Digital Signature Support for IMA/EVM

Dmitry Kasatkin

Casey Schaufler

Linux Security Summit 2011

08.09.2011

Agenda

- Introduction to IMA/EVM
- ksign – kernel RSA verification module
- IMA/EVM patches
- evm-utils
- module-init-tools
- Links
- Q&A

Introduction to IMA/EVM

- Kernel integrity subsystem includes 2 modules
  - Linux Measurement Architecture (IMA)
    - ensures integrity of file content
    - integrity measure: reference hash in security.ima
  - Extended Verification Module (EVM)
    - Ensures integrity of the file metadata
    - Integrity measure: reference HMAC in security.evm

IMA/EVM Use Case

- Individually installed systems
- System unique HMAC key
- Initial file-system labeling

Digital signature extension

- Software installation/update for CE/embedded devices is usually done by flashing a file-system image
  - The same image is flashed to multiple devices
  - Cannot be labeled using HMAC
    - Key is different on every device
- Digital signature extension provides a solution to perform labeling of the image using digital signatures.

ksign – RSA verification module

- API to verify RSA signature
- Derived from CentOS gnupg mpi library
    - ksign_verify
- linux/crypto/ksign.c
- linux/crypto/mpi/*

IMA/EVM patches

- Signature type is defined by the first byte of security.ima and security.evm
  - EVM_XATTR_HMAC
  - EVM_IMA_XATTR_DIGSIG
- IMA signature
  - Never replaced with a hash on file update
- EVM signature
  - Replaced with an HMAC after successful verification

evm-utils

- Signing
  - evmctl sign --imahash /path/to/file
    - Set hash for security.ima
  - evmctl sign --imasig /path/to/file
    - Set signature for security.ima
    - Kernel modules must have ima signature

evm-utils

- Importing public keys into the kernel keyrings
  - Separate keyrings for IMA and EVM
  - evmctl import –evm –pem
    /etc/keys/pubkey_evm.pem
  - evmctl import –ima –pem
    /etc/keys/pubkey_evm.pem

Label example

- echo Hello >foo
- sudo evmctl sign --imahash foo
- getfattr -e hex -m security -d foo
- # file: foo
- security.evm=0x030155475e4e0000bc16a96303fd3e7901040060bab44648764dca46ad71827a48c3e171b7e9444b47b79b7bd7c7f1783852be9b4f038f2c1dd57320b257619b9fa3a9cadea2c679faf83a9755f2a015995ec43332fdedcc2c72cb87f2eb25a8ef524c3ec78134aaa5b6dd18c8c1bf5e16d886a03dd36587aa927e07154c0009cdaf71c1fcbc37fa15a8bd153ba360bf73bafb
- security.ima=0x011d229271928d3f9e2bb0375bd6ce5db6c6d348d9

Image labeling

- File-system image labeled as the last step of image building process
- Example how to label whole file-system
  - `find / \( -fstype rootfs -o -fstype ext3 -o -fstype ext4 \) ! -path "/lib/modules/*" -type f -uid 0 -exec evmctl sign --imahash '{}' \;`
  - `find /lib/modules ! -name "*.ko" -type f -uid 0 -exec evmctl sign --imahash '{}' \;`
  - `find /lib/modules -name "*.ko" -type f -uid 0 -exec evmctl sign --imasig '{}' \;`

Enable IMA/EVM

- Has to be enabled before mounting rootfs
  - From initramfs
- evm_enable.sh

```
# load EVM hmac key
keyctl add user kmk "testing123" @u
keyctl add encrypted evm-key "load `cat /etc/keys/evm-key`" @u

# load IMA/EVM public keys
evmctl import –ima –pem /etc/keys/pubkey_evm.pem
evmctl import –evm -pem /etc/keys/pubkey_evm.pem

# enable EVM
echo "1" > /sys/kernel/security/evm
```

module-init-tools

- modprobe and insmod are modified to pass signature as kernel module parameter 'ima='
  - They verify if signature support is enabled in kernel by looking to /sys/kernel/security/ima/module_check

Links

- IMA/EVM
  - http://linux-ima.sourceforge.net/
- kernel:
  - git://git.kernel.org/pub/scm/linux/kernel/git/kasatkin/ima-ksign.git
- evm-utils
  - git://gitorious.org/meego-platform-security/evm-utils.git
- module-init-tools
  - git://gitorious.org/meego-platform-security/module-init-tools.git