Software Cannot Protect Software: An Argument for Dedicated Hardware in Security and a Categorization of the Trustworthiness of Information

Air Force Institute of Technology
Matthew Judge
Paul Williams
Yong Kim
Barry Mullins

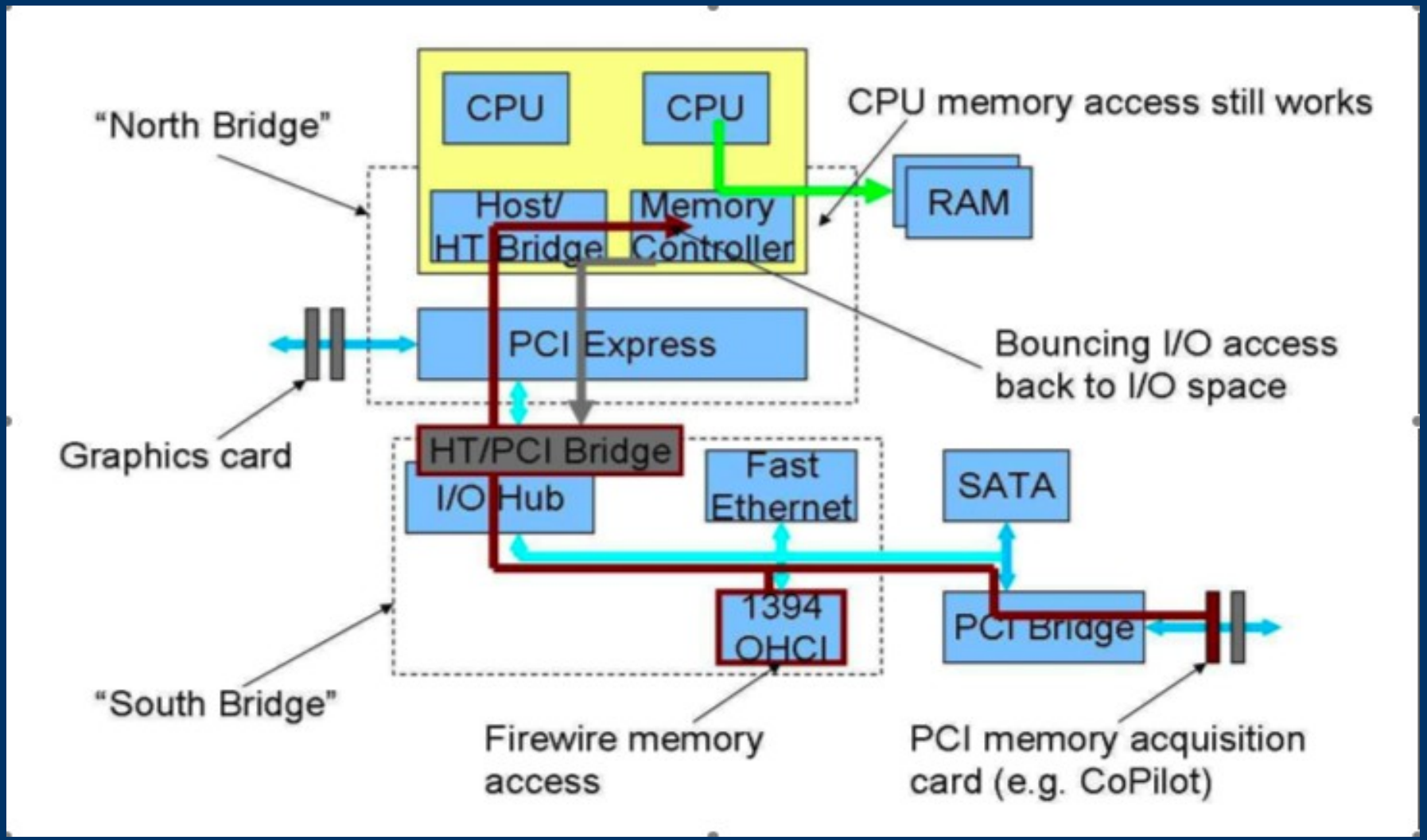
Overview

- Current Security Classifications
- Defeat of Hardware RAM Acquisition
- Why Hardware?
  - Trustworthiness of Information
- Security Hardware Requirements

Current Security Classifications

- Kuperman's Timeliness of Detection
  - Real-time Detection
  - Near Real-time Detection
- Mott's Hardness of Security System
  - Ranges from Open (no) security to Complete Security
  - Loose/Semi-hard Security desirable level
  - Classification does not discuss accuracy of information received by security system

Defeat of Hardware-Based RAM Acquisition



Defeat of Hardware-Based RAM Acquisition

- Corrupts RAM information being sent to PCI Bus
  - Remaps PCI Bus access into I/O address range
  - PCI Bus never sees actual contents of memory
- Processor access to memory unaffected

Lesson: Hardware is not an automatic solution

Why Hardware?

