Proposal for Master's Degree Project

Title: Structuring the Security Requirements Analysis and Specification for the Internet of Things

Advisor and Contact
Pedro R. M. Inácio (inacio@di.ubi.pt), Ph.D.

Summary / Scope
The Internet of Things (IoT) is seen nowadays as a major business enabler. The number of devices connected to the Internet is booming, proving the raw potential of processing and communicating data using all kind of devices, spanning from simple sensors to powerful smartphones, drones or computers.

Unfortunately, the security of the devices, and consequently of the IoT, is not coping with the technological evolution on this area. Frequently, security (and many other aspects) is not taken into consideration during the infancy of a technology, though many efforts and emphasis has been placed on this particular aspect in the last few years. Tackling security problems on later stages comprises many times a bigger challenge, mostly because the devised solutions have to be compatible with previous technologies, compromising security by design.

This master's project is thus focused on IoT security. It touches areas such as Operating Systems, Networking, Information Security, Programming and Software Engineering. Its main idea is to study the security requirements analysis process for the IoT, striving for the delineation of the workflow that best suits the identification, structured documentation and implementation of security requirements. It thus aims to contribute to the development of *secure by design* IoT.

The project should output a tool (e.g., web application) for assisting a human in the identification of the security requirements and elaboration of the associated software engineering documentation. The tool should guide the user trough the workflow in a friendly and comprehensive manner. The source code of the tool should be released as open-source.

The main research challenges are to (i) study and structure the security requirements analysis workflow for the IoT, and (ii) translate that knowledge and workflow into a user-friendly tool. It will require substantial effort in the definition of system and attack models, as well as security requirements. This effort will later help in the development of the tool.

During this master's project, the student will have the chance to engage in discussions with other people involved in the area of information security, as well as the opportunity to improve his or her knowledge in several computer science fields, namely computer networks and programming.

Objectives

As hinted in the previous discussion, this master's project has three main objectives:

1. Study the security requirements analysis workflow;
2. Develop system and attack models, as well as defining security requirements for typical IoT scenarios;
3. Implement a tool to assist a user in the process of identifying the IoT scenario, the associated security requirements, the system and attack models, up to the identification of the potential mechanisms that should be applied to fulfil the requirements and producing high quality (security wise rich) software engineering documentation.

Tasks

In order to achieve its objectives, the following tasks are proposed as an initial work plan for this master's project:

Task 1 Getting acquainted with the context of the problem at hands and with the objectives of the project, as well as with the technologies involved. Revision of the specialized literature and related works (2 months);

Task 2 Produce a catalog of IoT scenarios, as well as system and attack models (1 month);

Task 3 Propose a workflow for security requirements analysis for IoT scenarios (2 months);

Task 4 Implement a tool to assist in the security requirements analysis workflow and propose security mechanisms to cope with the requirements (1 month);

Task 5 Validation and fine-tunning of the tool (1 month);

Task 6 Writing of the master's dissertation, technical documentation and a conference paper (3 months, eventually distributed and interleaved with the time periods of other tasks).

Timetable

An approximate scheduling for the execution of the previously identified tasks is included below. The execution of a given task in a given month is marked with a cross (x).

Task \ Month	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
1	x	x									
2			x								
3				x	x						
4						x					
5							x				
6								x	x	x	

Expected Outcomes and Dissertation

The most visible outcome of this master's project is a tool for assisting in the security requirements analysis of applications and systems developed for the IoT. Nonetheless, the underlying proposed workflow, models and documentation comprise the main outcomes of the project. Computer programs developed within the scope of project are expected outcomes also, and may be the subject of a scientific conference paper. The final dissertation, entitled *"Structuring the Security Requirements Analysis and Specification for the Internet of Things,"* may be written in English, in view of the international dissemination of scientific work.

References

[1] I. Alqassem and D. Svetinovic, "A taxonomy of security and privacy requirements for the Internet of Things (IoT),"2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, 2014, pp. 1244-1248.

[2] Musa Samaila, Miguel Neto, Diogo A. B. Fernandes, Mário M. Freire and Pedro R. M. Inácio, "Security Challenges of the Internet of Things,"in Beyond the Internet of Things: Everything Interconnected, Jordi Mongay Batalla, George Mastorakis, Constandinos X. Mavromoustakis and Evangelos Pallis (Eds.), Springer, In Press.