Fedora IoT

Overview of Security Direction

Presented by
Peter Robinson
Principal IoT Architect

Overview

- Why are we different?
- Minimal OS and Standard Enterprise practices
- Userspace security tech - SELinux
- OCI Containers
- Secure-boot / TPM2
- Secure credential storage
- Integrity Measurement Architecture
- Future enhancements overview

Why are we different?

Why are we different?

- The devices look like enterprise devices
- Need data centre level security without the DC
- Real pirates are a real problem in IoT
- Devices WILL be stolen, mitigate and minimize risk
- All the security tech will be (is?) wanted in the data centre too, just not as high a priority as the latest Kubernetes
- IoT should be driving security, not trailing it!

Minimised OS

Minimised OS

- Reduced size Fedora using rpm-ostree
- Ostree provides read-only root filesystem with atomic upgrades (and roll-back if necessary)
- Not yet minimal enough
- Work ongoing to untangle dependencies
- Minimise the footprint you minimise the attack surface
- Moving to API for management, management apps/daemons will move to containers

Standard Enterprise practices

Standard practices

- Use existing Enterprise understanding of Linux
- Similar process for security management
- Enterprise measures work fine
- Expanded for IoT use cases and scale
- Firmware updates via LVFS and fwupdmgr
- “Keep the baby when discarding the bath water”

Userspace security technologies

Userspace security tech

- SELinux
- Seccomp – enhancing ssh and others
- CGroups – Moving to version 2 for F-31
- namespaces
- Systemd – using namespaces, seccomp etc to limit access, in some cases limiting or eliminating entire classes of vulnerabilities

OCI Containers

Containers

- A means of containment
- One troublesome or compromised application shouldn’t affect others
- Update each app stack independently
- Update base OS independently

Secure-boot / TPM2

Secure-boot / TPM2

- Secure boot ensures trusted software is booted by the firmware in the boot chain
- UEFI Secure boot ensures roll-back protection
- TPM2 part of TSS 2.0 spec from Trusted Computing Group
- TPM2 used to measure boot, store credentials
- Both hardware and firmware implementations

Secure credential storage

Secure credential storage

- Using TPM2 to store credentials in hardware
- Encrypt root file system using clevis and tpm2* stack
- Store network credentials in TPM2
- Store random other credentials in TPM2 using clevis

Integrity Measurement Architecture

IMA

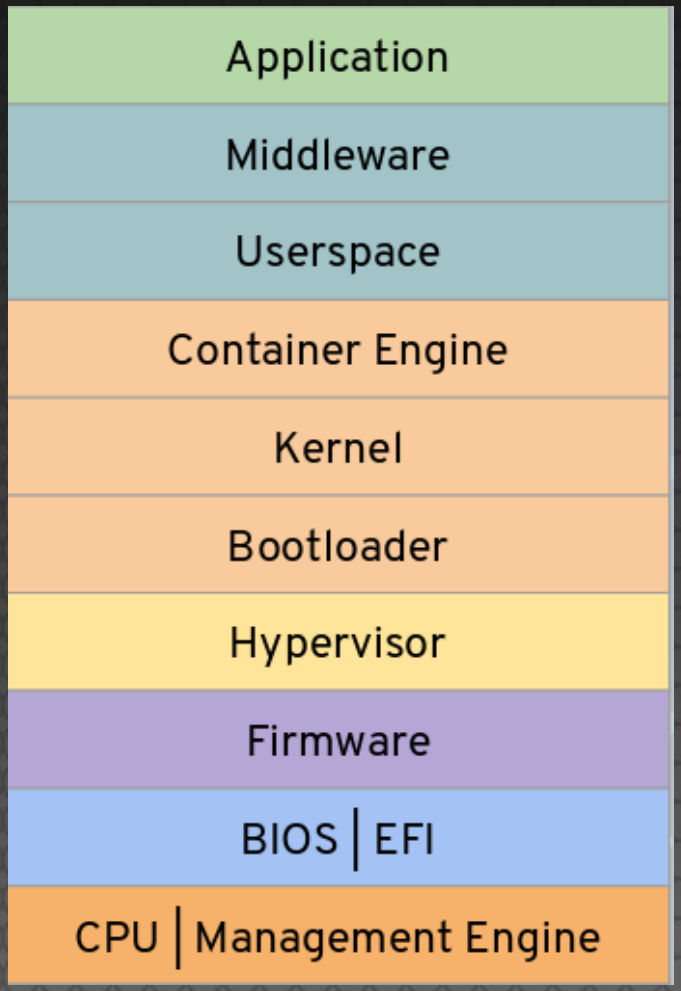
- Integrity management architecture
- Part of Linux kernel with user space tools
- Initial IoT enforcing policy coming with F-31
- Measures the userspace binaries and files for change
- Attesting the boot and bits haven’t changed
- Remote attestation that the bits haven’t changed

