Physical Attacks on Tamper Resistance: Progress and Lessons

Dr Sergei Skorobogatov
University of Cambridge Computer Laboratory

2nd ARO Special Workshop on Hardware Assurance
11–12 April 2011, Washington DC, USA

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. I will overview tools and techniques used for data extraction and discuss challenges that still exist for modern chips together with ways they could be overcome including recently introduced attacks. I will also discuss latest achievements and future plans.