Linux Kernel Development, how it all works

Greg Kroah-Hartman

gregkh@linuxfoundation.org
git.sr.ht/~gregkh/kernel-development

All of this is just my personal opinion, based on being a Linux kernel developer since 1999 and part of the Linux kernel security team since it was created in 2005.

Nothing in here reflects the opinion of the Linux Foundation or any other Linux kernel developer.

But hopefully I can convince them to agree with me.

Linux size – overall

81,500 files

36,780,000 lines

Kernel release 6.5.0

Linux size – what you use

5%-10%

Kernel release 6.5.0

~9 changes per hour

Kernel release 6.5.0

New* release model

- Release every 2-3 months
- All releases are stable

* As of January, 2004

“Cambridge promise”

- We will not break userspace

– July 2007

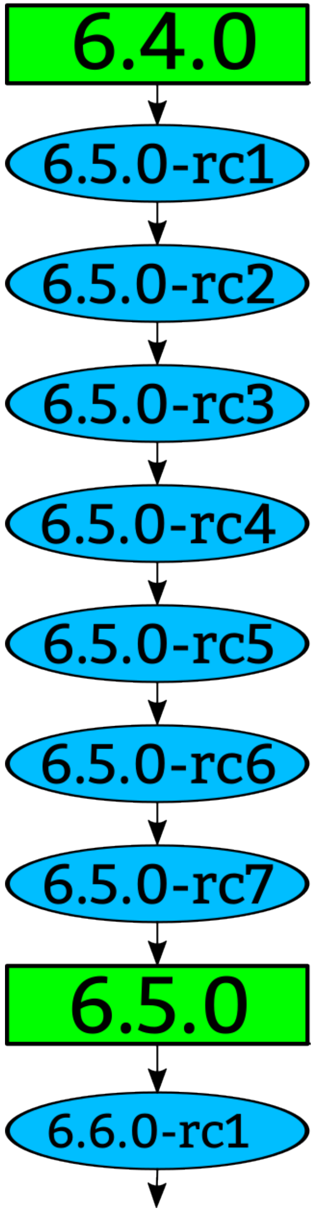
“Cambridge promise”

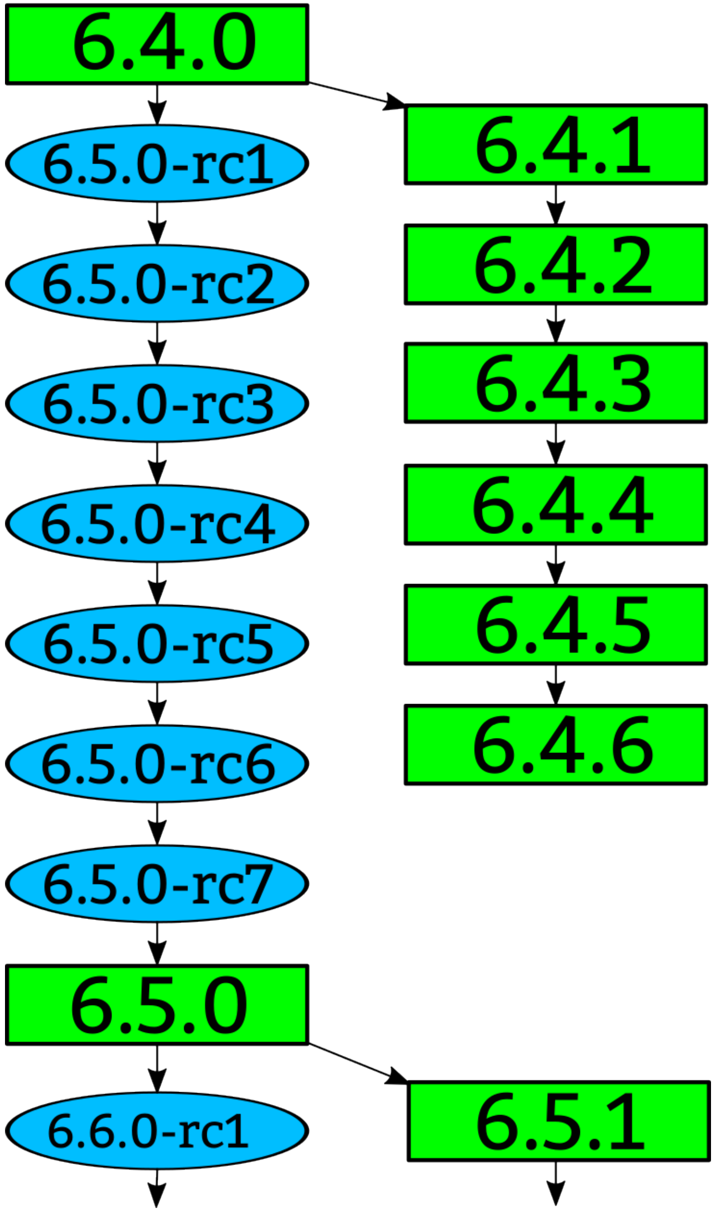
- We will not break userspace on purpose

