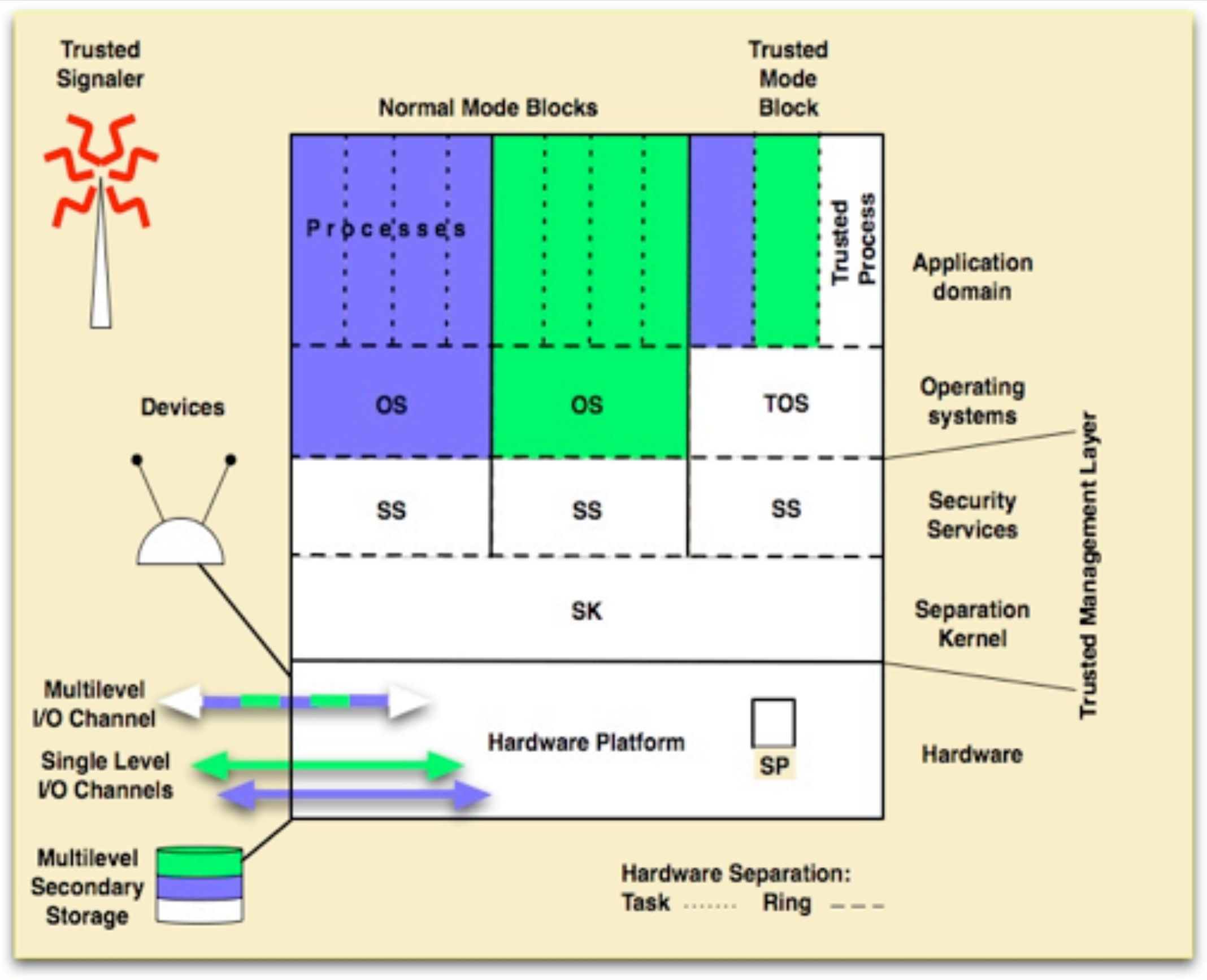
