IBM Research

What is LIM/IMA?
2.6.30 でコッソリ入った LIM/IMA って何?

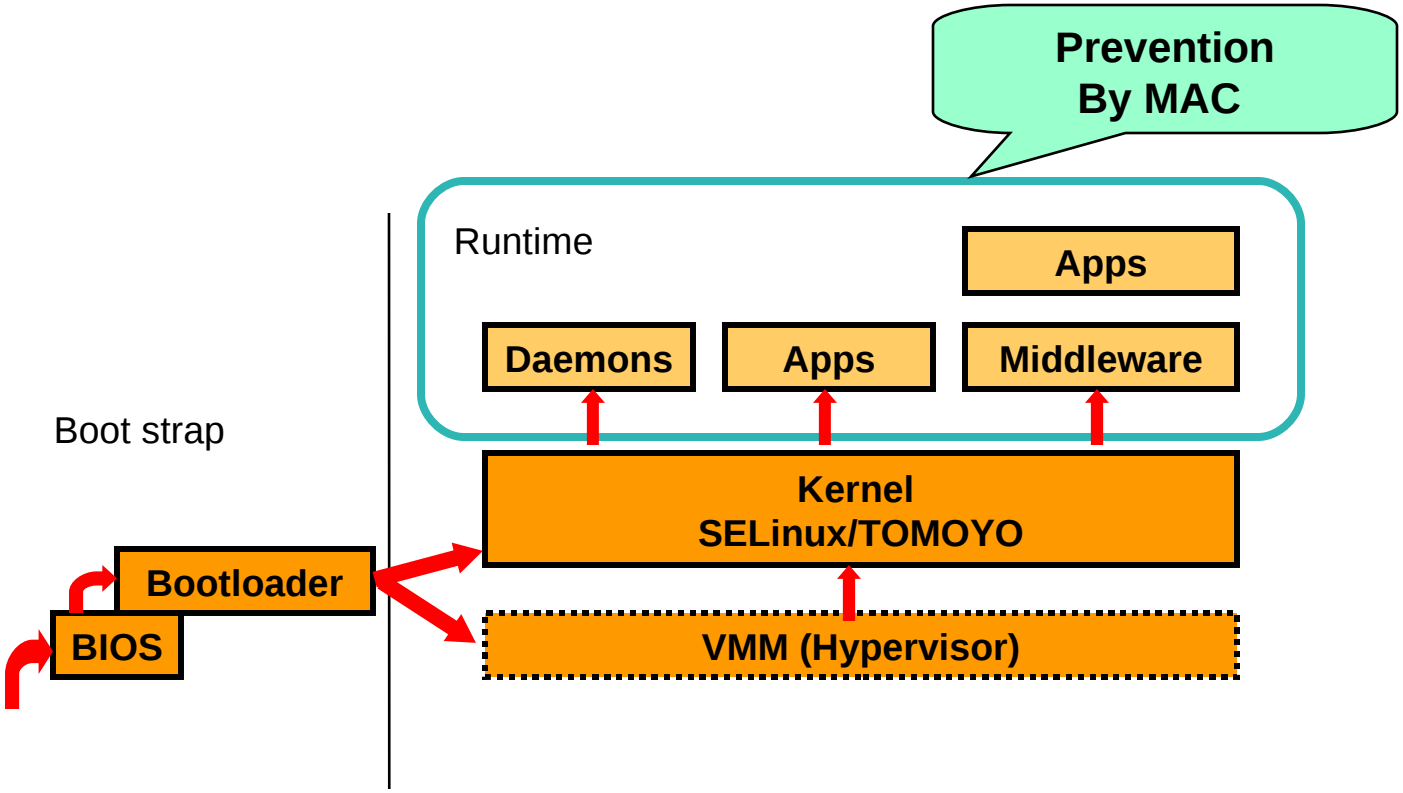
LIM: Linux Integrity Module
IMA: Integrity Measurement Architecture

Seiji Munetoh / IBM Tokyo Research Laboratory
Mimi Zohar / IBM Watson Research Center

