Simulating Valleytronics Logic at Gate Level

A C++ Library and Example for Building Fully Electric Valleytronic Processors

T. Jacovich[1]

[1]Department of Physics
The George Washington University

ECE 6120: Advanced Microarchitecture Final Presentation

Introduction to Valleytronics

- Aegis is a buckler(shield) wielded by Athena and given to her by Zeus.
- It is also the name of a near-ship anti-missile defense system.

Design Requirements

The AEGIS Architecture is a processor designed to provide secure and verifiable computation when the only trusted component is the CPU package (and, optionally, a portion of the kernel known as *SKernel*) This requires:

- Memory Integrity Verification
- Encryption/Decryption of Off-Chip Memory
- Secure Context Manager

We will break each of these sections down and discuss its specific implementation in AEGIS

The AEGIS Architecture

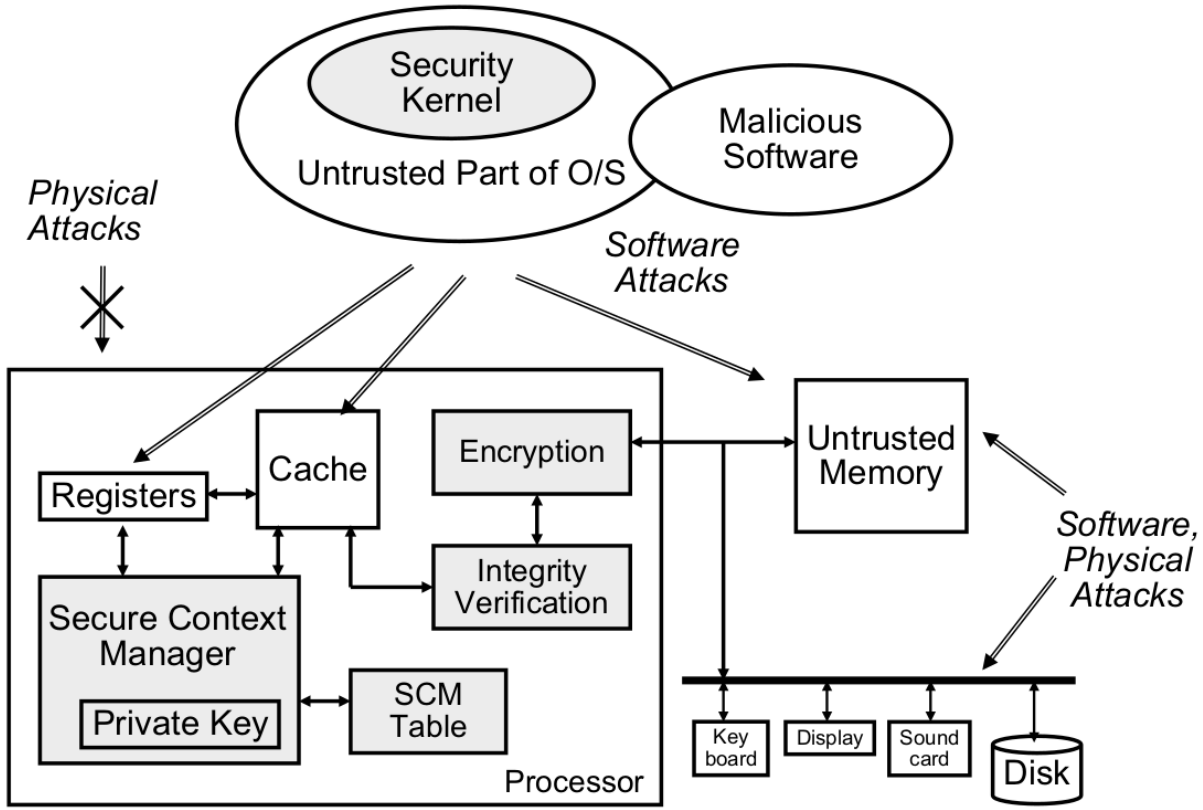

Figure 1: Our secure computing model.

Tamper-Evident Processing

Verifiable computations need a way to identify and prevent operations from being tampered with.