

Share This Story



576

Linus Torvalds Admits He's Been Asked To Insert Backdoor Into Linux

[samzenpus](#) posted about 7 months ago | from the getting-in dept.

darthcamaro writes

"At the Linuxcon conference in New Orleans today, Linus Torvalds joined fellow kernel developers in answering a [barrage of questions](#) about Linux development. One question he was asked was whether a government agency had ever asked about inserting a back-door into Linux. Torvalds responded 'no' while shaking his head 'yes,' as the audience broke into spontaneous laughter. Torvalds also admitted that while he has a full life outside of Linux he couldn't imagine his life without it. 'I don't see any project coming along being more interesting to me than Linux,' Torvalds said. 'I couldn't imagine filling the void in my life if I didn't have Linux.'"

- Better reliability
 - Greater functionality
 - Lower system cost
- ▶ Get your EVM and join the revolution!

Inductive
Sensing

TEXAS INSTRUMENTS



576 comments

[load all](#)[All](#)[Insightful](#)[Informative](#)[Interesting](#)[Funny](#)[Threshold](#)

2

▼ Would probably be found (5, Funny)

[MadX \(99132\)](#) | about 7 months ago | ([#44891237](#))

If such a mechanism was coded in, the nature of open source would mean it would be found by others. This in turn would compromise the trust of the ENTIRE kernel. That trust can take years to build up - but be destroyed in a heartbeat.

[↩ Reply](#)[9 hidden comments](#)

▼ Re:Would probably be found (4, Insightful)

[phantomfive \(622387\)](#) | about 7 months ago | ([#44891249](#))

That trust can take years to build up - but be destroyed in a heartbeat.

You'd think so, but somehow people still trust Windows, even though it most certainly has been compromised.

[↩ Reply](#)[1 hidden comment](#)

▼ Re:Would probably be found (4, Insightful)

[DerPflanz \(525793\)](#) | about 7 months ago | ([#44891257](#))

Being compromised isn't the issue. The Linux kernel has been compromised as well.

The issue here, is that there is a backdoor being built-in deliberately. That could compromise trust.

[↩ Reply](#)[1 hidden comment](#)

▼ **Re:Would probably be found (5, Insightful)**

[phantomfive \(622387\)](#) | about 7 months ago | ([#44891277](#))

*The issue here, is that there is a backdoor being built-in deliberately.
That could compromise trust.*

There is [\[americablog.com\]](#) [that possibility](#) [\[wikipedia.org\]](#). Once again, this is a possibility we've known about for a while, and it hasn't caused people to leave Windows in droves. I think it's something most people just must not care about.

[↩ Reply](#)[1 hidden comment](#)

▼ **Re:Would probably be found (4, Interesting)**

[vague regret \(1834800\)](#) | about 7 months ago | ([#44891557](#))

According to the [recent human brain study](#) [\[alternet.org\]](#), ☐ *facts do not matter*. So no wonder people still believe in things like Windows (or open-source) safety and security...

[↩ Reply](#)

▼ **Re:Would probably be found (5, Interesting)**

[Joining Yet Again \(2992179\)](#) | about 7 months ago | ([#44891757](#))

From the description of the study, it seems to me that people who have formed an opinion won't change it just because they see a single piece of potentially falsified or misleading evidence. For example (looking at one of the experiments), if someone has an opinion on joblessness in the US - which might bring in factors of job stability, hours worked or attainment of a living wage - seeing a single graph on number of employed people in recent years does ☐ not allow us to conclude that joblessness has been reduced under Obama, unless you have a very primitive interpretation of "joblessness".

The only damning conclusion is that some academics are so arrogant that they assume test subjects must be faulty if they don't immediately believe the academic's interpretation of some data presented to them.

[↩ Reply](#)

▼ **Re:Would probably be found (5, Interesting)**

[michelcolman \(1208008\)](#) | about 7 months ago | ([#44891647](#))

Then again, the back door would be easier to find by criminals. I don't personally care that much about the NSA snooping through my e-mails. But if some criminal can read them just as easily, it's a different story.

