FAME
Fault Aware Microprocessor Extension Demonstrator

Chinmay Deshpande, Marjan Ghodrati, Bilgiday Yuce, Abhishek Bendre,
Conor Patrick, Nahid Farhady Ghalaty, Leyla Nazhandali, Patrick Schaumont
Bradley Department of Electrical and Computer Engineering
Virginia Tech
Blacksburg, USA

I. The FAME Project

FAME is a collection of hardware techniques for microprocessor architectures to detect fault injection attacks, and to mitigate fault analysis through an appropriate response in software. The FAME processor is developed both as an architecture concept as well as a chip prototype.

Fault injection is a powerful hacking tool, affecting all forms of cryptography. However, there are no generic techniques to deal with the security threat of faults. The current countermeasures are based on redundancy, causing overhead in hardware, or crippling performance in software. The FAME processor uses fault countermeasures that combine fault detection in microprocessor hardware with fault response in the software application. The fault detection in hardware uses static (design-time) and dynamic (runtime) techniques for in-situ fault detection.

These fault-detecting hardware extensions are optimized for power and cost, and they can be controlled from the software application. The impacts of this project are safer, more trustworthy microprocessors that are aware of their physical environment and the associated threats to their internal processing.

The results of the FAME project have been previously presented at FDTC 2015 [1], HASP 2016 [2], ISVLSI 2016 [3], SAC 2016 [4], FDTC 2016 [5]. The FAME demonstrator has not been previously presented.

II. Demonstration

The FAME demonstrator consists of the following components.

- Printed Circuit Board with control-FPGA and FAME DUT;
- External clock generator and power supplies;
- Control PC with glitch generation and FAME debug software.

The FAME DUT can be either the FPGA prototype of the FAME processor or a daughter PCB with the FAME chip. The demonstration shows how FAME is able to detect fault injection and respond to it through an appropriate software response.

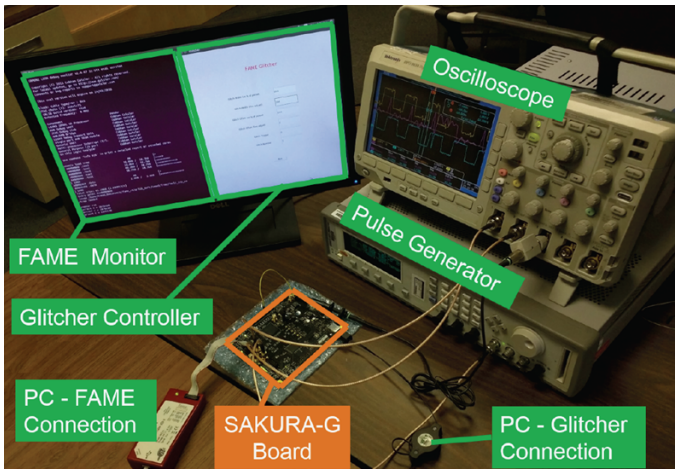

Fig. 1. FAME Demonstrator

References

[1] Bilgiday Yuce, Nahid Farhady Ghalaty, and Patrick Schaumont, "Improving fault attacks on embedded software using RISC pipeline characterization", in *2015 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2015, Saint Malo, France, September 13, 2015*, 2015, pp. 97–108.

[2] Bilgiday Yuce, Nahid Farhady Ghalaty, Chinmay Deshpande, Conor Patrick, Leyla Nazhandali, and Patrick Schaumont, "FAME: fault-attack aware microprocessor extensions for hardware fault detection and software fault response", in *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016, HASP@ICSA 2016, Seoul, Republic of Korea, June 18, 2016*, 2016, pp. 8:1–8:8.

[3] Chinmay Deshpande, Bilgiday Yuce, Nahid Farhady Ghalaty, Dinesh Ganta, Patrick Schaumont, and Leyla Nazhandali, "A configurable and lightweight timing monitor for fault attack detection", in *IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2016, Pittsburgh, PA, USA, July 11-13, 2016*, 2016, pp. 461–466.

[4] Conor Patrick, Bilgiday Yuce, Nahid Farhady Ghalaty, and Patrick Schaumont, "Lightweight fault attack resistance in software using intra-instruction redundancy", *IACR Cryptology ePrint Archive*, vol. 2016, pp. 850, 2016.

[5] Bilgiday Yuce, Nahid Farhady Ghalaty, Harika Santapuri, Chinmay Deshpande, Conor Patrick, and Patrick Schaumont, "Software fault resistance is futile: Effective single-glitch attacks", in *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016*, 2016, pp. 47–58.