### 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

#### 5dc9dc532fa80824ff12380d08aaf00a

VS

#### 5dc9dc532fa80824ff12380d08aaf00A



## Security is economically constrained.

## 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.



#### **CC3** Architecture

## "All things equal, complexity loses. All things not quite equal – ditto."

– Al Viro, LKML



Will general purpose OS distributions remain relevant?





## ComDel Innovation ISO 9001:2000

## 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**





#### DakTech Assembly And Support

### Iso-Identity Integrity Measurement Architecture

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

– Bruce Schneier





## **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 limt 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: $A_{\text{MASK}} = P_{\text{MASK}} \wedge (Eff_{\text{MASK}} \vee Per_{\text{MASK}})$



## Subject Pseudonyms

- Implemented to avoid issues with writable files, eg 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?