УДК 004.056.5

УГРОЗЫ БЕЗОПАСНОСТИ «ИНТЕРНЕТА ВЕЩЕЙ»

ГАРЕЛИК Д. Г.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

E-mail: lumenusbass@gmail.com

Аннотация. Обзор и оценка различных угроз безопасности «интернета вещей» и потенциальных способов защиты от них.

Abstract. Review and assess various security threats to the Internet of Things and potential ways to protect against them.

Каждый день устройства IoT подвергаются опасности со стороны злоумышленников. Под угрозой оказываются аутентификация, целостность данных, контроль доступа. Анализ показывает, что 70 % процентов устройств IoT имеют крайне слабую защиту либо она отсутствует вовсе. Ниже приведены основные направления применения устройств IoT и их угрозы безопасности.

Медицинские устройства

PMD (Personal Medical Device) через беспроводной интерфейс связываются с базовой станцией, которая в дальнейшем используется для считывания состояния устройства, обработки медицинских отчетов или настройки и обновления медицинского устройства.

Существует несколько типов атак на медицинские устройства:

– перехват данных, при котором происходит утечка информации о пациенте:

– изменение целостности пакета информации, передаваемой по беспроводной сети, при которой изменяется сообщение с информацией;

– атаки, направленные на быстрый разряд батареи PMD.

Роутеры

Средний «возраст» прошивки на среднестатистическом роутере составляет порядка 3-4 лет. Этот возраст коррелирует со средним возрастом самого роутера. Пользователь чаще меняет само устройство чем обновляет его программное обеспечение. В текущий момент установлено, что пароли, в 15 случаев из 100, не менялись со значений по умолчанию, таким образом, доступ к управлению устройством можно получить, методом перебора типовых паролей по умолчанию.

Камеры и видеорегистраторы

В настоящее время злоумышленник может потенциально получить доступ более чем к

3,5 миллионам камер по всему миру. При этом для доступа к видео произвольно взятого пользователя требуется всего пара запросов в Shodan, один в Google, VLC-медиаплеер и не более 60 секунд времени. Порядка 90% всех DVR-камер, которые используются для видеонаблюдения предприятиями малого и среднего бизнеса, содержат те или иные уязвимости и могут быть взломаны.

Навигаторы

Системы глобального позиционирования глубоко проникли во все сферы нашей жизни, что большинство людей пользуются ими, не задумываясь о том, насколько им можно доверять. Между тем уже есть множество примеров, подтверждающих, что подобные системы уязвимы к разнообразным атакам, включая *spoofing*, то есть подмену сигнала.

Беспроводное управление

Компьютерные мыши и клавиатуры с радиоинтерфейсом и USB-трансивером не защищены от взлома: инструмент для осуществления атаки можно собрать из доступных комплектующих, а вестись она может с расстояния до 1 км. Исследователи Positive Technologies протестировали безопасность устройств Logitech, A4Tech и Microsoft и смогли перехватить данные, передаваемые клавиатурами и мышами, дешифровать трафик и осуществить ряд других атак. Обнаруженные уязвимости могут

приводить к утечке паролей, платежных реквизитов, персональных данных и другой важной информации.

Датчики (электричество, вода, сигнализация)

В ходе одного из исследований умных сетей электроснабжения (*smart grid*) были обнаружены тысячи пользовательских веб-панелей управления системами мониторинга солнечных электростанций. Примерно 5% систем вообще не требовали пароля для входа на страницу конфигурации, у остальных 95% систем пароль был, но его оказалось достаточно легко подобрать. Обойдя авторизацию, злоумышленник может удаленно установить модифицированную прошивку или просто поменять параметры системы, что приведет к аварии.

Безопасность устройств IoT, конфиденциальность и угрозы.