– July 2007

Version numbers mean nothing

2.6.x → 3.x	2011
3.x → 4.x	2015
4.x → 5.x	2019
5.x → 6.x	2022


6.4.0
6.5.0-rc1
6.5.0-rc2
6.5.0-rc3
6.5.0-rc4
6.5.0-rc5
6.5.0-rc6
6.5.0-rc7
6.5.0
6.6.0-rc1


6.4.0
6.5.0-rc1
6.5.0-rc2
6.5.0-rc3
6.5.0-rc4
6.5.0-rc5
6.5.0-rc6
6.5.0-rc7
6.5.0
6.6.0-rc1
6.4.1
6.4.2
6.4.3
6.4.4
6.4.5
6.4.6
6.5.1

Stable kernel rules

- Bugfix
- Less than 100 lines
- New ids or quirks
- Must be in Linus’s tree

`https://www.kernel.org/doc/html/latest/process/stable-kernel-rules.html`

Longterm kernels

- One picked per year
- Maintained for at least 2 years*

4.14 4.19 5.4 5.10 5.15 6.1

* sometimes longer

Longterm kernels

4.14	13 changes / day
4.19	15 changes / day
5.4	18 changes / day
5.10	23 changes / day
5.15	27 changes / day
6.1	36 changes / day

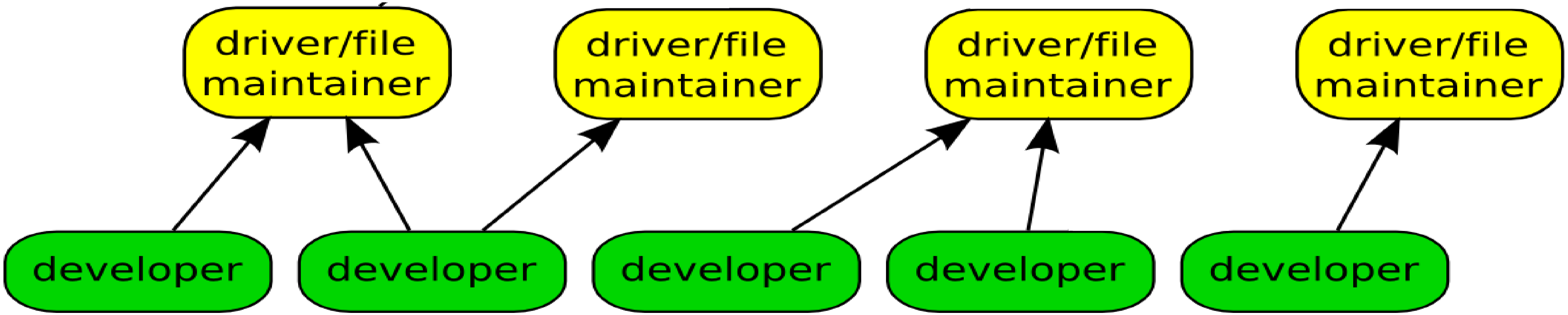
Kernel releases

- Every release is stable
- 12+ year old guarantee to not break things
- No fear to ever upgrade