- Reduce Avenues of Attack
- Trustworthiness of Information
- Additional/Different Information Available
- Timeliness of Detection

Software Deficiency

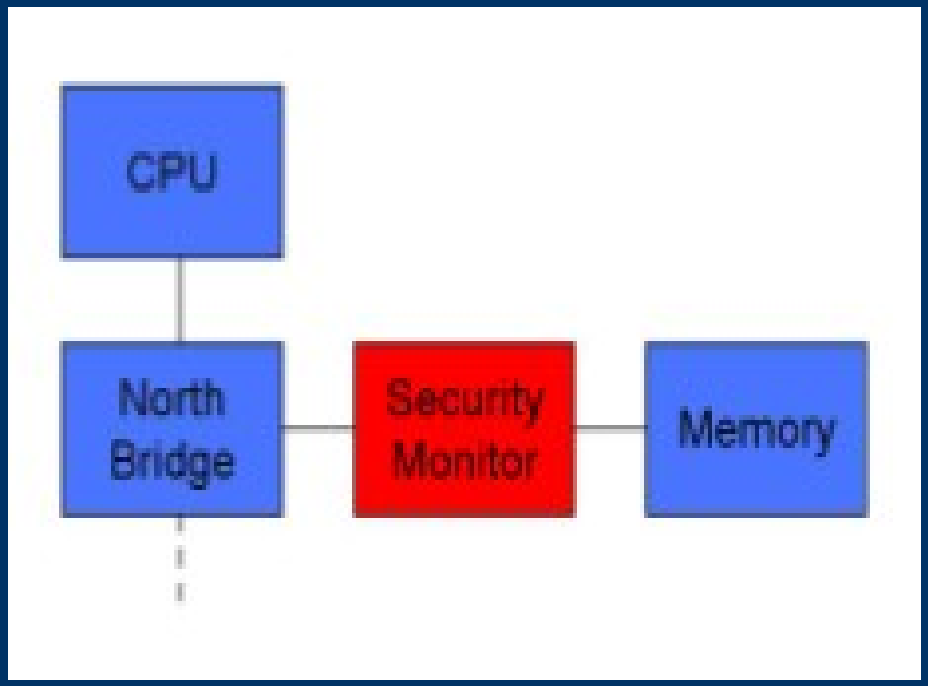
- Software alone cannot guarantee *Real-time Detection*
- Once kernel is corrupted, monitor is vulnerable
  - Virtual Machines reduce complexity of kernel, but does not solve this issue
- Software always offers no better than *Second-hand Information*

Trustworthiness of Information

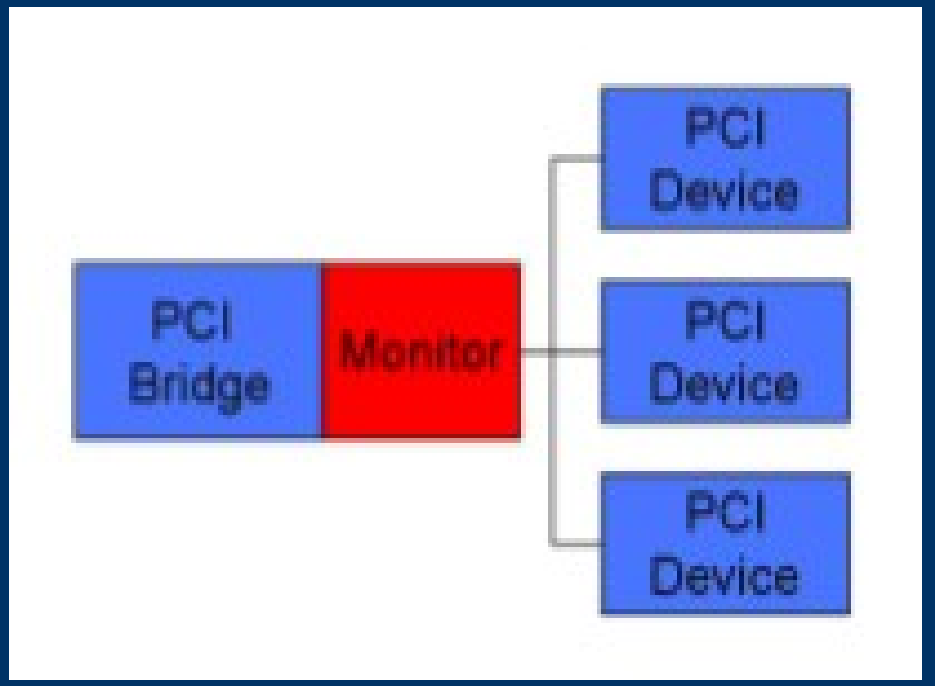
- Immediate Information
  - Monitor inline between system and device
- First-hand Information
  - Monitor on same bus as device
- Second-hand Information
  - System components inline between monitor and device

Trustworthiness of Information

Immediate



First-hand



What Do We Mean by Hardware Security?

- Dedicated hardware for security
  - FPGA
  - Processor running software
- *Communication* between production system and security system in hardware

Hardware security does NOT mean exclusively hardware – only hardware separation between production and security system

Security Hardware Requirements

- First-hand Information
- Dedicated Monitors
- Explicit Hardware Communication
- Dedicated Storage
- Dedicated Security Process

Summary

- Current Security Classifications
- Defeat of Hardware RAM Acquisition
- Why Hardware?
  - Trustworthiness of Information
- Security Hardware Requirements

Questions or comments?