OpenTitan based Multi-Level Security in FPGA System-on-Chips

Sujan Kumar Saha, Abigail N. Butka, Muhammed Kawser Ahmed and Christophe Bobda

Department of Electrical and Computer Engineering, University of Florida

Email: sujansaha@ufl.edu and cbobda@ece.ufl.edu

FPT'23 Yokohama

Motivation

Today's embedded systems are powered by heterogeneous SoCs to increase system performance, scalability, and flexibility. Modern SoCs integrate hardware and software from multiple vendors that are not trusted. Hence, the security and reliability are impacted by the increased cyber attacks. Existing works [1,2] does not provide flexibility and complete isolation as memory is shared. To combat these, we present a security framework for heterogeneous SoCs in this work. Our Contributions are as follows.

- A OpenTitan Root-of-Trust subsystem-based security framework to prevent illegal access from software to hardware IPs and peripherals.
- Access Control Security policy description in binary format and run-time policy update mechanism.
- A prototype implementation showing the case studies and the corresponding overhead analysis is provided.

Background

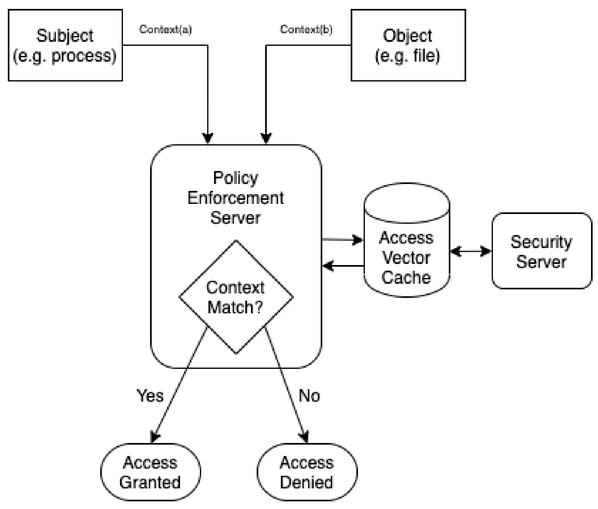

Figure 1: Overview of FLASK

Flux Advanced Security Kernel (FLASK): An access authentication mechanism that is imposed on subjects and objects in an operating system with security kernel extension. The security server governs the security policies and enforcement server grant access based on the policies, overall, providing a multi-level security (MLS) layer using domain separation.

System Model: A heterogeneous SoC is considered for this research where multiple accelerator IPs, I/O peripheral, and memories are connected in the system along with host processor using system bus.

Threat Model: Due to the presence of untrusted software, two attack scenarios are considered.

- ❖ Malicious software can directly access an accelerator IP and illicitly extract sensitive data by accessing the driver module.
- ❖ Malicious application can send read/write request while another application is using the IP.

Proposed Architecture

OpenTitan Subsystem based MLS in System-on-Chip (SoC): As shown in Figure 2, we propose to integrate OpenTitan [3] as a security subsystem in SoC due to it's lightweight and highly configurable RISC-V processor and a wide range of crypto IPs. We suggest to add HW policy server inside the subsystem to hold security policies and access enforcement components, IPFWs with IPs to add an integrated HW MLS into SoCs to enable domain separation in hardware.

