УДК 004.5
DOI 10.33764/2618-981X-2024-8-2-176-182

*Д. Н. Титов[1], Е. В. Рыжкова[1]**

Анализ атак на Интернет вещей

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: alena.tarasova.2014@.ru

Аннотация. Интернет вещей объединяет преимущества обработки данных, аналитики и использует возможности Интернета для принятия решений в отношении физических объектов реального мира. Это система, в которой интеллектуальные объекты связаны между собой и имеют доступ к Интернету в качестве основы взаимосвязи для сбора и обмена информацией с использованием «Вещей». Интернет вещей стал одним из основных направлений исследований во всем мире.

Ключевые слова: Интернет вещей, DoS атаки, кибератаки, противодействие атакам

*D. N. Titov[1], E. V. Ryzhkova[1]**

Analysis of Attacks on the Internet of Things

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: alena.tarasova.2014@.ru

Abstract. The Internet of Things combines the benefits of data processing, analytics and uses the power of the Internet to make decisions regarding physical objects in the real world. It is a system in which intelligent objects are interconnected and have access to the Internet as the basis of interconnection for collecting and exchanging information using “Things”. The Internet of Things has become one of the main areas of research around the world.

Keywords: Internet of things, DoS attacks, cyber attacks, countering attacks

Введение

Такие устройства, как Интернет вещей (IoT), занимают значительное место в нашей повседневной жизни благодаря технологической революции, беспроводным устройствам и системам связи. Возможность перенести физические вещи в цифровой мир становится все более вероятной благодаря современным технологиям. Сети Интернета вещей оказывают влияние на различные области деятельности человека, включая домашний мониторинг и мониторинг повседневной жизни. Интернет вещей объединяет преимущества обработки данных, аналитики и использует возможности Интернета для принятия решений в отношении физических объектов реального мира. Это система, в которой интеллектуальные объекты связаны между собой и имеют доступ к Интернету в качестве основы взаимосвязи для сбора и обмена информацией с использованием «Вещей». Интернет вещей стал одним из основных направлений исследований во всем мире.

Но все это привело к тому, что Интернет вещей сегодня подвергается различным обширным угрозам безопасности. Это вызывает необходимость создания систем безопасности в различных областях, включая идентификацию/аутентификацию, конфиденциальность, надежность и отказ.

Киберпреступники ищут уязвимости устройств и используют их, чтобы получить преимущество при проведении атак, что с самого начала усиливает потребность в безопасности. Киберзлоумышленники могут атаковать приложения Интернета вещей с помощью различных методов, которые можно разделить на четыре категории: физические атаки или атаки на восприятие, сетевые, программные или прикладные атаки и атаки с шифрованием. Возможны физические, сетевые и прикладные атаки на систему Интернета вещей, а также атаки на методы шифрования.

Методы и материалы

В этой работе рассмотрим физические атаки – атаки на безопасность Интернета вещей.

Эти атаки возникают в результате взлома оборудования системы Интернета вещей, такого, как датчики, и злоумышленники получают доступ к ним, например, подключая USB-накопитель. По оценкам, 70% всех кибератак начинаются изнутри, намеренно или случайно, со стороны людей. Эта атака может ограничить срок службы или функциональность оборудования.

Помехи в узлах WSN (Беспроводная сенсорная сеть). Атака глушения узлов в WSN осуществляется злонамеренными узлами в сети, которые создают помехи, нарушают или глушат используемые радиосигналы, отправляя бесполезную информацию в используемом диапазоне частот [1]. Злоумышленник может отключить службу устройства IoT, если ему удастся заблокировать датчик ключа. В случае атаки с помехами статистические характеристики потока пакетов будут временно колебаться. В зависимости от своей силы источник помех может вывести из строя всю систему или только небольшую ее часть. Эта блокировка может быть временной, периодической или постоянной.

Атака с физическим ущербом – это атака, которая приводит к физическому повреждению целевой инфраструктуры. Злоумышленник может получить доступ к устройствам, физически повреждая объекты сети IoT в своих интересах.

Атака вторжения в узел – это атака, при которой злоумышленник повреждает сенсорный узел. Можно заменить весь сенсорный узел или вывести из строя часть аппаратного обеспечения. Скомпрометированный узел может быть создан путем физического изменения или замены узла, и злоумышленник может взять этот узел под контроль. Получив доступ, злоумышленник может изменить конфиденциальную информацию, например, общие криптографические ключи/учетные данные, а также нарушить функциональность более высоких уровней связи.

При атаках социальной инженерии вредоносные действия осуществляются посредством взаимодействия между людьми. Атаки социальной инженерии могут включать один или несколько этапов. Злоумышленник начинает со сбора ис-

ходных данных, необходимых для проведения атаки, таких как потенциальные пути проникновения и неадекватные процедуры безопасности. Затем злоумышленник пытается завоевать доверие жертвы, поощряя дополнительное поведение, нарушающее принципы безопасности, и получает необходимую информацию.

Внедрение вредоносного узла. При такой атаке злоумышленник физически развертывает вредоносный узел в сети IoT, который собирает информацию или изменяет коммуникационные данные для передачи неверной информации другим узлам. Таким образом контролируется передача и прием потока данных и работа узлов.

