Semi-Invasive Extension to Physical Attacks

Dr Sergei Skorobogatov
University of Cambridge Computer Laboratory

Workshop IV: Special purpose hardware for cryptography: Attacks and Applications

December 4 - 8, 2006, Los Angeles

Abstract. Many modern applications demand a high level of security protection from various attacks against confidentiality and integrity of the information stored inside semiconductor chips.

Secure microcontrollers can always be attacked with invasive techniques, but this usually requires very expensive equipment, knowledgeable attackers and a long time to succeed. In contrast, non-invasive techniques could be implemented by hobbyists, but require insider information about device functionality. 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. As a result, semi-invasive techniques are important to consider in the security evaluation of semiconductor chips, as they offer fast and effective attacks.

I will survey the area of semi-invasive attack technologies, focusing primarily on optical probing methods. Laser scanning techniques, already extensively used for failure analysis, also need consideration in hardware security analysis. For example, laser injected photocurrent can be used to determine the logic state of a CMOS transistor. I will present recent results from combining semi-invasive optical techniques with non-invasive power analysis for extracting information about chip functionality and SRAM memory contents.