Certifying Program Execution with Secure Processors

Benjie Chen Robert Morris
Laboratory for Computer Science
Massachusetts Institute of Technology

Motivation

- All PCs may soon include trusted computing HW
- Potential impact far greater than copy-protection!

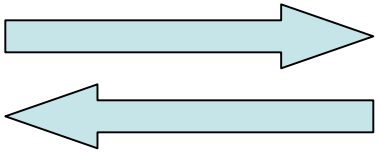
Goal: explore appropriate hardware and software design

Secure Remote Login

Alice @ Internet Cafe

Is anyone monitoring my keystrokes?

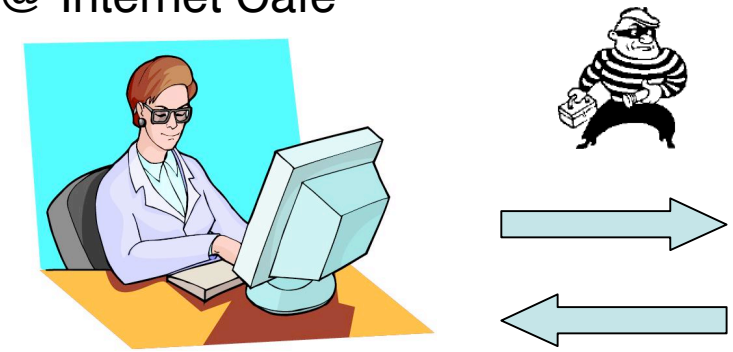