Атака лишения сна. Устройства Интернета вещей запрограммированы на использование режима сна, позволяющего оставаться в режиме пониженного энергопотребления как можно дольше, не оказывая негативного влияния на приложения узла; следовательно, это продлевает срок службы батареи. Злоумышленник взаимодействует с узлом таким образом, что его действия кажется разрешенными; однако его намерение состоит в том, чтобы поддерживать узел-жертву активным, что приведет к более высокому энергопотреблению и выходу из строя.

Атаки внедрения вредоносного кода: злоумышленник физически атакует устройство и внедряет вредоносный код, чтобы скомпрометировать систему и получить доступ. Это можно сделать, вставив в узел USB-накопитель с вредоносной программой или вставив каналы связи, используя такие методы, как вставка вредоносных кодов/пакетов данных, которые кажутся законными; изменение кодов/пакетов данных после захвата; замена ранее обмененных сообщений между узлами. Цель атаки может быть различной, например, для кражи данных, получения контроля над всей или частичной системой и распространения червей.

Радиопомехи на RFID: RFID – это технология автоматической идентификации, при которой связь осуществляется с использованием радиочастот (RF) и передаваемым идентификационным кодом (ID). В этой атаке сигнал скомпрометирован путем создания и отправки шумовых сигналов поверх радиочастотного сигнала, который используется для передачи RFID.

Клонирование тегов. При атаке клонирования злоумышленник хочет иметь тег, который будет иметь те же характеристики, что и исходный тег, и в конечном итоге сможет заменить его. В ходе этой атаки злоумышленник сможет скопировать информацию электронной метки RFID или смарт-карты в клонированную метку. Перехват, подслушивание и другие технологии используются в атаках клонирования для получения всех данных из исходного тега, включая кодировку и информацию о клиенте.

Атака подслушивания, также известная как атака спуфинга или слежения, представляет собой кражу информации, передаваемой с использованием беспроводной связи. Для подслушивания злоумышленник может использовать антенну для получения передаваемых данных в системе RFID. Чтобы добиться успеха,

злоумышленник находит слабое соединение, чтобы использовать его для перенаправления сетевого трафика.

При атаке подделки тега цель злоумышленников – изменить идентичность тега. Злоумышленники могут подделать метку в RFID-системе, используя метод манипулирования меткой. Злоумышленники получают доступ к каналу связи, подделав метку IoT-устройства.

Атака с отключением: злоумышленник может использовать радиосигнал большей мощности, чем разрешенная в этом диапазоне это может вывести устройства из строя.

Репликация объекта. Поскольку устройства Интернета вещей не контролируются физически в удаленных местах, злоумышленник при атаке этого типа может физически вставить новое устройство/объект в сеть. Например, злонамеренный объект может быть добавлен путем репликации его идентичности. В результате такая атака может привести к значительному снижению производительности сети.

Аппаратный троян: атака аппаратным трояном была признана основной проблемой безопасности интегральной схемы во многих различных формах исследований. Как и в случае других атак, целью злоумышленника является получение доступа и сбор конфиденциальной информации и прошивки. В ходе этой атаки злоумышленник злонамеренно модифицирует интегральную схему. Атаки аппаратных троянов планируются на этапе проектирования и остаются неактивными до тех пор, пока разработчик не отправит им сигнал – триггер или событие.

Результаты

Ниже покажем меры противодействия физическим атакам. Табл. 1 показывает физические атаки с нарушением целей безопасности и мер противодействия [2, 3].

Таблица 1

Физические атаки с нарушением целей безопасности и мер противодействия

Физические атаки	Последствия	Контрмеры
Узел помех	Нарушение связи, сокращение срока службы [4]	Скачкообразная перестройка частоты, применение теории игр [5], расширение спектра, использование более низкого рабочего цикла, приоритетных сообщений.
Физический урон	Аппаратный контроль контрагента, утечка конфиденциальной информации [6]	Использовать безопасную физическую конструкцию, устанавливать защиту от несанкционированного доступа и самоуничтожение.
Вмешательство узла	Аппаратный контроль, утечка конфиденциальной информации [7]	Устойчивость к клонированию и самоуничтожение, снижение утечки информации (добавление рандомизированной задержки, намеренно генерируемый шум, балансировка весов Хэмминга, усиление архитектуры кэша, экранирование), ин-

