Military Technical Academy

Abstract

Doctoral School for Defense and Security Systems Engineering
Doctor of Philosophy

Security implications of the Internet of Things

by Eng. Bogdan-Cosmin CHIFOR

Internet of Things (IoT) is a domain which comprises network enabled ubiquitous computing devices employed by multiple areas like transportation, telecommunication, health, industrial and many others. The IoT concept began as a subject approached by the technology press and academia research, but in the latest years becomes a reality, being supported by multiple hardware and software companies. IoT has its' origins in the Wireless Sensor Networks and extends this concept by envisioning a world where Internet connected embedded devices help in automating and improving the user daily tasks. Thus, IoT devices are imagined to be managing multiple actions, starting from home based tasks and ending with industrial tasks. Taking into consideration the way that IoT impacts the user, appropriate security mechanism must be designed in order to address both privacy and safety. IoT security is considered one of the most important IoT verticals, being a key factor which influences the acceptance and large scale deployment of IoT solutions.

IoT security receives even more attention due to the current cybersecurity context, where new vulnerabilities appear constantly. The IoT devices are an attractive target for hackers because these devices are a sink for user private data and can also be used as an attack vector (e.g. for DoS attacks), if multiple devices are compromised. The particularity of the IoT world is that a security breach could also endanger human lives, besides causing economical costs. Another particularity of the IoT world is the difficulty of designing security solutions, due to computational/consumption limitations, limited I/O capability, deployment use-case and many others. Taking into consideration these IoT characteristics and adding the multitude of hardware/ software platforms along with the lack of standardization, there is a stringent need of new security solutions. An important requirement of the researched security solutions is to address issues like interoperability and modularity, the IoT landscape being a dynamic one which requires pluggable and generic structures.

This thesis explores multiple IoT security vectors like cryptographic algorithms, network security, trust, reputation and privacy, by analyzing the current state of the art and by proposing new security solutions. The research from this thesis is use-case oriented and analyzes the benefits and the drawbacks of deploying a security solution in a particular IoT scenario like smart-home or smart city and addresses the particularities of each analyzed use-case. The main goal of this thesis is to analyze and propose platform agnostic security solutions which address the requirements of each layer from the IoT computing stack.