Login session



Trusted server

Partial Solutions

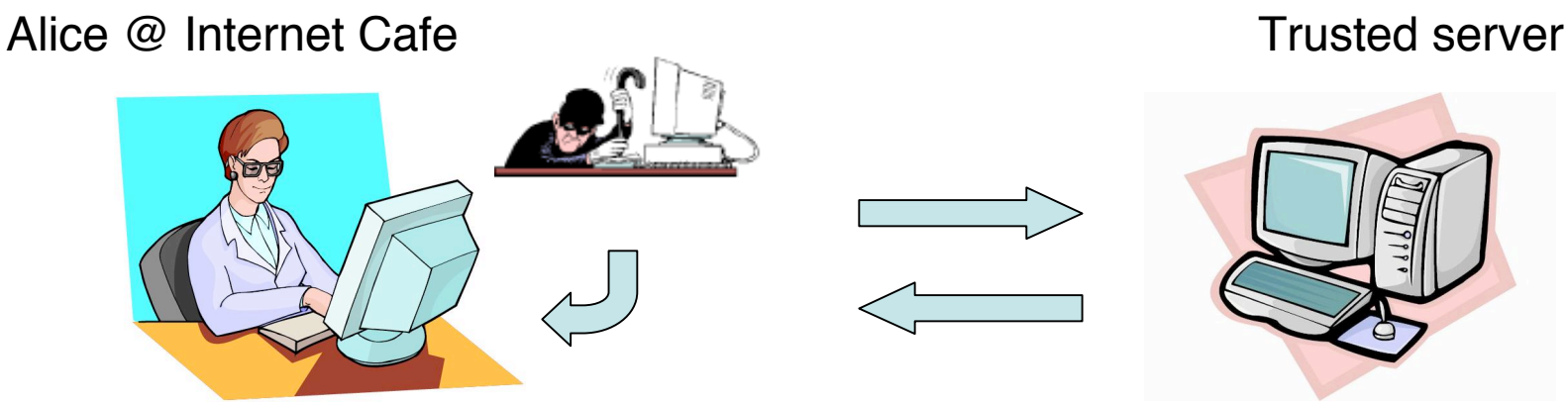
Alice @ Internet Cafe



Trusted server

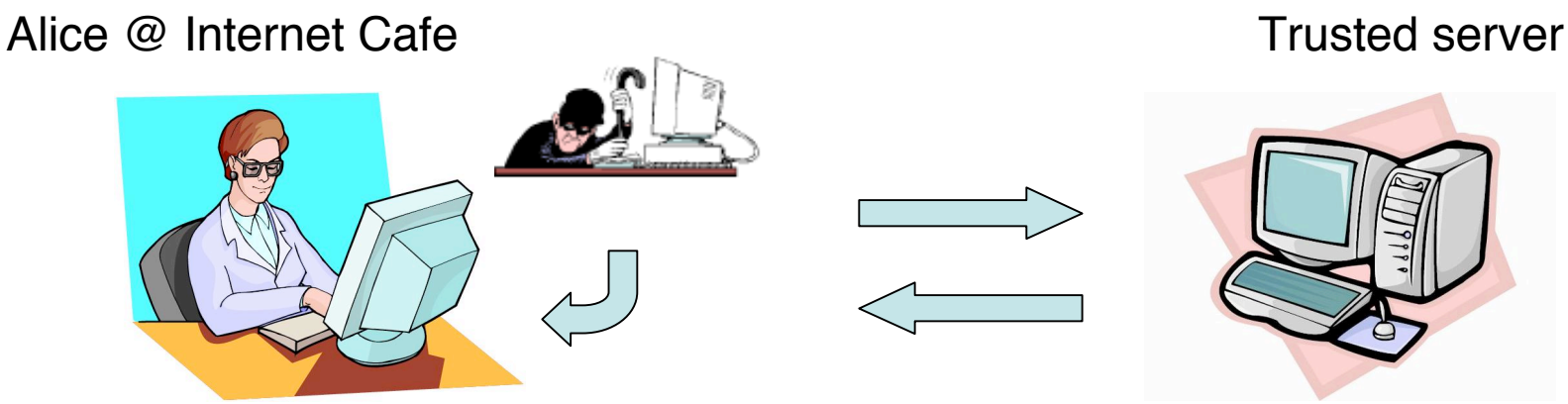
Attack	Solution
Network sniffing	Encrypt session (e.g. ssh)
Fake login prompt	One-time phrase from server
Sniffing login password	One-time password; Personal smart-cards

We Won't Try To Solve



- Modified keyboard or display
  - To steal keystrokes and data
- A camera can spy even personal laptops

