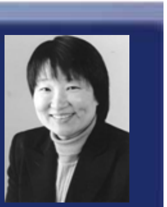
SecureCore

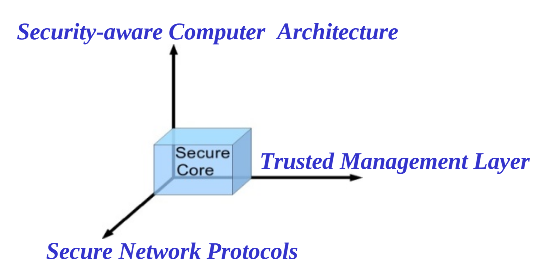


Ruby B. Lee[*] (PI), Cynthia Irvine[+], Terry Benzel[#], Mung Chiang[*]
Princeton University[*], Naval Postgraduate School[+], Information Science Institute/USC[#]
http://securecore.princeton.edu/

Trustworthy Commodity Computing and Communication

- *Commodity devices access secret or sensitive information whose leakage can cause irreparable privacy, financial and national security breaches.*
- Build security into computers from the hardware up
- Hardware trust anchors to tether and protect trusted applications software, without relying on commodity OS
- Software-Hardware Trusted Computing Base with Separation Kernel, Trusted OS, Trusted Path Application
- Architectural mitigation of covert and side channels
- Clean-slate architectural design
- Deployable solutions for commodity computers

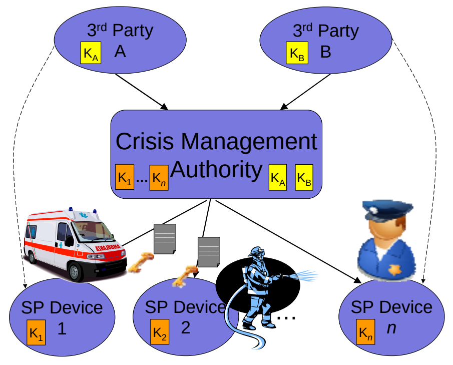
Architectural foundation for trustworthy commodity products for mobile computing and communications



Security without compromising performance, cost, energy consumption and usability

Remote and Transient Trust

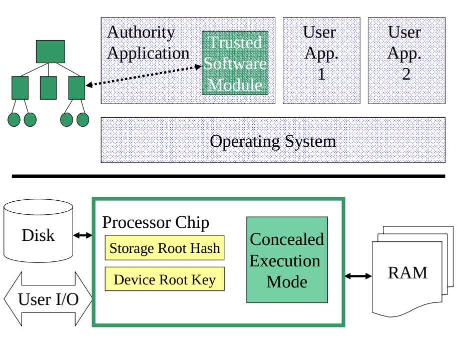
example: Emergency Response



Jeffrey Dwoskin and Ruby B. Lee, "Hardware-rooted Trust for Secure Key Management and Transient Trust," *Proc. of the 14th ACM Conference on Computer and Communications Security (CCS 2007)*, pp. 389-400, October 2007.

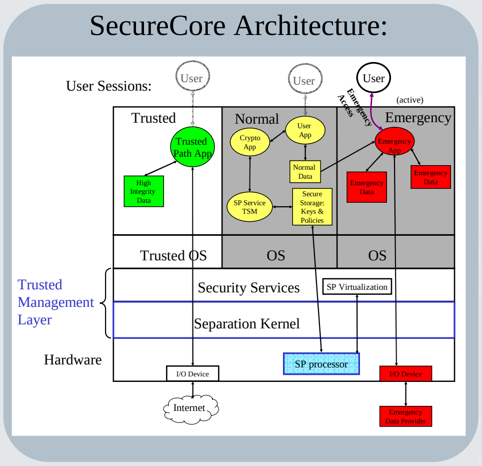
Secret Protecting (SP) Architecture

minimal hardware trust anchors protecting trusted software and storage



Jeffrey Dwoskin and Ruby B. Lee, "Hardware-rooted Trust for Secure Key Management and Transient Trust," *Proc. of the 14th ACM Conference on Computer and Communications Security (CCS 2007)*, pp. 389-400, October 2007.

