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
    - http://tomoyo.sourceforge.jp/wiki-e/?TomoyoLive
- 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.”*
- Full statements with Japanese translation is found at http://lists.sourceforge.jp/mailman/archives/tomoyo-users/2006-April/000062.html

Dec. 8, 2006

- **Satoru Ueda** of CELF (Consumer Electronics Linux Forum) asked me to demonstrate TOMOYO Linux at their technical meeting.
  - http://tree.celinuxforum.org/CelfPubWiki/JapanTechnicalJamboree12
- 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

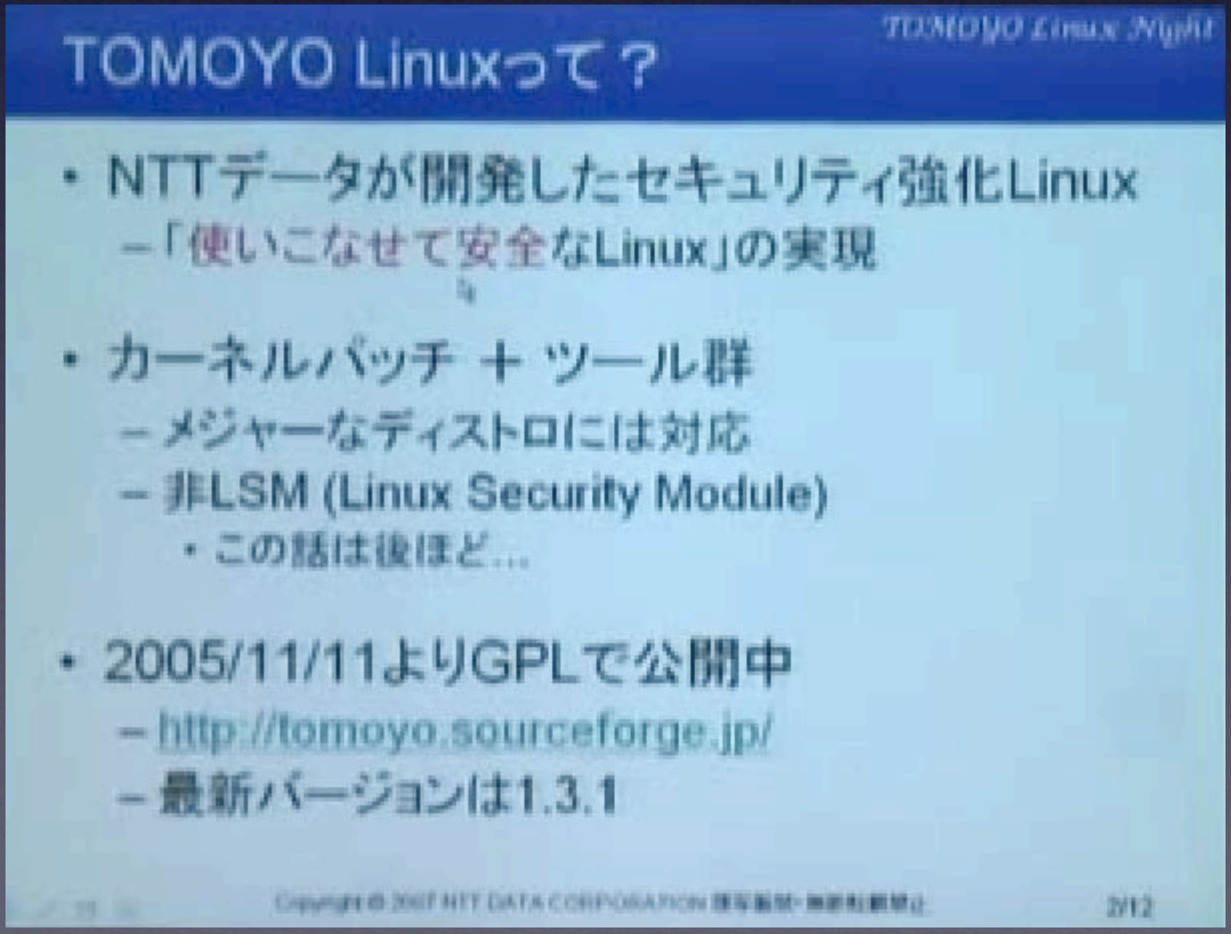
- **Hiro Yoshioka** of Miracle Linux gently asked me to introduce TOMOYO Linux to a pretty famous Japanese community, YLUG (Yokohama Linux Users Group)
- I accepted as usual not knowing what would happen ...

“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)



TOMOYO Linux Night

TOMOYO Linuxって？

- NTTデータが開発したセキュリティ強化Linux
  - 「使いこなせて安全なLinux」の実現
- カーネルパッチ ＋ ツール群
  - メジャーなディストロには対応
  - 非LSM (Linux Security Module)
    - この話は後ほど…
- 2005/11/11よりGPLで公開中
  - http://tomoyo.sourceforge.jp/
  - 最新バージョンは1.3.1

Copyright © 2007 NTT DATA CORPORATION 複写複製・無断転載禁止 2/12

March 2007

- 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

Apr. 18, 2007

ELC2007!

- We had
  - 2 sessions (presentation and tutorial)
- Not many people came to our session as expected, but ...

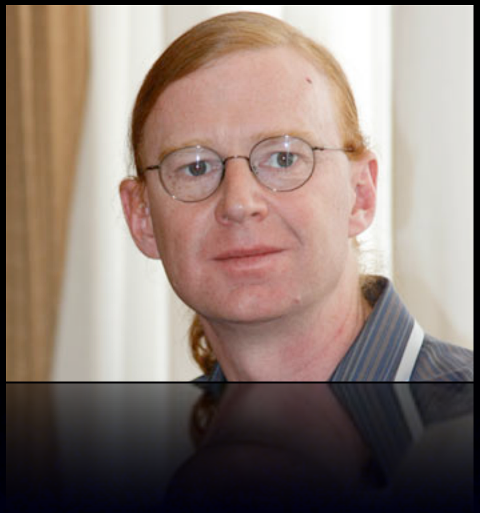
There he was!

(**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.
- http://tomoyo.sourceforge.jp/wiki-e/?WhatIs#mainlining
  - 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!