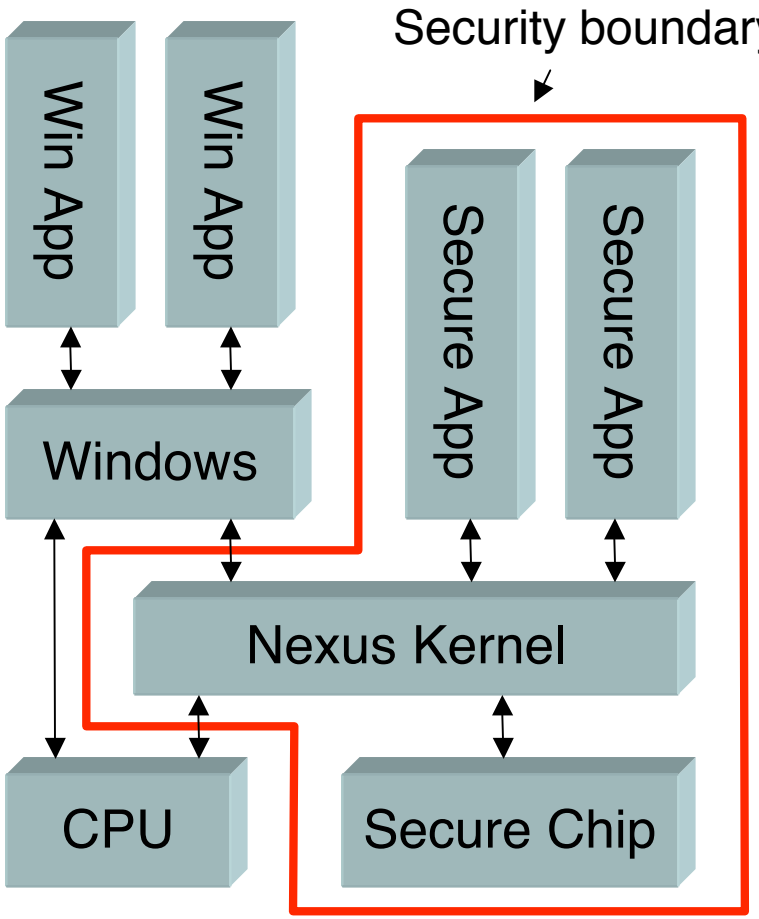
Hard-to-Prevent Attacks



- Attacks by owner of the terminal
  - Install bad ssh software
