Realities of Mainlining
- Case of the TOMOYO Linux Project -

Toshiharu Harada
<haradats@nttdata.co.jp>
<haradats@gmail.com>

NTT DATA CORPORATION

July 9, 2008
TOMOYO Linux

✴ “pathname-based” Mandatory Access Control (MAC) enhancements
✴ Started as a R&D project of NTT DATA CORPORATION in 2003
✴ Available as open source since Nov. 2005
✴ LiveCD is available
✴ TOMOYO is a registered trademark of NTT DATA CORPORATION
Toshiharu (project manager)  Kentaro (LSM version)  Tetsuo (main architect)

Project members
Instructions

✴ During the presentation, I will ask a couple of questions to the guests.

✴ Guests have the plate and are expected to show us the answer.
Instructions

✈ During the presentation, I will ask a couple of questions to the guests.

✈ Guests have the plate and are expected to show us the answer.
Exercise

- What's your name?
  - Andrew Morton
  - Paul Moore
  - James Morris
Question

- Have you ever heard of “TOMOYO Linux”

- I tried TOMOYO Linux and liked it
- Yes
- What is it?
March 2003

- Project launched at Kayabacho in Japan without
- kernel development experiences
- specific goal
- smart, experienced project manager
When we started

🌟 We didn’t know the words “mainline”, “upstream” and “OLS”

🌟 We never thought of making our work to be merged in the Linux kernel

🌟 But now mainline is our major concern
There has been changes

- We met many people
- Some people told us, some suggested, some demanded ...
April 2006
Meeting with Russell

Russell Coker has visited Japan
We showed him an early version TOMOYO Linux and received some comments
He was the first person that suggested mainlining
“Use the Linux auditing for event logging”

“Use LSM interfaces. If you can entirely use LSM interfaces then TOMOYO can be a candidate for inclusion ...”

“I suggest is to have equivalence classes (let’s call them domains). This means that “vi” and “emacs” will be considered to have identical security properties ...”

We have done the above by now
He wrote to me

“If you mostly use LSM interfaces then you will save significant amount of work in terms of maintaining support for new kernels and also save development work for everyone who wants to use your system along with other patches.”

Dec. 8, 2006

★ **Satoru Ueda** of CELF (Consumer Electronics Linux Forum) asked me to demonstrate TOMOYO Linux at their technical meeting.


★ I spoke to them,

★ “please send requests/questions in Japanese”

★ “please use TOMOYO Linux”

★ And got ...
Unexpected Comments

🌟 They said

🌟 “We want to use only in-tree modules”
🌟 “Why don’t you try mainlining?”
🌟 “Think global go out the world”
🌟 “Try submitting ELC2007 (Embedded Linux Conference 2007)”
Feb. 8, 2007

* Hiro Yoshioka of Miracle Linux gently asked me to introduce TOMOYO Linux to a pretty famous Japanese community, YLUG (Yokohama Linux Users Group)

* I accepted as usual not knowing what would happen ...
Feb. 8, 2007

✴ Hiro Yoshioka of Miracle Linux gently asked me to introduce TOMOYO Linux to a pretty famous Japanese community, YLUG (Yokohama Linux Users Group)

✴ I accepted as usual not knowing what would happen ...
“We will fix you!”

- It was a meeting of the Hell
- They compelled us to try mainlining
- We were scolded and they told us to see the world
- They even demanded us to challenge OLS
- It was only 7 days to the deadline and I didn’t know what OLS was :-) huh!
Evidence tells ...

✿ There is a movie.

✿ The 72th kernel reading party (92 min)
ELC2007 and OLS2007, both submissions were accepted despite of my expectations

The beginning of the hard days
We worked hard

✴ Jumped in the LKML AppArmor threads
✴ Started making new TOMOYO Linux patches that use LSM
✴ We wanted to post them to LKML before OLS2007
We had

- 2 sessions (presentation and tutorial)
- Not many people came to our session as expected, but ...
There he was!

(Jonathan Corbet attended our session)
There he was!

(Jonathan Corbet attended our session)
Suggestions from the Heaven

- “Try making TOMOYO Linux to be merged”
- “Talk with AppArmor people”

- We were encouraged, very very deeply
- We’ve followed the above advices before OLS2007
TOMOYO Linux LKML logs

- We are maintaining a Wiki page to follow our postings.


