CC3: An Identity Attested Linux Security Supervisor Architecture

Richard Engen MSFS, Johannes Grosen MS Scott Stofferahn, Greg Wettstein R.Ph., Ph.D. *
IDfusion, LLC

* = Primary Author/Presenter
The State of Security

Security is economically constrained.

5dc9dc532fa80824ff12380d08aaf00a

vs

5dc9dc532fa80824ff12380d08aaf00A
Irreversible Compromises

- Life safety systems.
- Privileged healthcare information.
- Personally sensitive information.

No ex-post-facto redress.
In the Beginning - NHIN

- Greatest identity problem in the world.
- 2008 CC1/2
  - Deterministic location of medical records in under five seconds over 3 million+ provider identities.
- Network perimeter defined by integrity verified platforms.
- Required mobile/autonomous devices.
"All things equal, complexity loses. All things not quite equal – ditto."

– Al Viro, LKML

CC3 Architecture

Will general purpose OS distributions remain relevant?
System Components

• Security bootloader – sboot.
  – Initializes system identity and root filesystem.

• System security supervisor – sinit.
  – Attests and maintains platform behavioral status.

• Environment launchers:
  – Native binaries.
  – Virtual machines.
  – Containerized systems.

13 megabyte base system load
Identity Attested Remote Attestation

- Implemented with POSSUM.
- Authenticated with OTEDKS.
  - Epoch/identity based key generation.
  - Validated with NIST randomization tests over a 32 bit time epoch.
- IVY 'identity cartridges' encapsulate counter-party information.

Autonomous Attestation
"In the future, company names will be a 32 character hex string"

– Bruce Schneier

\[ I_M = H_M(R_M \| H_M(C)) \]
I3MA Platform Model

- **Premise 1**
  - Interaction of actor and subject identities yield a behavior identity.

- **Premise 2**
  - Platform behavior is full set of behavioral identities.

- **Premise 3**
  - Platform measurement is time invariant extension sum of device identity extended platform behaviors.

Multi-variate platform behavioral modeling.
Behavioral Compromise Modeling

- Extra-dimensional.
  - Platform behavior goes 'off-contour'.
  - Detectable by integrity measurement.

- Intra-dimensional.
  - Platform behavior remains 'on-contour'.
  - Requires probabilistic methods.

Mathematical limit of integrity measurement.
iso-identity IMA policy

Policy:

- map func=BPRM_CHECK capability=any
- map func=FILE_MMAP mask=MAY_EXEC capability=any
- map func=MODULE_CHECK uid=0
- map func=FILE_CHECK mask=^MAY_READ capability=any

Capability based measurement triggers:

$$A_{\text{MASK}} = P_{\text{MASK}} \land (E_{\text{Eff MASK}} \lor P_{\text{Per MASK}})$$
Subject Pseudonyms

- Implemented to avoid issues with writable files, e.g., password, log files.
- Configured by security supervisor during system initialization process.
- Synthetic file hash derived from platform identity.
- Overrides TOMTOU/open-writers violations.
- Removed by security_inode_unlink().
Securityfs Interface
/sys/kernel/security/ima/iso-identity

-r--r------ 1 root root 0 Aug 11 02:31 contours
-r--r------ 1 root root 0 Aug 11 02:31 forensics
--w-------- 1 root root 0 Aug 11 02:31 host_identity
--w-------- 1 root root 0 Aug 11 02:31 map
-r--r------ 1 root root 0 Aug 11 02:31 measurement
--w-------- 1 root root 0 Aug 11 02:31 pseudonym
--w-------- 1 root root 0 Aug 11 02:31 sealed

Sealing platform disables further configurations and enables forensics.

Development and mgmt. of behavioral model.
Current Work

- System upgrade management.
- Integrating mandatory access labels.
- Support for ambient capabilities.
- Implementing behavioral namespaces.

Role of behavioral attestation in re-insurance and indemnification?