SecureCore Architecture:



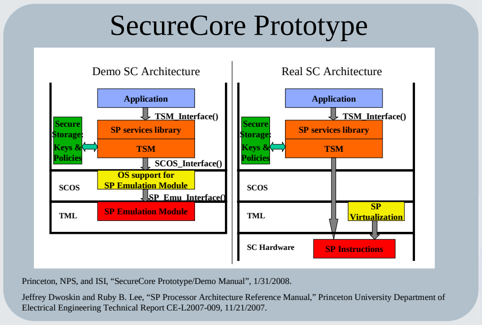
Secure Cache Architecture

- Problem: Information leak via software cache-based side channel attacks
- Our solution: Random Permutation cache (RPcache) randomly swaps cache lines on a cache miss so processes see different memory to cache mappings
  - Hardware solution solves root of problem
  - Applies to legacy software and future attacks
  - No increase in cache access time with clever circuits
  - Negligible performance degradation
- New work: improve performance and fault-tolerance and power consumption, in addition to security!

Zhenghong Wang and Ruby B. Lee, "New Cache Designs for Thwarting Software Cache-based Side Channel Attacks", *International Symposium on Computer Architecture, ISCA'07*, June 2007.

- Accomplishments:
  - Emergency response with transient trust
  - Secret Protecting (SP) architecture for security-aware processors
    - New authority-mode and sensor-mode
  - Trusted Path Application and Emergency Partition
  - SecureCore Prototype with SP emulation
  - New cache architectures that are immune from software side-channel attacks
  - Integrated memory authentication
  - Secure key management in sensor-nets
  - Security metrics for networking protocols

SecureCore Prototype



Princeton, NPS, and ISI, "SecureCore Prototype/Demo Manual", 1/31/2008.

Jeffrey Dwoskin and Ruby B. Lee, "SP Processor Architecture Reference Manual," Princeton University Department of Electrical Engineering Technical Report CE-L2007-009, 11/21/2007.

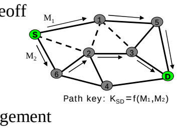
TEC-tree Memory Authentication

- Problem: Memory subject to spoofing, splicing and replay attacks (hardest)
- Our solution: Tamper-Evident Counter tree
  - Has parallelizable check and update
  - Confidentiality for free
    - Block encryption with added redundancy
  - Fast detection of spoofing and splicing attacks after 1st level tree check
  - Detects replay attacks
- New work: from embedded systems to general purpose systems

Reouven Elbaz, David Champagne, Ruby B. Lee, Lionel Torres, Gilles Sassatelli and Pierre Guillemin, "TEC-Tree: A Low Cost, Parallelizable Tree for Efficient Defense against Memory Replay Attacks", *Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007)*, September 2007.

Secure Networking Protocols

- Availability, Fairness and Performance
  - Fairness-Performance tradeoff
  - Availability-Throughput tradeoff
- New work: Secure networking protocols
  - Hop-based key management
  - Path-based key management
  - Joint resource and trust management



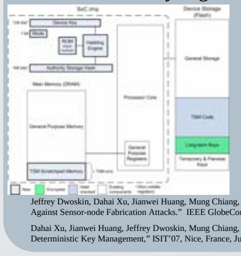
Path key: $K_{SD} = f(M_1, M_2)$

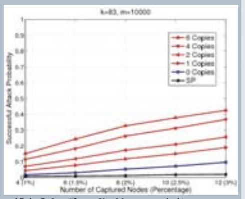
T. Lan, X. Lin, M. Chiang, and R. B. Lee, "How bad is suboptimal rate allocation?" Proc. IEEE INFOCOM, April 2008.

D. Xu, Y. Li, M. Chiang, and A. R. Calderbank, "Optimal provisioning of elastic service availability", Proc. IEEE INFOCOM, May 2007.

Sensor-mode SP architecture

enables Secure Key Mgmt. for mobile ad-hoc networks





Jeffrey Dwoskin, Dahai Xu, Jianwei Huang, Mung Chiang, and Ruby B. Lee, "Secure Key Management Architecture Against Sensor-node Fabrication Attacks." IEEE GlobeCom 2007, Washington, DC, November 2007

Dahai Xu, Jianwei Huang, Jeffrey Dwoskin, Mung Chiang, and Ruby Lee, "Re-examining Probabilistic Versus Deterministic Key Management," ISIT'07, Nice, France, June 2007.

NSF Cyber Trust Annual Principal Investigators Meeting
March 16-18, 2008
New Haven, CT