АРХИТЕКТУРА БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ *IoT*

Ганшин Д.Г., Сальников В.С., Цопа А.И.
Харьковский национальный университет радиоэлектроники

Интернет вещей (*Internet of Things, IoT*) – это новая точка развития информационно-коммуникационных технологий (ИКТ) и средство кардинального повышения возможностей человека при взаимодействии с внешней средой (физическими и виртуальными вещами).

Задача построения безопасной, целостной, непротиворечивой и системно развивающейся модели архитектуры *IoT* находится в развитии и заинтересованные страны (США, Германия, ЕС и др.), а также крупные международные компании *(CISCO, INTEL, IBM)* и организации *(ITU, IEEE, ETSI, IWF, W3C)* предлагают свои модели и ведут активную работу в области стандартов, покрывающих все уровни архитектуры *IoT*.

Целью представленной работы является анализ различных видов интерпретации архитектуры безопасности *IoT*.

С учетом сложности *IoT* создание четырехуровневой эталонной модели по Рекомендации *ITU-T Y.2060* [1] позволяет выделить основные компоненты системы и оценить их взаимосвязь. Основными уровнями модели при этом являются: уровень устройства; уровень сети; уровень поддержки услуг и поддержки приложений; уровень приложений. Между этими уровнями действуют возможности управления и обеспечения безопасности:

– на уровне устройства: аутентификация, авторизация, проверка целостности устройства, управление доступом, защита конфиденциальности и целостности данных;

– на уровне сети: авторизация, аутентификация, конфиденциальность данных об использовании и данных сигнализации, а также защита целостности данных сигнализации;

– на уровне приложения: авторизация, аутентификация, защита конфиденциальности и целостности данных приложения, защита неприкосновенности частной жизни, аудит безопасности и антивирусная защита.

Всемирный форум *IoT (IoT World Forum)* [2] уделяет больше внимания вопросам разработки приложений, промежуточного ПО, безопасности и функций поддержки для корпоративного интернета вещей. Предложенная *IWF* семиуровневая модель архитектуры безопасности *IoT* представлена на рис.1.

Потенциальные угрозы безопасности, возникающие в среде *IoT,* нужно рассматривать с точки зрения эталонной модели. На каждом уровне модели присутствуют угрозы безопасности, как специфичные только для этого уровня, так и общие для всей модели. Так, на всех уровнях модели присутствует угроза несанкционированного доступа к приложению или устройству. В случае исполнительных устройств несанкционированный доступ может привести к несанкционированным действиям самой вещи. На уровне приложения – это угрозы утечки информации, нарушения целостности данных и неприкосновенности частной жизни.

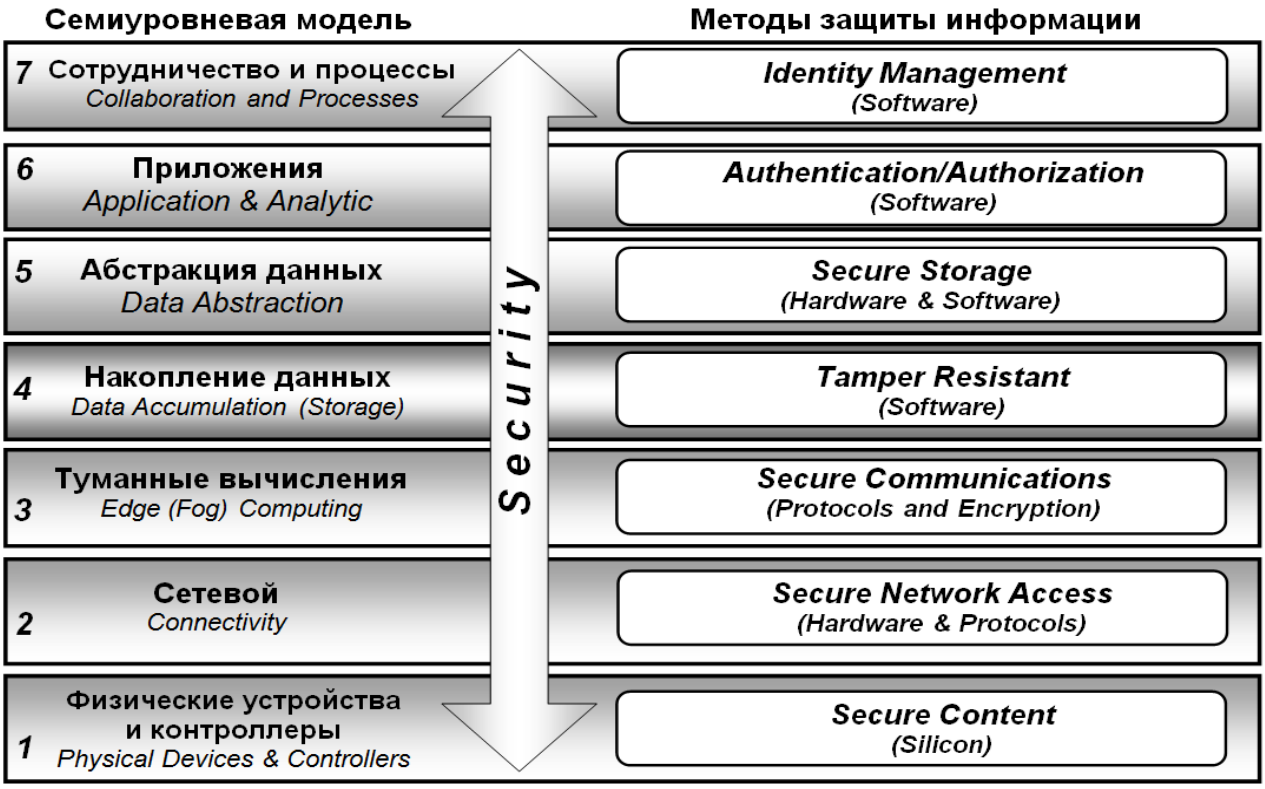

Рисунок 1. Эталонная модель *IWF* архитектуры безопасности *IoT*

На уровне сети – угрозы утечки данных об использовании сигнализации и нарушения их целостности. На уровне устройства – угрозы несанкционированного вскрытия, несанкционированного контроля/управления, утечки данных, хранящихся в устройстве, повреждения их целостности.

Высокий уровень неоднородности в сочетании широкой гаммой систем *IoT* увеличивает число угроз безопасности владельцев устройств, которые используются для взаимодействия людей, машин и вещей. Традиционные меры обеспечения безопасности и соблюдения конфиденциальности не могут быть применены к технологиям *IoT*, в частности из-за их ограниченной вычислительной мощности. Кроме того, большое количество подключенных устройств порождает проблему маштабируемости.

Также важную роль в *IoT* инфраструктуре играют механизмы адаптации и восстановления, которые должны обеспечивать эффективную работу распределенной системы *IoT* при возникновении изменений в окружающей среде. Соответственно, к вопросам безопасности нужно относиться также с высокой степени гибкости. Наряду с традиционными решениями для обеспечения безопасности необходимо использовать специальные механизмы, встроенные в сами устройства с целью оперативной диагностики, изоляции и профилактики нарушений безопасности.

Глубокий анализ архитектуры *IoT* может служить ориентиром для разработчиков распределенных информационных систем в плане того, каким образом обеспечивать надежность и безопасность новых сервисов.

1. Recommendation *ITU-T Y.2060 SERIES Y*: Provides an overview of the Internet of things (*IoT*) (06/2012).

2. *CISCO*, «The Internet of Things Reference Model», White Paper, June 2014.