Towards Agile and Privacy-Preserving Cloud Computing

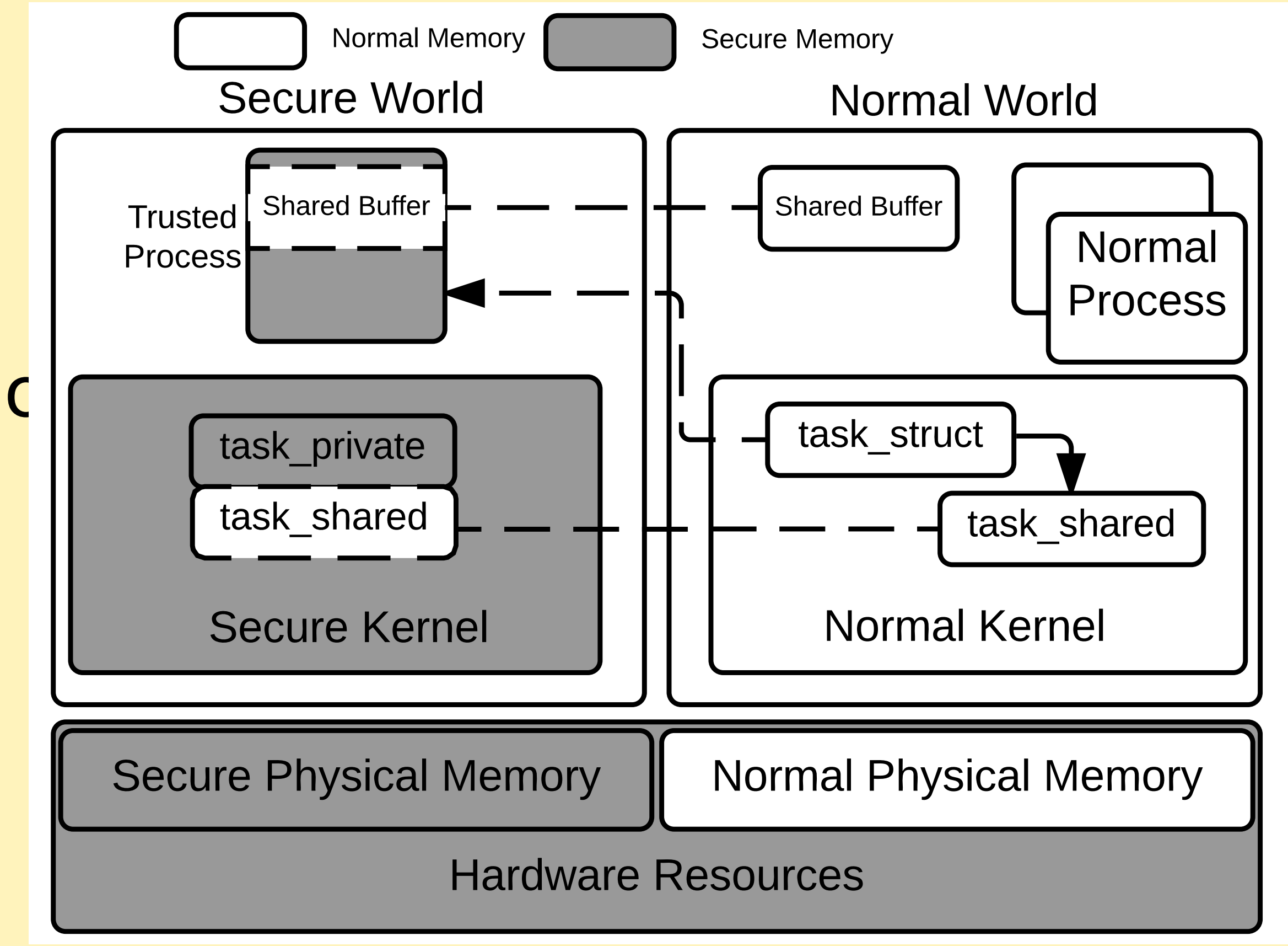
Meng Yu, University of Texas at San Antonio (CNS-1422355)
Peng Liu, Pennsylvania State University (CNS-1422594)