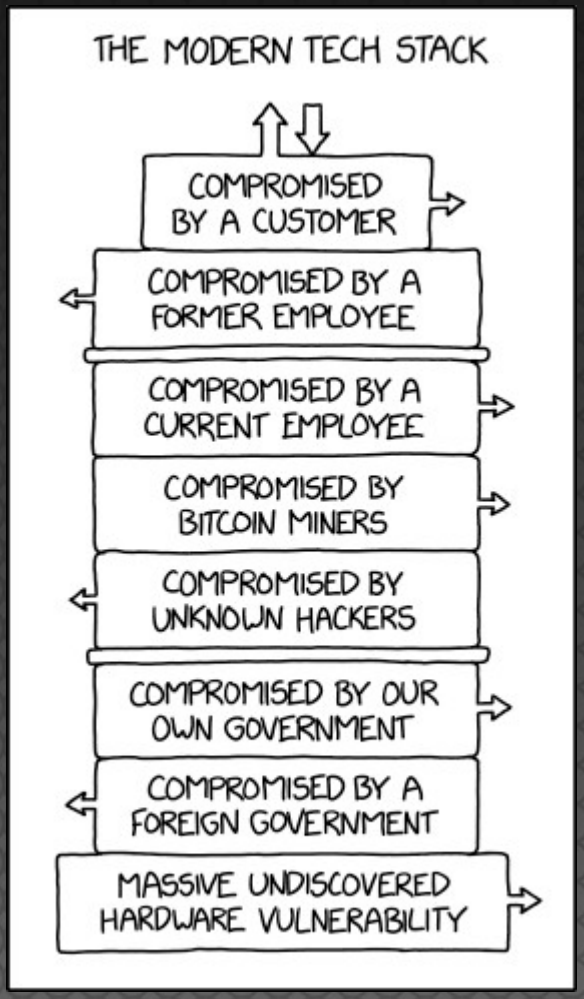
Future enhancements

Future enhancements

- Improvements to secure-boot
- Enhancements for credential storage
- Improved IMA policies and remote attestation
- Run-time integrity and confidentiality of apps ensuring secure connectivity:
  - Enarx: now part of Confidential Computing Consortium, along side MS OpenEnclave
  - Announced today at Linux Security Summit
  - https://confidentialcomputing.io

