

Reconfigurable Hardware for High-Security/High-Performance Embedded Systems

The SAFES Perspective

Authors:

Guy Gogniat¹, Tilman Wolf², Wayne Burleson², Jean-Philippe Diguët¹,
Lilian Bossuet³, and Romain Vaslin²

Presented by:

Brian Woods
UNCC

February 14, 2013

¹University of South Brittany

²University of Massachusetts

³University of Bordeaux

Overview

- Motivation
- Background
- Related Work
- Introduction
- Main Architecture
- Experiment Set Up
- Results
- Conclusions
- References

Motivation

- People feel security is big concern. 52% for phones and 47% said that credit card security concerns is an obstacle prevents mCommerce [1].
- Increasing usage of mobility devices like:
 - ▶ Personal Digital Assistants (PDAs)
 - ▶ Cellphones
 - ▶ Other Personal Mobile Devices (PMDs)
- Growing computational power for cracking data

Background

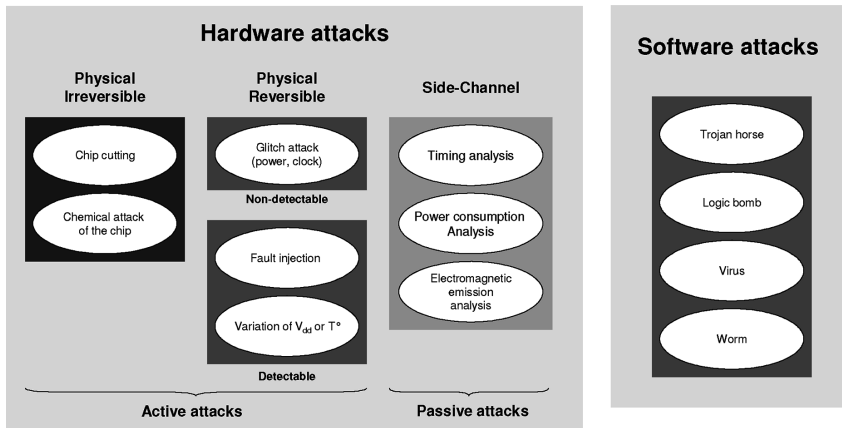


Figure: Types of Attacks[2]

Background

- Only focus on hardware attacks
- System needs to be:

Symptom-free No data leaks to disable passive attacks

Security-aware Aware of it's state and vulnerabilities

Activity-aware Must detect irregularities with sensors

Agile Able to predict or quickly detect an attack and to act fast to update security measures

Robust Tamper tolerant to resist physical attacks

- High performance
- Power aware/efficient

Related Work

- Processor based methods, but this is costly in resources
- Using accelerators/coprocessors but these don't address the attack issues
- Energy efficiency, but like the above they don't consider attacks
- Programmable accelerators have been used but not to detect and change the configuration

SAFES Architecture

- System on a chip with with *reconfigurable logic*
- The reconfigurable logic can be dynamically reconfigured
- Monitors to detect attacks
 - ▶ Power monitor
 - ▶ Clock monitor
 - ▶ Bus monitor
 - ▶ Channel monitor
 - ▶ Primitive monitor

SAFES Architecture

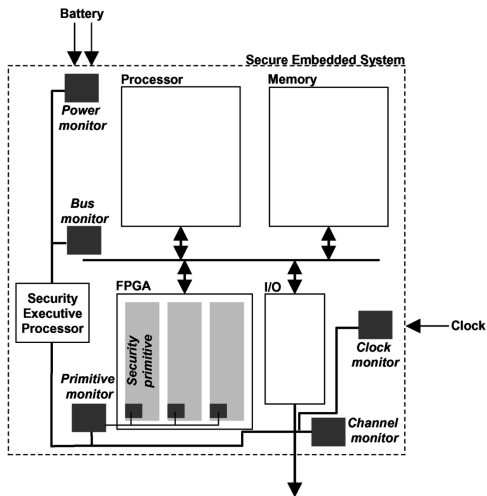


Figure: High level Overview[2]

Reconfigurable Motivation

- Acceleration of security algorithms
- Flexibility over application specific circuits
- Configuration can vary for:
 - ▶ Throughput
 - ▶ Latency
 - ▶ Area
 - ▶ Reliability
 - ▶ Power

Reconfigurable Architecture

- Processor acts at the master
- Reconfigurable logic is split into security primitives
- Main components of the security primitives are:
 - ▶ Datapath
 - ▶ Security Primitive Controller (SPC)
 - Communicates to the processor for function of the datapata
 - Reconfigures the datapath
 - Memory mapped
 - ▶ System Security Controller (SSC)
 - Monitors the datapath
 - Checks the system state through themonitors
 - Main goal is to detect attacks against the primitive
 - Memory mapped

Bibliography I

- [1] epaynews.com, *ePaynews.com - payment news and resource center - Statistics for Mobile Commerce*,
<http://www.epaynews.com/statistics/mcommstats.html>, 2004
- [2] T. Wolf et al, *Reconfigurable Hardware for High-Security/High-Performance Embedded Systems: The SAFES Perspective*, Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.16, no.2, pp.144-155, Feb. 2008