Real-world attacks against security hardware

Christof Paar

Abstract: Through the steady rise of interconnected embedded systems, the vision of pervasive computing has become reality over the last few years. As part of this development, the PC-centric Internet is evolving into the Internet of Things. It turns out that securing networked embedded devices is quite a different matter from traditional Internet security. Prominent examples for embedded security 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 hacking into critical automotive functions. Perhaps not surprising, embedded security is much more closely tight to the underlying hardware than in the case of traditional network security. In this presentation I will talk about some of our research projects over the last few years in the area 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. 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 hardware. 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 is 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 has recently been adopted as ISO standard.

The "dark" side of our research deals with vulnerability analysis of embedded system. First, we show an implementation attack against a modern contactless smart card equipped with the -- cryptographically highly secure -- 3DES algorithm. The card is widely used in authentication and payment systems. The second attack breaks the bit stream encryption of current FPGAs. We were able to extract AES and 3DES keys using the power traces from a single power-up of the target device. Once the key has been recovered, an attacker can clone, reverse engineer and alter a pressingly secure hardware design.

Biography: Christof Paar has the Chair for Embedded Security at the University of Bochum, Germany, and is affiliated professor at the University of Massachusetts at Amherst. He co-founded, with Cetin Koc, the CHES (Cryptographic Hardware and Embedded Systems) conference. Christof's research interests include highly efficient software and hardware realizations of cryptography, physical security, penetration of real-world systems, trusted systems and cryptanalytical hardware. He also works on real-world applications of embedded security, e.g., in cars, consumer devices, smart cards and RFID.

Christof has over 150 peer-reviewed publications and is co-author of the textbook Understanding Cryptography (Springer, 2009). He has given invited talks at MIT, Yale, Stanford University, IBM Labs, Sun Labs. He has taught cryptography extensively in industry, including courses at GTE, NASA, Motorola Research, and Philips Research. Christof is Fellow of the IEEE. He co-founded ESCRYPT Inc. - Embedded Security, a leading system provider in applied security which was acquired by Bosch.