

FreedomHEC Taipei 2008

TOMOYO Linux:

pragmatic and manageable security for Linux

Kentaro Takeda

takedakn@nttdata.co.jp

NTT DATA CORPORATION

TOMOYO is a registered trademark of NTT DATA CORPORATION in Japan.

Linux is a trademark of Linus Torvalds.

Red Hat is a registered trademark of Red Hat, Inc.

SUSE is a registered trademark of Novell, Inc.

Ubuntu is a registered trademark of Canonical, Ltd.

Mandriva is a registered trademark of Mandriva, Inc.

Turbolinux is a registered trademark of Turbolinux, Inc.

Other names and trademarks are the property of their respective owners.

About

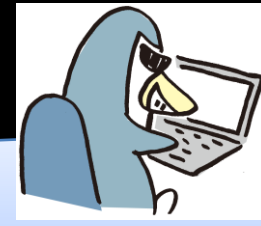
- This is the second part of “secure Linux” session.
- Focused on our work, TOMOYO Linux.
- TOMOYO is a MAC extension, and it provides “pragmatic and manageable” security.
- Let’s get started!

TOMOYO Linux

- Developed by NTT DATA CORPORATION.
- Freely available under GPL since Nov, 2005.
- a MAC extensions for Linux.
 - Other ones: SELinux, Smack, AppArmor
- TOMOYO hooks various system calls and check whether the request is correct or incorrect.



Normal Linux



User

Application

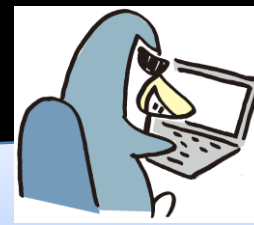
Application

Application

Kernel



TOMOYO Linux



User

Application

Application

Application

TOMOYO Linux



Kernel

OK?
not OK?

Why is TOMOYO pragmatic and manageable?

- Readable and understandable policy.
- Automatic policy learning mode.
- Interactive judging in enforcing mode.

Readable and understandable policy

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

- /bin/bash executed by /usr/sbin/sshd
 - may execute /bin/ls
 - may read /home/takedakn/.bashrc
 - may read and write
/home/takedakn/.bash_history .

Readable and understandable policy

```
<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
allow_network   TCP bind      192.168.1.128 80
allow_network   TCP listen   192.168.1.128 80
allow_network   TCP accept   192.168.0.0-192.168.255.255 1024-65535
```

- /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
 - may bind and listen 192.168.1.128:80
 - may accept connections from 192.168.0.0/16:1024-65535 .

Readable and understandable policy

- It's easy to read, isn't it? 😊
- Is it easy to write?
 - ...not difficult, but...
- It's bothering work to write from scratch. ☹️

➔ Automatic policy learning

Automatic policy learning

- Seeing is believing.



Automatic policy learning

- A kind of access analysis.
- You can understand your Linux deeply by browsing learned policy.
- “Understanding is protecting.”

TOMOYO workflow

- **Set learning mode.**
- Just use your Linux.
- Tune policy.
 - Use wildcard and address/port range.
- **Set permissive mode.**
 - Policy violation won't be denied, but reported.
- Use your Linux and watch report.
- **Set enforcing mode!**

People say

- “It sounds great, but the lack of permission causes trouble, doesn’t it?”



- Yes, it does. ☹
 - That’s the way MAC is.
- However, TOMOYO supports you even in enforcing mode.

➔ Interactive judging

Interactive judging

- Have you ever seen this?



Interactive judging

- You can choose {deny, allow, allow&learn} for policy violation in enforcing mode.
 - deny: deny this request.
 - allow: allow this request (ask me again next time).
 - allow&learn: allow this request and add it into policy (i.e. don't ask me again).
- Especially suits in system update.

Interactive judging

- Seeing is believing.



Because TOMOYO is pragmatic and manageable,

- TOMOYO is NOT for...
 - Security wizard.
- TOMOYO is for...
 - Averagely experienced Linux administrator.

Possibilities of TOMOYO

- Security.
 - Of course. ☺
- **Application development and debugging.**
 - TOMOYO can visualize the behavior of application.
- Education.
 - “How does my Linux work?”
 - You can understand your Linux deeply.