>linuxsymposium

TOMOYO Linux

http://tomoyo.sourceforge.jp/wiki-e/

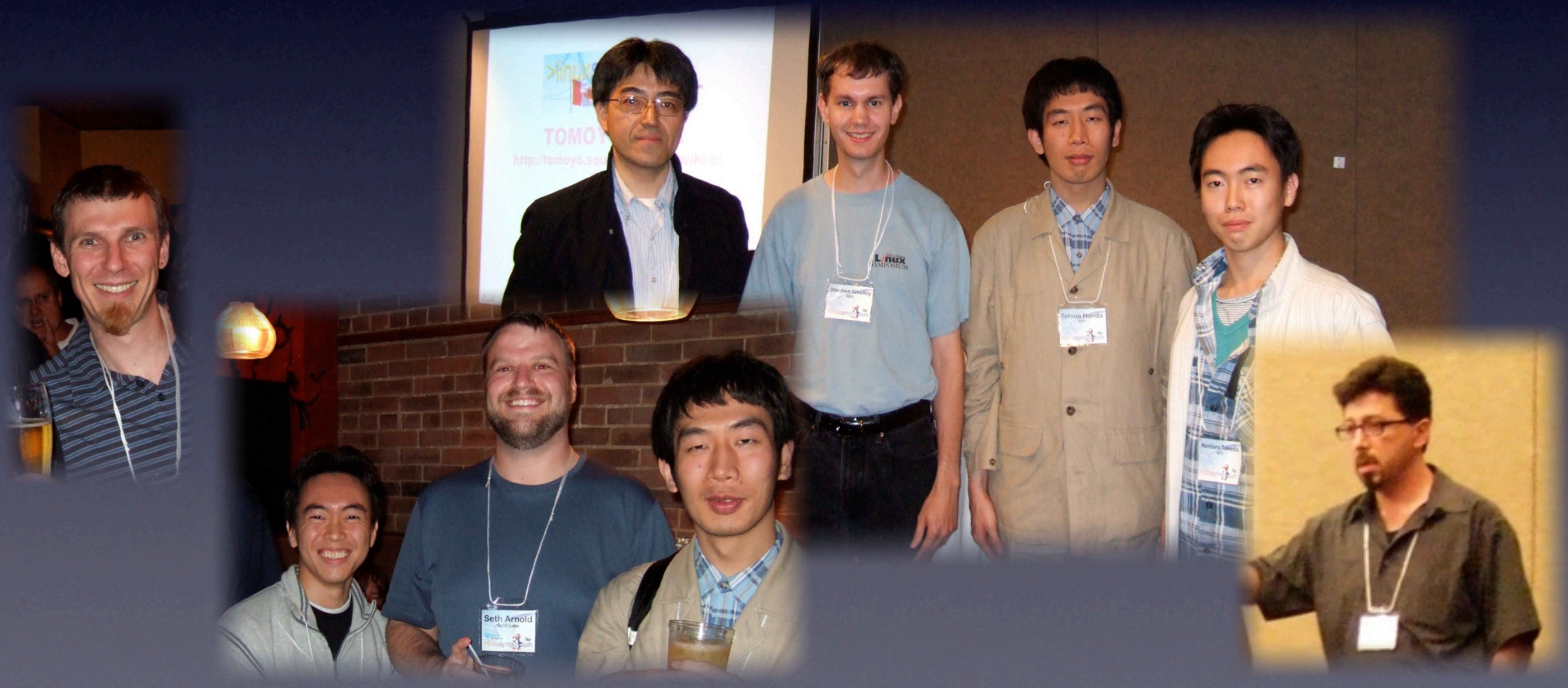
BoF

June 29, 2007

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

(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 ...

Question

- 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
  - http://tomoyo.sourceforge.jp/wiki-e/?OLS2007-BOF

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

Oct. 2, 2007

- 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

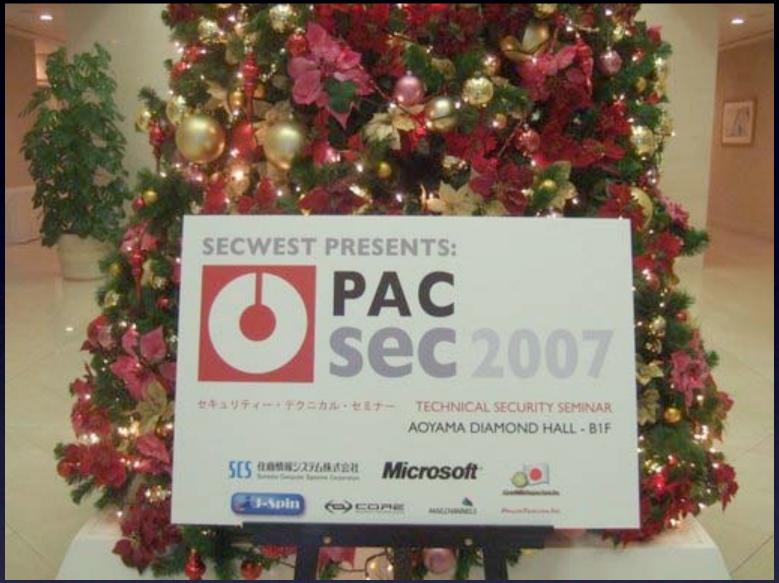
- Positive feedbacks are always Good!
- Negative feedbacks and NACK are “Not BAD”
- No feedbacks is BAD

Question

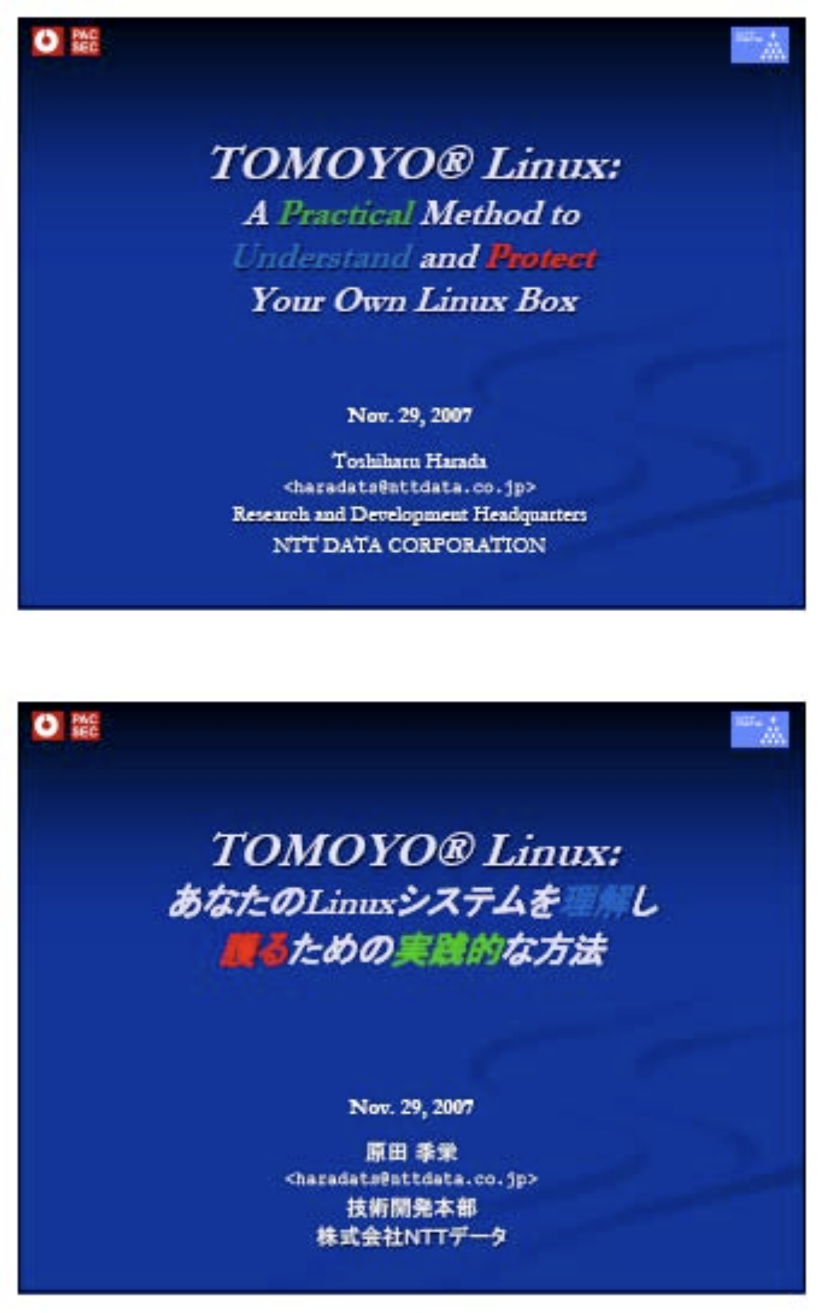
- How can this (*no* feedbacks) happen?
- What should we do when there is no feedbacks?

Nov. 29, 2007

PacSec2007


SECWEST PRESENTS:
PAC sec 2007
セキュリティー・テクニカル・セミナー
TECHNICAL SECURITY SEMINAR
AOYAMA DIAMOND HALL - B1F
Microsoft

Dragos in Tokyo



TOMOYO® Linux:
A Practical Method to
Understand and Protect
Your Own Linux Box

Nov. 29, 2007

Toshiharu Harada
<haradats@nttdata.co.jp>
Research and Development Headquarters
NTT DATA CORPORATION

