS/SSL и IPSec — два наиболее распространённых протокола, используемых для обеспечения таких требований безопасности, как целостность (информация не изменяется в процессе передачи), аутентичность (получатель может подтвердить источник информации) и конфиденциальность (данные шифруются для защиты от прослушивания). В модели TCP/IP TLS/SSL расположены между транспортным и прикладным уровнями, тогда как IPSec реализует безопасность на уровне Интернета.

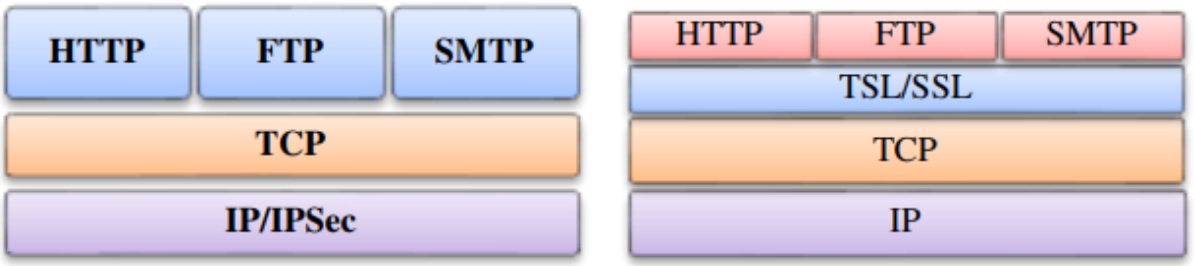

Рисунок 3 – Модель безопасности IPsec и TLS/SSL

TLS/SSL — это не единый протокол, а набор стандартизированных процедур, предназначенных для выполнения таких задач, как проверка подлинности выданных сертификатов и обеспечение безопасности информации при обмене между сервером и клиентом. Кроме того, для гарантии целостности данных применяются хеш-алгоритмы.

Некоторые алгоритмы шифрования и аутентификации в SSL включают DES, Triple DES, DSA (Digital Signature Algorithm), KEA (Key Exchange Algorithm), MD5 (Message Digest Algorithm), RSA (алгоритм, разработанный Ривестом, Шамиром и Адлеманом), RC2, RC4 и SHA-1 (Secure Hash Algorithm). Выбор подходящего алгоритма шифрования для SSL-сессии осуществляется в процессе установления соединения (handshake) между сервером и клиентом.

Примеры приложений, использующих TLS/SSL, включают NSIIOP, HTTP, FTP, Telnet, IMAP, IRC и POP3, как показано на рисунке 4.

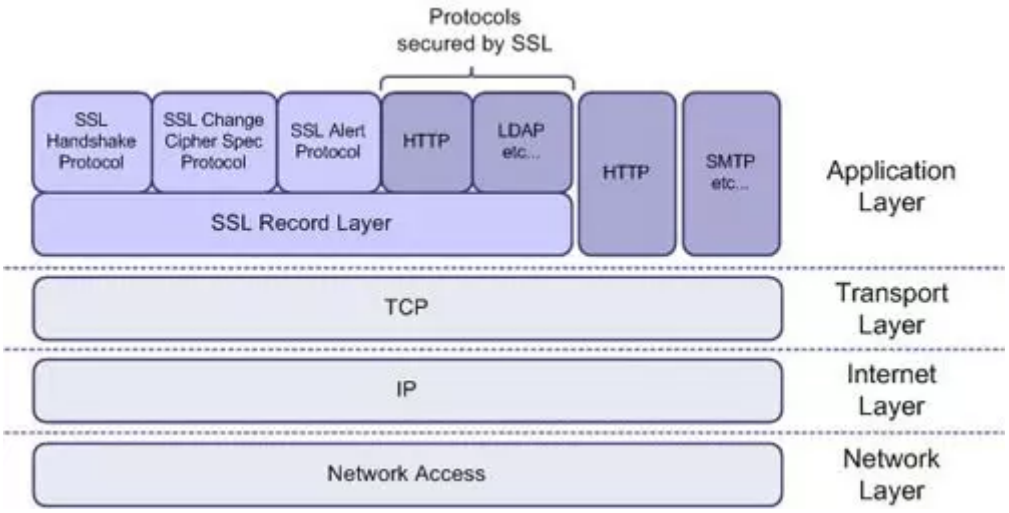

Рисунок 4 – Структурная модель TLS/SSL

IP Security (IPSec) — это протокол, стандартизированный IETF (Internet Engineering Task Force) с 1998 года, предназначенный для повышения механизмов шифрования и аутентификации информационных потоков, передаваемых по сети с использованием протокола IP. Как показано на Рисунке 5, IPSec можно рассматривать как расширение протокола IP, реализуемое одинаково для версий IPv4 и IPv6. Для IPv4 применение IPSec является опциональным, тогда как для IPv6 этот протокол безопасности обязателен.