Конфиденциальность пользователей может быть скомпрометирована различными способами, для превентивной защиты использовать базовые правила обеспечения безопасности:

1) *Защита жизненного цикла данных по принципу end-2-end.* Для обеспечения безопасности данных в среде IoT во всей сети предоставляется сквозная защита данных. Данные собираются с различных устройств, подключенных друг к другу, и мгновенно передаются другим устройствам. Таким образом, необходим фреймворк для защиты данных и управления конфиденциальностью информации в полном жизненном цикле данных;
2) *Планирование безопасности.* Взаимодействие между устройствами в IoT может дифференцироваться в зависимости от ситуации. Следовательно, все устройства должны поддерживать требуемый уровень безопасности. Например, когда локальные устройства и датчики, используемые в домашней сети, безопасно взаимодействуют между собой, их связь с внешними устройствами должна осуществляться с той же политикой безопасности, что позволит сохранить приватность данных;
3) *Видимая безопасность и приватность.* Большинство проблем безопасности и приватности возникает из-за неправильной настройки прав пользователей. Пользователям сложно соблюдать политику безопасности полностью самостоятельно, поэтому необходимо выбрать такие механизмы защиты, которые будут применяться автоматически.

Основные проблемы IoT

Проблема безопасности – самая большая проблема в IoT. Данные приложений «интернета вещей» могут быть промышленными, корпоративными, потребительскими или личными. Эта информация подлежит защите от кражи или несанкционированного доступа. Например, приложения IoT могут хранить личную информацию о здоровье пациента или коммерческую о работе магазина.

Среди наиболее важных проблем, относящихся к IoT:

1) *конфиденциальность данных.* Некоторые производители смарт-телевизоров собирают данные о своих клиентах для анализа их предпочтений по отношению к контенту, поэтому такая информация может быть украдена во время передачи по сети;
2) *отсутствие стандартизации*. Существует множество стандартов, для IoT-устройств, которые в зависимости от страны или региона кардинально отличаются в рабочих диапазонах и типах модуляции, используемых в устройствах, поэтому сложно установить четкую границу между разрешенными и запрещенными устройствами, подключенными к интернету;
3) *технические сложности*. В связи с масштабностью использования устройств IoT весь трафик, создаваемый ими, соизмеримо увеличивается. Следовательно, существует потребность в увеличении пропускной способности сети. Это влечет за собой необходимость размещать и архивировать огромное количество данных для анализа.

Анализ различных видов атак и варианты решений

IoT сталкивается с различными типами угроз, включая активные и пассивные атаки, которые могут легко повлиять на работоспособность системы в целом. При пассивной атаке злоумышленник просто обнаруживает концентратор устройств или предпринимает попытку украсть информацию, но

никогда не воздействует физически. Однако активные атаки могут повлиять на реальную работоспособность устройств.

Активные атаки делятся на две подкатегории: внутренние атаки и внешние атаки. Такие атаки могут помешать взаимодействию умных устройств. Следовательно, политика безопасности должна активно применяться для предотвращения вредоносных атак на устройства. В этом разделе приведены различные типы атак, характер и проявление угрозы и оценка степени опасности. Угрозы классифицируют по четырем различным типам в зависимости от их проявления и предполагают возможные решения для защиты:

1) атака низкого уровня (злоумышленник пытается воздействовать на домашнюю сеть, но его атака не удалась);
2) атака среднего уровня (злоумышленник перехватывает пакеты данных, но не нарушает их целостность);
3) атака высокого уровня (осуществляется в сети умного дома, изменяет целостность данных или модифицирует данные);
4) атака чрезвычайно высокого уровня (злоумышленник атакует сеть, получает несанкционированный доступ и делает сеть недоступной, отправляя массовые сообщения или блокируя сеть).

Список использованных источников

1. J. S. Kumar and D. R. Patel. A survey on internet of things: Security and privacy issues. – International Journal of Computer Applications, vol. 90, no. 11, 2014.
2. Бирюков, А. А. Информационная безопасность. Защита и нападение / А. А. Бирюков. — 1-е изд. — 2016 : ДМК, . — 417 с. — Текст : непосредственный. Интернет угроз. — Текст : электронный // IoT : [сайт]. — URL: https://iot.ru (дата обращения: 18.10.2020).