TOMOYO® Linux:
あなたのLinuxシステムを理解し
護るための実践的な方法

Nov. 29, 2007

原田 季栄
<haradats@nttdata.co.jp>
技術開発本部
株式会社NTTデータ

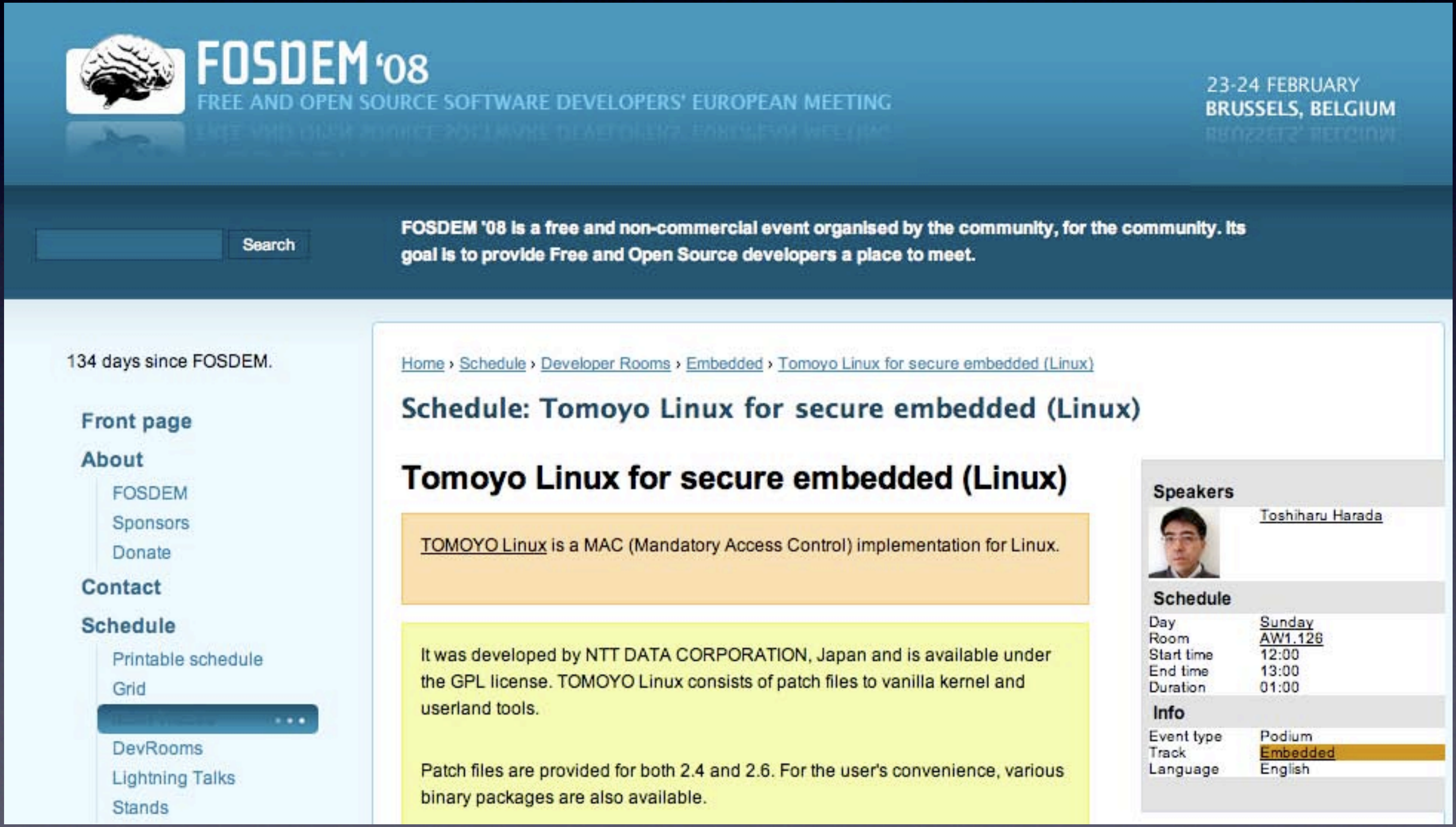
http://sourceforge.jp/projects/tomoyo/document/PacSec2007-handout.pdf

Dec. 25, 2007
Posted Security Goal

- **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



FOSDEM '08 is a free and non-commercial event organised by the community, for the community. Its goal is to provide Free and Open Source developers a place to meet.

134 days since FOSDEM.

Home › Schedule › Developer Rooms › Embedded › Tomoyo Linux for secure embedded (Linux)

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

Toshiharu Harada

Schedule

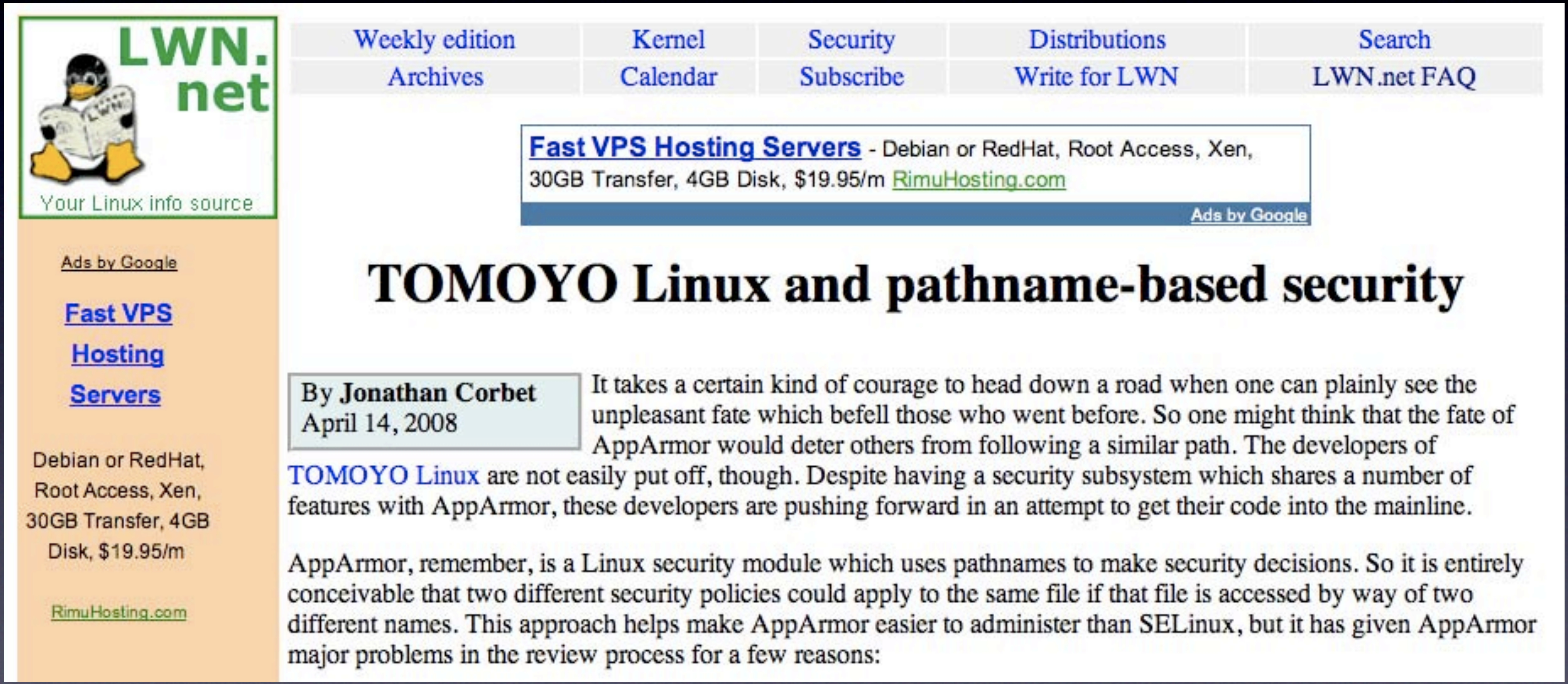
Day	Sunday
Room	AW1.126
Start time	12:00
End time	13:00
Duration	01:00

Info

Event type	Podium
Track	Embedded
Language	English

http://sourceforge.jp/projects/tomoyo/document/fosdem2008.pdf

Apr. 14, 2008
TOMOYO on LWN.net



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:

