Notice and Invitation

Oral Defense of Doctoral Dissertation

The Volgenau School of Engineering, George Mason University

Rajesh Velegalati

Bachelor of Engineering, SIR C.R.R College of Engineering, India, 2006

Master of Science, George Mason University, 2009

Developing an Integrated Environment for Detecting and Mitigating Side-channel and Fault attacks on Hardware Platforms

Monday, February 2nd, 2015, 10:00 AM

Nguyen Engineering Building, Room 3507

All are invited to attend.

Committee

Dr. Jens-Peter Kaps, Chair

Dr. Kris Gaj

Dr. Jill K. Nelson

Dr. Angelos Stavrou

Abstract

Recent years have seen a dramatic increase of market adoption and utility of so called "smart" devices by people from all walks of life. These devices play a central role in how people are entertained, communicate, network, work, bank and shop. There are billions of applications which provide users unprecedented ease of access to a plethora of programs, they also are providing a fertile environment for the distribution of hostile applications or malware. Additionally, the increased power of these mobile devices makes them more suitable for a host of business purposes, which can also result in the exposure and compromise of corporate data and systems. Finally, the very portability of mobile devices means that they are highly susceptible to loss and theft. The information accessed by these devices is secured using cryptographic algorithms. Advances in Field Programmable Gate Array (FPGA) technology have led to reduction in power and cost making them a suitable alternative for mobile devices. The reconfigurability of FPGAs facilitates quick changes or upgrades in the security requirements to mitigate any newly found vulnerabilities. A hallmark of FPGAs is that parallelized architectures can be implemented efficiently, and thus they are an attractive platform for implementations of cryptographic algorithms.

However, physical implementations of encryption algorithms on any hardware device are proven to leak secret information in the form of so called *Side channels* and also during sudden change in operational characteristics of the crypto-device i.e. via *Fault Injection*. The research in this area shows that Side Channel Analysis (SCA) attacks and Fault Injection (FI) pose a major threat because the physical implementations of the cryptographic devices are difficult to control and often result in unintended leakage of information. Generally, all hardware implementations of cryptographic algorithms are assumed to be vulnerable to SCA and FI attacks, if there are no special precautions in the implementation. Differential Power Analysis (DPA) attacks are an efficient form of SCA attacks. Several countermeasures against DPA were proposed, however development of countermeasures which makes use of FPGA features are at an infancy stage. As a part of this dissertation we developed a new countermeasure against DPA which has low-area overhead and makes use of FPGA intrinsic features. In order to validate the new countermeasure proposed, we developed an open-source tool called Flexible Opensource workBench fOr Sidechannel analysis - FOBOS. FOBOS can not only be used for research, but also for educational purposes. We propose a methodology for detecting glitches in hardware implementations on FPGAs using a delay based sampling technique. We use this methodology to validate that our proposed countermeasure is free from early evaluation effects.

Additionally, a new class of fault attacks was explored, which uses an electro magnetic field to induce faults in the target device. The Electro Magnetic Fault Injection (EMFI) perturbation is effective and non-invasive in nature. In this dissertation, we describe the background, methodology and experimental setup required to conduct EMFI. The impact of different types of probes used in EMFI attacks is explored and a calibration process used for lab experiments is presented. We discuss our preliminary results and conclude that EMFI is a viable strategy for an attacker attempting to break a cryptographic implementation.