What: security/ima/policy
Date: May 2008
Contact: Mimi Zohar <zohar@us.ibm.com>
Description:

The Trusted Computing Group(TCG) runtime Integrity Measurement Architecture(IMA) maintains a list of hash values of executables and other sensitive system files loaded into the run-time of this system. At runtime, the policy can be constrained based on LSM specific data. Policies are loaded into the securityfs file ima/policy by opening the file, writing the rules one at a time and then closing the file. The new policy takes effect after the file ima/policy is closed.

rule format: action [condition ...]

action: measure | dont_measure
condition:= base | lsm
base: [[func=] [mask=] [fsmagic=] [uid=]]
lsm: [[subj_user=] [subj_role=] [subj_type=]
[obj_user=] [obj_role=] [obj_type=]]

base: func:= [BPRM_CHECK][FILE_MMAP][FILE_CHECK]
mask:= [MAY_READ] [MAY_WRITE] [MAY_APPEND] [MAY_EXEC]
fsmagic:= hex value
uid:= decimal value
lsm: are LSM specific

default policy:

```
# PROC_SUPER_MAGIC
dont_measure fsmagic=0x9fa0
# SYSFS_MAGIC
dont_measure fsmagic=0x62656572
# DEBUGFS_MAGIC
dont_measure fsmagic=0x64626720
# TMPFS_MAGIC
dont_measure fsmagic=0x01021994
# SECURITYFS_MAGIC
dont_measure fsmagic=0x73636673

measure func=BPRM_CHECK
measure func=FILE_MMAP mask=MAY_EXEC
measure func=FILE_CHECK mask=MAY_READ uid=0
```

The default policy measures all executables in bprm_check, all files mmapped executable in file_mmap, and all files open for read by root in do_filp_open.

Examples of LSM specific definitions:

SELinux:

```
# SELINUX_MAGIC
dont_measure fsmagic=0xF97CFF8C

dont_measure obj_type=var_log_t
dont_measure obj_type=auditd_log_t
```

```
                ima_policy..txt
        measure subj_user=system_u func=FILE_CHECK mask=MAY_READ
        measure subj_role=system_r func=FILE_CHECK mask=MAY_READ

Smack:
        measure subj_user=_ func=FILE_CHECK mask=MAY_READ
```