The Yin and Yang Sides of Embedded Security

Christof Paar

Ruhr Universität Bochum, Germany
Christof.Paar@rub.de

Abstract. Through the prevalence of interconnected embedded systems, the vision of pervasive computing has become reality over the last few years. 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 heavily 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. For us embedded security researchers, the following definition of yin and yang can be useful for resolving this seemingly conflict: "The concept of yin yang is used to describe how polar opposites or seemingly contrary forces are interconnected and interdependent in the natural world, and how they give rise to each other in turn." (OK, the "natural world" part is not a 100% fit here.) In this presentation I will talk about some of our research projects over the last few years which dealt with both the yin and yang aspect of embedded security.

In 1–2 generations of automobiles, car2car and car2infrastructure communication will be available for driver-assistance and comfort applications. The emerging car2x standards call for strong security features. The large number of data of up to several 1000 incoming messages per second, the strict cost constraints, and the embedded environment makes this a challenging task. We show how an extremely high-performance digital signature engine was realized using low-cost FPGAs. Our signature engine is currently widely used in field trials in the USA. The next case study addresses the other end of the performance spectrum, namely lightweight cryptography. PRESENT, one of the smallest known ciphers which can be realized with as few as 1000 gates. The cipher was designed for extremely cost and power constrained applications such as RFID tags which can be used, e.g., as a tool for anti-counterfeiting of spare parts, or for other low-power applications. PRESENT is currently being standardized by ISO.

As "yang examples" of our research we will show how two devices with very large deployment in the real world can be broken using physical attacks. First, we show a recent attack against a modern contactless smart card equipped with 3DES. The card is widely used in authentication and payment systems. The second attack breaks the bit stream encryption of current FPGAs. These are reconfigurable hardware devices which are popular in many digital systems. We were able to extract AES and 3DES key from a single power-up of the reconfiguration process. Once the key has been recovered, an attacker can clone, reverse engineer and alter a presumingly secure hardware design.

D.J. Bernstein and S. Chatterjee (Eds.): INDOCRYPT 2011, LNCS 7107, p. 93, 2011.