Secure apps in Enclaves

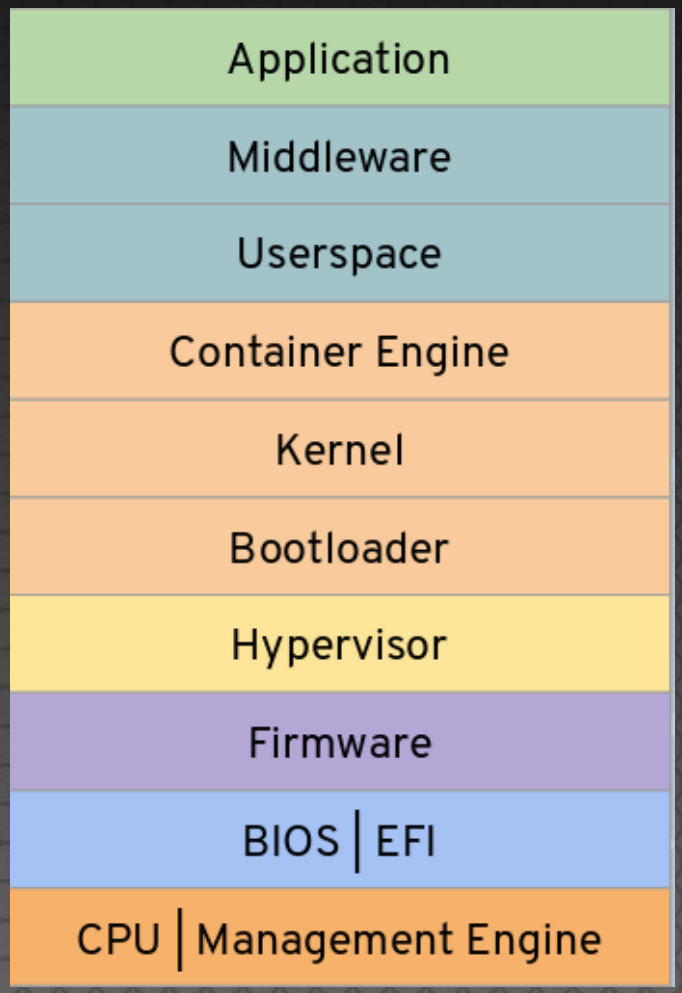


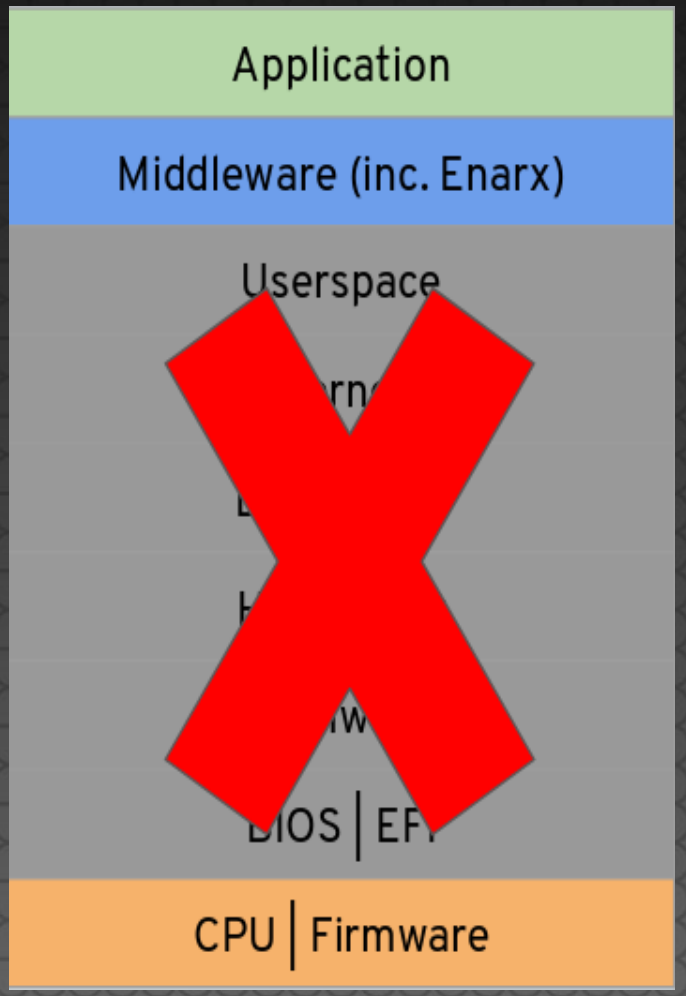


https://xkcd.com/2166/

fedora

What is Enarx?





http://enarx.io/

fedora

Questions?

Contact:
pbrobinson@fedoraproject.org