  - Install bad operating system/device driver
  - Even w/ trusted OS, can snoop memory with DMA

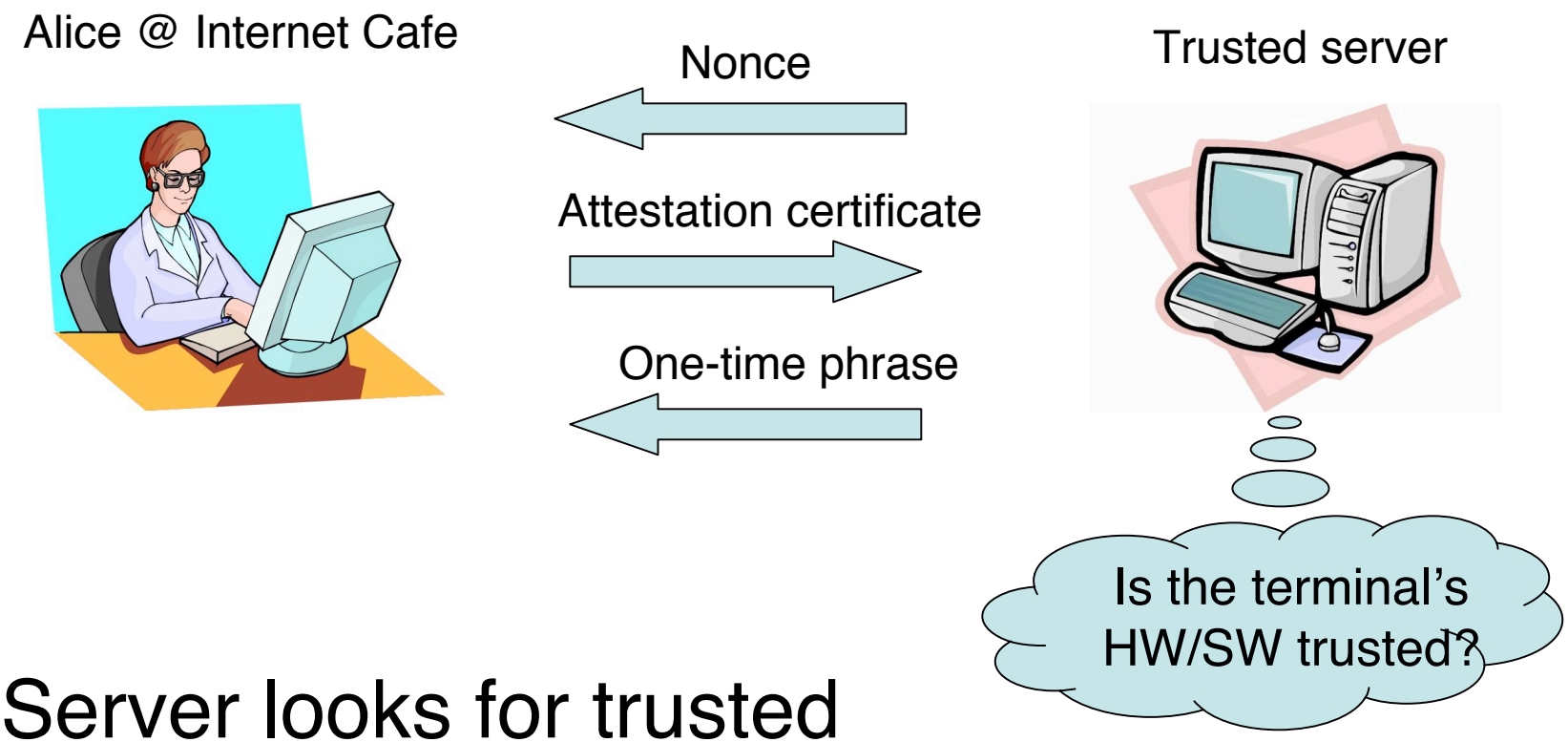
Can Trusted Computing Help?