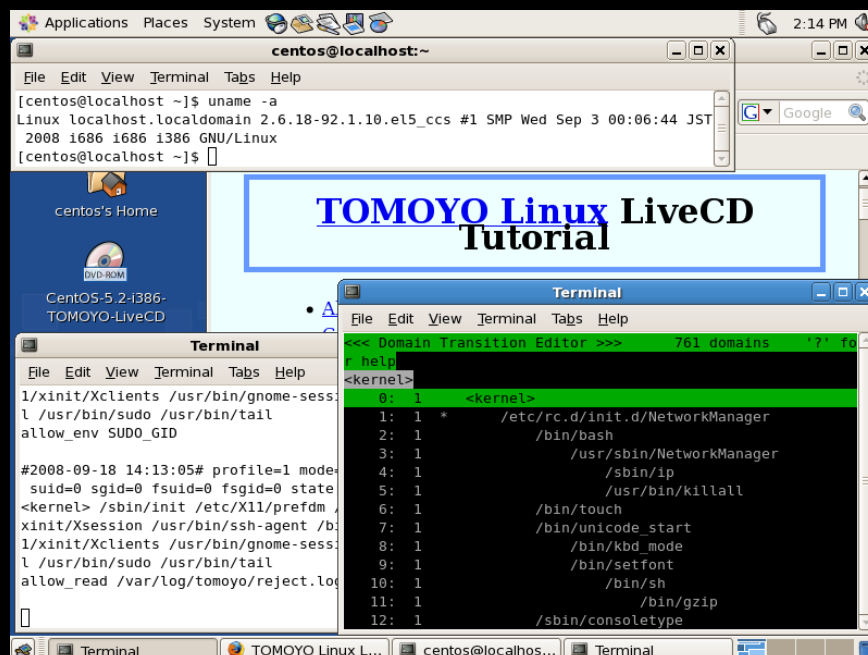
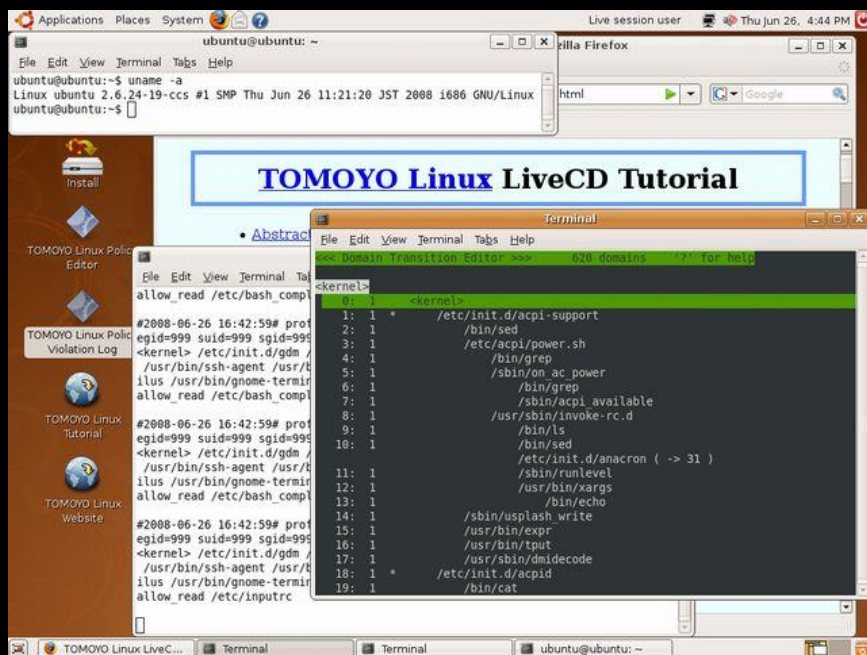


Installation

- Download and install kernel package.
 - For Red Hat (CentOS), SUSE, Ubuntu, Fedora, Debian
- Download and install tools package.
 - For Red Hat (CentOS), SUSE, Ubuntu, Fedora, Debian, Mandriva, Turbolinux
- Run `/usr/lib/ccs/init_policy.sh` .
- Reboot!

Need easier way to try?

- LiveCD available
- Ubuntu, CentOS



Mainlining

Current Linux kernel source tree

```
$ find linux-2.6/security -type d
linux-2.6/security/
linux-2.6/security/keys
linux-2.6/security/selinux
linux-2.6/security/selinux/include
linux-2.6/security/selinux/ss
linux-2.6/security/smack
```




Future... (our hope)

```
$ find linux-2.6/security -type d
linux-2.6/security/
linux-2.6/security/keys
linux-2.6/security/selinux
linux-2.6/security/selinux/include
linux-2.6/security/selinux/ss
linux-2.6/security/smack
linux-2.6/security/tomoyo
```

- Our largest mission, now in progress.

<http://lwn.net/Articles/277833/>

**LWN.net**
Your Linux info source

[Weekly edition](#) [Kernel](#) [Security](#) [Distributions](#) [Search](#)
[Archives](#) [Calendar](#) [Subscribe](#) [Write for LWN](#) [LWN.net FAQ](#)

TOMOYO Linux and pathname-based security

By Jonathan Corbet
April 14, 2008

It takes a certain kind of courage to head down a road when one can plainly see the unpleasant fate which befell those who went before. So one might think that the fate of AppArmor would deter others from following a similar path. The developers of TOMOYO Linux are not easily put off, though. Despite having a security subsystem which shares a number of features with AppArmor, these developers are pushing forward in an attempt to get their code into the mainline.

Not logged in
[Log in now](#)
[Create an account](#)
[Subscribe to LWN](#)

Weekly Edition
[Return to the Kernel page](#)

Sponsored link
Vyatta – Linux &

Pointers

- [Presentation material]
 - <http://sourceforge.jp/projects/tomoyo/docs/freedomhetapei-tomoyo.pdf>
- [Official]
 - <http://tomoyo.sourceforge.jp/>
- [English portal]
 - <http://elinux.org/TomoyoLinux>
- [Mailing list]
 - <http://lists.sourceforge.jp/mailman/listinfo/tomoyo-users-en>
 - low traffic, feel free to post anything ☺
- [LiveCD]
 - <http://tomoyo.sourceforge.jp/wiki-e/?TomoyoLive>

Thank you!



Any questions?