LSS 2015: linux-integrity subsystem status

Mimi Zohar

Linux Integrity Subsystem Status Update

- Where's the Linux Integrity Subsystem being used?
- Userspace support for appraisal
- New and continuing kernel development
- Summary
- References

Where's the Linux Integrity Subsystem being used?

Based on just this year's LSS talks:

- Measurement & attestation: servers, cloud, routers
- Enforcing local file integrity: embedded devices

others are extending it:

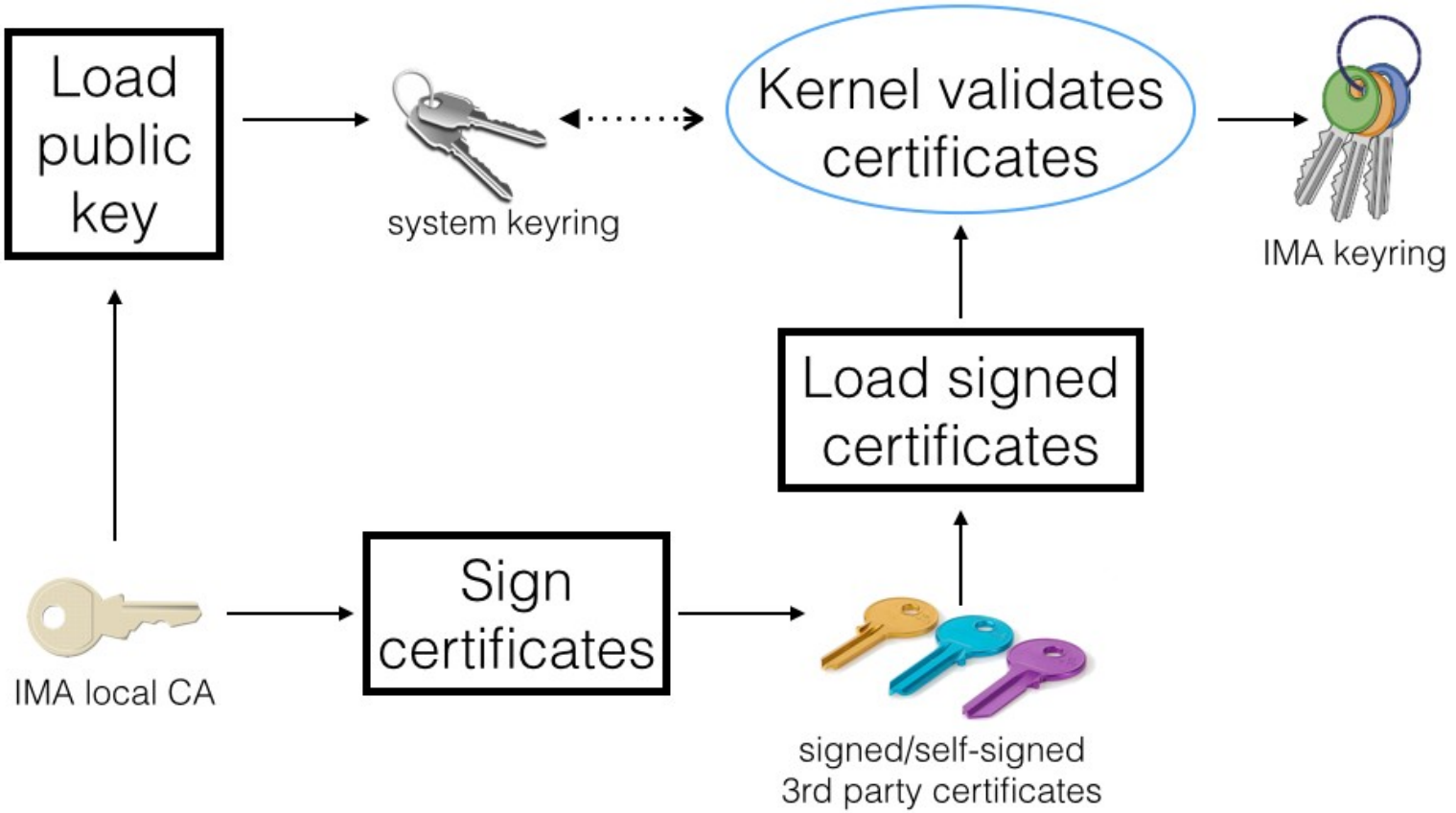
- Mutual identity authentication

and previously mentioned last year:

- Incident Response

Userspace support for appraisal

*"Extending the secure boot **certificate** and signature chains of trust to the OS" (Fin Gunter/Mimi)*



Userspace support for appraisal

- Methods of loading the localCA on the kernel system keyring
  (Builtin key, MoK key (RH patches), reserving memory)

- Signing distro and 3rd party keys with the localCA key
- Loading distro and 3rd party keys on the IMA keyring
  - Dracut patches (upstreamed)
  - Initramfs-tools IMA support (todo)

- Including file signatures in software packaging tools
  - RPM (expected in beta release)
  - Debian (Bug#766267: debhelper)

New and continuing kernel development

- Closing measurement gaps:
  - *(Upstreamed)* Additional policy options (eg. euid, ^mask)
  - *(NEW)* Preserving the measurement list across kexec (Josh Sklar)
  - *(NEW)* Initramfs xattr support (Mimi)

- *(NEW)* Namespacing IMA (Yuqiong Sun)
- Locking “mutable” files (Dave Safford)

  http://kernsec.org/files/lss2014/safford_tcb_integrity.pdf
- Directory support (Dmitry Kasatkin)

Namespacing IMA (Yuqiong Sun)

Per container:

- Measurement list
  - Measurement & appraisal policy
  - Measurement list template definition

- Enforcing local file integrity
  - Authorized local-CA key
  - IMA appraisal keyring

Summary

- Measurement & attestation is being used today
- Enforcing local file integrity is being used today, but mainly on embedded devices.
- As soon as package managers support files signatures **and software comes signed**, enforcing file integrity will also be feasible in non-embedded environments.
- Continuing to close measurement gaps
- Extending IMA to support containers

References

- LSS 2015: CC3: An Idenitry Attested Linux Security Supervisor Architecture
  (Richard Engen MSFS, Johannes Grosen MS, Scott Stofferahn, Greg Wettstein R.Ph., Ph.D)
- LSS 2015: IMA/EVM: Real Applications for Embedded Networking Systems
  (Petko Manolov, Konsulko Group, and Mark Baushke, Juniper Networks)
- LSS 2015: IMA/EVM on Android Device
  (Dmitry Kasatkin, HuaweiTechnologies)
- LinuxCon 2015: Extending the Secure Boot signature and certificate chains of trust to the OS
  (Fin Gunter, Hypori, Mimi Zohar, IBM)
  http://events.linuxfoundation.org/sites/events/files/slides/Extending-Secure-Boot.pdf
- IEEE 2015: Scalable Attestation: A Step Toward Secure and Trusted Clouds
  (Stefan Berger, Kenneth Goldman, Dimitrios Pendarakis, David Safford, Ray Valdez,
  Mimi Zohar)
- LSS 2014: Extending the Linux-integrity subsystem for the TCB protection
  (David Safford/Mimi Zohar, IBM)
  http://kernsec.org/files/lss2014/safford_tcb_integrity.pdf