Microsoft Palladium (NGSCB)



- Secure boot
  - Keep fingerprints of BIOS, B/L, Nexus in secure chip
- Attestation
  - Nexus computes fingerprint of secure app
  - Secure chip signs all fingerprints
- Keyboard driver in Nexus
- Modified HW guides DMA

Remote Login w/ Palladium



- Server looks for trusted
  - Chip, BIOS, boot loader, Nexus, ssh

Palladium Pros

- Pros
  - Detect un-trusted chip, BIOS, boot loader
  - Detect un-trusted Nexus and ssh
  - Prevent DMA of memory of trusted apps

Palladium Pros and Cons

- Pros
  - Detect un-trusted chip, BIOS, boot loader
  - Detect un-trusted Nexus and ssh
  - Prevent DMA of memory of trusted apps
- Cons
  - Can you keep the Nexus small?

Palladium Pros and Cons

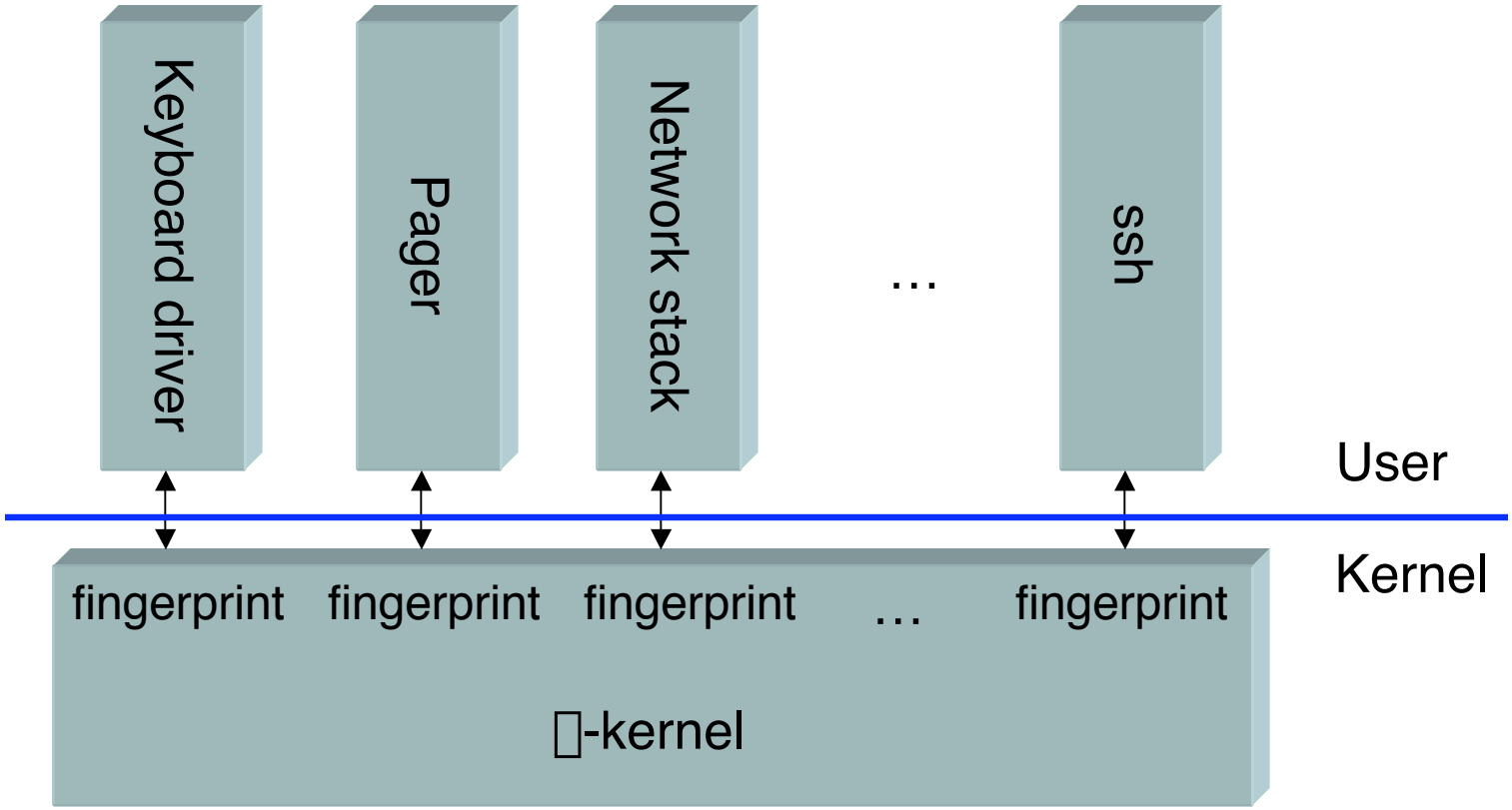
- Pros
  - Detect un-trusted chip, BIOS, boot loader
  - Detect un-trusted Nexus and ssh
  - Prevent DMA of memory of trusted apps
- Cons
  - Can you keep the Nexus small?
  - Can you verify Windows' services?