- Each posting is linked to a corresponding LWN.net article.
June 13, 2007

🌟 LKML debut of TOMOYO Linux

🌟 We wrote URL to reduce the e-mail size ...

🌟 Not in LKML standard coding style ...

🌟 Tabs were not properly handled ...

🌟 Full of failures
Message from Mr. SELinux

Stephen Smalley sent me a message

“If you really want feedback or to get your code into the kernel, you need to do more than post a URL to the code - you need to break your code down into a number of patches and post them...”

I appreciated his consideration
Message from Japanese community

✴ from Goto-san @fujitsu

✴ “You should choose mm tree or rc as base of the patches”

✴ “Be careful to follow the LKML standard CodingStyle (checkpatch.pl might help)”

✴ “Use quilt”

✴ We didn’t understand those basic rules
How to start

• It’s simple, just give it a try
• You don’t have to be perfect (as we were)
• There are people who would help you
• You just need to “go out” to be visible
What You Need to Join the kernel development

- The source code of Linux
- Enormous documentations and genius tools are included as part of Linux
- Mail program that understands threads and ...
What You Need to Join the kernel development

- The source code of Linux
- Enormous documentations and genius tools are included as part of Linux
- Mail program that understands threads and ...

Courage
Where to find the source?

• Visit www.kernel.org

• Browse LXR sites
  • http://tomoyo.sourceforge.jp/cgi-bin/lxr/source
  • http://lxr.linux.no/

• Use Git (http://git.or.cz/)
Jun. 29, 2007

Ottawa!

(photo: just waiting for the time of our very first session at OLS)
Stephen Smalley, Chris Wright, Joshua Brindle, Seth Arnold, Hadi Nahari and other secure-OS guys came to my session

What a pleasure!
AppArmor and SELinux guys began fighting
AppArmor and SELinux guys began fighting
AppArmor and SELinux guys began fighting

I thought ...
why in my session ...
Do you recognize “(>_<=)”?

- Yes
- Don’t know (tell me)
Answer

- (>_<!) auch!
- (^_^) happy
- (T_T) sad (crying)
- How about “orz”?
anyway ...

✶ It was a really wonderful experience
✶ We met many people
✶ We found we were with community
✶ Unforgettable day

✶ I wrote a wiki page

OLS2007

The night of miracle

★ Stephen spared his time to talk with US after the session!!!

★ He suggested us TOMOYO Linux get married with SELinux or AppArmor
OLS2007

The night of miracle

Stephen spared his time to talk with US after the session!!!

He suggested us TOMOYO Linux get married with SELinux or AppArmor
Linus suddenly appeared in SMACK thread and spoke out loud

I’m tired of this “only my version is correct” crap. The whole and only point of LSM was to get away from that.

Linus’ message sounded like a chance (sorry for James ...), so we rushed to prepare the 3rd posting
“only my version is correct” crap?

- Linus’ words raised me questions
- I didn’t think SELinux people (or James) meant only SELinux was correct ...
- Single solid security vs. choices
Questions?

- Should Linux have multiple choices for fundamental security mechanism?
  - Yes
  - No
  - Other (let me say!)
Oct. 11, 2007

Shock

- We got 0 (zero) feedbacks for our 4th posting

- This is sort of TOMOYO Linux project’s difficulties
Positive feedbacks are always Good!

Negative feedbacks and NACK are “Not BAD”

No feedbacks is BAD
Question

• How can this (*no* feedbacks) happen?

• What should we do when there is no feedbacks?
Nov. 29, 2007
PacSec2007

Dragos in Tokyo

Serge E. Hallyn has suggested to enhance

- TOMOYO provides no sort of information flow control
- TOMOYO is purely restrictive
- Learning mode is primary source of policy so you depend on change of behavior to detect intruders
- but any intruder who attempts to do something which the compromised software wouldn’t have done should be stopped and detected
Feb. 24, 2008

FOSDEM’08

Schedule: Tomoyo Linux for secure embedded (Linux)

Tomoyo Linux for secure embedded (Linux)

TOMOYO Linux is a MAC (Mandatory Access Control) implementation for Linux.

It was developed by NTT DATA CORPORATION, Japan and is available under the GPL license. TOMOYO Linux consists of patch files to vanilla kernel and userland tools.

Patch files are provided for both 2.4 and 2.6. For the user’s convenience, various binary packages are also available.

