Proposal for Analysis of Security In a Modern Processor

Justin Cox and Tyler Travis
Department of Electrical and Computer Engineering
Utah State University
Logan, Utah 84322
email: justin.n.cox@gmail.com, tyler.travis@aggiemail.usu.edu

***Abstract*— Hardware security is an ever increasing area of study since exploits have been found on computer systems. People are able to look at the memory of a system to see what is processing. This paper proposes adding an extra level of security between the memory and the pipeline. This layer would encrypt data headed to memory and decrypt the data headed to the pipeline making the data held in memory incomprehensible to the attacker. To make the added cryptographic system more secure, research will be done on the benefits of utilizing a Physically Unclonable Function (PUF). Further analysis will be done on how this will affect the processors performance.**

***Index Terms*—encryption, decryption, security, pipeline, PUF.**

I. INTRODUCTION

Over the years, there have been many advancements made to computer architecture. These advancements have been primarily focused on improving performance and power consumption. As a result, the security of these architectures has been neglected. Malicious attacks on computer systems are becoming more common and as a result there is greater need for more secure systems.

The optimal solution to this problem is to completely redevelop the architectures with security as a top priority. However this option is not very practical as it would be far too expensive to replace the current processors and there is a need to support legacy machines. Therefore, we propose to create security modules that can be added to current processor architecture.

II. OBJECTIVE

The objective of this project is to implement a more secure version of current processor architecture. The goal is to provided the maximum amount of security while maintaining performance at a reasonable level for the CPU.

III. METHODOLOGY

The following subsections will describe how this project will fulfill the objective. The first subsection will describe how the data will be protected by cryptography. The next section will describe how the cyptograhic modules will be improved using a PUF. The last subsection will outline the methods used to measure the performance of the proposed system.

A. Encryption and Decryption of Data

The memory can be modified by an attacker and as a result the attacker is able to change the execution flow of a program. Therefore to prevent the attacker from knowing where to modify the data, it is important for the CPU to encrpyt data being stored into memory. Initially, we will encrypt memory that is stored in registers, cache, RAM, and virtual memory [1]. If the performance decreases significantly, encryption will be exclude from the registers and/or cache. Assuming the pipeline is trusted, data being pushed into the pipeline will be decrypted.

These encryption and decryption modules will be built and added into gem5.

B. Physically Unclonable Function (PUF)

A PUF is used to generate secrets extracted from a physical device due to manufacturing differences. This uniqueness can be used for more secure key generation for encryption/decryption [2]. Since the PUF output is generated by a physical device, a predetermined secret will be used to simulate the PUF output.

C. Benchmarking and Performance

The simulator that this project will use is gem5. The security modules will be added on to several different processor benchmarks found in gem5. A chosen application will be run on all benchmarks without the added security modules and again with the added security modules. The performance will be compared between the results.

REFERENCES

[1] G. Edward Suh, C. W. O'Donnel, I. Sachdev, and S Devadas. Design and Implementation of the AEGIS Single-Chip Secure Processor Using Physical Random Functions. *Proceedings of the 32nd annual international symposium on Computer Architecture*, 2005.

[2] M. Deutschman, "Cryptographic Applications with Physically Unclonable Functions," M.S. Thesis, Inst. Mathematics, Alpen-Adria-Universität Klagenfurt, Klagenfurt, Austria, 2010.