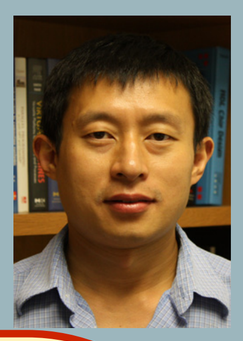
Architecting against Software Cache-based Side Channel Attacks

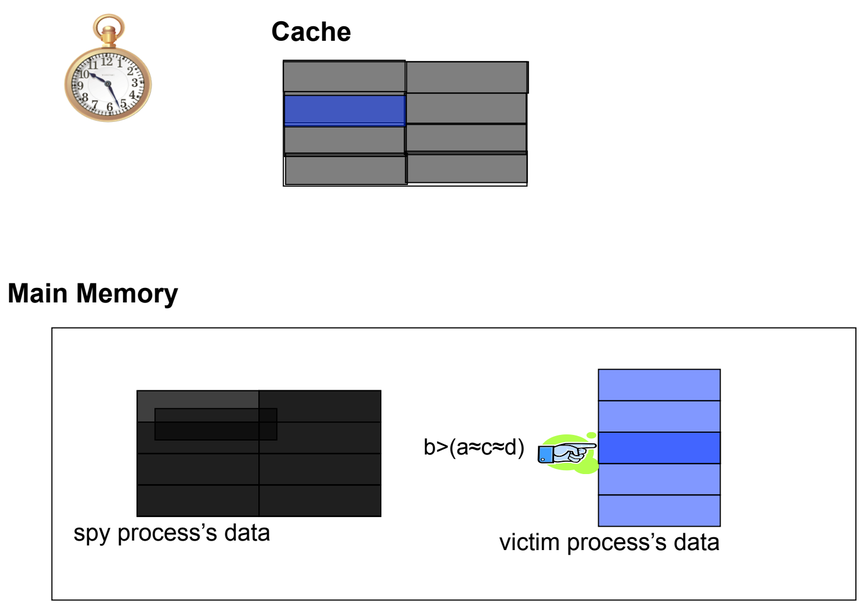
Huiyang Zhou, North Carolina State University



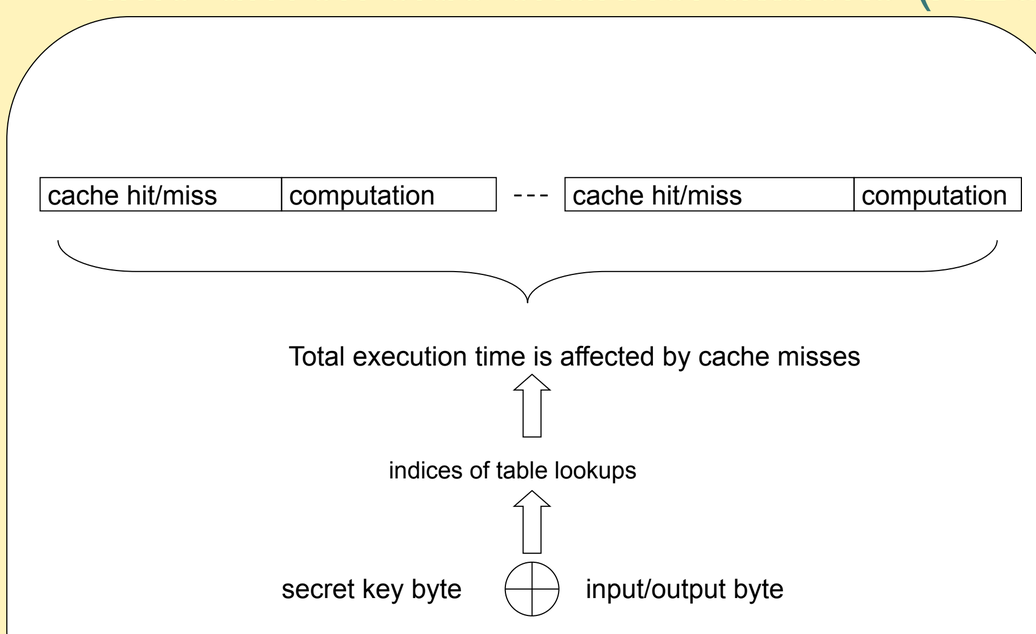
Problem: *Using cache-like architectural components including data caches, instruction caches, or branch target buffers as a side channel, software cache-based side channel attacks are able to derive secret keys used in cryptographic operations through legitimate software activities*