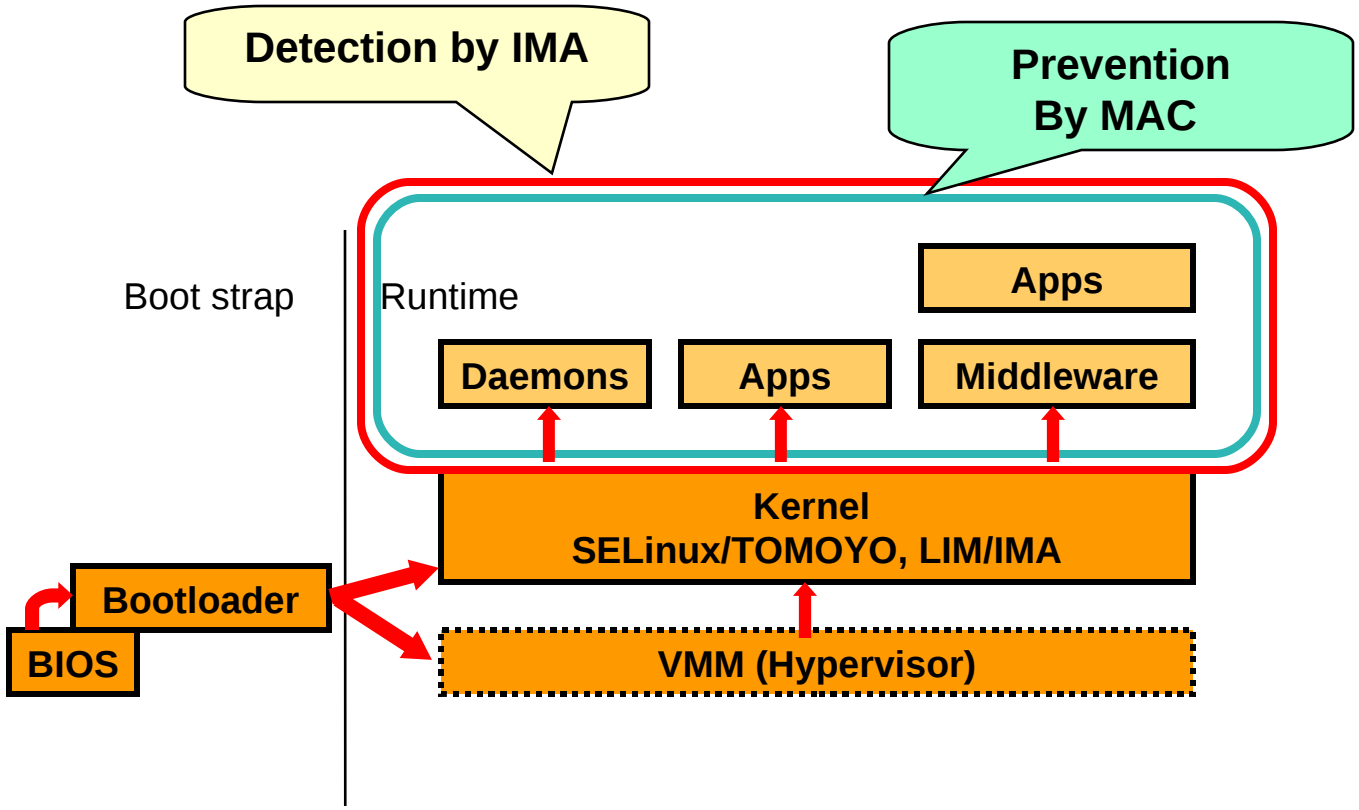
Three aspects of “security”

- Prevention – LSM modules (SELinux,TOMOTO)
  - An LSM module protects files from unauthorized modification
- ***Detection – LIM modules (IMA,EVM)***
  - IMA measures the files. The measurement list can be used to detect the reading or execution of malware.
    - Measures all system sensitive files - executables, mmapped libraries, and files opened for read by root, Measurement can be controlled by policy
    - Extended Verification Module (EVM) protects persistent files from off line modification, but this is not included in the current IMA release. We're working on extending IMA to appraise the measurements
- and Remediation – Package Management (yum, apt-get)