Project overview

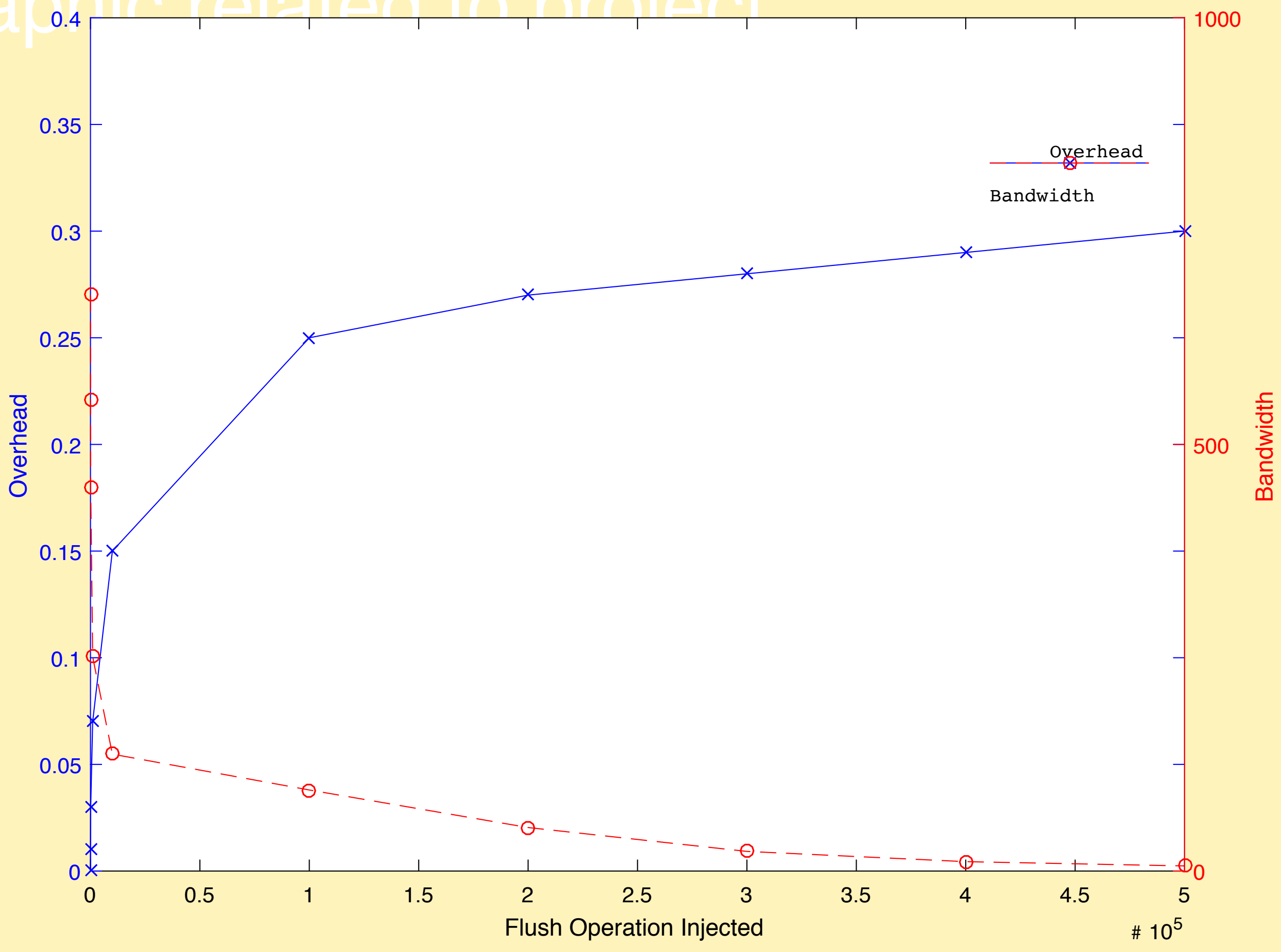
The major goal of the project is to provide mechanisms for fast configuration of a cloud platform, and at the same time, provide protections to applications in case of a compromised operating system or malicious environment.