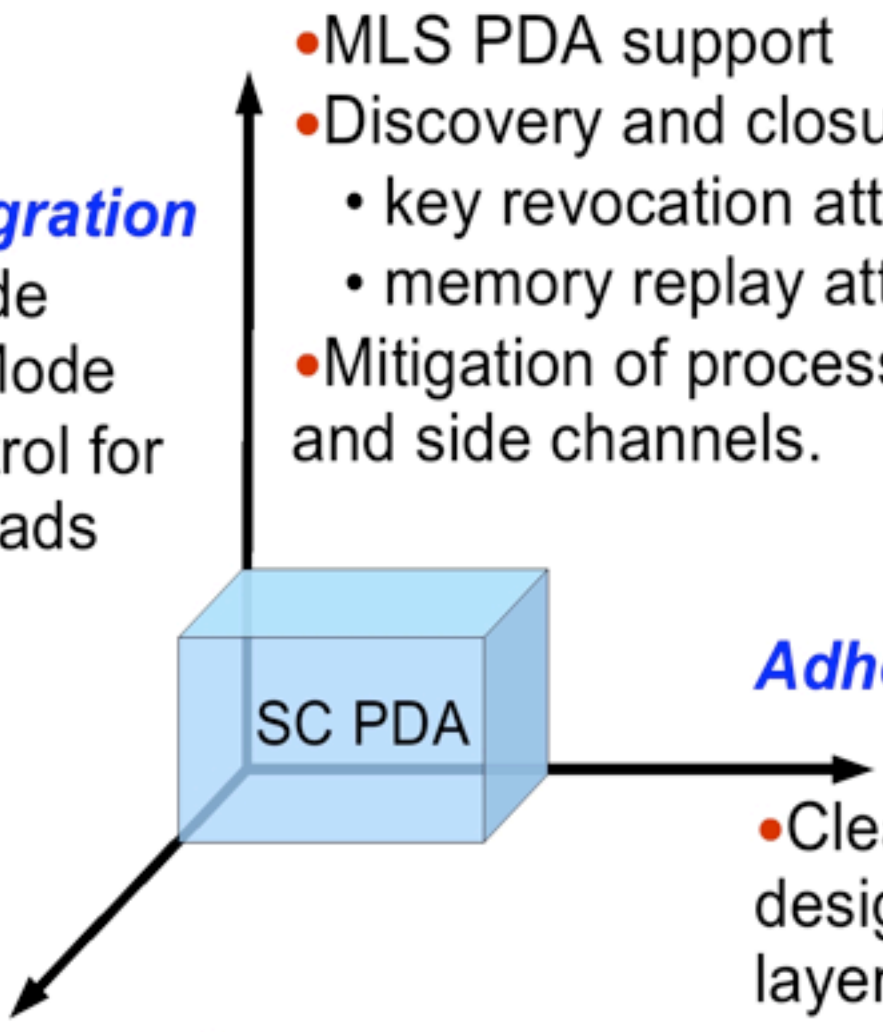
SecureCore

