

Secure Systems Research at IBM's Thomas J. Watson Research Center



Stefan Berger, Ramón Cáceres, Kenneth Goldman, John Linwood Griffin, Ronald Perez, David Safford, Reiner Sailer, Enriquillo Valdez, Leendert van Doorn, Xiaolan Zhang

http://www.research.ibm.com/secure_systems_department/

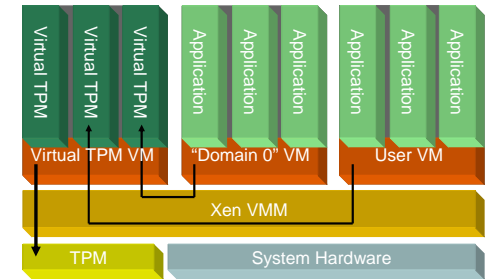
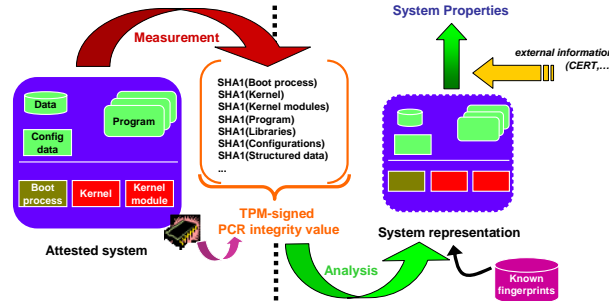
© 2005 IBM Corporation

Overview

- Targeting foundational solutions to real-world system-oriented security problems
- Recent areas of impact include:
 - Cryptographic coprocessors and subsystems
 - Information flow control and data protection
 - Leveraging trusted computing technologies for integrity measurement and remote attestation
 - Mandatory access control architecture & implementation
 - Mobile computing design and deployment issues
 - Security analysis toolkits
 - Security engineering instruction and consulting
 - Virtualization and cross-platform security
- We're friendly folks—come talk with us in person!

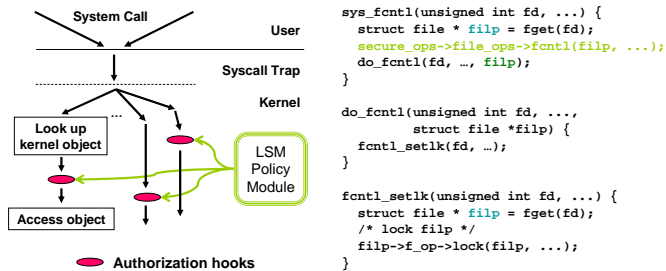
Leveraging trusted computing hardware to measure software integrity

- The Trusted Platform Module (TPM) enables the integrity verification of the executable code loaded into a system's run-time
- Various properties of a system are validated by remotely comparing these measurement against known measurements
- Virtual TPMs, validated by the physical TPM, can provide a per-VM root of trust for each VM in a virtual machine monitor



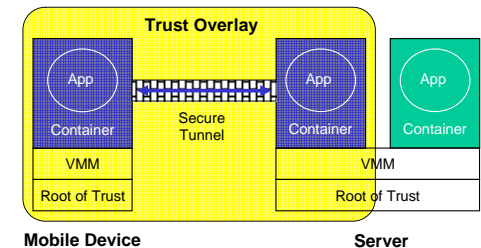
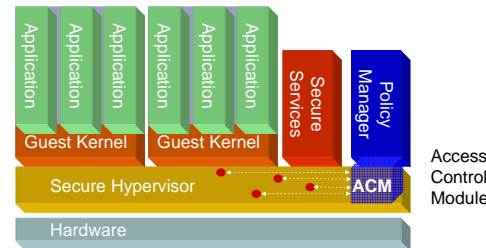
Static code analysis for complete mediation

- Static analysis tools are useful for detecting vulnerabilities and verifying security properties of source code
 - Detection of data race TOCTTOU attacks
 - Verification of the complete mediation property



Isolation and secure resource sharing in virtualized environments

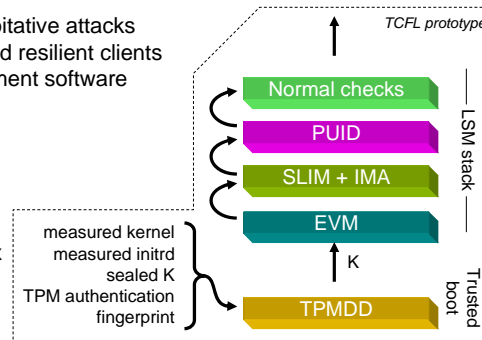
- Enforcement of mandatory access control policies on inter-VM operations allows controlled sharing of resources
- The sHype architecture combines admission control with information flow mediation to protect the data used by a VM
- Bridging the roots of trust across multiple systems enables uniform specification and enforcement of access control policies
- One motivating environment is commercial applications with medium assurance requirements



Tying it all together: Trusted computing for Linux (TCFL)

- Client system risk continues to increase with the number and diversity of exploitative attacks
- Protection strategies need to make use of all available security features to build resilient clients
- TCFL prototype demonstrates synergy among hardware, OSes, and management software

- **Trusted boot**
 - BIOS fingerprint sensor
 - GRUB measurement
 - TPM device driver
 - Initrd master key unsealing and verification
- **Integrity protection**
 - SLIM: simple Linux integrity module
- **Integrity attestation**
 - IMA: integrity measurement architecture
- **Security domains**
 - UnionFS: stacked, copy-on-write, sandbox
 - Per-process filesystem namespaces
 - PUID: persistent user ID
- **Integrity measurement**
 - EVM: extended verification module



Longer-term vision: Trusted Virtual Domains (TVD)