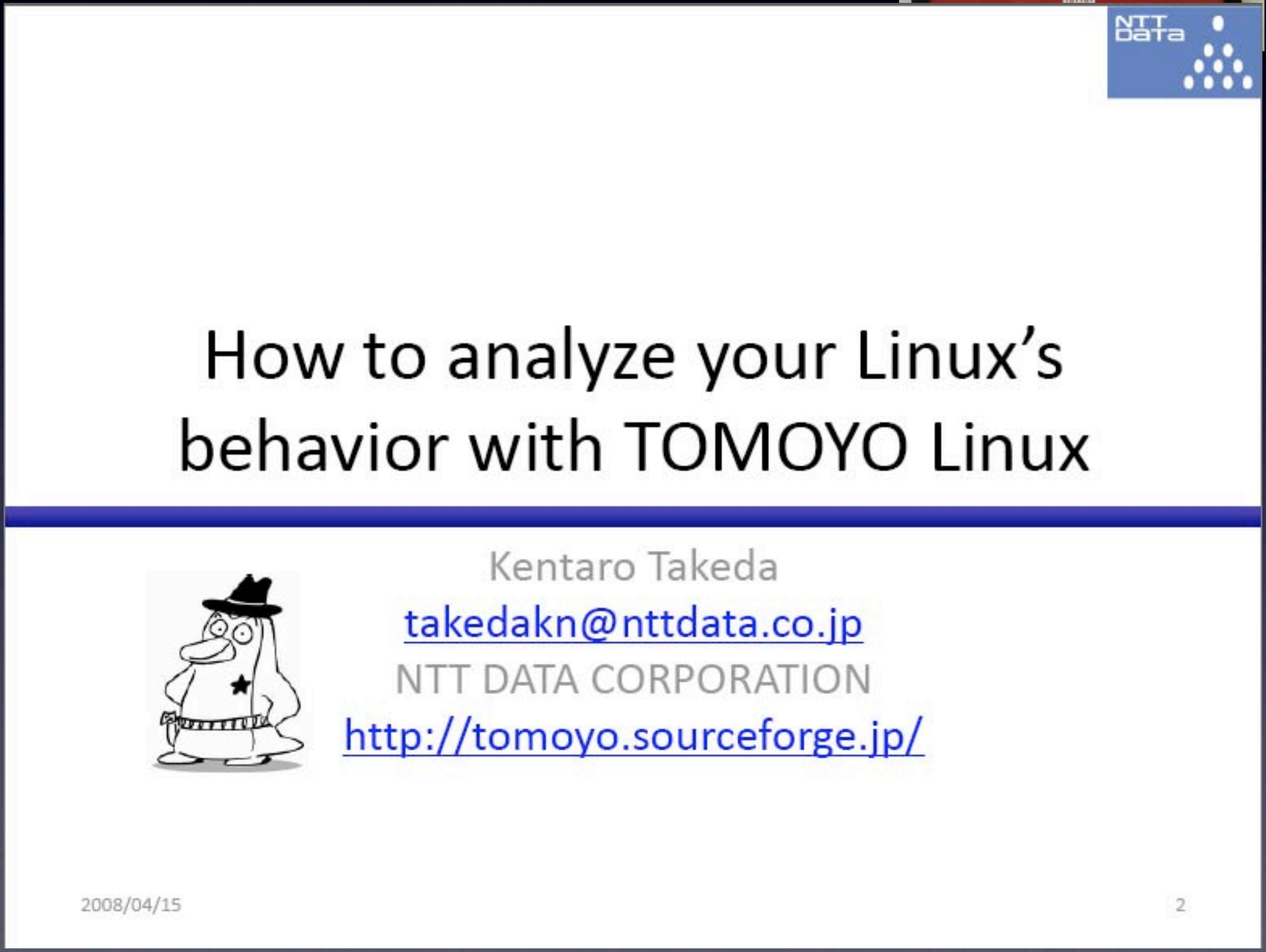
http://lwn.net/Articles/277833/

What a nice surprise to see my project on LWN.net!

Apr. 25, 2008

ELC2008

1997 FELLOW
Steve Wozniak
For his invention of the first single-board microprocessor-based microcomputer, the Apple I; co-founder Apple Computer.



