004.773

Использование Active Data для защиты конфиденциальности в Туманных Вычислительных Сетях

Литвинов Е. М. (Университет ИТМО)
Научный руководитель: к.т.н. Викснин Илья Игоревич (Университет ИТМО)

В работе предложен подход применения Active Data (AD) для улучшения защиты конфиденциальности устройств, которые можно отнести к категории Fog Computing (FC/Туманные вычислители), EDGE и IoT. Отличительной особенностью рассматриваемых устройств (IoT, EDGE) является очень ограниченные вычислительные ресурсы: flash память (ПЗУ) составляет порядка 16 Мб, оперативная память (RAM) – порядка 1-2 Мб

Введение.

Рассмотрены понятия EDGE, IoT, FC, ключевые характеристики соответствующих конечных устройств с точки зрения пользователей. Необходимость рассмотрения такого рода устройств с точки зрения пользователя обусловлено значительным разбросом интересующих характеристик в зависимости от выбранного пользователя. Например, для сотовых операторов EDGE устройства – это базовые станции, с необходимым оборудованием для построения сотовой сети. Их можно охарактеризовать наличием достаточно большой вычислительной мощности. Но в то же самое время, для пользователя – конечные устройства (EDGE/IoT) могут быть «умная лампочка», «датчик влажности», что в свою очередь характеризуется очень ограниченными вычислительными ресурсами.

Основная часть.

Представлены сценарии атак на конфиденциальность информации со стороны конечных устройств, подтверждающие актуальность информационной безопасности. Формализована задача обеспечения информационной безопасности для FC и EDGE/IoT. Один из примеров – взлом систем BMS со стороны «умного выключателя». Другим примером может служить взлом казино через «умный аквариум».

Одним из рассматриваемых подходов для решения задачи обеспечения информационной безопасности устройств FC является технология Active Data (AD), обеспечивающая повышение уровня конфиденциальности информации при общении между туманными вычислителями. Основная идея данной технологии заключается в том, что устройство получает некоторый объем данных и безопасно исполняет код, представленный в этих данных. Основой исполнения подобного рода кода являются виртуальные машины.

Однако, ключевой трудностью является ограниченные ресурсы конечных устройств. Если gateway/router работают под управлением Linux, то конечные устройства имеют baremetal firmware и/или в лучшем случае ту или иную разновидность embedded RTOS, для которой уже не применимы стандартные возможности (например, iptables).

Выводы.

Следующим шагом проведения исследования будет создание программного фреймворка, позволяющего реализовать минимальный функционал виртуальных машин на конечных устройствах.

Литвинов Е. М (автор) e-mail: egor21@gmail.com
Телефон: +7-905-255-22-00

Викснин И. И. (научный руководитель)