Fault and side-channel attacks on memory

Dr Sergei Skorobogatov
University of Cambridge Computer Laboratory

PASTIS 2010: PAca Security Trends In embedded Systems
16–17 June 2010, Gardanne, France

Abstract. Tamper resistance of secure semiconductor devices like microcontrollers and smartcards was an important subject since the outbreak of attacks in the late nineties. Embedded memory in microcontrollers, smartcards, FPGAs and ASICs is among the security concerns as it usually stores critical parts of algorithms, secret data and cryptographic keys. It seemed to be relatively easy and straightforward to attack silicon chips ten years ago. Many of those old and well known tools are no longer work for modern chips. However, this did not mean a relief for hardware manufacturers and developers as new tools and techniques have emerged posing even greater threat. One of the greatest shake-ups happened in 2002 with introduction of optical fault injection attacks. This lead to separation of a new class of attacks called semi-invasive which appeared as being inexpensive and very efficient. This even forced the revision of certain security evaluation requirements. Despite to a long time since introduction, optical attacks still bring many surprises, while their danger and effectiveness is sometimes dangerously underestimated. There are many examples of successful attacks on embedded memory like SRAM, EEPROM and Flash. I overview tools and techniques used for data extraction and discuss challenges that still exist for modern chips together with ways they could be overcome. Then some examples of hardware security failures in real systems will be presented followed by future plans and directions for further research.