TOMOYO Linux Overview

Kentaro Takeda
takedakn@nttda.co.jp
NTT DATA CORPORATION

TOMOYO is a registered trademark of NTT DATA CORPORATION in Japan.
Linux is a trademark of Linus Torvalds.
Other names and trademarks are the property of their respective owners.
About

- Part 1 (this part)
  - Brief introduction and demo.
  - Current status.

- Part 2 (from Tetsuo Handa, a main architect of TOMOYO)
  - Deep inside of TOMOYO for security guys. 😊
TOMOYO Linux

- A pathname-based MAC for Linux kernel.
- Developed by NTT DATA CORPORATION.
- Available under GPL.
The concept of TOMOYO is “Pathname-based security”, of course. 😊

Tetsuo will talk about “pathname’s role” in part 2, I introduce some aspects of TOMOYO.
Main features of TOMOYO

- Designing and enforcing “state transition”.
  - Monitors and judges program execution requests.
  - Performs state transition by execution.
- Observing and restricting requests within each state.
  - Monitors and judges read/write requests to files.
State transition by execution

/sbin/init

/sbin/mingetty

/etc/rc.d/rc.sysinit

/sbin/mingetty

/bin/login

/sbin/start_udev

/sbin/start_udev

/bin/unicode_start

/bin/unicode_start

/bin/kbd_mode

/bin/kbd_mode

/bin/setfont

/bin/setfont

Copyright (C) 2009 NTT DATA CORPORATION
Attractive feature of TOMOYO

- Automatic policy learning.
  - Accumulating access permissions within each domain.
  - With pathname, of course. 😊

- It’s not essential part as a security module.
- But very attractive and friendly for averagely experienced administrators.
State (=domain) transition occurs automatically.

Example) domains of postfix

```
/usr/sbin/postfix
/etc/postfix/postfix-script
    /etc/postfix/postfix-script
    /bin/sh
    /bin/grep
    /bin/uname
    /usr/sbin/postconf
/usr/lib/postfix/master
    /usr/lib/postfix/cleanup
    /usr/lib/postfix/local
    /usr/lib/postfix/pickup
    /usr/lib/postfix/qmgr
    /usr/lib/postfix/trivial-rewrite
```

Each line indicates a domain.
### ACLs

```plaintext
<kernel> /usr/sbin/httpd
allow_read /var/www/html/*
allow_read /etc/httpd/*.conf
allow_read /usr/lib/httpd/modules/*.so
allow_write /var/log/httpd/*_log
allow_create /var/run/httpd.pid
allow_unlink /var/run/httpd.pid
```

- **/usr/sbin/httpd**
  - may read `/var/www/html/*` and `/etc/httpd/*.conf` and `/usr/lib/httpd/modules/*.so`
  - may write `/var/log/httpd/*_log`
  - may create and unlink `/var/run/httpd.pid`
Domain transition and ACLs

```
<kernel> /usr/sbin/sshd /bin/bash
allow_execute  /bin/ls
allow_read    /home/takedakn/.bashrc
allow_read/write /home/takedakn/.bash_history
```

(snip)

```
<kernel> /usr/sbin/sshd /bin/bash /bin/ls
allow_read  /etc/group
allow_read  /etc/nsswitch.conf
allow_read  /etc/passwd
```
Demo

- Linux 2.6.28
- mmotm-2009-01-09-16-44
- TOMOYO (LSM version) revision 2031
Two versions of TOMOYO

- non-LSM version
  - Our start point.
  - Full-featured version.
    - file, network, etc...

- LSM version
  - Only file restriction feature for now.
  - Proposing to mainline now.
LSM for pathname based MAC

- LSM was not designed to implement pathname based security module.
  - vfsmount * wasn’t available inside LSM module.
- Now, new LSM hooks are placed where vfsmount * is available in Linus’ tree.
  - “[PATCH] Introduce new LSM hooks where vfsmount is available”
- We’re proposing TOMOYO’s body now.
Thank you!

takedakn@nttdata.co.jp

Let’s dive deeper into TOMOYO.