How to analyze your Linux's behavior with TOMOYO Linux

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

2008/04/15

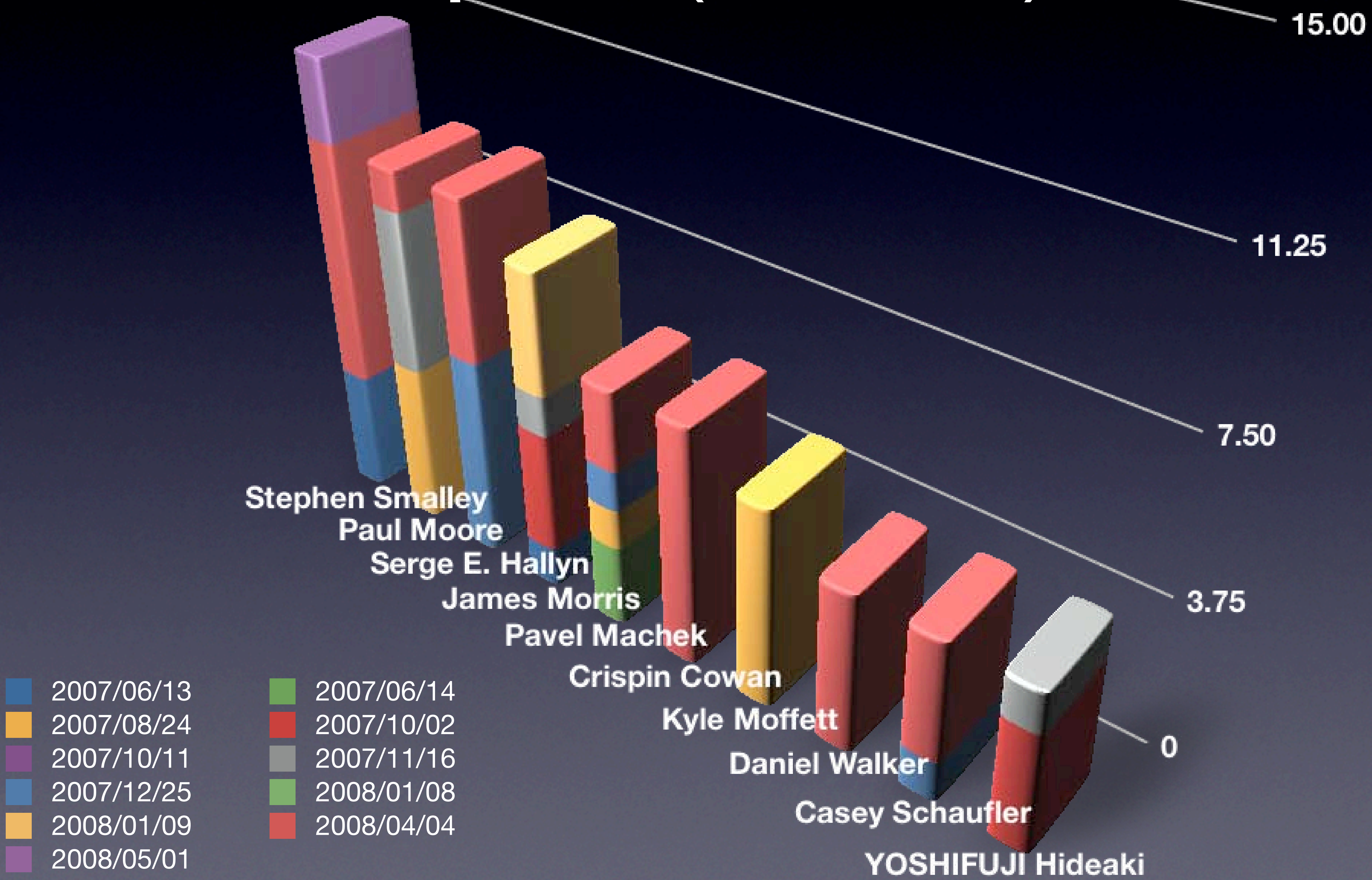
2

http://sourceforge.jp/projects/tomoyo/document/elc2008.pdf

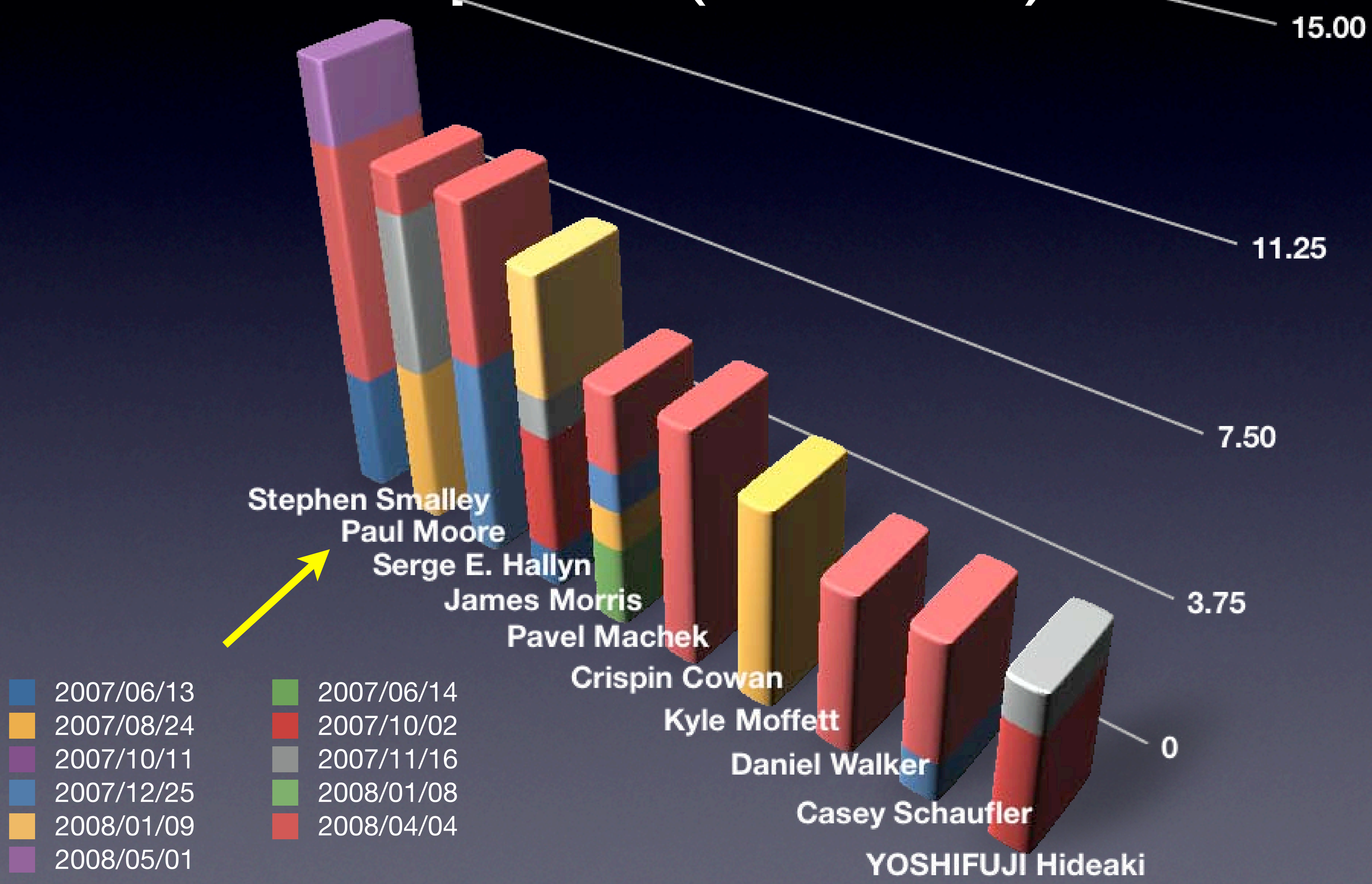
TOMOYO threads posters top 10 (thanks!)

- 🟦 2007/06/13
- 🟧 2007/08/24
- 🟪 2007/10/11
- 🟦 2007/12/25
- 🟧 2008/01/09
- 🟪 2008/05/01
- 🟩 2007/06/14
- 🟥 2007/10/02
- ◼ 2007/11/16
- 🟩 2008/01/08
- 🟥 2008/04/04

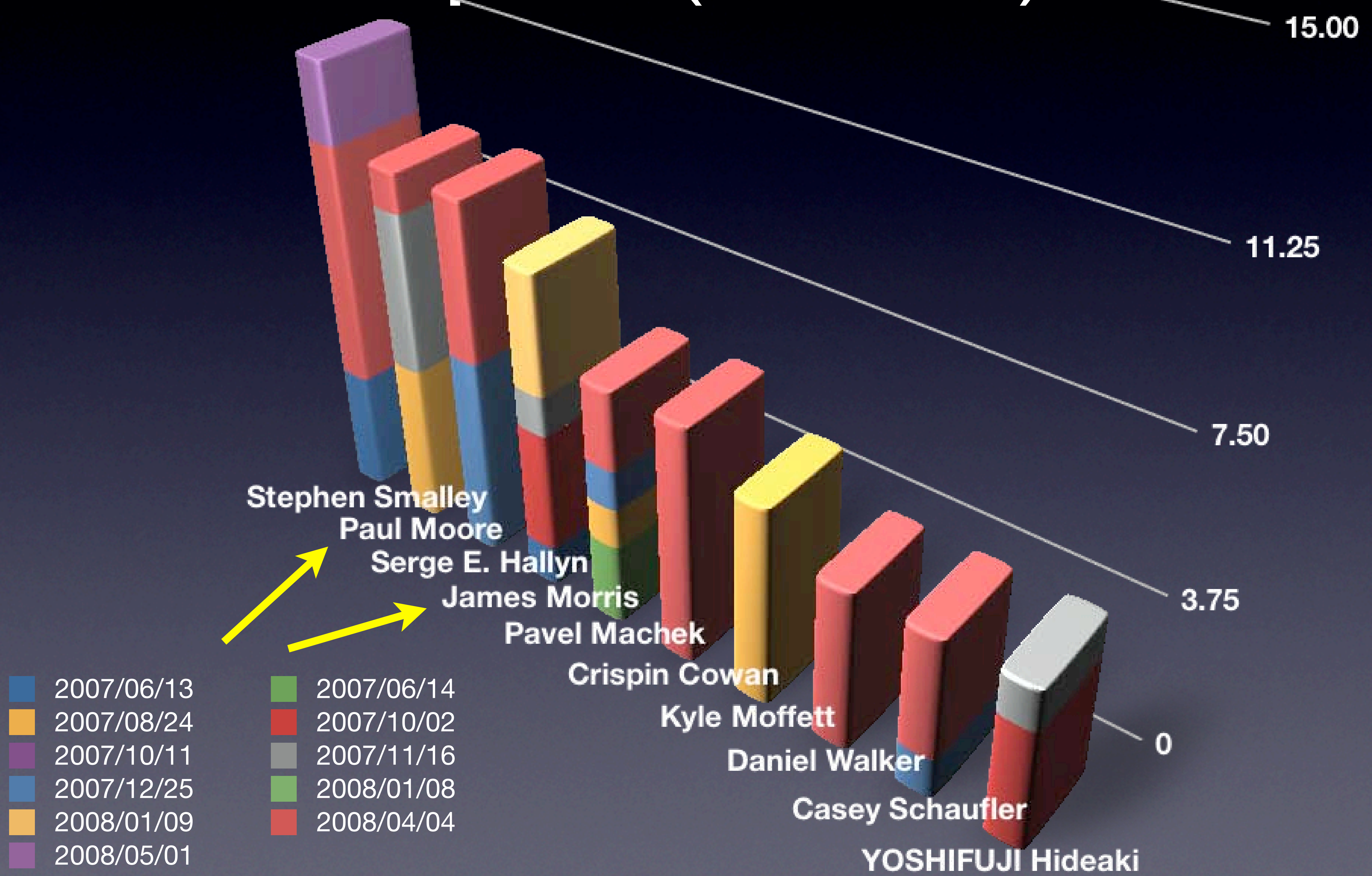
TOMOYO threads posters top 10 (thanks!)



TOMOYO threads posters top 10 (thanks!)



TOMOYO threads posters top 10 (thanks!)

