IMA/EVM: Real Applications for Embedded Networking Systems

Petko Manolov, Konsulko Group
petko.manolov@konsulko.com
Mark D. Baushke, Juniper Networks, Inc.
mdb@juniper.net
2015 Linux Security Summit, Seattle, WA

2015 Linux Security Summit, Seattle, WA

Glossary

Term	Definition
EVM	Extended Verification Module
FS	File System
IMA	Integrity Measurement Architecture
immutable	File whose state cannot be modified after it is created
LSM	Linux Security Module
MAC	Mandatory Access Control
MOK	Machine Owner Key
PCR	Platform Configuration Register
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure

Glossary (cont)

remote attestation	Given a TPM, remote users provides a nonce and receives a signed (by AIK) block with the nonce and PCR values.
SquashFS	Squash File System - read-only file system with extended attributes support
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TPM	Hardware Trusted Platform Module
TSS	Trusted Software Stack
VFS	Linux kernel's Virtual File System layer
X509	X.509 is an ITU-T standard for PKI and PMI.
xattr	Extended Attributes

IMA/EVM Integrity Features

- Collect – measure a file before it is accessed.
- Store – add the measurement to a kernel resident list and, if a hardware Trusted Platform Module (TPM) is present, extend the IMA PCR
- Attest – if present, use the TPM to sign the IMA PCR value, to allow a remote validation of the measurement list.
- Appraise – enforce local validation of a measurement against a “good” value stored in an extended attribute of the file.
- Protect – protect a file's security extended attributes (including appraisal hash) against off-line attack.

IMA/EVM history

- The first three functions were introduced with Integrity Measurement Architecture (IMA) in 2.6.30.
- The last two features were originally posted as a single EVM/IMA-appraisal patch set for in the 2.6.36 timeframe, but were subsequently split.
- EVM was upstreamed in Linux 3.2, using a simpler and more secure method for loading the `evm-key`, based on the new Kernel Key Retention Trusted and Encrypted keys.
- Support for protecting file metadata based on digital signatures was upstreamed in the Linux 3.3.
- IMA-appraisal was upstreamed in Linux 3.7.

Goals

- The primary goal of this work is to provide a mechanism for letting a company distribute a secure system which includes signed binaries along with a mechanism for the owner of the box to authorize the addition of other third party signed applications.
- It should be possible for the system to support Secure Boot, or Measured Boot with TPM for remote attestation.
- It should be possible to augment the IMA policy multiple times after boot.

Achievements - First Problem

- The first problem we ran into was the lack of certificate hierarchy in the current Linux kernel. Certificates/keys were dumped in kernel's source root directory. IMA keys could be signed by CA in the system's keyring, but no actual hierarchy is implemented.
- Introduced was intermediate keyring (MOK - machine owner keyring, IMA root CA keyring, whatever the name) which would only accept certificates signed by one in the system keyring. Adding certificates is dynamic, which allow for more flexible certificate management and runtime CA additions. This also makes possible execution of software signed not only by the machine owner, but also a machine tenant.
- IMA code was modified to allow key imports to its keyring only if signed by certificate in the MOK or in the system's keyring. Patches sent to Mimi Zohar.

Achievements - Second Problem

- Second obstacle was the lack of IMA blacklist and revocation keyring. Most certificates and IMA keys, respectively, are short lived (an year or so) so those were also introduced. Patches available.
- SquashFS images used as main storage FS. Its R/O mode makes possible to omit EVM checks. Adds additional security by not allowing writes.
- Modified the kernel to allow dynamic IMA policy loading as additional SquashFS images (signed by different keys, subject to different rules) may be mounted on the fly. The files that contain the new IMA rules must be properly signed.

Future Work

- Using the TPM to securely store an EVM private key used to sign immutable files.
- Using crypto extention of EXT4 (upstreamed in 4.1) along with EVM for protecting R/W filesystem objects.

Conclusions

- Security is a hard to do right. Not very helpful, but true. :)
- Introducing CA hierarchy to the kernel (strictly in context of IMA) gives enough flexibility to have dynamic certificate and key import, blacklisting or revocation.
- Contemporary large network devices may securely run software signed by the manufacturer, the machine owner, one or more tenants.

Questions?

- Petko Manolov

  petko.manolov@konsulko.com
- Mark D. Baushke

  mdb@juniper.net

```
KeyID: 0x4B535BBE 09365856, Finger Print:
29772B12 FADB186A C29E54D7 4B535BBE 09365856
```