



Calhoun: The NPS Institutional Archive
DSpace Repository

NPS Scholarship

Publications

2008-03-08

SecureCore West (Poster)

Lee, Ruby B.; Irvine, Cynthia; Benzel, Terry; Chiang, Mung

<https://hdl.handle.net/10945/35360>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



SecureCore WEST

Ruby B. Lee* (PI), Cynthia Irvine*, Terry Benzel#, Mung Chiang*
 Princeton University*, Naval Postgraduate School*, Information Science Institute/USC#
 NSF Grant No. CNS-0430487, CNS-0430566 and CNS-0430598



Trustworthy Commodity Computation and Communication

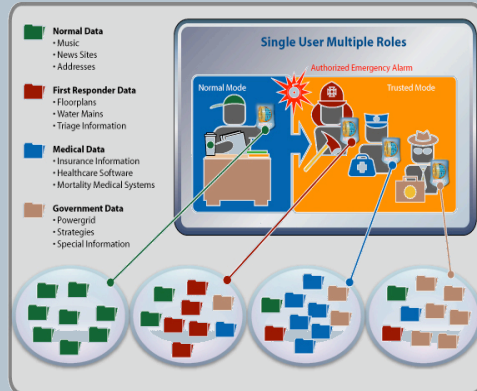
Enables dynamic, "transient trust" security policies for achieving the appropriate availability of highly sensitive information during emergencies in the face of determined adversaries.

- Research goal: Worked example of architectural foundation for trustworthy commodity mobile devices
 - Multi-use, multi-context operations
- Approach: Clean-slate, HW/SW co-design
 - Clean-slate design allows "break-through" ideas
 - Secure-by-design architecture via tight integration
- Design goal: Security with performance, low cost and usability
- New *least privilege separation-kernel* and *trusted services software* to enforce MAC and securely manage resources

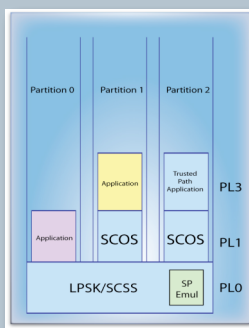
Accomplishments

- Concept of operation
 - Multilevel-secure (MLS) multi-use handheld device
 - Different functional contexts correspond to different user roles:
 - Everyday and emergency
 - Normal or trusted
 - Support inter-context secure sharing of information
- Trustworthy security architecture that can support dynamic security policies and services
 - Core building blocks
 - Security-aware processor extensions
 - Least privilege separation kernel
 - Trusted security services
 - Secure operating-system services
 - Trusted path application

Concept of Operation



Functional Prototype Design



- Three partitions
- Software-emulated SP module
- LPSK utilizes hardware security mechanisms
 - Segmentation
 - Cal gates
 - Hardware privilege levels
 - Task state management
- SCSS and LPSK co-locate in same privilege level
- Secure Attention Key (SAK)
 - Keyboard input
 - Focus switch via SAK
- Simple crypto key management application

SecureCore Software Architecture

Layer	Functions and Policies
TPA Trusted Path Application	Trusted Path interface to security-critical services
SCOS SecureCore Operating System	Application Management Identification and Authentication Operating System Services
SCSS SecureCore Security Services	MLS Support and Interpretation Resource Virtualization Object Management Focus Management Trusted Channel Management Inter-Partition Routing
LPSK Least Privilege Separation Kernel	Partitioning of Resources Resource Management MAC Enforcement Partitioning Scheduling Cross-Partition and Inter-Process Communication

SP HW Architecture

- User-mode: enables controlled and secure access to user's secrets
- Authority mode: enables *transient, policy-controlled access* to third-party protected information, remotely
- Reduced mode: for use in low power applications

Contributing Members

(alphabetically ordered)
 Ganesha Bhaskara#, Paul Clark*,
 Timothy Levin*, Thuy Nguyen*,
 Mark Orwat*, David Shifflett*,
 Timothy Vidas*



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