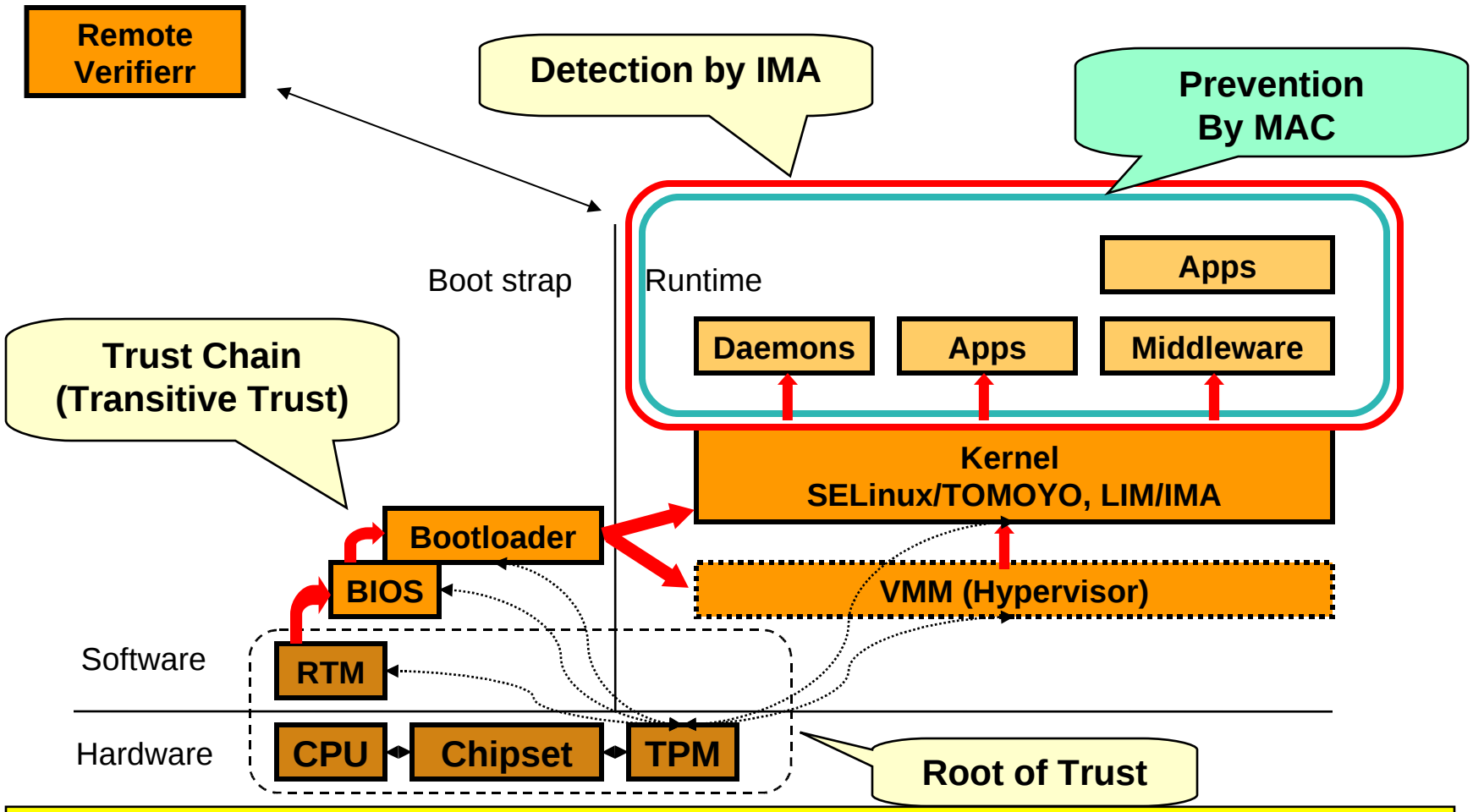
Linux Components



Components of Trusted Computing Platform



Components of Trusted Computing Platform (Full)



The platform (TCB) “integrity” is protected form software attacks and some hardware attacks (depend on security strength of HW)