[↩ Reply](#)

▼ **Re:Would probably be found (5, Insightful)**

[Anonymous Coward](#) | about 7 months ago | ([#44891689](#))

You seem to assume that there are no criminals at all part of "the NSA". Considering the number of employees they have with most having fairly complete access it is almost certain that there are criminals with access to a lot of NSA data.

[↩ Reply](#)

▼ **Re:Would probably be found (5, Insightful)**

[AlphaWolf_HK \(3042365\)](#) | about 7 months ago | ([#44891707](#))

It is foolish to assume that the people working for the government are perfect angels who could never mean you any harm; this has never been true and never will be true.

[↩ Reply](#)

▼ **Re:Would probably be found (4, Insightful)**

[Joce640k \(829181\)](#) | about 7 months ago | ([#44891755](#))

What if it was your neighbor reading your mail? Would you still shrug it off?

[↩ Reply](#)

▼ **Re:Would probably be found (2, Interesting)**

[gigahertz \(2653757\)](#) | about 7 months ago | ([#44891325](#))

Most of us don't feel important enough to worry about some government knowing our secrets. Yes, we know this gives a means for those governments to identify the people who have something to hide, and that isn't always a good thing, but it's easier than being paranoid.

↩ Reply

▼ Re:Would probably be found (5, Insightful)

[AlphaWolf_HK \(3042365\)](#) | about 7 months ago | ([#44891349](#))

You don't even need to have something to hide; you just need to anger the wrong people at the wrong time. What the government thinks is 'bad' is not necessarily what you think is 'bad,' so you're always in danger, no matter how unimportant you believe yourself to be.

↩ Reply

1 hidden comment

▼ Re:Would probably be found (2)

[AlphaWolf_HK \(3042365\)](#) | about 7 months ago | ([#44891473](#))

They don't have to torture you to make your life miserable.

↩ Reply

1 hidden comment

▼ Re:Would probably be found (5, Insightful)

[Talar \(1245824\)](#) | about 7 months ago | ([#44891601](#))

This, and add to it that whatever is 'bad' doesn't have to be 'bad' today since the data will be kept practically forever for any future government to analyze. If you still don't have anything to hide you must have a confidence in both the current and all future governments that is so unshakeable I'd almost call it stupidity.

↩ Reply

▼ Re:Would probably be found (4, Insightful)

[ObsessiveMathsFreak \(773371\)](#) | about 7 months ago | ([#44891749](#))

What a lot of people fail to recognise is that the people in charge of governments and the state tend to have the mentality and vindictiveness of very small children. Unfortunately, they also have an adults guile. Assuming that small children will behave rationally,

reasonably, or for the common good is not a legitimate strategy.

↩ Reply

▼ Re:Would probably be found (4, Insightful)

[Rosco P. Coltrane \(209368\)](#) | about 7 months ago | ([#44891269](#))

Yes, that's the conventional wisdom with open-source. But tell me: when was the last time you went inspect the code deep in the kernel? How many open-source code users do you think have the time, desire and ability - and probably paranoia - to go and inspect the code in *any* open-source project of reasonable size, let alone something as complex as the kernel?

I don't think someone could slip funny code in the main kernel tree - too many specialists reviewing the patches - but I'm convinced that if Canonical, SuSE or RH wanted to distribute a tainted kernel, they could do it undetected for a very long time, if not indefinitely.

↩ Reply

[3 hidden comments](#)

▼ Re:Would probably be found (4, Interesting)

[Starky \(236203\)](#) | about 7 months ago | ([#44891297](#))

Code does not have to be fully reviewed for the open source development process to discipline attempts at compromise. There is a nonzero probability that any given piece of code will be reviewed for reasons other than looking for a back door, and if the probability is higher than trivial, it would dissuade parties from attempting to surreptitiously put in a back door. If a back door were found, the contributor would be known and repercussions would follow.

Moreover, I would not be at all surprised if foreign governments who have a national security interest in running uncompromised operating systems have devoted time and resources specifically to code review of the kernel for potential compromises.

