Hardware-Software Security Research Challenges

Ruby B. Lee
Princeton University

Cybersecurity R&D Themes Panel
May 19, 2010, Oakland, California.

A possible rationale for a few themes

- Security must be end-to-end and top-to-bottom (preferably bottom-to-top)
- There are no silver bullets or easy answers
- However, with finite funds and the escalation of cyber attacks and increasing damages, are there some research directions that have game-changing potential?
- By proposing a shared vision and common goals, can we inspire the research community to produce novel, effective, synergistic and deployable results?

Impact of Game-Change Vision on Research

- Goal: Significantly improve cyber security by changing the rules of the game, so that effective attacks are much harder to achieve
- Requires out-of-the-box rethinking of systems
  - hardware, software, networking
  - holistic, at all levels
- Implicitly includes clean-slate designs in security research!
  - Compatibility with existing systems not an absolute requirement, BUT
  - new architectures should be realistically deployable

“Security without compromising Performance, Energy consumption, Cost and Usability”

Lee’s mantra

Example: Current Game

- Applications developer may put in comprehensive security policies and mechanisms for a security-critical task, or to protect the confidentiality or integrity of secret, sensitive or critical information
- However, this can easily be undermined by
  - a compromised lower layer of systems software, or
  - independent hardware mechanisms and policies

  for which the application developer has no control
- Attacker's strategy: Attack Below
- Problems: all-powerful and all-seeing, complex OS; security solutions that ignore hardware

Tailored Trustworthy Spaces (New Game)

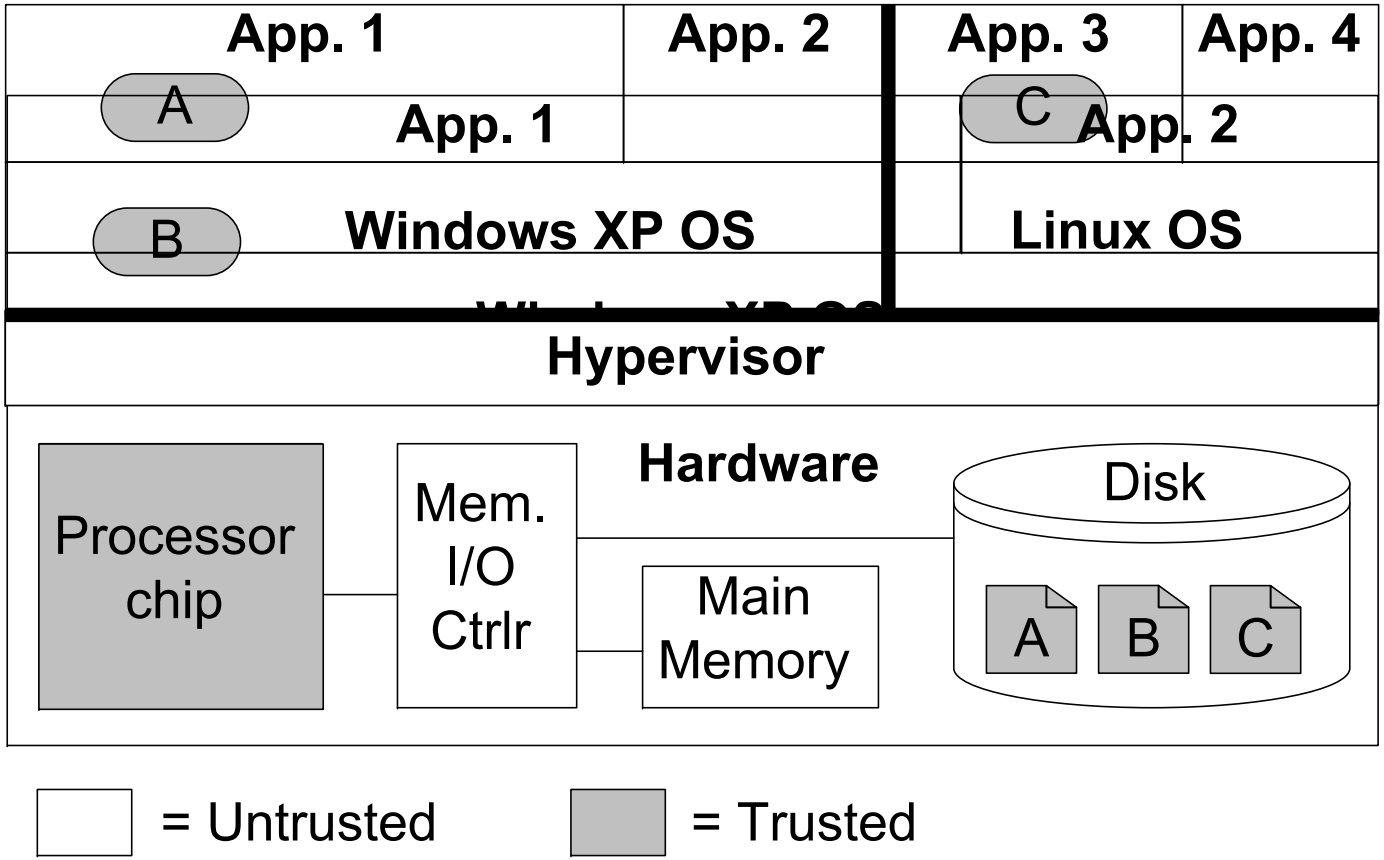
- Can we change the game so that the stakeholders **can control** their own destiny?
- Can we define new hardware-software architectures that enable applications to **be responsible** for their own security?
  - Minimize the "blame game"
  - Minimize the attack surface
  - Resilient execution of security-critical tasks even in the presence of malware in the system
  - Data that protects itself from security violations
  - "Tailored attestation" and data provenance