In this project year we focused on two problems: 1) protecting applications in a hardware isolated environment against a malicious operating system; 2) measure and mitigate side-channels based on last level cache memory.

Mc



Graphic related to project



Approach

Protection using ARM TrustZone

- The protected application will be put into an isolated memory area and all system services will be delegated by a secure kernel inside the secure area.

Mitigating Side-Channels

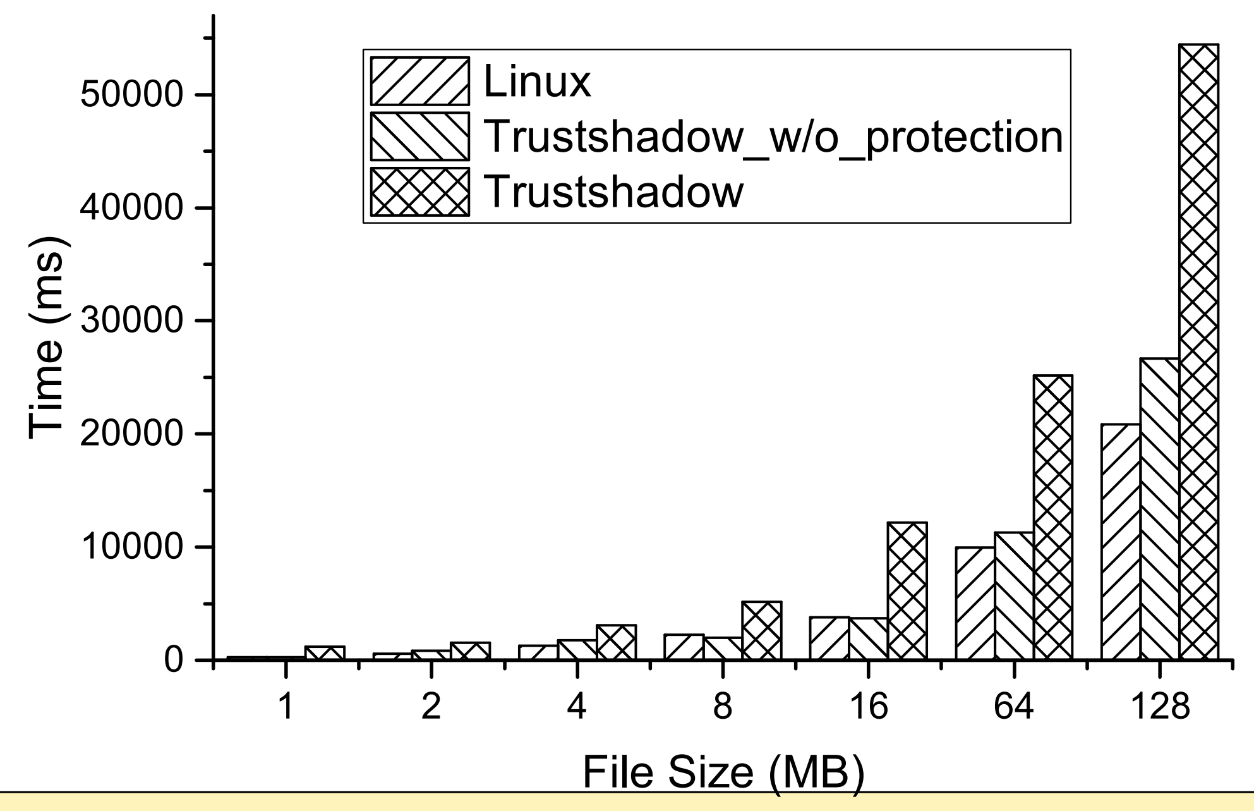
- Noises are injected to the side-channels to control the maximum bandwidth available to the attacker.

What we have done for protection

A prototype system has been built to evaluate the effectiveness and efficiency of the protection. The techniques can be used to protect crucial applications against an untrusted operating system.

What we have done for side-channels

We have done evaluation on both x86 and ARM architectures. The noise injections are done in either VMM, or a control VM in order to evaluate the effectiveness of defense in a virtualization environment.



Examples of noise injection in a side channel.

Original

Noisy

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

University #1 Logo

University #2 Logo