↩ Reply

▼ Re:Would probably be found (4, Insightful)

[rioki \(1328185\)](#) | about 7 months ago | ([#44891347](#))

Do you compile your programs from source and check that it is the last valid version from the project or do you install rpm or deb binary packages? Even if the actual project is vetted, it is near impossible to validate everything that

comes though the automatic updates. This is definitely a point of failure, since you only need one person, the person that has access to the signing keys and the update server. So you trust canonical, red hat, SuSe to be fully vetted? Open source is better than closed source vendors, but in the end, if you download binaries you are in the mercy of the person who built them.

↩ Reply

▼ **Re: Would probably be found (3, Informative)**

[Anonymous Coward](#) | about 7 months ago | ([#44891409](#))

As Thompson explains in his Reflections on trusting Trust (<http://cm.bell-labs.com/who/ken/trust.html>) even if you download everything in source form, and review it, you are still susceptible to manipulation if you use the compiler binary and haven't reviewed it's source.

Or the source of the compiler compiling that compiler, and so on.

↩ Reply

▼ **Re: Would probably be found (4, Insightful)**

[Mr. Freeman \(933986\)](#) | about 7 months ago | ([#44891419](#))

You raise a good point, and there's actually a lot of evidence proving you correct. There have been more than a few security vulnerabilities that have persisted in the code for various widely-used pieces of open-source software for years. One was even found and patched but then quickly reverted without anyone noticing.

What people fail to understand is that proper security reviews are more than "let's just take a look at the code and make sure that it's not sending email to the NSA." You also can't perform a proper review with a bunch of hobbyist coders, you need highly-trained experts. Every single line of code needs to be checked, double checked, and triple checked against every single other line in the code to make sure that there isn't anything that could possibly compromise the security of the system. These failures are always subtle and usually unintentional.

This is best summed up with an example. Any idiot can look at the code and say "wait a second, this code copies the decryption key and sends an email to the NSA!" Only a very methodical search with a lot of people can say "hey, we've determined that this implementation of this specific part of this specific algorithm probably doesn't have a large amount of randomness over a long period of time. It likely decays such that the complexity is reduced to such and such a number of bits after such and such an amount of time and in these specific situations. This

is a problem!"

↩ Reply

3 hidden comments

▼ Re:Would probably be found (4, Insightful)

jamesh (87723) | about 7 months ago | (#44891533)

*How many open-source code users do you think have the time, desire and ability - and probably paranoia - to go and inspect the code in *any* open-source project of reasonable size, let alone something as complex as the kernel?*

There's a whole industry evolved around finding exploitable holes in Windows, and there's no source available for that at all[1]. You can be sure the bad guys have given it a thorough going over and if there was a generic hole (I doubt you could slip an "if password = NSA then accept" style patch by the gatekeeper so it would need to be subtle and generic) it would be found. Admittedly this is not ideal but as soon as the bad guys use their exploit it will be effectively disclosed and then fixed.

[1] actually it would be reasonable to assume that at least some source for windows is in the hands of the bad guys...

↩ Reply

2 hidden comments

▼ Re:Would probably be found (2)

Bert64 (520050) | about 7 months ago | (#44891721)

[1] actually it would be reasonable to assume that at least some source for windows is in the hands of the bad guys...

And that is the worst part...

The malicious groups have more access than the good guys. A legitimate security researcher cannot get to see the source code without complying with the terms dictated by the vendor, while a malicious hacker can obtain copies of the source and go through it freely.

↩ Reply

▼ Re:Would probably be found (4, Insightful)

[mwvdllee \(775178\)](#) | about 7 months ago | ([#44891279](#))

If anybody were somehow forced to submit a backdoor, it would be very easy to just tip off a random fellow developer to "discover" it.

↩ Reply

▼ **Re:Would probably be found** (5, Insightful)

[jma05 \(897351\)](#) | about 7 months ago | ([#44891285](#))

It's unlikely that such a backdoor, should it exist, would be coded so obviously, since the source is published. Instead, it would more likely be in the form of a subtle buffer overflow that results in previlige escalation or such, such that when found, it could simply be labeled as a bug rather than an backdoor... plausible deniability.