Some Research Questions

- How to use the services of system software (e.g., OS) without trusting it completely?
- Can new hardware-software mechanisms provide a secure execution environment for security-critical software modules, in spite of a compromised OS and malware in parts of the system?
- How to achieve security solutions that have the flexibility and adaptability of software, with the trust anchors, non-bypassable enforcement and performance of hardware?
- How to determine if remote end-points are trustworthy, and if sufficient trust exists across heterogeneous systems?
- How to grade trustworthiness of software and hardware?

Feasibility Example:

e.g., SP and Bastion architectures

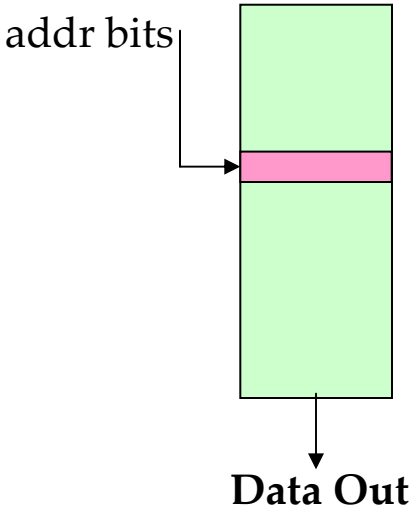


Current Game

- Fundamental performance optimization methodology: **Make frequent paths fast, infrequent paths slow**
- Problem: enables information leakage through side-channel and covert-channel attacks;
  - Processor or cache-based side channels are extremely fast and easy to launch (through software, even remotely)
  - Undermines software isolation mechanisms, e.g., Virtual Machines
- Attacker's strategy: Exploit hardware performance (or power) optimization mechanisms to leak information
- New Game: Need new methodologies for improving performance and security simultaneously
  - e.g., based on randomization

Feasibility example: improving Cache performance and security simultaneously

Direct-Mapped caches

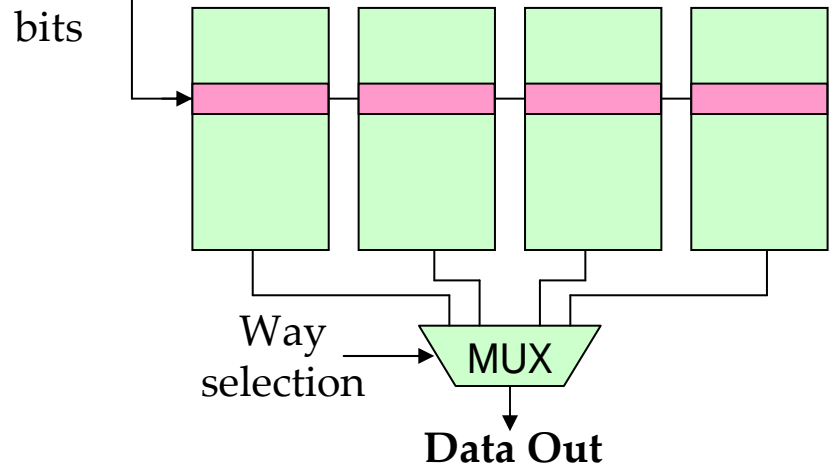


Lower access time

Lower power per access

Associative caches

e.g., 4-way SA cache



Lower cache miss rate

Newcache achieves best of both classes of cache architectures

Hard Research Problems

- How to define tailored trustworthy spaces, their attack surfaces and protect them from attack?
- What are fundamental hardware-software requirements and architectures that enable tailored trustworthy spaces?
- What are new methodologies for improving system performance that do not leak protected information?
- How to employ efficient randomization techniques to provide a moving target defense, or bio-inspired computing, etc., to increase resiliency to attacks?

Challenge the status quo

Think of facts as merely assumptions