Физические атаки	Последствия	Контрмеры
		теграция физически неклонируемой функции (PUF) в устройство.
Социальная инженерия	Датчики контроля [8]	Облачная обработка и обратная связь, методы резервного копирования, обучение пользователей Интернета вещей, защита от несанкционированного доступа и самоуничтожение.
Вредоносное внедрение узла	Незаконное наблюдение [9], контроль потока данных; атака человек посередине	Алгоритм сжатия данных, расчет достоверности пути, безопасное обновление прошивки, механизмы на основе хэша, шифрование, техника аутентификации.
Атака лишения сна	Выключение узла	Система обнаружения вторжений [10], алгоритм Firefly и нейронная сеть Хопфилда, функция радиального смещения.
Внедрение вредоносного кода	Потеря целостности программного обеспечения, доступ к конфиденциальной информации и получение доступа, DoS	Цепочка доверия, безопасность конечных точек API, схема мониторинга и обнаружения трафика, защита от несанкционированного доступа и самоуничтожение, IDS.
Радиочастотные помехи	Блок сообщений [11], DoS	Информация на основе расстояния, команда безопасного уничтожения меток, метки электронного кода продукта (EPC), связь с расширенным спектром, схема формирования луча с защитой от помех.
Клонирование тегов	Несанкционированная копия тега	Схема вероятности атаки, рандомизация тегов, шифрование, методы на основе хэша, структура аутентификации, команда отключения сна, изоляция, блокировка, оценка расстояния, интеграция PUF в RFID-метки.
Подслушивание	Извлечение важной сетевой информации [12]	Безопасная загрузка, недорогая демилитаризованная зона, методы шифрования, перенос данных на серверную часть.
Подделка тегов	изменение данных в памяти тегов	Водяной знак аутентификации и восстановления водяной знак, интеграция PUF в RFID-метки, механизмы на основе хеш-функции, шифрование, RFID-уровень защиты от несанкционированного доступа, интеграция опции сигнализации для активных меток.
Атака сбоя	Нарушать или искажать состояние приложений	Случайная последовательность скачков времени и случайная перестановка, безопасный физический дизайн.
Репликация объектов	Сеть управления	Трехмерные обратные цепочки ключей на основе знаний о развертывании, шифрование, методы на основе хэша, упрощенные картографические схемы.

Физические атаки	Последствия	Контрмеры
Аппаратный троян	Изменение функций чипов и утечка конфиденциальной информации [12]	Временная тепловая информация, электромагнитное излучение, оценка сигнала по побочному каналу (на основе отпечатка задержки пути, на основе нарушения симметрии, на основе тепловых и энергетических показателей, приложения машинного обучения), активация трояна.

Заключение

С появлением и быстрым ростом приложений Интернета вещей злоумышленники и исследовательское сообщество постоянно привлекают внимание к выявлению уязвимостей в системе его безопасности, начиная от атак на устройства и заканчивая атаками на транспортировку данных. Более того, благодаря применению интеллектуальных технологических инноваций физический мир объединяется с виртуальным миром, что усугубляет уязвимости промышленных систем на базе Интернета вещей. В этой статье обсуждаются не только проблемы безопасности и конфиденциальности на основе Интернета вещей, но также представлены меры противодействия угрозам безопасности. В дальнейшем планируется обсуждать вопрос о различных правилах безопасности, текущие исследования в отрасли и недавно разработанные методы атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Довгаль В.А., Довгаль Д.В. Управление ресурсами в Интернете Вещей // Дистанционные образовательные технологии: материалы II Всерос. науч.-практ. конф., г. Ялта, 2017 г. Симферополь: АРИАЛ, 2017. – С. 168–173.
2. Evans D. Internet of Things. Cisco, white paper. URL: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_01FINAL.pdf (дата обращения: 16.04.2024).
3. Накиев Р.Р., Ульянов В.В. Анализ уязвимостей интернета вещей (iot) и способы их предотвращения // Вестник науки. – № 7 (64). – Т.4. – 2023.
4. Тавасиев Д.А., Команов П.А., Ревазов Х.Ю., Семиков В.С. Анализ методов выявления уязвимостей во встроенном программном обеспечении IoT устройств // Международный научно-исследовательский журнал. 2020. № 1-1 (91). С. 34–37.
5. Баев Д.А., Волков Р.О., Зонов А.Д. Мониторинг безопасности в IOT-сетях // StudNet. – 2021. – №6. – С. 1122
6. Абраров Р.Р., Бурлаков М.Е. Уязвимости протокола маршрутизации в MESH-сети стандарта 802.11S // Вестник ПНИПУ. – 2017. – №23. – С. 66.
7. Гатиятуллин Т.Р., Сухова А.Р. К вопросам обучения основам информационной безопасности сотрудников предприятия // Символ науки. – 2015. – №12. – С. 129.
8. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей // Математическое и информационное моделирование: сборник научных трудов. Выпуск 16. Тюмень: Тюменский государственный университет, 2018. С. 347–356.
9. Оралбаев Е.А. Обнаружения DDoS-атак ботнетов в сетях доступа IoT // Актуальные вопросы современной науки и образования. Монография. – Пенза, 2021. – С. 190–200.
10. Горев А.В. Интеллектуальный анализ DDoS-атак ботнета на IoT устройства при помощи Sap Analytics Cloud // Безопасность информационного пространства. Сборник трудов

XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2021. – С. 10–14.

11. Баженов А.С. Обзор DDoS атак на IoT устройства // Наука настоящего и будущего. – 2019. – Т. 1. – С. 122–125.

12. Тавасиев Д.А., Команов П.А., Ревазов Х.Ю., Семиков В.С. Анализ методов выявления уязвимостей во встроенном программном обеспечении IoT устройств // Международный научно-исследовательский журнал. 2020. – № 1-1 (91). – С. 34–37.