Palladium Pros and Cons

- Pros
  - Detect un-trusted chip, BIOS, boot loader
  - Detect un-trusted Nexus and ssh
  - Prevent DMA of memory of trusted apps
- Cons
  - Can you keep the Nexus small?
  - Can you verify Windows' services?
  - Non-DMA attacks on memory

How Can We Improve Palladium's Security and Verifiability?

Use Small □-kernel



- □-kernel allows attestation of all OS modules

Flexible Security Boundary

- Secure Remote Login's security boundary
  - ssh program
  - -kernel
  - keyboard driver
  - BIOS, B/L, secure chip
- Some apps need more, some less
  - E.g. pager, network stack

-kernel Challenges

- Can we maintain a modular system?
  - Small kernel & OS modules - verifiability

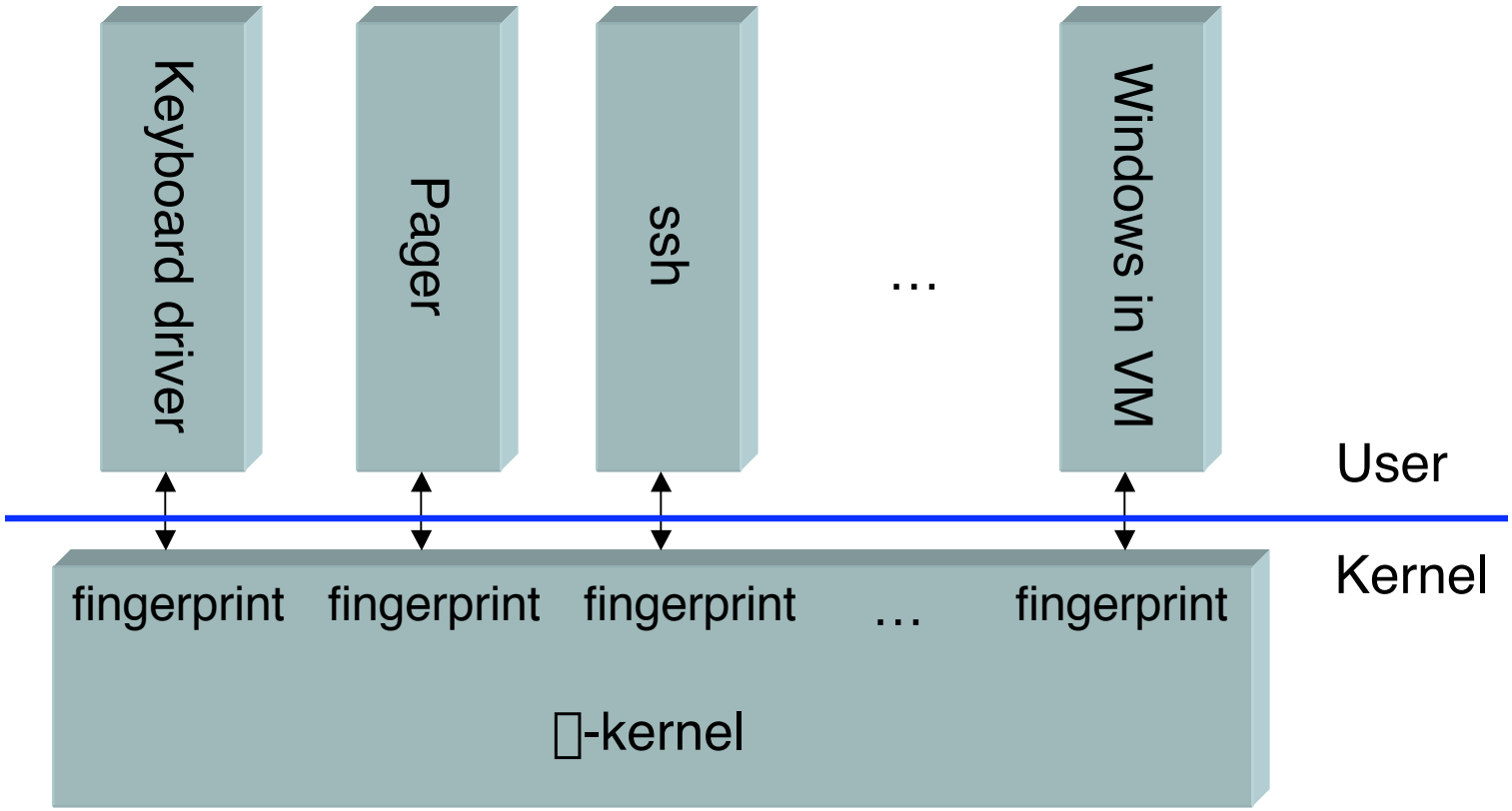
□-kernel Challenges

- Can we maintain a modular system?
  - Small kernel & OS modules - verifiability
- What about performance?
  - Careful engineering & SMT?