IPSec в основном основан на алгоритмах симметричного шифрования. Помимо общих требований, важным условием для IPSec является обеспечение уникальности каждого получаемого и отправляемого пакета данных.

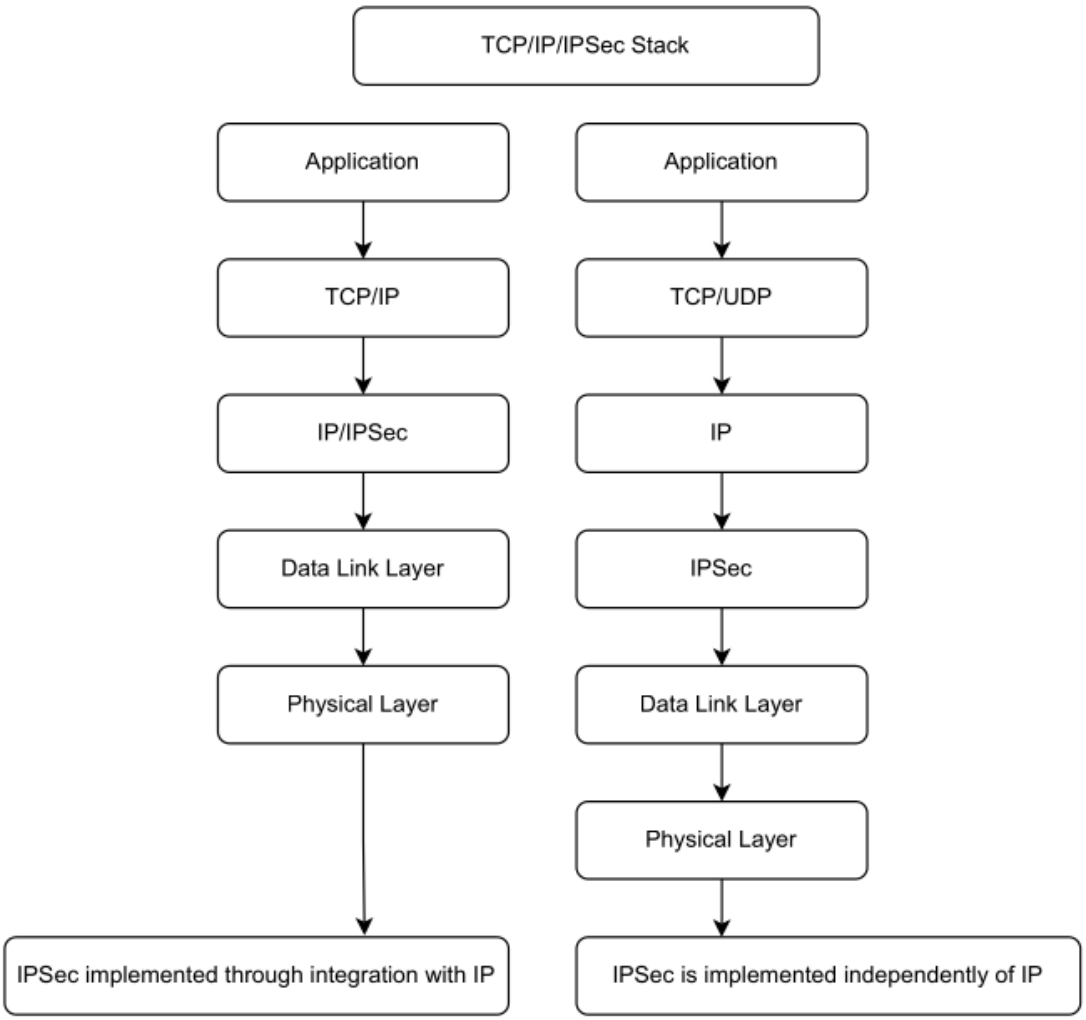

Рисунок 5 – Модель приложения IPSec в TCP/IP

2.3. Безопасность данных сенсоров

Самая важная задача сенсорного уровня — обеспечить конфиденциальность пользователей. Конфиденциальность достигается на основе нескольких основных принципов: пользователь должен быть осведомлён о том, что данные, касающиеся его, собираются сенсорными устройствами; пользователь имеет право решать, прекращать или продолжать процесс сбора данных; личная информация пользователя должна храниться в тайне.

Для обеспечения этих принципов необходимы соответствующие методы встроенного программирования. Помимо уже упомянутых протоколов безопасности, особое внимание следует уделять обучению пользователей процедурам и механизмам информационной безопасности, чтобы снизить риски незаконного доступа или кражи личных данных со стороны киберпреступников.

