Tamper resistance and physical attacks

Dr Sergei Skorobogatov
University of Cambridge Computer Laboratory

Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks

June 12th-15th 2006, Louvain-la-Neuve

Abstract. Major applications, such as mobile phone identification and pay-TV receivers, have pushed low-cost crypto-processors toward everyday use. In the last five years, dedicated crypto chips have been embedded in devices from game console accessories to printer ink cartridges and mobile phone batteries. These applications demand a high level of security protection from various attacks against confidentiality and integrity of the information stored inside the security chips. Hardware engineers should be well familiar with attack technologies in order to design a system with appropriate level of security protection at a minimal cost.

I will survey the area of hardware security and discuss the progress in attack technologies and protections.

Three classes of physical attacks can be distinguished by the way the device is accessed. Non-invasive techniques, such as timing, power or electromagnetic analysis, glitch attacks or exploits of data remanence, require only moderately sophisticated equipment and knowledge to implement. However, insider information about device functionality can be helpful. The large complexity of modern chips leaves less room for non-invasive attacks. Nevertheless, security holes in designs and careless dealing with confidential information can lead to such attacks. Invasive attacks, such as reverse engineering followed by microprobing or FIB editing, give almost unlimited capabilities to extract information from chips. However, these normally require expensive equipment, knowledgeable attackers and time. Semi-invasive optical probing and fault injection attacks, in which the chip is depackaged but the passivation layer remains intact, fill the gap between non-invasive and invasive types, being both inexpensive and easily repeatable.

In the last part of the talk I will present my own recent results in hardware security research.

References

Sergei Skorobogatov, Low Temperature Data Remanence in Static RAM, Technical Report UCAM-CL-TR-536, University of Cambridge,Computer Laboratory, June 2002

Sergei Skorobogatov, Ross Anderson, Optical Fault Induction Attacks, Cryptographic Hardware and Embedded Systems Workshop (CHES-2002), LNCS 2523, Springer-Verlag, ISBN 3-540-00409-2, pp.2-12

David Samyde, Sergei Skorobogatov, Ross Anderson, Jean-Jacques Quisquater, On a New Way to Read Data from Memory, First International IEEE Security in Storage Workshop, December 11, 2002, Greenbelt Marriott, Maryland, USA

Sergei Skorobogatov, Semi-invasive attacks – A new approach to hardware security analysis, Technical Report UCAM-CL-TR-630, University of Cambridge,Computer Laboratory, April 2005

Ross Anderson, Make Bond, Jolyon Clulow, Sergei Skorobogatov, Cryptographic Processors – A Survey (Invited Paper), IEEE Proceedings, Special Issue on Cryptography and Security, February 2006, Vol.94, No.2, pp.357-369. Full version is available as a Technical Report UCAM-CL-TR-641

Sergei Skorobogatov, Data Remanence in Flash Memory Devices, Cryptographic Hardware and Embedded Systems Workshop (CHES-2005), LNCS 3659, Springer-Verlag, ISBN 3-540-28474-5, pp.339-353