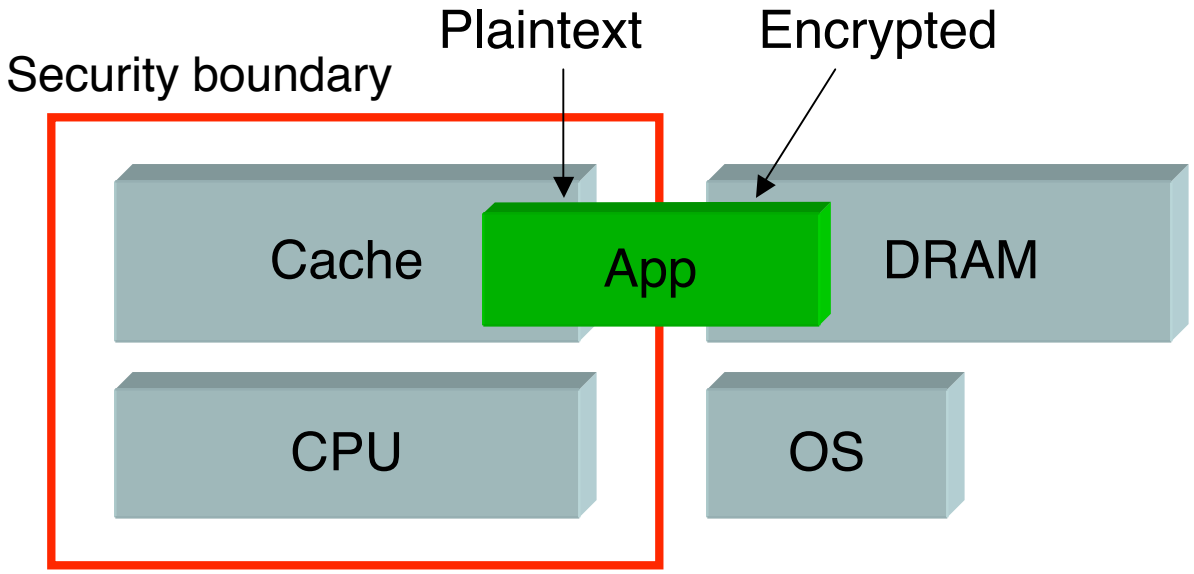
□-kernel Challenges

- Can we maintain a modular system?
  - Small kernel & OS modules - verifiability
- What about performance?
  - Careful engineering & SMT?
- What about popular apps?

Un-trusted Apps Run In VM



XOM (Lie et al 00) Prevents DRAM Attacks



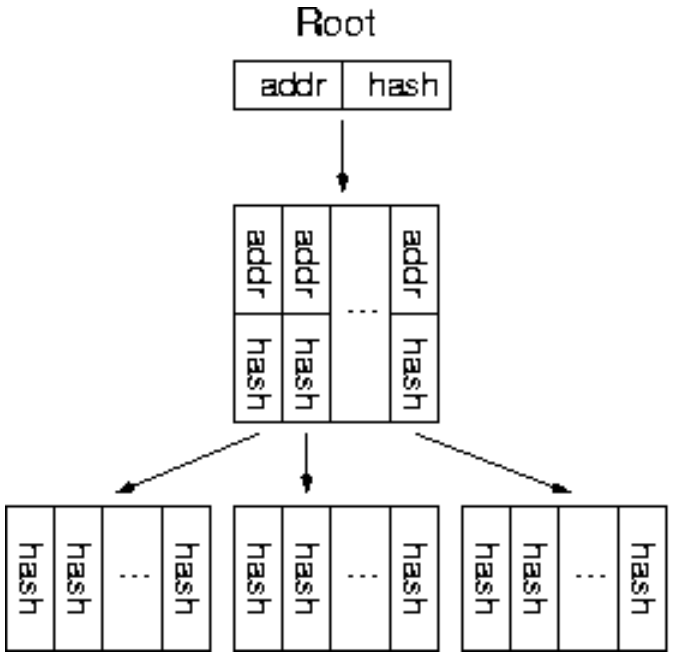
- Processor decrypts copy-protected program
- HW/FW implements crypto-paging (Yee 94)
- Cannot easily find out what OS is running

