SecureCore

Ruby B. Lee (PI) and M. Chiang, Princeton University
C. Irvine, Naval Postgraduate School, and T. Benzel, USC-ISI
http://palms.ee.princeton.edu/securecore

Trustworthy Commodity Computing and Communications

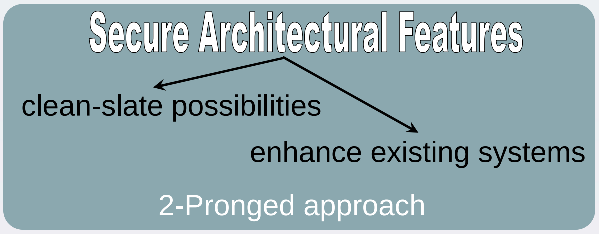
Research in the design of secure integrated core architectures for trustworthy operation of mobile computing devices

Including:

Security-aware Processor and Hardware
Secure Operating System Kernel
Secure Network Protocols.

Identification of Security Needs from a user's perspective.

Robust and Resilient Architecture surviving attacks.


Secure Architectural Features

2-Pronged approach

For resource-constrained, ubiquitous computing platforms exemplified by secure embedded systems and mobile PDAs

Comparison to state of the art

Current approach:

- add-on, optional or peripheral security and software "patch and pray"
- software solutions above an insecure O.S. and processor core; networking entirely separate design
- suffering performance, cost and usability to achieve security

New approach:

- clean-slate design of core security: built-in default mode of operation is secure
- hardware-software-networking security at the core of every commodity computing and communications device
- security without compromising performance, cost and usability

The SecureCore Processor and Hardware Platform provide minimalist hardware security enablers and enforcers that are essential for secure O.S. and Networking functions. It also provides the basis for trustworthiness from a user's perspective, such as:

User-Centric Security Features:	Example Processor/Platform Architecture:
• Protection for sensitive or secret information stored locally or remotely and accessed through public networks via multiple devices	• "Secret Protected" SP-processor and trusted I/O: HW to protect critical master keys, secure entry of user master-key and concealed execution mode
• Protection from information leakage	• Architecture to minimize covert channels
• Protection from Internet-scale epidemics such as viruses, worms, DDoS	• Containment architecture; least privilege and authorization; runtime HW monitoring
• Protection from adversarial control or use of device through software vulnerabilities	• Processor defenses and safety net for software security vulnerabilities that slip through static checks
• Cryptographic protection without sacrificing performance or adaptability	• "No-overhead" crypto with flexible novel processor Instruction Set Architecture or very fast, low-cost HW
• Provide secure ad-hoc networking for continuous communication among portable devices	• Clean-slate light-weight protocol stack for secure management of connectivity, mobility, key, and radio resources

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Annual Principal Investigator Meeting
Sept. 25 - 27th, 2005
Newport Beach, California

Princeton University

rblee@princeton.edu