CE Linux Forum
Worldwide Embedded Linux Conference 2007

TOMOYO Linux – Tutorial session

Kei Masumoto and Kentaro Takeda

NTT DATA CORPORATION

TOMOYO Linux Project
http://tomoyo.sourceforge.jp/
Contents

- Background knowledge of TOMOYO Linux

- Part 1 – How to use “Automatic policy generation” functionality.

- Part 2 – How to protect Internet servers using TOMOYO Linux.

- Part 3 – Advanced TOMOYO Linux functionality.
  - Network access control, etc..
Background Knowledge

Main points.

1. Operation mode of TOMOYO Linux.
   - Disabled → Generating → Permissive → Enforcing.
   - Details will be shown in part 1.

2. How to read TOMOYO Linux access policy.
   - Similar to UNIX-OS permission expression.
Background knowledge

How to read the policy of TOMOYO Linux

- **/bin/login** executed by **/sbin/mingetty** can access only the following resources:
  - executing **/bin/bash** (domain transition)
  - reading **/etc/passwd**, **/etc/shadow**
  - reading/writing to **/var/log/lastlog**
  - writing to **/var/run/wtmp**
1. Policy generation and enforce

- Main points.
  
  - The “Automatic policy generation” functionality is the essential of TOMOYO Linux.
  
  - Users can use that functionality only executing a few commands.
  
  - In enforcing mode, an user can execute only operations executed in policy generation mode.
1. Policy generation and enforce

**GENERATING**

```
setprofile -r 1 '<kernel> /usr/sbin/sshd /bin/bash' > /dev/null
```

**ENFORCING**

```
ls
```

```
Operation not permitted
```

```
shutdown -h now
```

```
rm -rf /
```

```
Operation not permitted
```

```
tail -3 /etc/mtab
```

```
Operation not permitted
```

```
tail -3 /etc/mtab
```

```
Operation not permitted
```

```
head: /etc/mtab: Operation not permitted
```

**only operations executed in policy generation mode are permitted**
1. Policy generation and enforce

- These policies are automatically generated by operations.
- Each execution invokes a domain transition.
  - Even if one uses BusyBox, TOMOYO Linux can separate domains.
2. Apache policy

Main points

- The main reason to use TOMOYO Linux is to protect Internet servers from being cracked.
- This tutorial shows how TOMOYO Linux protects Internet servers from being cracked.
- Also, users can use “patterns” when the server accesses various resources and access policy is complex.
2. Apache policy
2. Apache policy

- Read accesses to the web contents

- Some of the available patterns
  - ¥* : any letters which do not contain ‘/’
  - ¥? : any single letter except for ‘/’
  - ¥$ : any decimal number
  - ¥X : any hexadecimal number
3. Towards higher security

Main points.

- TOMOYO Linux can control not only files but also various resources.

- “Network access control” is a major functionality towards higher security.

- Users can use this functionality in the same way – using “change to advanced generation mode”
3. Towards higher security

```
<kernel> /busybox/usr/sbin/httpd
  0: 4 /var/www/`
  1: 4 /var/www/`/`/
  2: 4 /var/www/`/`/`/
  3: 4 /var/www/`/`/`/`/
  4: 4 /var/www/`/`/`/`/`/
  5: allow_network TCP accept 10.0.0.0-10.255.25.255 1024-65535
  6: allow_network TCP bind 0.0.0.0 80
  7: allow_network TCP listen 0.0.0.0 80
```
3. Towards higher security

- Network access control

```plaintext
allow_network
    TCP accept : protocol
    10.0.0.0-10.255.255.255 : IP address range
    1024-65535 : port range
```

- Similar to iptables for each domain

- Other controllable resources
  - capability, signal, argv0
  - mount/umount, chroot, pivot root
Thank you for your attention

Any Questions?