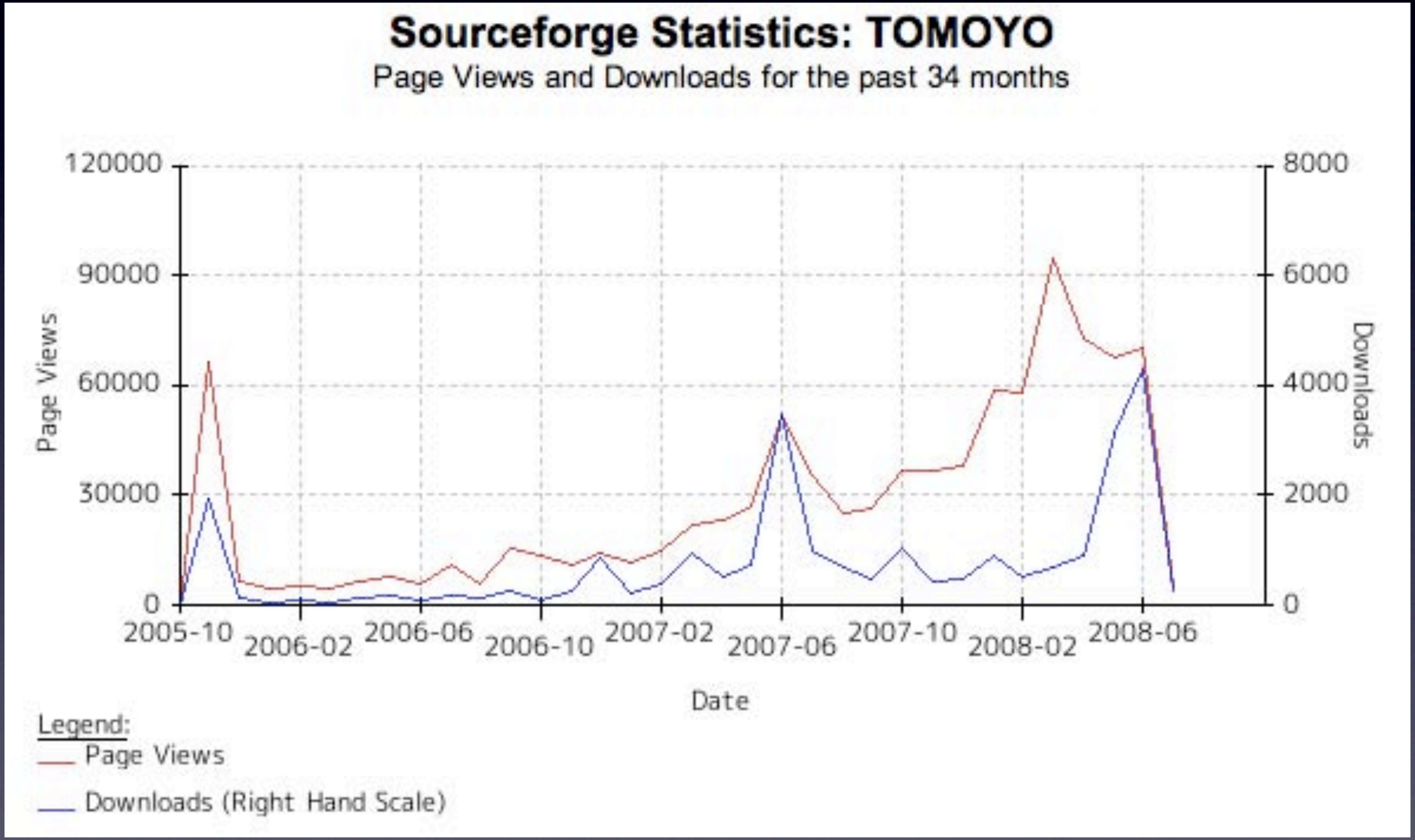


Paul, James and ...

