УДК 004.056.53

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПОСТРОЕНИЯ БЕЗОПАСНОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ ВЕЩЕЙ

Шептунов В.Ю. (Университет ИТМО)
к.т.н. Маркина Т.А. (Университет ИТМО**)**
Научный руководитель – к.т.н. Маркина Т.А.
(Университет ИТМО)

В работе рассмотрены требования безопасности “Интернет вещей” (Internet of Things - IoT), а также составлен обзор основных угроз уязвимостей, атак и безопасности системы в целом. Подробно изучены во всех ракурсах уровни Интернета вещей и рассмотрены угрозы и атаки на каждый из этих уровней. Далее проанализированы общие технологии безопасности “Интернет вещей”, а также службы безопасности, используемые в системах централизованного управления IoT-устройствами.

Введение. В современном обществе человека окружают “умные” устройства. Их спектр становится всё более разнообразным с каждым годом: от смартфонов, которые не уступают в производительности некоторым стационарным вычислительным устройствам, беспроводных камер, принтеров и сканеров, способных выходить в Интернет, заканчивая холодильниками, которые сами при необходимости могут совершать покупки через всемирную паутину. Такое обилие “самостоятельных” устройств в жизни создаёт потенциальную угрозу информационной безопасности. Они могут стать посредниками при нерегламентированной пересылке конфиденциальной информации.

Большинство стандартных методов обеспечения безопасности для интернета вещей являются неэффективными. Вопрос безопасности IoT — тема, которая в последнее время получила широкое распространение ввиду того, что устройства обрели частичную независимость от человека. Существует большое количество исследований, в ходе которых хакеры находят уязвимости почти во всей технике: начиная от систем охраны, беспилотных автомобилей, портативной электроники заканчивая чайниками и холодильниками, в общем, во всех устройствах интернета вещей.

Основная часть. Для защиты системы необходимо задействовать несколько базовых технологий безопасности на всех уровнях IoT. На практике выделено четыре уровня IoT:

1. уровень элементов;
2. сетевой уровень;
3. сервисный уровень;
4. прикладной уровень.

При проектировании системы управления безопасностью IoT важно понимать, какие проблемы информационной безопасности могут возникнуть, чтобы проработать соответствующие меры безопасности. В основе проектирования подобных систем должна лежать архитектура эталонной модели IoT.

Основная задача разработчиков систем централизованного управления IoT-устройствами состоит в том, чтобы на этапе проектирования учесть все возможные угрозы, оценить риски, обеспечить выполнение требования совместимости проектируемой системы с эталонной архитектурой IoT, организовать управление безопасностью сети по тем же принципам, что и многоуровневой эталонной архитектуре.

На каждом уровне подробно рассмотрены угрозы безопасности, атаки, их цели и способы их нахождения уязвимостей системы и использования данных уязвимостей против пользователя или системы.

Выводы. В результате проведенных исследований были составлены развернутые требования к безопасности IoT. Описываемые требования сопровождены методами проверки. Составлен

обзор технологий, архитектурных особенностей и ограничений безопасности IoT. Детально описаны применяемые на текущий момент технологии безопасности IoT, а также описаны архитектурные особенности, ограничения и причины, обусловливающие их.
Также было выяснено что для защиты системы необходимо задействовать несколько базовых механизмов безопасности на всех уровнях IoT. Например, на уровне физических устройств и контроллеров (элементов), таких как датчики и разного рода интеллектуальные граничные узлы, механизмы безопасности для устройств IoT должны быть как можно менее ресурсоёмкими, по причине низкого энергопотребления и низкой вычислительной возможности устройств. Без эффективной защиты данные, собранные узлами, могут быть захвачены злоумышленниками или использованы для повреждения сетевой системы.

Шептунов В.Ю. (автор) Подпись
Маркина Т.А. (автор) Подпись

Маркина Т.А. (научный руководитель) Подпись