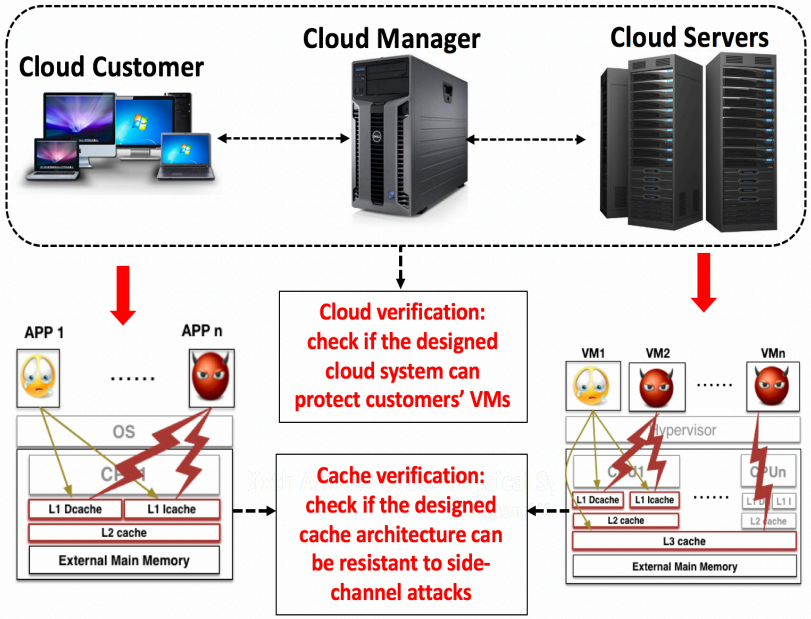
Practical and Scalable Security Verification of Security-Aware Hardware Architectures

Challenge:

- How to systematically check new security architectures and identify the conditions under which they work.
- How to develop security invariants and model complex hardware-software architectures, and attackers, to conduct security verification.

Solution:

- For distributed cloud system, propose new security invariants, model and verify the system, and identify the necessary and sufficient conditions.
- For cache architecture, specify fundamental properties to eliminate side-channel information leakage and verify if these properties can be satisfied.



Security Verification of hardware architectures

➢Develop methodology to check the security properties of hardware-software security architectures at design time.

➢Reduce the attack surface in cloud computing.

➢Verify a secure cache's resilience to side-channel attacks on caches.

Scientific Impact:

- Identify the necessary and sufficient conditions that the cloud provider should adopt to protect virtual machines running in clouds.
- Propose methodologies for security verification of a cache's resilience to cache side-channel attacks.

Broader Impact:

- Design a general methodology for verifying different hardware-software security-aware architectures.
- Researchers and computer architects can use this method to check their designs before costly implementations.
- Customers will gain assurance about their computations running on these security-verified architectures.

Prof. Ruby B. Lee, Princeton University

NSF SaTC-1526493

Contact: rblee@princeton.edu