More release information in greater detail:

http://www.kroah.com/log/blog/2018/02/05/linux-kernel-release-model/

developer developer developer developer developer



driver/file maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
developer
developer
developer
developer
developer

```
commit ecf85e481a716cfe07406439fdc7ba9526bbfaeb
Author:     Robert Jarzmik <robert.jarzmik@free.fr>
AuthorDate: Tue Apr 21 20:33:10 2009 -0700
Commit:     Greg Kroah-Hartman <gregkh@suse.de>
CommitDate: Thu Apr 23 14:15:31 2009 -0700

    USB: otg: Fix bug on remove path without transceiver

    In the case where a gadget driver is removed while no
    transceiver was found at probe time, a bug in
    otg_put_transceiver() will trigger.

    Signed-off-by: Robert Jarzmik <robert.jarzmik@free.fr>
    Acked-by: David Brownell <dbrownell@users.sourceforge.net>
    Signed-off-by: Greg Kroah-Hartman <gregkh@suse.de>

--- a/drivers/usb/otg/otg.c
+++ b/drivers/usb/otg/otg.c
@@ -43,7 +43,8 @@ EXPORT_SYMBOL(otg_get_transceiver);
 void otg_put_transceiver(struct otg_transceiver *x)
 {
-       put_device(x->dev);
+       if (x)
+               put_device(x->dev);
 }
```