Borrow Crypto-Paging

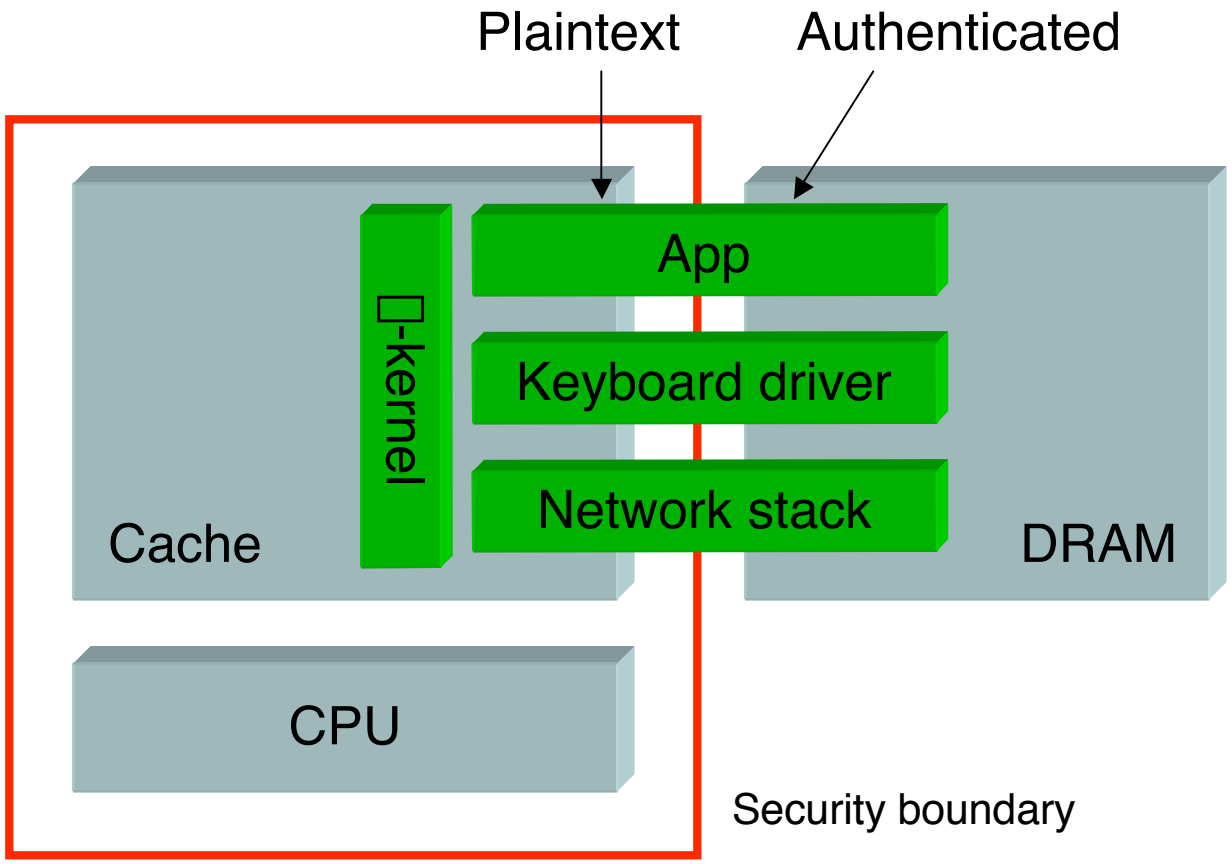
- Use tamper-resistant processor
  - Cache is trusted and safe
- Run □-kernel in secure processor
- □-kernel authenticates data to/from DRAM

Memory Authentication

- Merkle tree
  - Tree of hashes
  - Parent authenticates children
  - Leaves authenticate physical memory
  - Secure processor stores root
  - Trap handler uses/updates tree when loading or evicting cached data



Cerium


Plaintext
Authenticated
App
Keyboard driver
Network stack
-kernel
Cache
DRAM
CPU
Security boundary

Secure Remote Login w/ Cerium

Alice @ Internet Cafe

Nonce

Trusted server

Secure Remote Login w/ Cerium

Alice @ Internet Cafe

Nonce

Signed certificate

Trusted server

Certificate contains:
nonce and fingerprints of
BIOS, B/L, -kernel, user-
level keyboard driver, ssh

Secure Remote Login w/ Cerium

Alice @ Internet Cafe

Nonce

Signed certificate

One-time phrase

Trusted server

Cerium Enables Many Apps

- User can find out if a computer executed the user's program faithfully!
- Many useful applications
  - Secure remote execution (e.g. SETI@home)
  - Secure P2P network

Conclusion

- Trusted computing HW enables new apps
- Cerium supports Secure Remote Login
  - Merges good ideas from Palladium & XOM
  - Provides security and verifiability
- We should explore how to use trusted computing HW to build cool systems!