Hardware Implementation of Information Flow Signatures for Security

Prateek Patel, Indian Institute of Technology, Kharagpur
ADVISORS: Prof. R. K. Iyer, Prof. Z. T. Kalbarczyk, Nithin Nakka

Background

- Insider attacks - Exploit operating system or application vulnerabilities to
  - tamper with arbitrary memory locations
  - write malicious binaries on a disk.
- Hardware defences against malicious tampering ensure that attacks are detected reliably and with very low latencies.
- The RSE - a hardware framework to interface with the processor and monitor the state of processor to ensure the reliability and security of the executing code.

- Information flow signature technique –
  - Utilize static analysis to derive dependency tree for critical variables.
  - Encode dependencies for critical variables as signatures
  - Check that the signature is not violated at runtime.

Goals

- Synthesize and run the IFS module on FPGA based hardware.
- Run test applications to verify that the hardware is initialized and working correctly.
- Develop an application emulating the power grid scenario.
- Demonstrate application monitoring using IFS module.

Fundamental Questions/Challenges

- Identifying trusted instructions and critical data and keeping track of corresponding memory locations and program counters.
- Creating a new application program for the power grid scenario.
- Interfacing the application program running on the developed hardware with the client applications on remote computer to emulate the power grid system scenario.

Research Plan

Working Platform:
- For Compilation – Synplify pro, Xilinx ISE
- For simulations/debugging on software - ModelSim
- Hardware Synthesis – Xilinx virtex2 pro XC2VP30
- Environment - Leon 3 Processor + RSE Module

- Writing test applications to check and verify IFS module
- Creating an application to mimic the TCP/IP protocol for communicating with clients.
- Identifying critical data and trusted instructions
  - Keeping track of data address and instruction program counters
  - Augmenting the application with proper check instructions.

Research Results

- Simulated and verified that IFS module.
- Synthesized IFS for FPGA hardware and tested with web server application.
- Created a new application in the power grid context.
- Demonstrated IFS module detection of an attack against the application.