UNIVERSITY OF TARTU

Institute of Computer Science

**Raman Shapaval**

**Security Risk Management for the IoT systems**

**Master’s Thesis (30 EAP)**

Supervisor(s): Dr. Raimundas Matulevicius

Associated Professor in Software Systems

Institute of Computer Science

University of Tartu

Tartu 2017

**Abstract**

**What is the problem?**

Since 2012 the number of units in global infrastructure for the information society (The Internet of Things) has grown twice. With this number also has grown the amount of possible threats and risks, which influence security on all levels of the system.

**Is this a real problem?**

According to Third Quarter, 2016 State of the Internet / Security Report based on data gathered from the Akamai Intelligent Platform (https://www.akamai.com/us/en/solutions/intelligent-platform/) the total number of DDoS attacks in Q3 2016 increased in 71% compared to Q3 2015. With 623 Gbps data transfer attack it was largest DDoS ever and this fact will only increase the number of future attack events.

**What is our solution (technical contribution)?**

The paper combines knowledge of Security Risk Management with existing practice in securing in IoT into a framework, which aim is to cover vulnerabilities in IoT systems.

(How it will be done technically I do not know. I will give an answer on the next three question as soon as I will finish the research in Existing practice in securing IoT so I could find out what I can contribute to already existing solutions.)

**How does this solve the problem?**

**Is this a real solution?**

**Why is this good?**

1. **Introduction**

This chapter aims on the problem and provides its detailed explanation.

1. **Security Risk Management**

Here will be general information about fundamentals of Secure System Modeling containing detailed explanation of generic domain model for Information Systems Security Risk management.

1. **The Internet of Things**

This chapter answers the question “What is IoT?”.

* 1. **What is The Internet of Things?**

The definition of the IoT varies and depends on such factors as:

* Application perspective
* Technological perspective
* Industry context, etc.

Simply we can define the IoT as a space of all hardware connected to the Internet. For example, every smartphone, PC, laptop, smartwatch and other wearable devices can be a part of the IoT as soon as they can connect to the Internet to share data, collect data or just simple interact with other devises.

If we look at more strict definitions, then according to the Wikipedia (https://en.wikipedia.org/wiki/Internet\_of\_things) the IoT can be described as “ the network of physical devices, vehicles, home appliances, and other items [embedded](https://en.wikipedia.org/wiki/Embedded_system) with [electronics](https://en.wikipedia.org/wiki/Electronics), [software](https://en.wikipedia.org/wiki/Software), [sensors](https://en.wikipedia.org/wiki/Sensor), [actuators](https://en.wikipedia.org/wiki/Actuator) and [network connectivity](https://en.wikipedia.org/wiki/Internet_access) which enable these objects to connect and exchange [data](https://en.wikipedia.org/wiki/Data)”.

As we can see from the Figure 1, the IoT can be divided into two main parts:

* + - 1. Industrial Internet of Things
      2. Consumer Internet of Things

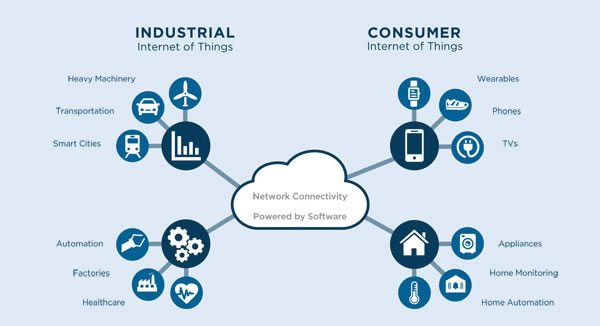
****

Figure 1: *General IoT specification.*

* 1. **Industrial IoT**

Industrial Internet of Things represents the part of IoT used in manufacturing. According to <http://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT> industrial IoT (also called “The Industrial Internet”) accumulates in itself such technologies:

* Machine learning in big data mining
* Collecting and studying data from sensors
* Machine to machine (M2M) communication
* Formal methods, etc.

The Industrial Internet has already become inadmissible part of the modern manufacturing, positively influencing business intelligent efforts with respect to time/money consumption.

* 1. **Consumer IoT**

For nowadays consumers the IoT has become the main source of information supplement, health care, education, personal security and many other irreplaceable aspects of the modern life.

1. **Securing IoT**

This chapter describes what assets in IoT should be protected. What risks and threads could be faced and how to cover the vulnerabilities in IoT systems according to existing practice.

1. **Framework development**

In this chapter, the process of framework developing from idea to working prototype will be described.

1. **Validation/Experiments**

Here will be description of two tests based on existing IoT system (coffee case):

1. Test how we can brake existing system
2. Test how we can protect it with previously developed framework