IMA/EVM on Android Device

Dmitry Kasatkin

dmitry.kasatkin@{gmail,huawei}.com

Huawei Security Competence Center, Finland

Linux Security Summit 2015
Seattle, August 20 – 21, 2015

Agenda

- Android Kernel versions
- Kernel configuration
- Image creation
- IMA initialization
- Q&A

Android kernel versions

- Current Android devices are still running very old kernels
- Nexus 5 → 3.4
  - IMA appraisal is missing from that kernel
- Even new flagship devices are still 3.10

Kernel configuration

- Kernel/arch/arm64/configs/<hw>_defconfig

- +# Integrity
- +CONFIG_INTEGRITY=y
- +CONFIG_IMA=y
- +CONFIG_IMA_MEASURE_PCR_IDX=10
- +CONFIG_IMA_AUDIT=y
- +CONFIG_IMA_LSM_RULES=y
- +CONFIG_INTEGRITY_SIGNATURE=y
- +CONFIG_IMA_APPRAISE=y
- +CONFIG_EVM=y
- +CONFIG_TCG_TPM=y
- +# Keys
- +CONFIG_KEYS=y
- +CONFIG_KEYS_DEBUG_PROC_KEYS=y
- +CONFIG_TRUSTED_KEYS=y
- +CONFIG_ENCRYPTED_KEYS=y

Image creation

- Android has few images
  - Boot.img, system.img, userdata.img, cache.img, …
- Create image without requiring root privileges
- Key creation
  - Build/core/ima_key_gen.sh
    - Keys go to boot.img, which is usually signed
  - Build/core/Makefile
    - $(INSTALLED_RAMDISK_TARGET): $(MKBOOTFS) $(INTERNAL_RAMDISK_FILES) $(EVMCTL) | $(MINIGZIP)
    - @$(TOPDIR)build/core/ima_key_gen.sh $(PRODUCT_OUT)
- Image labeling
  - make_ext4fs
    - system/extras/ext4_utils

ima_key_gen.sh

```
#!/bin/sh

#setup the environment variables
CUR_DIR=`pwd`
HUAWEI_PRODUCT_ID=$1
PRIVATE_PEM="${CUR_DIR}/out/host/linux-x86/bin/privkey_evm.pem"
PUBLIC_PEM="${HUAWEI_PRODUCT_ID}/root/pubkey_evm.pem"

# if RSA key pair does not exist, generate new one; otherwise use old one
if [ ! -f "$PRIVATE_PEM" ] || [ ! -f "$PUBLIC_PEM" ]; then
    openssl genrsa -out $PRIVATE_PEM 1024
    openssl rsa -pubout -in $PRIVATE_PEM -out $PUBLIC_PEM
fi

EVMCTL_DIR=${CUR_DIR}/out/host/linux-x86/bin

# generate pubkey_evm.pem.bin & pubkey_evm.pem.keyid,
# which will be loaded to kernel keyring by ima_init during start up

${EVMCTL_DIR}/evmctl --rsa convert $PUBLIC_PEM
```

make_ext4fs

- Creates filesystem image without requiring root permissions
- Has support to set xattrs: for SELinux labels
- Updated to to compute and set 'security.ima' and 'security.evm'
- It calls 'evmctl' to compute signatures
  - Actually probably 'libimaevm' must be used instead
  - Evmctl is statically linked for build server convenience

evmctl

- Tool to generate signatures
- Updated to accept file metadata information on the command line
- New parameters

```
-c, --caps        use custom Capabilities for EVM(unspecified: from FS, empty: do not use)
-i, --ino         use custom inode for EVM
-m, --ima         use custom IMA signature for EVM
-x, --selinux     use custom Selinux label for EVM
-e, --uid         use custom UID for EVM
-g, --gid         use custom GID for EVM
-o, --mode        use custom Mode for EVM
-q, --generation  use custom Generation for EVM(unspecified: from FS, empty: use 0)
```

Initialization

- Update **device/<vendor>/<device>/BoardConfig.mk** file
  - BOARD_KERNEL_CMDLINE += ima_audit=1 ima_tcb ima_appraise_tcb ima_appraise=fix evm=fix

- Update Device/<vendor>/<device>/init.xxx.rc
  - On early-init
    - Exec /sbin/ima_init
  - Add “iversion” mount flag

- Device/<vendor>/<device>/fstab.xxx
  - Add “iversion” mount flag

ima_init

- Usually we use script to initialize IMA/EVM
  - Had to use busybox
  - But on our device with busybox boot.img exceeded partition size
- ima_init_key.c C program
  - Mount securityfs
  - Add keyrings
  - Read and add keys
  - Read policy
    - /ima_policy
  - Enabled EVM
    - Actual EVM key is read from TEE by the kernel directly

Links

- Will publish Wiki around this topic on
  - https://sourceforge.net/p/linux-ima/wiki/Home/
-

Questions?