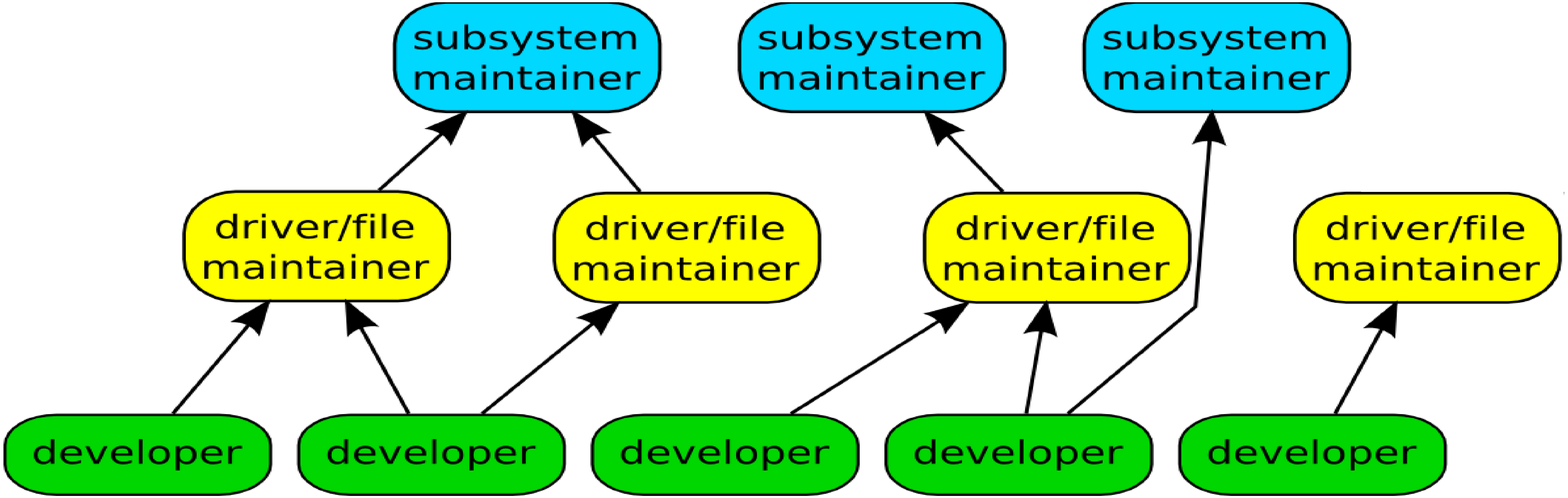
Developer’s Certificate of Origin

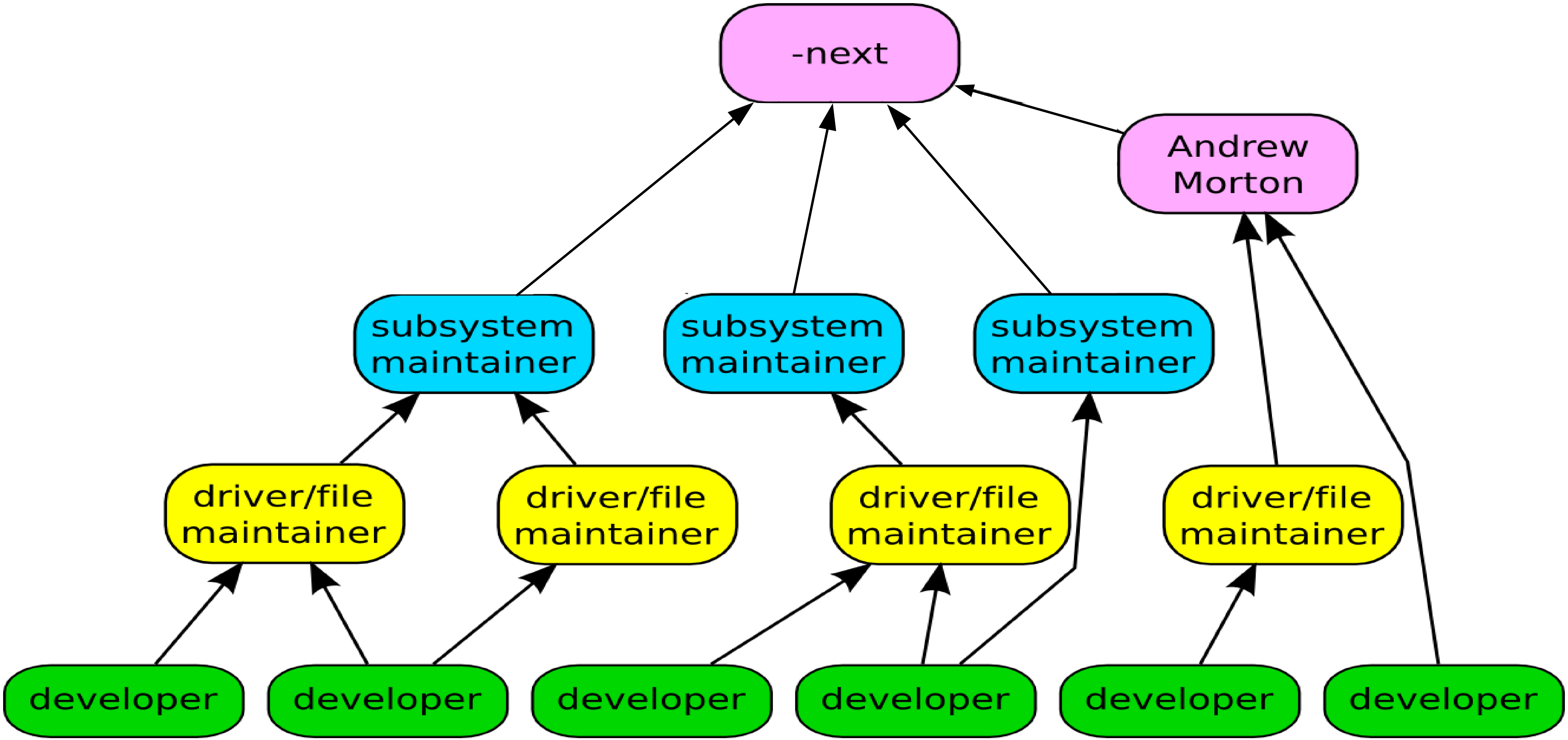
(a) I created this change; or

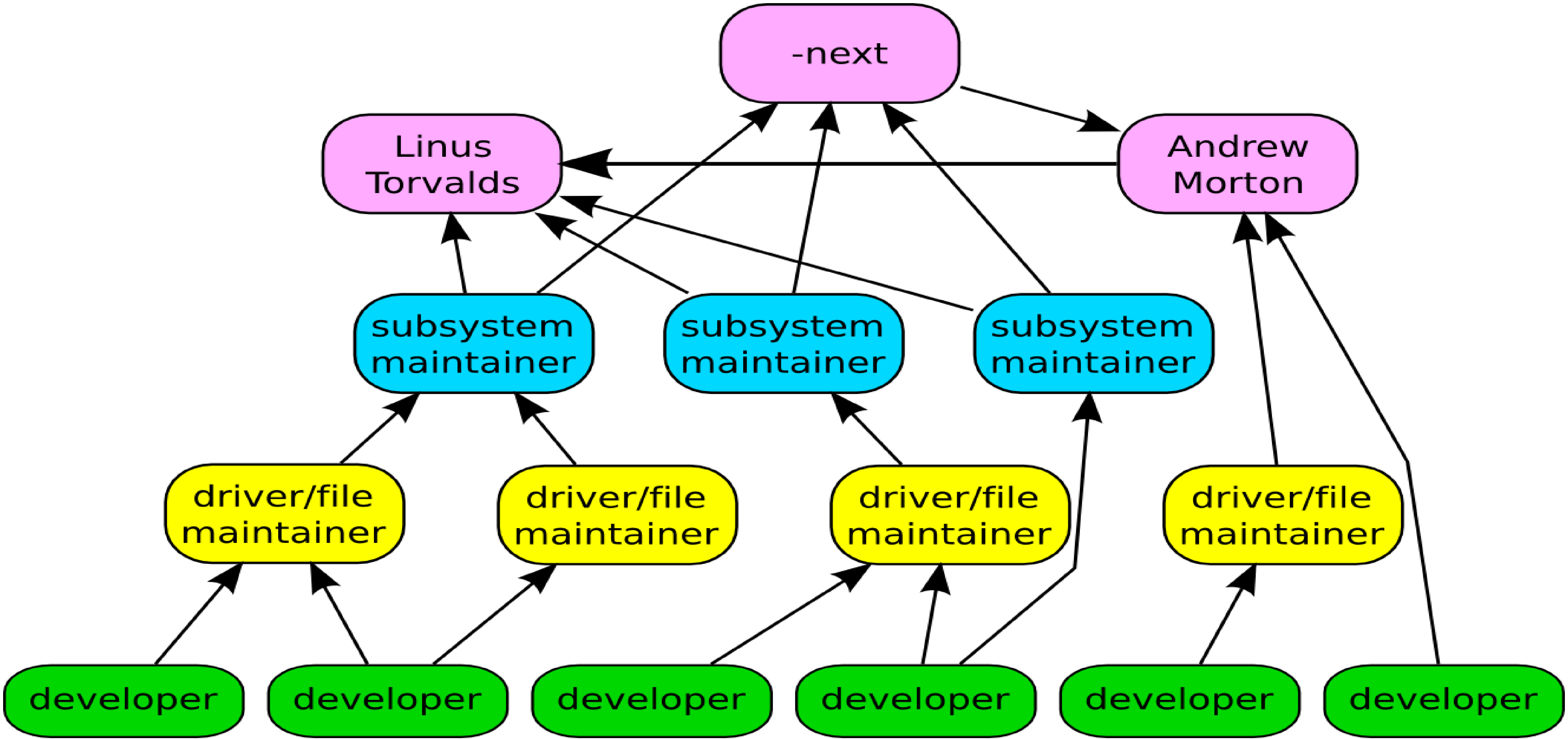
(b) Based this on a previous work with a compatible license; or

(c) Provided to me by (a), (b), or (c) and not modified

(d) This contribution is public.


subsystem maintainer
subsystem maintainer
subsystem maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
developer
developer
developer
developer
developer


-next
Andrew Morton
subsystem maintainer
subsystem maintainer
subsystem maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
developer
developer
developer
developer
developer
developer


-next
Linus Torvalds
Andrew Morton
subsystem maintainer
subsystem maintainer
subsystem maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
driver/file maintainer
developer
developer
developer
developer
developer
developer
developer

The world has changed

- 80%+ of the world's servers runs non-commercial distribution kernels*
- inter-company interactions achieve nothing
- The "community" does not sign NDAs

