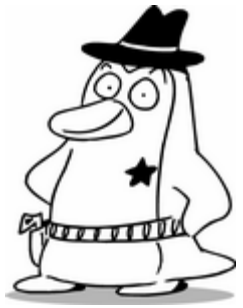
CE Linux Forum
Worldwide Embedded Linux Conference 2007

TOMOYO Linux – Tutorial session

Kei Masumoto and Kentaro Takeda

NTT DATA CORPORATION
http://www.nttdata.co.jp/en/index.html

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.

How to read the policy of TOMOYO Linux

- **/bin/login** executed by **/sbin/mingetty** can access only 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

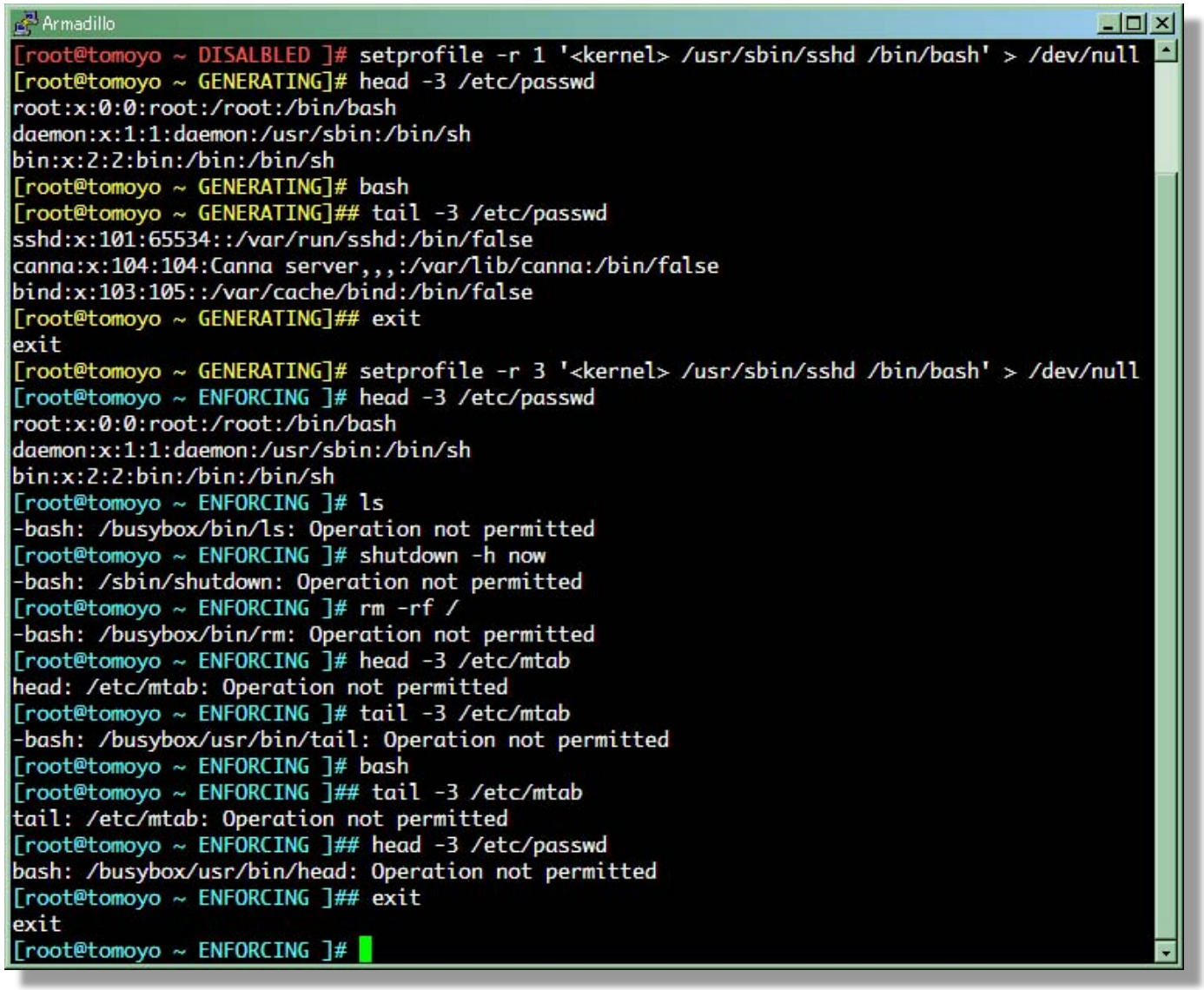
- Main points.
  - The “Automatic policy generation” functionality is the essential of TOMOYO Linux.
  - Users can use that functionality only executing a few commands.
  - In enforcing mode, an user can execute only operations executed in policy generation mode.