Ниже перечислены некоторые вопросы безопасности на уровне сенсорных устройств в IoT:

“Умные” устройства: Для эффективного и безопасного подключения необходимо наличие “умного” устройства, способного обеспечивать безопасность, шифрование, аутентификацию, таймеры, кеширование, прокси, межсетевой экран и т. д. Следовательно, устройство должно обладать достаточной мощностью для работы в среде IoT.

Обработка на границе (Edge processing): Умные устройства обеспечивают мощность, возможности развития, удобство и полезность с течением времени, могут обрабатывать данные локально до их отправки в облако, уменьшая объём больших данных, передаваемых в облако. Чувствительная информация не обязательно должна отправляться в облако — данные могут быть обработаны и упакованы в отдельные сообщения, которые затем безопасно передаются различным получателям. Эффективная обработка на уровне устройств способствует усилению общей сетевой безопасности.

2.4. Безопасность уровня поддержки и облачных вычислений

Уровень поддержки относится к программному обеспечению и вспомогательным технологиям для решений IoT, где данные с устройств собираются, анализируются, обрабатываются и отображаются в соответствии с заранее определёнными стандартами и форматами. Уровень поддержки, а особенно облачные вычисления, считаются ключевыми факторами для широкого применения и распространения IoT.

Вопросы безопасности IoT на уровне поддержки и облачных сервисов включают идентификацию, аутентификацию и шифрование устройств и машин. Пользователи, получающие доступ к облачным сервисам, обычно используют два метода аутентификации — пароль в сочетании с механизмом одноразового пароля, тогда как для машинных устройств более эффективна обработка цифровых сертификатов.

Цифровые сертификаты используют асимметричную систему аутентификации, которая не только подтверждает транзакцию, но и шифрует канал от устройства до облака до аутентификации. Кроме того, они обеспечивают шифрование идентификации, что очень трудно достичь с помощью обычного userid/password.

2.5. Безопасность уровня приложений

Потребности в безопасности приложений могут различаться. Поэтому обмен данными между различными технологическими платформами должен быть

унифицирован. Это важный аспект для обработки больших данных и контроля активности с целью обеспечения безопасности и надёжности сети IoT, включая защиту конфиденциальности, контроль доступа к данным, защиту электронных устройств, предотвращение утечек информации и защиту авторских прав на программное обеспечение.

Распространённые угрозы на уровне приложений включают использование уязвимостей переполнения буфера, межсайтовый скриптинг (cross-site scripting), SQL-инъекции, простые пароли, уязвимости повышения привилегий и атаки типа отказ в обслуживании (DoS).

Для обеспечения безопасности на уровне приложений предложены следующие решения:

1. Использование безопасных технологий программирования, а также антивирусного ПО для обнаружения уязвимостей сервисов и всех видов вредоносного кода.
2. Аутентификация данных и разработка кэширования для предотвращения атак на данные.
3. Внедрение механизма проверки сессий для двух и более запросов с одного источника, чтобы ограничить атаки повторного воспроизведения сообщений.
4. Проверка границ данных, шифрование, контроль доступа и другие меры для предотвращения утечек пользовательской информации.

Кроме того, доступность устройств, данных и сервисов является важным аспектом IoT-приложений. Вертикальная структура контроля помогает защитить системы от атак отказа в обслуживании и распределённых атак отказа в обслуживании (DDoS).

2.6. Безопасность IoT-систем на базе IP

Информационная безопасность — это обширная область. Для IoT было разработано множество технологий, среди которых особенно выделяется ZigBee, построенный на основе стандарта IEEE 802.15.4. Технология ZigBee использует коротковолновую связь и включает два уровня — физический и MAC (Medium Access Control). Благодаря функции беспроводного дистанционного управления, стабильной передаче данных и крайне низкому энергопотреблению, ZigBee становится всё более популярной и используется во многих приложениях, особенно в системах умного дома.

Кроме того, исследуются новые протоколы для обеспечения передачи и защиты информации в IoT, такие как RPL (Routing Protocol for Low-Power and Lossy Networks), UDP (User Datagram Protocol) и CoAP (Constrained Application Protocol). CoAP — это

протокол прикладного уровня, позволяющий IoT-устройствам взаимодействовать через Интернет. Для обеспечения безопасной передачи данных CoAP использует протокол Datagram Transport Layer Security (DTLS). DTLS поддерживает криптографические методы с большой вычислительной нагрузкой и разработан для сетевых протоколов, где размер сообщения не является критичным. Поэтому при совместном использовании с 6LoWPAN (IPv6 over Low-Power Wireless PAN) заголовок DTLS должен сжиматься специальными механизмами для обеспечения производительности IoT-системы.

