Hardware-based Security Solutions for the Internet of Things using Physical Unclonable Functions

Abstract. The Internet of Things (IoT) concept consists of numerous resource-constrained devices such as sensors, nodes and actuators that are connected together and with the Internet. By 2020 it is anticipated that the IoT paradigm will encompass approximately 20 billion connected devices. The interconnection of such devices provides the ability to collect huge amounts of data which are then processed and analyzed for further useful actions. A significant portion of the transacted data between IoT devices is private information which must, in no way, be eavesdropped or tampered with. Security in IoT devices is therefore of paramount importance for the further development of this paradigm. Such devices have typically limited area and energy resources, which makes the use of classic cryptographic solutions prohibitively expensive. Physically Unclonable Functions (PUFs) are a class of novel hardware security primitives that promise a paradigm shift in many security applications; their relatively simple architectures can answer many of the security challenges of the energy- constrained IoT devices. In this tutorial, we discuss the design challenges of secure IoT systems and how to use hardware security to tackle those challenges, then we explain the design principles of Physically Unclonable Functions, finally we discuss the reliability and security problems of PUF devices and present a number of enhancement techniques to remedy those shortcomings. The tutorial concludes with a summary of open research questions of the design of hardware-security schemes for IoT applications.

Instructor(s): Dr Basel Halak and Professor Mark Zwolinski, Dept. of Electronics and Computer Science, Southampton University, United Kingdom