History

- **1999-10 TCPA is founded**
- **2002-02 TPM v1.1b Spec**
- **2003-04 TCG is founded**
- **2003-08-01 Take Control of TCPA**
  - http://www.linuxjournal.com/article/6633
- **2004-08-12 Linux-IMA presentation at USENIX Security Symposium**
- **2004-11-04 LSM staking**
  - [RFC] [PATCH] [0/6] LSM Stacking
- **2005-05-20 IMA patch @LKML**
  - [PATCH 1 of 4] ima: related TPM device driver interal kernel interface
- **2005-06-17 Linux supports TPM drivers**
- **2005-07-22 Trusted Computing presentations at OLS**
- **2005-11-15 EVM, SLIM, IMA**
  - [RFC][PATCH 0/3] EVM, SLIM, IMA
- **2006-06-22 SLIM: Simple Linux Integrity Module patch @LKML**
  - [RFC][PATCH 0/3] Integrity Service and SLIM
- **2007-03-08 integrity service framework and provider**
  - [RFC][Patch 0/6] integrity service framework and provider
- **2007-03-23 integrity service framework and provider - 2nd**
  - [Patch 0/7] integrity service framework and provider
- **2007-06-18 LIM: Linux Integrity Module patch @LKML**
  - [RFC][Patch 0/3] integrity: Linux Integrity Module(LIM) and provider
  - [RFC][Patch 1/1] IBAC Patch
- **2009-06-09 LIM/IMA mainlined bv 2.6.30!!!**

How to use…

- **Build 2.6.30 kernel with**
  - CONFIG_IMA=y
- **Reboot**
  - You can see the measurement log at /sys/kernel/security/*/*

```
 Idx PCR       Type    Digest                                    EventData
-----------------------------------------------------------------------------
   0   0 0x00000008 4081b13dc986e581d587aa7fe6c61e02ef7312b2 [BIOS:EV_S_CRTM_VERSION
   1   0 0x00000001 8b5c22ae675ea440e2f403b4d5e88131fecc2a1c [BIOS:EV_POST_CODE(EV_C      _NOCERT)]
   2   0 0x00000001 d9f7d65755c884f6c25680d577f348523006eed3 [BIOS:EV_POST_CODE(EV_      E_NOCERT)]
<snip>
 198   8 0x00001205 a73c31a3abe77960ff8c631edf0dfd29112aa6f3 [GRUB:KERNEL /boot/vmlinuz-2.6.30-ima]
 199   8 0x00001305 f8422432a897cd434fa405e6c653ad12b6faacd6 [GRUB:INITRD /boot/initrd.img-2.6.30-ima]
 200   8 0x00000004 2431ed60130faeaf3a045f21963f71cacd46a029 [GRUB:EV_SEPARATOR, OS Event Separator]
 201   8 0x00001005 fac33a1fc0ad42c07d00322d64c23f67567f334a [GRUB:ACTION, Booting Big Linux Kenrel]
 202  10 0x00000000 173d86589890c0c8b9b42b5b1ee671aecfbec7c0 [IMA:boot_aggregate]
 203  10 0x00000000 8a11aa2017bfdf52ae1ab8cfb277fc651bc7d611 [IMA:/init]
 204  10 0x00000000 a078e19e5ea2bf75ed353fc6613f7132863618d5 [IMA:/init]
<snip>
 523  10 0x00000000 c5400a3dbdb4ec0e9814498095841fc4ccea0245 [IMA:/sbin/load_policy]
 524  10 0x00000000 b6de25749576ec1fe0b6e49c3394b1d97c737354 [IMA:ld-2.9.so]
 525  10 0x00000000 6935ae5654a23a6c773bbb2b2be05dc268f4d905 [IMA:ld.so.cache]
 526  10 0x00000000 62cba99abf93df49aaa59bf286e95e35a0f54f38 [IMA:libsepol.so.1]
 527  10 0x00000000 4831ec4abdaaa3d8e501fb1b87b9af8e4967d1bd [IMA:libc-2.9.so]
 528  10 0x00000000 6eaf6627796fb433c0fabc0ce92d7c143a0bf50a [IMA:libdl-2.9.so]
 529  10 0x00000000 3e362a6e51956838b20007340c000152b397aa5e [IMA:config]
 530  10 0x00000000 e1187509a3a9b439ee480bce606991178112de0e [IMA:policy.23]
```

Kernel が本物！

ポリシーが本物！

BTW, Setting up Trusted Computing Platform is still very hard :-P

Thanks!

For more information, see

TPM Device Driver > http://tpmdd.sourceforge.net/

Linux-IMA > http://linux-ima.sourceforge.net

TrouSerS (TSS) > http://trousers.sourceforge.net

OpenPTS > http://sourceforge.jp/projects/openpts/

TCG Specifications > https://www.trustedcomputinggroup.org

TOMOYO-Linux メインライン化おめでとう

- **TOMOYO** と **IMA** は一緒に使えるの？
  - 使えるはずです
  - TOMOYO のトレース機能と組み合わせて使うと楽しいと思います