Speakers

Toshikazu Harada

Schedule

<table>
<thead>
<tr>
<th>Day</th>
<th>Sunday</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room</td>
<td>AVN.120</td>
</tr>
<tr>
<td>Start time</td>
<td>12:30</td>
</tr>
<tr>
<td>End time</td>
<td>12:30</td>
</tr>
<tr>
<td>Duration</td>
<td>01:00</td>
</tr>
</tbody>
</table>

Info

Event type: Podium
Track: Embedded
Language: English

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.

AppArmor, remember, is a Linux security module which uses pathnames to make security decisions. So it is entirely conceivable that two different security policies could apply to the same file if that file is accessed by way of two different names. This approach helps make AppArmor easier to administer than SELinux, but it has given AppArmor major problems in the review process for a few reasons:

What a nice surprise to see my project on LWN.net!
How to analyze your Linux’s behavior with TOMOYO Linux

Kentaro Takeda
takedakn@nttdata.co.jp
NTT DATA CORPORATION
http://tomoyo.sourceforge.jp/

TOMOYO threads posters
top 10 (thanks!)
TOMOYO threads posters

top 10 (thanks!)
TOMOYO threads posters

top 10 (thanks!)
Paul, James and ...

- Are we missing someone? ... NO

- **HE** has sent Tetsuo personal messages several times as well as Stephen

- If you move, you will know there are people to help you
Statistics

Sourceforge Statistics: TOMOYO
Page Views and Downloads for the past 34 months

Legend:
- Red: Page Views
- Blue: Downloads (Right Hand Scale)
Statistics

Sourceforge Statistics: TOMOYO
Page Views and Downloads for the past 34 months

Legend:
- Page Views
- Downloads (Right Hand Scale)
Statistics

Sourceforge Statistics: TOMOYO
Page Views and Downloads for the past 34 months

Legend:
- Page Views
- Downloads (Right Hand Scale)
We are still in the middle of our way.

It might take a month, a year, or a decade, but we know we will never give up.

Merging TOMOYO Linux started as our mission, but now they are our personal goals.

We found joys in ourselves.
Question

• Do you think TOMOYO will be merged someday?

Send me the patches and I will merge them in my git tree

Someday, maybe

... I don’t want to mention now
When in doubt

🌟 Don’t worry, you can ask “HIM”
When in doubt

☆ Don’t worry, you can ask “HIM”
Question

- Who is “HE”?

× don’t know

○ “Me”
kernel.org development and the embedded world

Andrew Morton
<akpm@linux-foundation.org>
<akpm@google.com>
CELF Embedded Linux Conference
April 2008

http://www.celinux.org/elc08_presentations/morton-elc-08.ppt
please read and find HIM
kernel.org development and the embedded world

Andrew Morton
<akpm@linux-foundation.org>
<akpm@google.com>
CELF Embedded Linux Conference
April 2008

http://www.celinux.org/elc08_pre sentations/morton-elc-08.ppt
please read and find HIM
The merge decision (cont'd)

- When in doubt: ask me!
  - I can help
    - That's what I'm here for
      - I'm really nice!
        - And I have great legs
        - But I'll only help you if there's something in it for me
The merge decision (cont'd)

• When in doubt: ask me!
  - I can help
    • That's what I'm here for
      - I'm really nice!
    • And I have great legs
    • But I'll only help you if there's something in it for me

“if there's something in it for me”?
You can also ask ME

- I think I am a kind of nice person
- I will help you if I can
- I have legs, too (not great, though)
You can also ask ME

- I think I am a kind of nice person
- I will help you if I can
- I have legs, too (not great, though)
Question

• Will you help us Japanese developers?

- Yes
- No
I came to find

- There were many people to help us
- We were not required the perfectness
- Every experiences are real treasures ...
- Go out and find your story and treasures
it's not easy, but it's not impossible, either

painful sometimes, but not all time

yes, we are enjoying the whole process even in the difficulties

we can try because now we know it’s worth
Mainlining

✶ it’s not easy, but it’s not impossible, either
✶ painful sometimes, but not all time
✶ yes, we are enjoying the whole process even in the difficulties
✶ we can try because now we know it’s worth

It’s worth
What you need

• Read the documents, first (almost everything is already there)
• Start to live within the LKML and subscribe to LWN
• Attend community events and meetings (they will not kill you)
With a little from my friend
With a little from my friend

- http://elinux.org/TomoyoLinux
- http://tomoyo.sourceforge.jp/

Thank you (^_^)/~

see you @ols2008