Можно отметить, что решения в области безопасности разрабатываются под конкретные сценарии и часто не учитывают совместимость с существующими интернет-стандартами. Исследователи обнаружили серьёзные уязвимости, связанные с IoT, такие как Ghost и VENOM (Virtual Environment Neglected Operations Manipulation). Ghost позволяет хакерам выполнять удалённые команды для захвата управления Linux-сервером. VENOM затрагивает управление виртуальным дисковым приводом в QEMU — открытом эмуляторе компьютеров, используемом для управления виртуальными машинами. Хакеры могут использовать эти уязвимости для отправки специальных команд, вызывающих переполнение буфера и выполнение произвольного кода в процессе гипервизора конечного устройства.

В последние годы во всём мире произошли многочисленные масштабные кибератаки. По данным iot-analytics.com, в конце 2016 года масштабные DDoS-атаки на серверы DYN (крупного американского поставщика DNS) существенно снизили доступность многих популярных онлайн-сервисов в США, показав, что IoT-устройства могут быть инструментом хакеров для проведения таких атак.

Вьетнам также сталкивался с подобными проблемами: в конце 2014 года информация более чем с 1000 камер была украдена и широко распространена из-за недостаточного внимания пользователей к безопасности и не сменённых паролей по умолчанию перед подключением к Интернету. По статистике компаний Kaspersky и Symantec, число образцов вредоносного ПО, нацеленного на умные устройства, превысило 7000, из которых более половины появились в 2017 году. Вьетнам входит в число стран с наибольшим числом мобильных пользователей, подвергшихся атакам вредоносного ПО.

Корпорация VNPT также зафиксировала множество распределённых атак отказа в обслуживании (DDoS) с использованием IoT-устройств на интернет-магазины, финансовые и банковские организации, а также интернет-провайдеров. По данным VNPT,

количество серверов командного и контрольного центра (C&C), управляющих ботнетами, превысило 100 и продолжает расти.

Ясно, что IoT — это перспективная область исследований, но она несёт в себе множество серьёзных вызовов, среди которых:

1. Архитектура безопасности IoT: Несмотря на стабильное функционирование, создание безопасной архитектуры с глубокой защитой остаётся важной задачей для исследователей.
2. Механизмы обмена и управления ключами: Это важнейшая основа для повышения безопасности, но также самая сложная сторона криптозащиты. Легковесные алгоритмы и высокопроизводительные сенсорные устройства пока не получили широкого применения, что создаёт серьёзные трудности для сообщества разработчиков IoT.
3. Законодательство и регуляции: В настоящее время законодательство недостаточно учитывает технические особенности IoT-систем, особенно в вопросах национальной безопасности, корпоративной тайны и личной конфиденциальности. Необходимо разработать правила, стимулирующие правильное, масштабное и эффективное развитие IoT.
4. Требования к развивающимся приложениям: С ростом беспроводных сенсорных сетей, облачных вычислений, сетевых технологий, теории координированного управления в реальном времени и RFID, IoT быстро развивается. В то же время отсутствие процедур тестирования и оценки безопасности приложений приводит к появлению новых уязвимостей.
5. Управление IoT: В настоящее время управление IoT осуществляется недостаточно эффективно. Проблемы безопасности усложняются из-за ограничений по ресурсам и энергопотреблению устройств. При проектировании протоколов безопасности необходимо учитывать такие аспекты, как производительность, коммуникации, обработка данных и фрагментация пакетов для минимизации DoS-атак.

Заключение

Безопасность и защита информации — это чрезвычайно обширная область, и технологические решения в области безопасности всегда имеют относительный характер, затрудняя полное и окончательное удовлетворение требований целостности данных и защиты конфиденциальности пользователей. Для IoT эта проблема становится ещё более сложной из-за подключения миллиардов устройств и огромного количества различных пользователей. Перспективы технологического мира огромны, но вместе с тем они несут множество рисков и сложностей, которые создают серьёзные вызовы для учёных как внутри страны, так и на международном уровне. Эта курсовая работа предоставляет общий обзор IoT с акцентом на анализ существующих проблем и уязвимостей в области безопасности.

Список использованных источников

1. “How Many IoT Devices Are There in 2025”, https://techjury.net/industry-analysis/iot/.
2. “OWASP Board Votes”, https://www.owasp.org/index.php/OWASP_Board_Votes.
3. “AES Crypt”, https://www.aescrypt.com.
4. “Triple Data Encryption Standard (Triple-DES)”, http://www.vocal.com/cryptography/tdes/
5. “IDEA (International Data Encryption Algorithm)”, http://www.quadibloc.com/crypto/co040302.htm
6. “RSA” , https://en.wikipedia.org/wiki/RSA_(cryptosystem)
7. “Diffie–Hellman key exchange”, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
8. CoAP RFC 7252 Constrained Application Protocol, http://coap.technology/