* Embedded it is like 99%, look at what is in your pocket or in your home

Kernel security team

Kernel security team

Reactive security, not proactive

Kernel security team

Other groups do proactive security

From: Steve Bergman <steve@rueb.com>
To: linux-kernel@vger.kernel.org
Subject: Proper procedure for reporting possible security vulnerabilities?
Date: Mon, 10 Jan 2005 10:46:57 -0600

There seems to be some confusion in certain quarters as to the proper procedure for reporting possible kernel security issues. REPORTING-BUGS says send bug reports to the maintainer of that area of the kernel. However, what about areas for which a maintainer is not listed? (e.g. VM) It seems that some take that to mean send it directly to Linus and if you don't hear something back quickly, release an exploit to the wild.

So what is the preferred procedure and is it documented somewhere? Should it be made more prominent?

Thanks for any information,
Steve Bergman

https://lore.kernel.org/lkml/41E2B181.3060009@rueb.com/

```
From: Chris Wright <chrisw@osdl.org>
To: torvalds@osdl.org
Cc: akpm@osdl.org, alan@lxorguk.ukuu.org.uk,
   marcelo.tosatti@cyclades.com, linux-kernel@vger.kernel.org
Subject: [PATCH] Security contact info
Date: Wed, 9 Mar 2005 01:05:50 -0800

Add security contact info and relevant documentation.

Signed-off-by: Chris Wright <chrisw@osdl.org>

 MAINTAINERS                |    5 +++++
 REPORTING-BUGS             |    4 ++++
 Documentation/SecurityBugs |   38 ++++++++++++++++++++++++++++++++++++++
 3 files changed, 47 insertions(+)
```

https://lore.kernel.org/all/20050309090550.GW28536@shell0.pdx.osdl.net/

```
From: Chris Wright <chrisw@osdl.org>
To: torvalds@osdl.org
Cc: akpm@osdl.org, alan@lxorguk.ukuu.org.uk,
   marcelo.tosatti@cyclades.com, linux-kernel@vger.kernel.org
Subject: [PATCH] Security contact info
Date: Wed, 9 Mar 2005 01:05:50 -0800

Add security contact info and relevant documentation.

Signed-off-by: Chris Wright <chrisw@osdl.org>

...


+3) Non-disclosure agreements
+
+The Linux kernel security team is not a formal body and therefore unable
+to enter any non-disclosure agreements.
```

https://lore.kernel.org/all/20050309090550.GW28536@shell0.pdx.osdl.net/

Kernel security team

- security@kernel.org
- Small group of kernel developers
- Do not represent any companies

Kernel security team

- Triage reports
- Drag in responsible developers
- Work to create a fix as soon as possible
- Get it merged into Linus’s and stable trees

Kernel security team

- If you are brought in enough times, you are added to the alias to reduce the round-trip.

Kernel security team

- Fix the issue as soon as possible
- No embargoes longer than 7 days
- Do not do any kind of announcements

Linus in 2008

```
On Wed, 16 Jul 2008, pageexec@freemail.hu wrote:
>
> you should check out the last few -stable releases then and see how
> the announcement doesn't ever mention the word ’security’ while fixing
> security bugs

Umm. What part of ”they are just normal bugs” did you have issues with?
I expressly told you that security bugs should not be marked as such,
because bugs are bugs.

> in other words, it’s all the more reason to have the commit say it’s
> fixing a security issue.

No.
```

```
> > I'm just saying that why mark things, when the marking have no meaning?
> > People who believe in them are just _wrong_.
>
> what is wrong in particular?

You have two cases:

- people think the marking is somehow trustworthy.

  People are WRONG, and are misled by the partial markings, thinking that
  unmarked bugfixes are "less important". They aren't.

- People don't think it matters

  People are right, and the marking is pointless.
  In either case it's just stupid to mark them. I don't want to do it,
  because I don't want to perpetuate the myth of "security fixes" as a
  separate thing from "plain regular bug fixes".

  They're all fixes. They're all important. As are new features, for that
  matter.
```

```
> when you know that you're about to commit a patch that fixes a security
> bug, why is it wrong to say so in the commit?

It's pointless and wrong because it makes people think that other bugs
aren't potential security fixes.

What was unclear about that?

Linus
```

