Constructive and Destructive Aspects of Embedded Security in the Internet of Things

Christof Paar
Horst Görtz Institute for IT-Security
Ruhr Universität Bochum, Germany
christof.paar@rub.de

Through the prevalence of interconnected embedded systems, the vision of pervasive computing has become reality over the last few years. More recently, this evolutionary development has become better known as the Internet of Things. As part of this development, embedded security has become an increasingly important issue in a multitude of applications. Examples include the Stuxnet virus, which has allegedly delayed the Iranian nuclear program, killer applications in the consumer area like iTunes or Amazon's Kindle (the business models of which rely on IP protection) and even medical implants like pace makers and insulin pumps that allow remote configuration. These examples show the destructive and constructive aspects of modern embedded security. In this tutorial we will address both the constructive and "penetration testing" aspect of embedded security.

In the area of destructive embedded security implementation attacks, also known as physical attacks, are of crucial importance. Whereas a network-borne attacker usually can't exploit the physical environment of an application, embedded devices often allow this. For instance, an attacker can monitor the power or timing behavior of a device. Also she can force the device to malfunction, e.g., through power spikes, and deduct information from faulty outputs. Many systems which are otherwise secure become vulnerable against implementation attacks. In this talk, we will focus on side-channel attacks, or SCA, which form arguably the most powerful method among physical attacks. After developing the mechanics of DPA (differential power analysis), we will look at recent case studies in which real-world implementation were broken using SCA. This includes successful attacks against contactless smart cards and FPGAs.

With respect to constructive aspects of embedded security, we will look at the field of lightweight cryptography. The goal here is to provide security at the lowest possible "cost", e.g., measured in power consumption, code size or chip area. Over the last six years or so, this has become a very active area within symmetric cryptography. Very recently, even NSA released two lightweight ciphers, SIMON and SPECK. We will look at the motiviation for such ciphers, e.g., for passive RFID tags or anti-counterfeiting applications. We will then introduce several lightweight constructions and will compare them with AES.

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11..

Categories and Subject Descriptors

A.1 [**Introductory and Survey**]:

Keywords

security; embedded security; Internet of things; implementation attacks