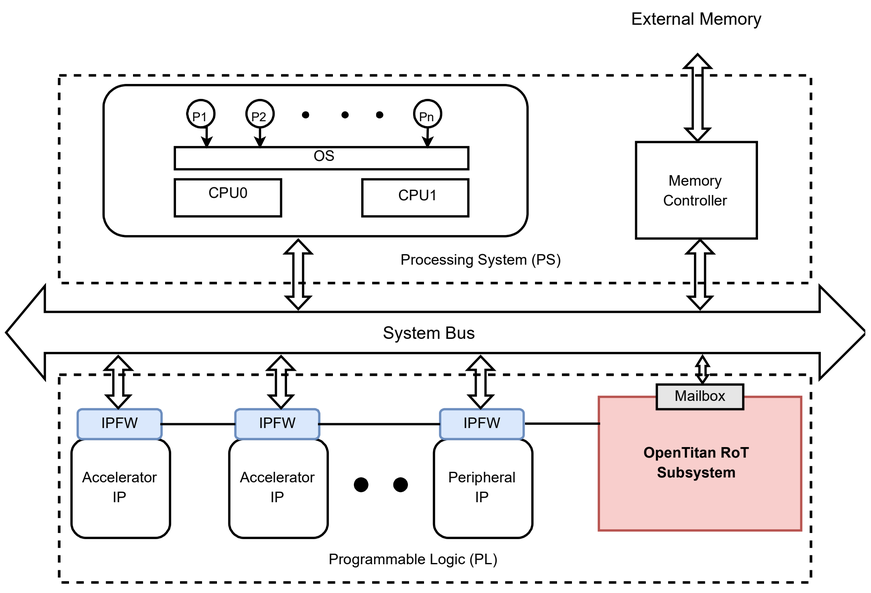

Figure 2: Secure SoC with OpenTitan subsystem and Multi-Level Security

Features

- Fine grain access control
- Dedicated and isolated connection among IPFWs and Policy server.
- Runtime policy update.
- Memory isolation for security related firmware.

Components

❑ **Hardware Policy Server:** A memory-based component integrated into the OpenTitan to hold access control policies. It's three major components are the memory, policy loading, and policy fetching unit. BRAM is utilized as the memory component. The policy loading unit is responsible for initial policy loading and run-time policy updates. The policy fetching unit extracts the security policies from the BRAM when requested by IPFW.

❑ **Secure Firmware:** Security policies are 32-bit binary values (16-bit process ID+14-bit IP Identifier+ 2-bit R/W permission). These binary values are loaded into the policy server by using secure firmware running on OpenTitan RISC-V processor. Runtime policy update is also handled by secure firmware.

❑ **IP Firewall (IPFW):** A security wrapper that enforces access control over the IPs. It has two major parts: An access vector cache (AVC) and policy lookup module (PLM). The AVC is a cache component that keeps the processes most recently used security context (IP Identifier and permission). The PLM checks the access permission of a request to access the IP. When an access request comes to the IPFW of an IP, first, the PLM checks the IP core ID of that request, then checks the IP identifier and permission. If the access permission is granted, the data is forwarded to the IP for acceleration. Otherwise, the PLM sends a policy fetching request to the policy server to get the corresponding policy.

Experimentation

- ➢ Experimentation is performed on Xilinx Zybo Z-7020 FPGA SoC board. It has ARM CPU in PS side, and PL side has OpenTitan subsystem, a RSA crypto module and IPFW.
- ➢ Two case studies:
  - ○ Mitigation of unauthorized software access to HW RSA crypto core.
  - ○ Concurrent access to RSA IP by exploiting two ARM cores are prevented by the IPFW .

TABLE I: FPGA Resource Utilization of Security Components

Component	Resource	Utilization	Utilization %
RoT Subsystem	LUT	13794	25.92
	FF	20017	18.81
IPFW	LUT	149	0.28
	FF	334	0.31
Policy Server	LUT	56	0.1
	FF	170	0.15

TABLE II: Execution Delay of IPFW and Policy Server

Component	Operation	Cycle Count
IPFW	AVC Hit	3
	AVC Miss	7
Policy Server	Policy Firmware Load	1 cycle per policy
	Policy Fetching	3

- ✓ Total FPGA resource consumption is 25.92% which includes the OpenTitan RISC-V processor, memory controller, and other peripheral IPs.
- ✓ The MLS components, IPFW and Policy server (can hold upto 16 policies) need less resources.
- ✓ Execution time can be as high as 7 cycles for worst case scenario.

Acknowledgements

This work was supported by DARPA under the Automated Integration of Secure Silicon (AISS) project. We would like to show our gratitude to Xilinx for providing the Zynq boards.

References

[1] Ngabonziza, B., Martin, D., Bailey, A., Cho, H., & Martin, S. (2016, November). Trustzone explained: Architectural features and use cases. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC) (pp. 445-451). IEEE.

[2] Saha, S. K., & Bobda, C. (2020, December). FPGA accelerated embedded system security through hardware isolation. In 2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST) (pp. 1-6). IEEE.

[3] OpenTitan, "OpenTitan root-of-trust silicon chip", https://opentitan.org/.