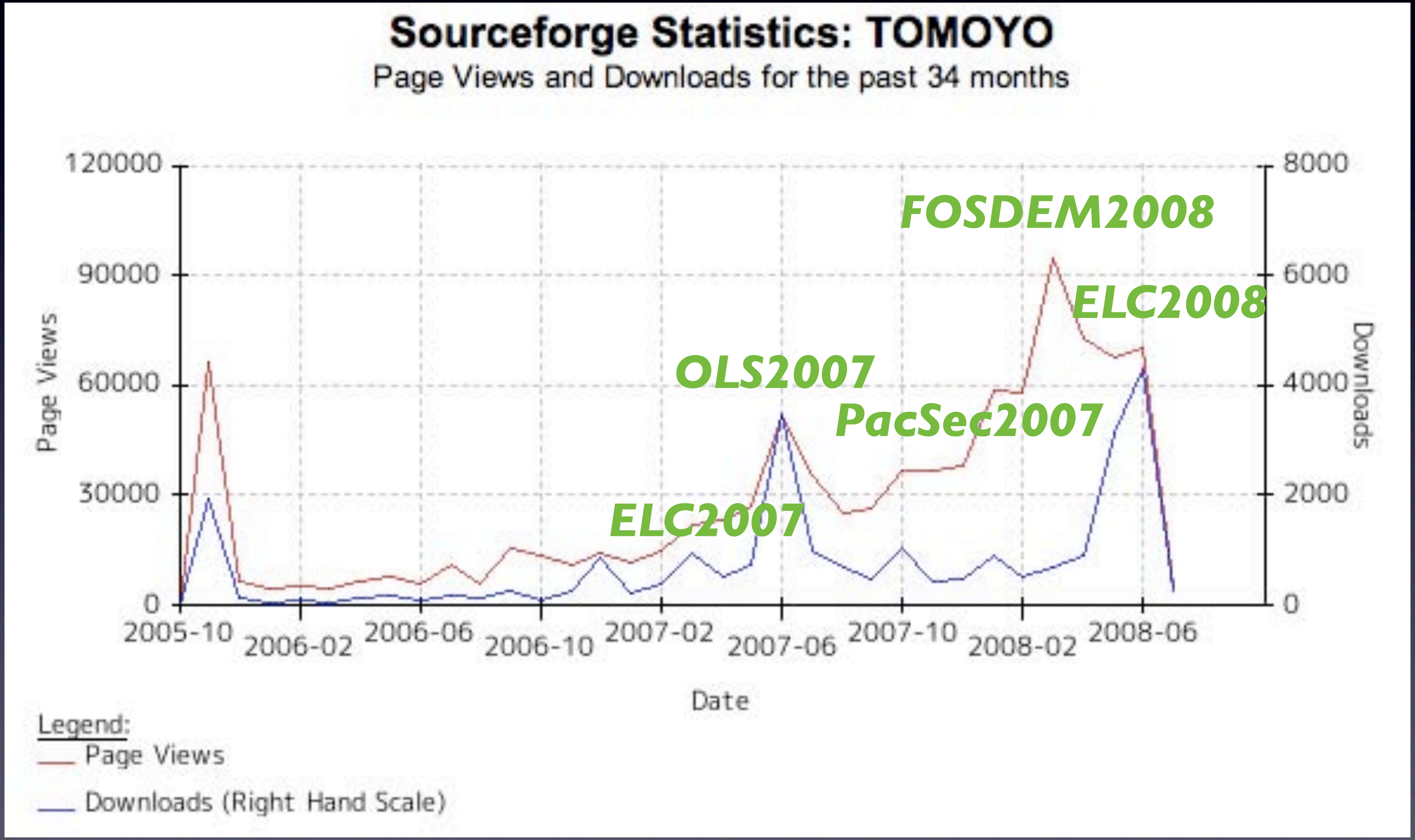
- Are we missing someone? ... NO

- 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

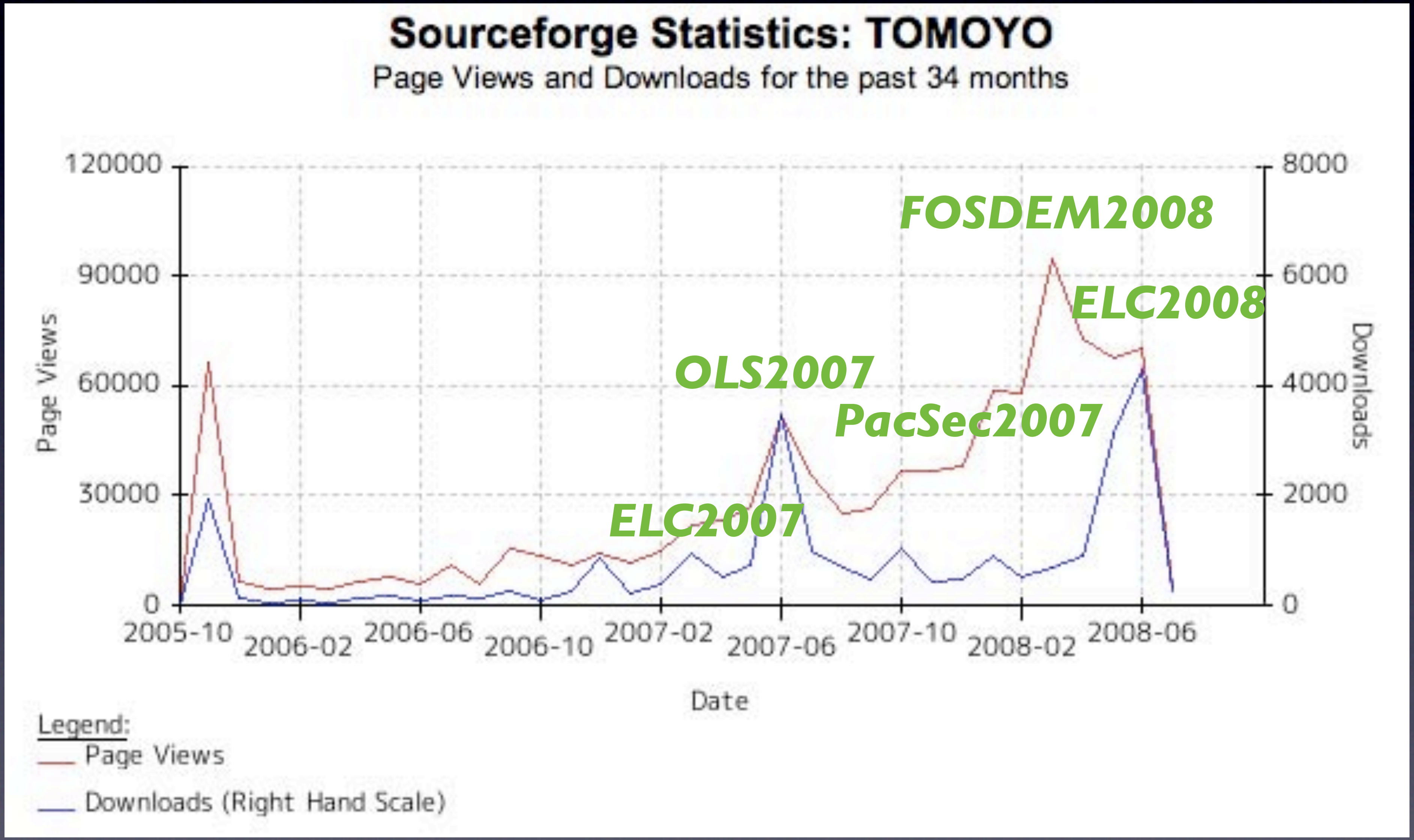

Sourceforge Statistics: TOMOYO
Page Views and Downloads for the past 34 months
120000
90000
60000
30000
0
Page Views
8000
6000
4000
2000
0
Downloads
2005-10
2006-02
2006-06
2006-10
2007-02
2007-06
2007-10
2008-02
2008-06
Date
Legend:
Page Views
Downloads (Right Hand Scale)

Statistics


Sourceforge Statistics: TOMOYO
Page Views and Downloads for the past 34 months
Page Views
120000
90000
60000
30000
0
Downloads
8000
6000
4000
2000
0
2005-10
2006-02
2006-06
2006-10
2007-02
2007-06
2007-10
2008-02
2008-06
Date
Legend:
Page Views
Downloads (Right Hand Scale)
FOSDEM2008
ELC2008
OLS2007
PacSec2007
ELC2007

OLS2008?

Statistics



Jul. 9, 2008 (today)

Current Status

- 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”

```
          ＿＿＿_
        ／      ＼
      ／  ─    ─ ＼
    ／   （●）  （●） ＼
    |      （__人__）   |   ひむ？
    /       ∩ノ ⊃     ／
    (  ＼  ／ ＿ノ   |  |
    .＼  “    ／__|   |
       ＼ ／＿＿＿ ／
```

Question

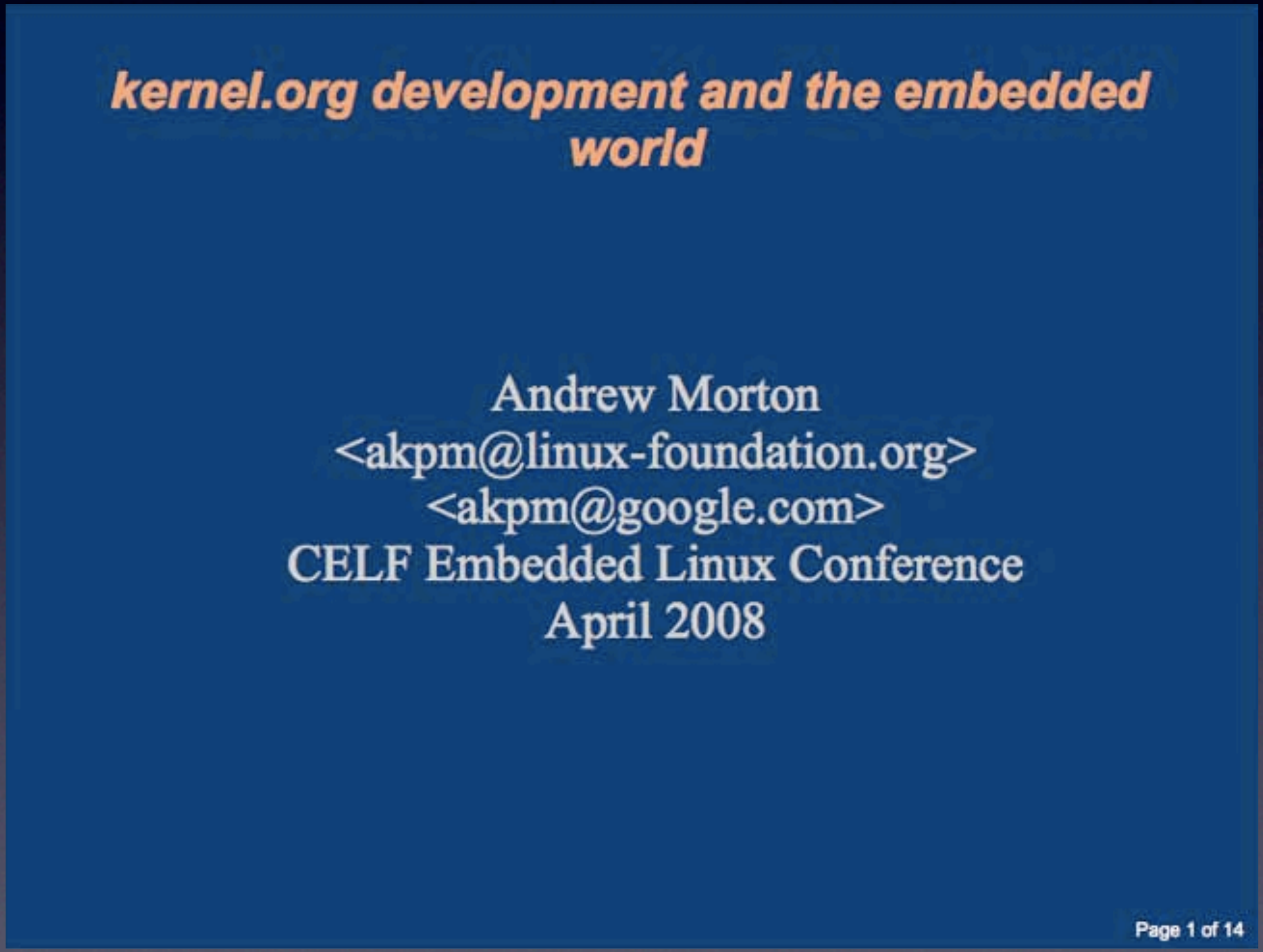
- Who is “HE”?

✖ **don’t know**

◎ **“Me”**

HIM

(page 13 of 14)