Above email:

https://lore.kernel.org/lkml/alpine.LFD.1.10.0807151620450.2867@woody.linux-foundation.org/

Whole thread:

https://lore.kernel.org/lkml/20080703035807.GA8190@kroah.com/

Reporting Security bugs:

https://www.kernel.org/doc/html/latest/admin-guide/security-bugs.html

Kernel security policy

- Almost all bugs can be a “security” issue

Kernel security policy

- A fix for a known bug is better than the potential of a fix causing a future problem as future problems, when found, will be fixed then.

Kernel security policy

- We do NOT know your use case!

Kernel security policy

- We do NOT know your use case!
- We do NOT know what code you use!

Kernel security policy

- We do NOT know your use case!
- We do NOT know what code you use!
- We do NOT want to know any of this!

“It's hard to capture the fact that a bug can be super serious in one type of deployment, somewhat important in another, or no big deal at all -- and that the bug can be all of this at the same time. Vulnerability remediation is hard.”

– Ben Hawkes

https://blog.isosceles.com/what-is-a-good-linux-kernel-bug/

Kernel security policy

- Fix known bugs as soon as possible
- Get releases out to users quickly
- Does not work for hardware bugs*

* Hardware vendors think they are special,
They are not, they are just slow…

Hardware security issues

- Handled separately
- Encrypted restricted email list
- No NDAs
- Cross company / OS coordination
- Embargoes are tolerated*

* for now...

Hardware security issues

- How this works:

  `https://www.kernel.org/doc/html/latest/process/embargoed-hardware-issues.html`

Kernel security team

- Does not do any kind of announcements
- Can not assign CVEs*
- No early announcement list

* This is on purpose

No pre-disclosure at all!

- All “early notice” lists are leaks and should be considered public.

No pre-disclosure at all!

- All “early notice” lists are leaks and should be considered public.
- Unless your project is not used by anyone.

No pre-disclosure at all!

- All “early notice” lists are leaks and should be considered public.
- Unless your project is not used by anyone.
- Otherwise, why would your government allow it to exist?

Security fixes

- Happen at least once a week
- Look like any other bugfix
- Many not known to be security related until years later
- No differentiation between bug types
- No CVEs for anything

CVEs mean nothing for Linux

https://kernel-recipes.org/en/2019/talks/cves-are-dead-long-live-the-cve/

> “If you are not using the latest stable / longterm kernel, your system is insecure”
>
> – me

Linux Kernel Development, how it all works

Greg Kroah-Hartman

gregkh@linuxfoundation.org
git.sr.ht/~gregkh/kernel-development

Bonus Slides!

Reporting security issues

```
On Wed, 16 Jul 2008, pageexec@freemail.hu wrote:
>
> we went through this and you yourself said that security bugs are *not*
> treated as normal bugs because you do omit relevant information from such
> commits

Actually, we disagree on one fundamental thing. We disagree on
that single word: "relevant".

I do not think it's helpful _or_ relevant to explicitly point out how to
tigger a bug. It's very helpful and relevant when we're trying to chase
the bug down, but once it is fixed, it becomes irrelevant.

You think that explicitly pointing something out as a security issue is
really important, so you think it's always "relevant". And I take mostly
the opposite view. I think pointing it out is actually likely to be
counter-productive.
```

Reporting security issues

For example, the way I prefer to work is to have people send me and the kernel list a patch for a fix, and then in the very next email send (in private) an example exploit of the problem to the security mailing list (and that one goes to the private security list just because we don't want all the people at universities rushing in to test it). THAT is how things should work.

Should I document the exploit in the commit message? Hell no. It's private for a reason, even if it's real information. It was real information for the developers to explain why a patch is needed, but once explained, it shouldn't be spread around unnecessarily.

Linus

Above email:

https://lore.kernel.org/lkml/alpine.LFD.1.10.0807151716510.2867@woody.linux-foundation.org/