1. Policy generation and enforce

GENERATING

ENFORCING

only operations executed in policy generation mode are permitted



1. Policy generation and enforce

```
<kernel> /usr/sbin/sshd /bin/bash

1 /busybox/usr/bin/head
1 /bin/bash
```

```
<kernel> /usr/sbin/sshd /bin/bash /busybox/usr/bin/head

4 /etc/passwd
```

```
<kernel> /usr/sbin/sshd /bin/bash /bin/bash

1 /busybox/usr/bin/tail
```

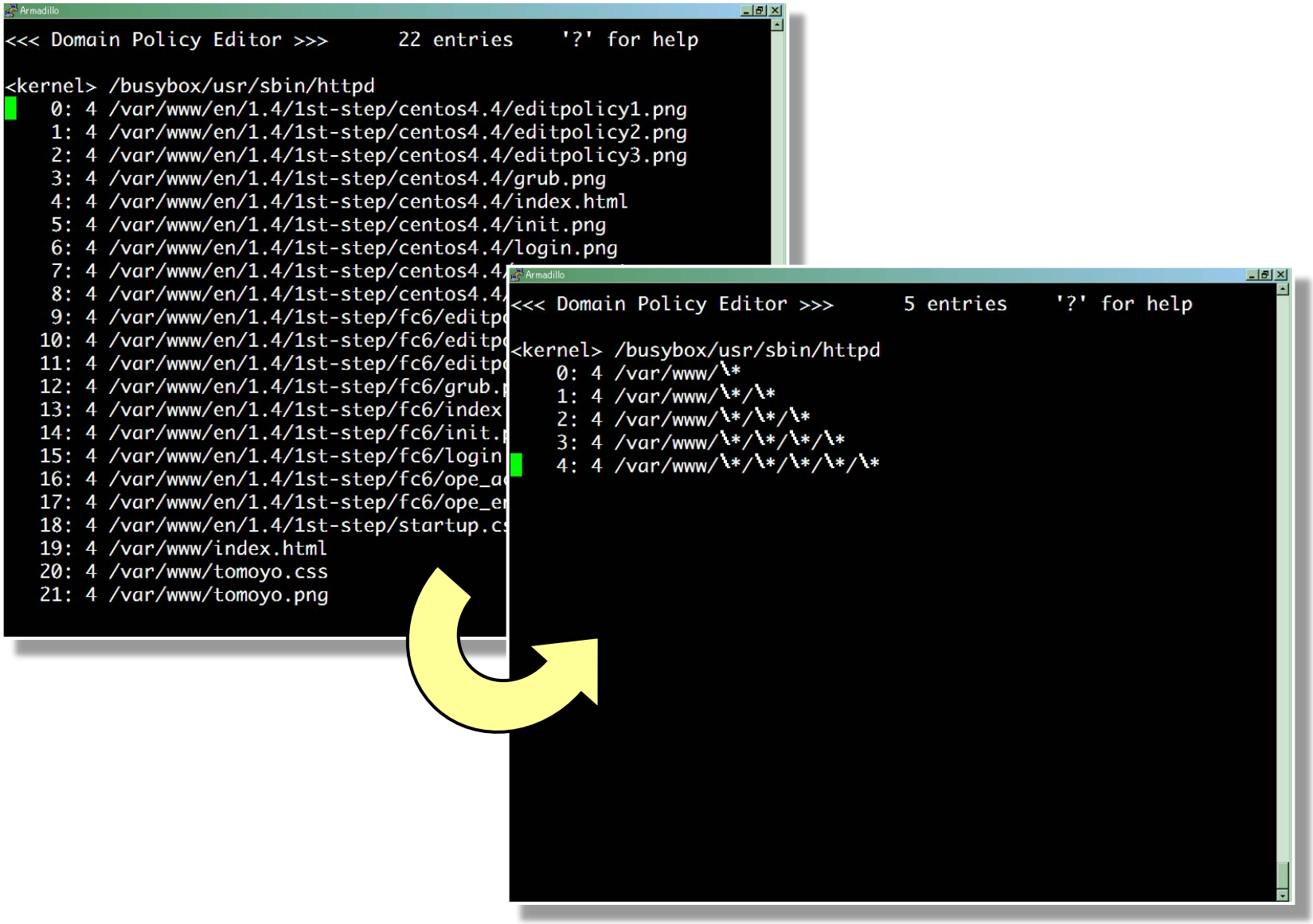
```
<kernel> /usr/sbin/sshd /bin/bash /bin/bash /busybox/usr/bin/tail

4 /etc/mtab
```

