Nexus: An Operating System for Trustworthy Computing

Alan Shieh    Dan Williams
Emin Gün Sirer    Fred B. Schneider

Department of Computer Science
Cornell University
Emerging hardware for trustworthy computing

Existing systems do not provide required execution environment
Nexus: A New OS

- Architecture for trustworthy computing
  - Small TCB
    - Software: User-level drivers and services
    - Hardware: Secondary storage not trusted
  - Fine-grain components
  - Strong isolation

- New abstractions
New abstractions

- **Active attestation** with descriptive, unforgeable names
  - Used for local and remote access control
  - Used for resource commitment

- **Secure memory regions** with mandatory access control
  - Used to implement trustworthy services
Naming via active attestation

- Exposes properties of process
  - Result of analysis
  - Reference monitors
  - Execution environment
- Captures run-time properties
  - Routing: “$k$ packets have been forwarded”
  - P2P: “Blocks $\{b_0, \ldots, b_k\}$ queued for Tx”
  - Anti-spam e-mail: “Human typed in message”
  - Resource commitment: “Program scheduled for $k$ quanta”
Secure memory regions

- Strong storage guarantees
  - Integrity
  - Confidentiality
  - Persistence

- Access control using active attestation

- Used to implement powerful user-level services
  - Security automata
  - Linear capability manager
Summary

- Working system with applications:
  - Capabilities-based media player
  - Spam-proof e-mail system
  - Tamper-evident system log
  - Attested MACEDON application

Isolated Protection Domains

- MPlayer
- E-mail
- Keymgr
- Linux compat
- Apache
- Pine
- exim
- ssh

Unprivileged

- Video driver
- Network driver
- Audio driver

Safe device access

Privileged

- Nexus user interface
- Nexus driver interface

IPC

Trusted computing