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

Trustworthy Commodity Computation and Communication

- Goal: Security without compromising performance, cost and usability using *minimalist and integrated* security architecture
- Foundation for trustworthy commodity mobile computing and communications devices like *Dual-use Multi-Domain* PDA
- New *minimal security-aware processor (SP)* architecture extensions to protect programs/data using cryptographic methods with trust for key-management, confidentiality and integrity rooted in HW
- New *least privilege separation-kernel* and *trusted services software* to enforce MAC and securely manage resources
- Detection/mitigation of covert and side channels at CPU, cache and system levels





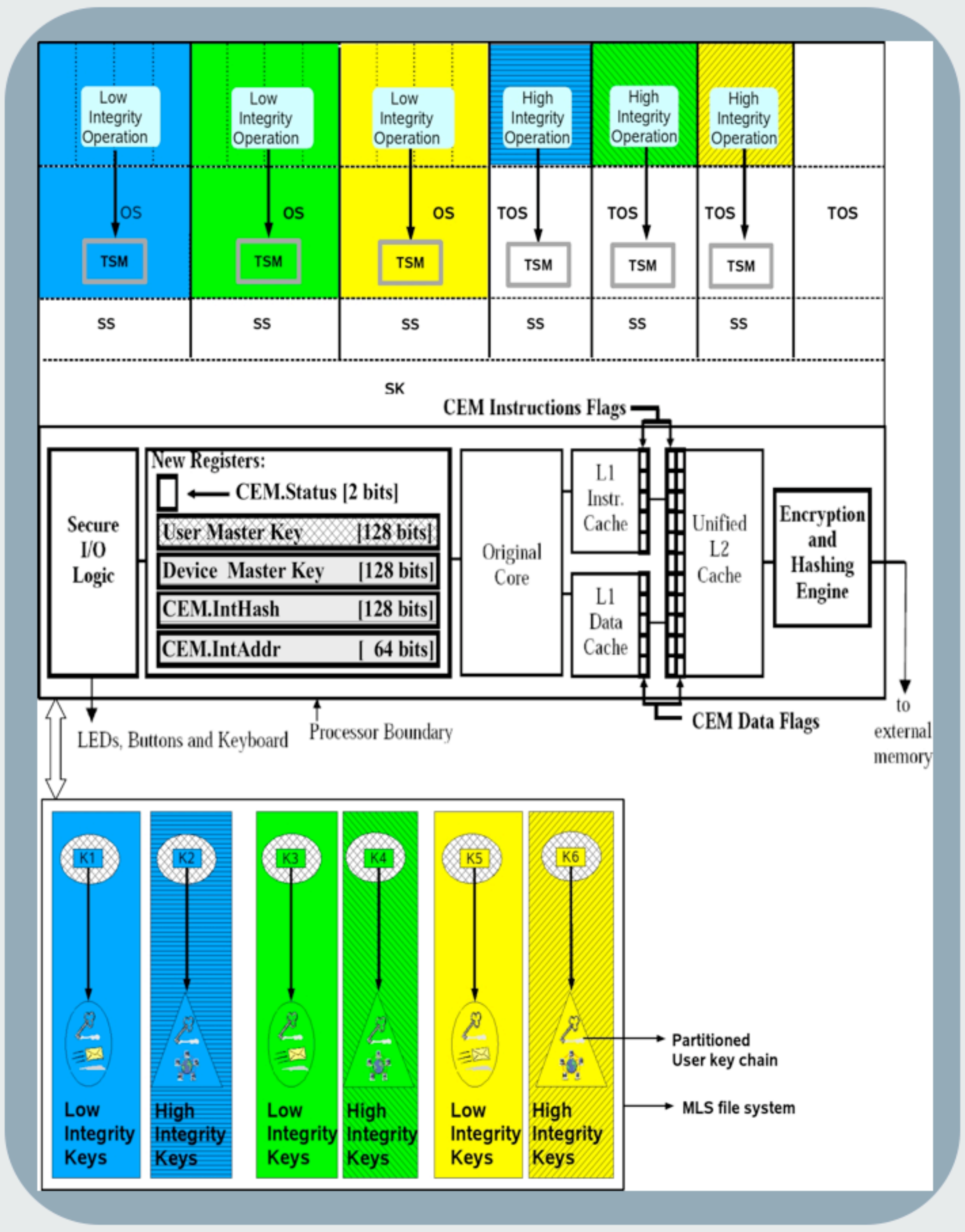
Security-Aware Processor (SP) architecture
- User Mode for normal operation
- Authority Mode for remote transient trust
- Reduced mode for sensor nets
- MLS PDA support
- Discovery and closure of attacks on SP
  - key revocation attacks
  - memory replay attacks
- Mitigation of processor-cache-based covert and side channels.

HW/SW Integration
- Trusted Mode w/Authority Mode
- Access control for SP/CEM threads

SC PDA

Adhoc Network Protocols
- Clean-slate protocol stack design examples using SP & layering optimizations

Separation kernel and trusted services software
- Transient-trust design
  - normal mode for COTS and trusted mode for high integrity operation
- Design for hosting OS and TOS, such as:
  - MLS policy interpretation - applying labels to blocks
  - Dynamic policy & resource changes
  - Scheduling and memory mapping for blocks and processes
- System Formal Security Policy Model prototype



SP HW Architecture

- User-mode: enables controlled and secure access to user's secrets
- Authority mode: enables transient, policy-controlled trust to third-party protected information, remotely
- Identified new SMT-based and speculation-based fast covert channels
- Proposed HW solutions against newly-discovered SW cache-based side channel attacks, without requiring SW changes

TML based Security Architecture and Integration

- New Multi-Domain system architecture metrics, compared 3 Security Architectures: SecureCore LPSK, MILS and Evaluated-Policy Security Kernel
- Trusted Path Application design to support transient trust usage model
- Initial set of hardware platform requirements
- Extension and integration of SP for covert-channel free sharing of crypto services

Adhoc Networking

- Probabilistic and deterministic mobile ad-hoc key-management, integrated with reduced mode SP

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Annual Principal Investigator Meeting

January 28-30, 2007

Atlanta, Georgia

PRINCETON UNIVERSITY

NAVAL POSTGRADUATE SCHOOL

Information Sciences Institute