kernel.org development and the embedded world

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

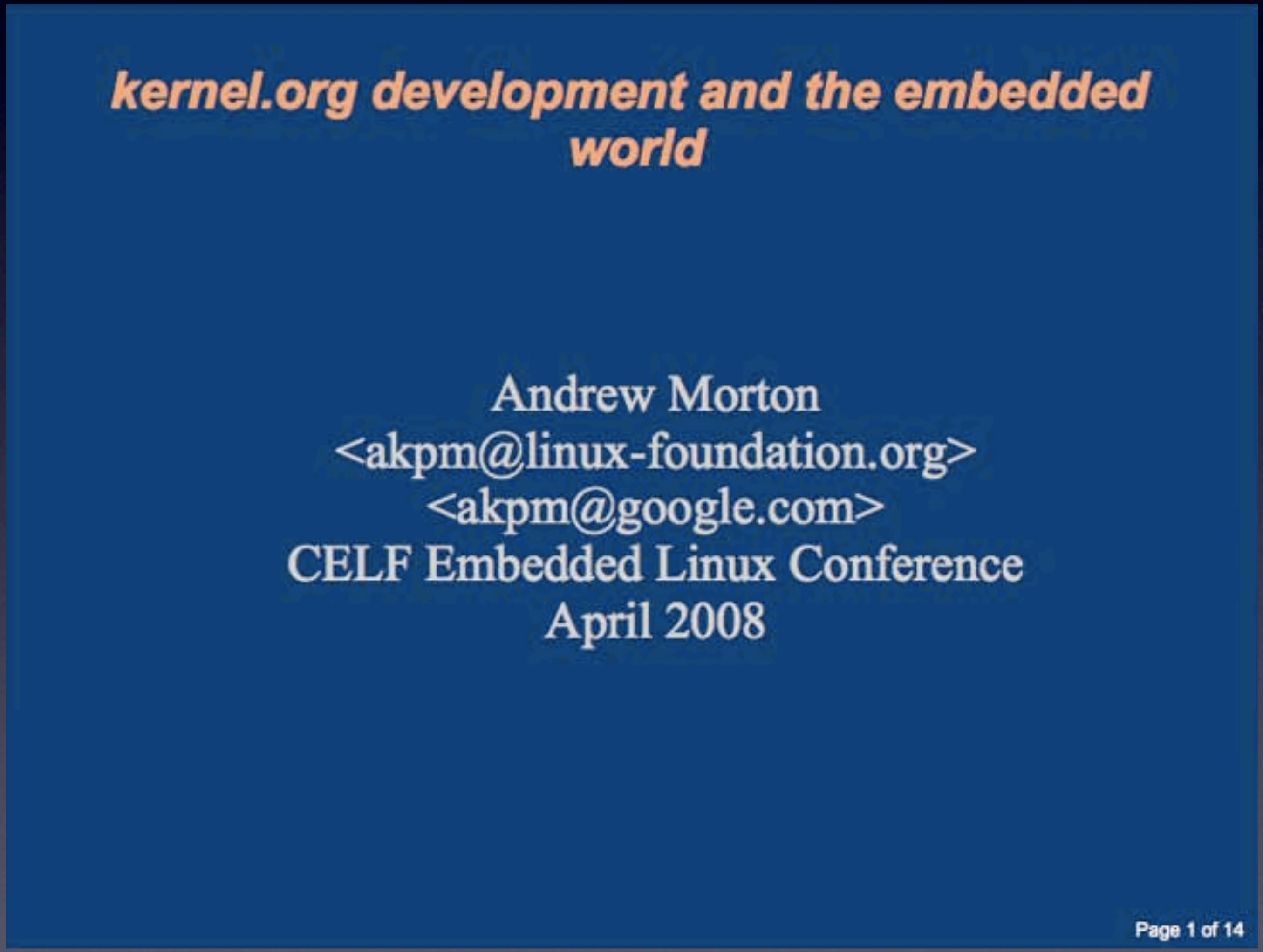
Page 1 of 14

http://www.celinux.org/elc08_presentations/morton-elc-08.ppt

please read and find HIM

HIM

(page 13 of 14)

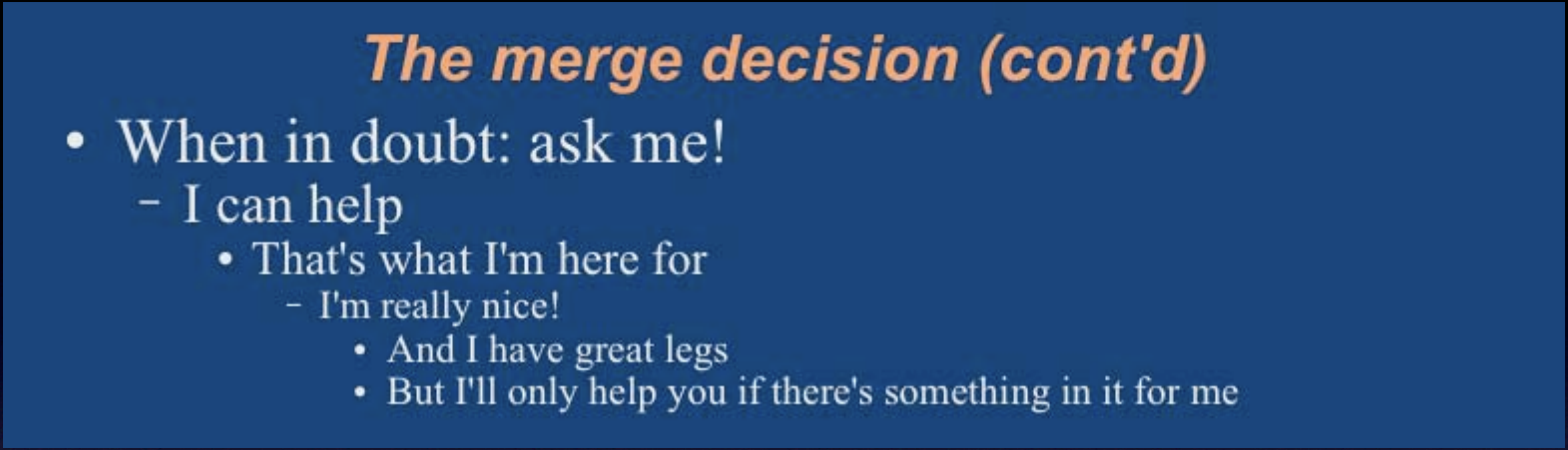


kernel.org development and the embedded world

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

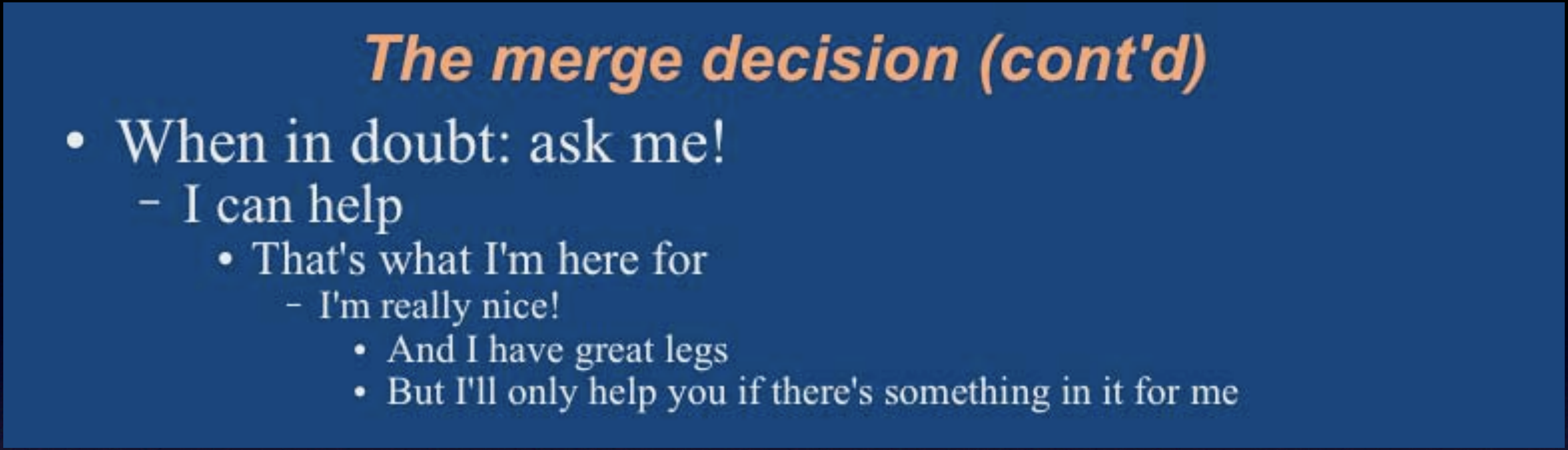
Page 1 of 14

http://www.celinux.org/elc08_presentations/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

```
　　　　 ＿＿＿_
　　 ／　　　　　＼
　／　　─　　　 ─ ＼
／　　 （●）　 （●） ＼
|　　　　　 （__人__）　 |   “if there’s something in it for me”?
/　　　　　∩ノ ⊃　　 ／
(　 ＼ ／ ＿ノ　|　 |
.＼ “　 ／＿＿|　 |
　　＼ ／＿＿＿ ／
```

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)

ImpressIT「チョコレートの国の侍」

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)

```
          ＿＿＿＿_
        ／        ＼
      ／  ─     ─  ＼
    ／    (●)   (●)  ＼
    |       （__人__）  |  みー？
    /       ∩ノ ⊃     ／
    (  ＼  ／ ＿ノ  |  |
    .＼  “   ／__|   |
       ＼ ／＿＿＿ ／
```

ImpressIT「チョコレートの国の侍」

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

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

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 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/
- http://sourceforge.jp/projects/tomoyo/

Thank you (^_^)/~

see you @ols2008