"Architecture for Protecting Critical Secrets in Microprocessors"

R. Lee, P. Kwan, J. McGregor, J. Dwoskin, Z. Wang

International Symposium on Computer Architecture 2005 (ISCA '05),
IEEE, pp. 2-13, 2005.

Summary

- Secrets? Keys.
- Protecting? Threat model:
  - Key exposure or tampering via…
    - Software attacks – including OS (ring 0)
    - Some hardware attacks – bus/memory/disk data snooping or tampering.
- Architecture? "Virtual Secure Co-Processor"

Secrets

- User Keychain
  - Tree of keys, each child encrypted by its parent.
  - Leaf keys can be used to protect external data – email, VoIP, …
  - Root is…
- User Master Key
  - E.g. cryptographically strong hash of a passphrase.
  - Entered by user via secure I/O path.
- Device Master Key
  - Protects TSM code and data.
  - Stored in non-volatile memory.
  - Created at init time; readable only by CPU's AES hardware.

Architecture

- Minimal trusted components:
  - Hardware
    - CPU, cache, AES, secure I/O.
  - Software
    - Trusted Software Module.
- TSM executes in Concealed Execution Mode.
- Code and data protected by Device Master Key:
  - Icache lines are signed in code stream; verified and tagged on load.
  - Dcache lines are encrypted and signed; decrypted, verified, and tagged on load; encrypted and signed on eviction.
  - Register file encrypted, signed and stored in-place on interrupt; OS handler requires no modification.

Security Analysis

- Protecting keys from hostile software? Done.
- Protecting USE of keys by hostile software? Not in scope.
  - Though suggestions given: verified OS kernel, secure boot, …
- Protecting users from hostile second-parties? …
  - Hardware owner – 'Secure I/O'? Nope.
  - TSM vendor? DMK read-only, TSM outside OS access model.
  - Hardware vendor?

Security Analysis, cont.

- No factory-installed code or secrets.
  - "...protected from compromise of the factory and its secrets database."
  - Cryptographic root of trust known to user.
- No facility for attestation; user-installed TSM.
  - Software root of trust specified by user.
- Compare & contrast.

Questions?