Objective: *Determining the root cause of cache-based side channel attacks; developing memory hierarchy that can defend against such attacks*

Access-driven side channel attacks



Time-driven side channel attacks (AES)



Analyzing cache based attacks

	Key-dependent control flow	Key-dependent table lookups	AES	RSA	Access-driven	Time-driven
Data Cache (D-Cache) Attacks		√	√	√	√	√
Instruction Cache (I-Cache) Attacks	√			√	√	
Branch Target Buffer (BTB) Attacks	√			√	√	

Root causes

For D-cache attacks, the source of leakage is cache misses of lookup table data, whose indices are key dependent.

For I-cache attacks, the source is cache misses of instructions, whose executions depend on secret keys.

For BTB attacks, the source is updates of critical conditional branch target addresses in BTB, which are determined by secret keys.

Hardware-Software Integrated Designs against cache-based attacks

Defending against D-Cache Attacks

- Improving Partitioned and Locked caches (PLcaches) and Random Permutation Caches (RPcaches)
- Securing Regular Caches with Informing Loads

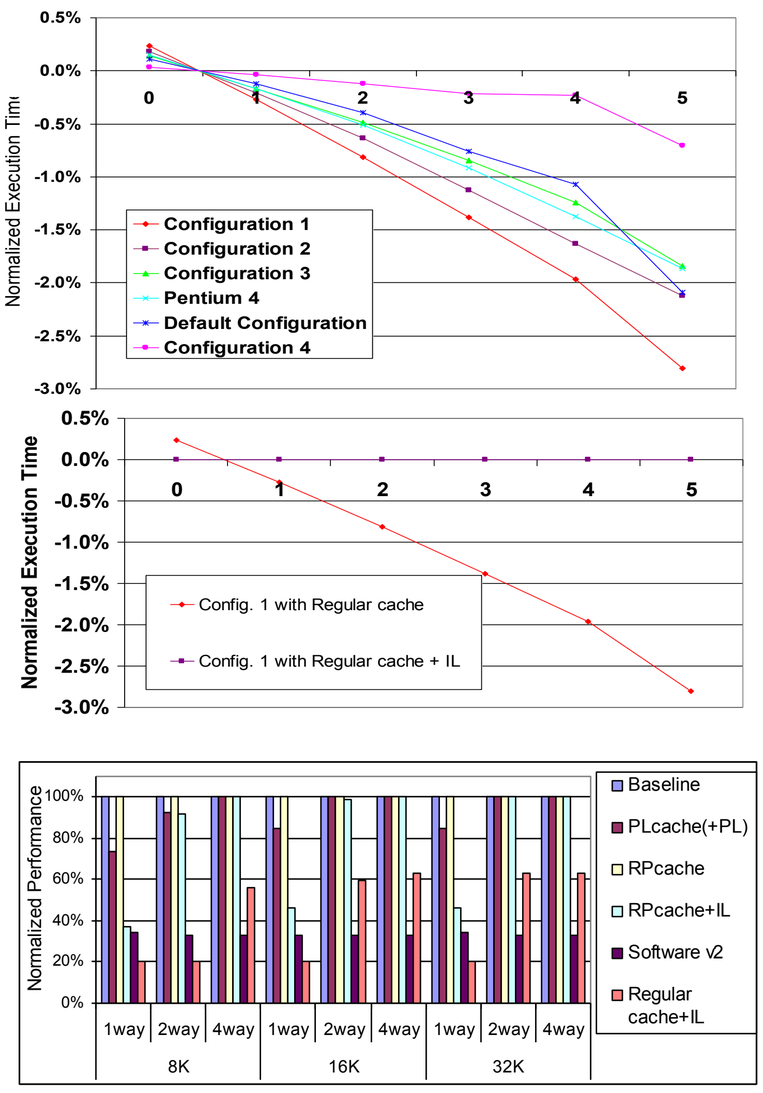
Defending against BTB Attacks

- Always update policy + software padding

Defending against I-Cache Attacks

- Improved PLcaches and RPcaches

Results



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

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

NC STATE UNIVERSITY