- 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

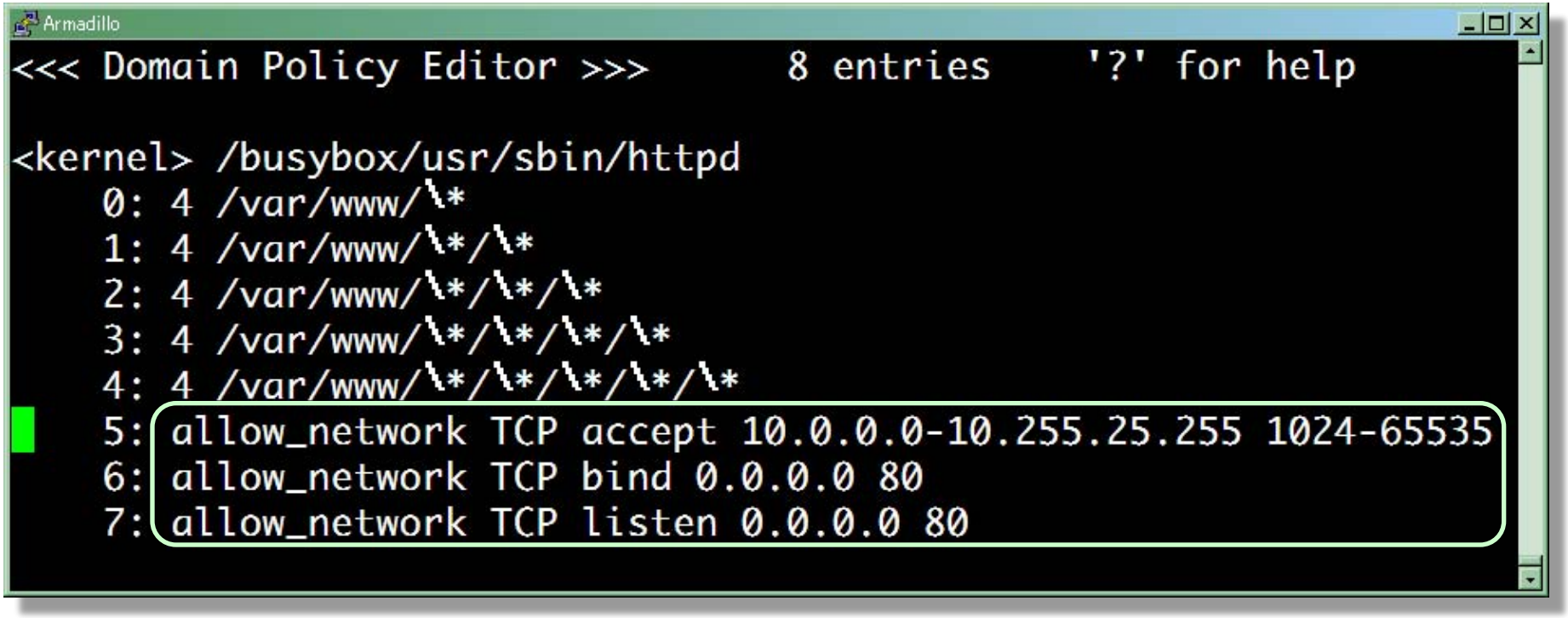
```
4 /var/www/¥*
4 /var/www/¥*/¥*
4 /var/www/¥*/¥*/¥*
4 /var/www/¥*/¥*/¥*/¥*
4 /var/www/¥*/¥*/¥*/¥*/¥*
```

- 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



3. Towards higher security

- Network access control

```
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?