↩ Reply

[3 hidden comments](#)

▼ **Yes** (5, Insightful)

[FatLittleMonkey \(1341387\)](#) | about 7 months ago | ([#44891463](#))

The nature of open source means it MAY be found by others. Sure you have a higher chance and an audit trail but you're making multiple assumptions here:

The difference is that with a closed source OS, if the other devs with access to the code find the backdoor, they can be ordered by the company to STFU or lose their jobs. The NSA only needs to compromise (either legally or illegally) the head of the company and that also gets them every single dev with access to the source.

There's no way for even Linus at his most shouty to completely control what other Linux devs discover. (And, as the previous poster noted, that makes it easy for Linus to tip off another dev on the sly to publicly "discover" and patch the "bug", without exposing Linus to legal issues from not cooperating with the NSA.)

Given the difference between "effortless to compromise" and "insanely difficult to compromise", which would you pick as the safest?

↩ Reply

▼ **Re:Would probably be found** (5, Insightful)

[Jeremi \(14640\)](#) | about 7 months ago | ([#44891293](#))

**If* such a mechanism was coded in, the nature of open source would mean it*

would be found by others. This in turn would compromise the trust of the ENTIRE kernel. That trust can take years to build up - but be destroyed in a heartbeat.

If it was obviously a deliberate back door, sure. Which is why the clever hacker/government-agency would be a lot more subtle -- rather than a glaring "if (username == "backdoor") allowRootAccess();" they'd put a [very subtle](#) [mit.edu] mistake into the code instead. If the mistake was detected, they could then simply say "oops, my bad", and it would be fixed for the next release, but other than that nobody would be any the wiser. Repeat as necessary, and the visible results might not look too different from what we actually have.

[↩ Reply](#)[2 hidden comments](#)

▼ **Re:Would probably be found** (3, Interesting)

[ozmanjusri \(601766\)](#) | about 7 months ago | ([#44891567](#))

I can't recall where I saw that stated, and I have no idea how that would work.

It was a potential exploit on Intel's Ivy Bridge RNGs, and it wouldn't work on Linux, as /dev/random etc mix RDRAND with many other sources of entropy.

[↩ Reply](#)

▼ **No, it might not** (5, Insightful)

[bitbucketer \(892710\)](#) | about 7 months ago | ([#44891323](#))

[Reflections on Trusting Trust](#) [bell-labs.com]

[↩ Reply](#)

▼ **Re:Would probably be found** (5, Informative)

[dmcq \(809030\)](#) | about 7 months ago | ([#44891563](#))

Have a look at some of the code from the 'Underhanded C Contest' at <http://underhanded.xcott.com/> [xcott.com] where people write code that looks straightforward and nice and clear but contains deliberate evil bugs. I think that should remove any complacency and the NSA has a lot of money to spend on people posing as developers never mind the ones they stick onto standards bodies.

[↩ Reply](#)

▼ Re:Would probably be found (2)[cardpuncher \(713057\)](#) | about 7 months ago | ([#44891619](#))

Or possibly, the discovery of such a mechanism would conveniently distract attention from the possibility of, say, a backdoor in the processor itself by means of which an unlikely but valid instruction stream might, for example, give kernel privileges to a program running in user mode. An open source software exploit might be intended to be found, and removed, thus restoring your false sense of security in your possibly compromised hardware.

[↩ Reply](#)**▼ Re:Shaking? (5, Informative)**[Pikewake \(217555\)](#) | about 7 months ago | ([#44891275](#))

Unless you're in Albania, Bulgaria or Macedonia ;)

[↩ Reply](#)**▼ Re:Shaking? (5, Interesting)**[waitamin \(2811853\)](#) | about 7 months ago | ([#44891309](#))

This is so weird to most Europeans and Americans.... A common question by American teachers in my high-school in Bulgaria was, "does it make sense", usually followed by about half the people shaking their heads and half the people nodding, to the obvious (yet silent) horror of the teacher. They got used to it eventually.

What is best however is the never-ending rotational head movement that some people from the Indian subcontinent use.

[↩ Reply](#)[1 hidden comment](#)**▼ Re:Shaking? (2)**[Camembert \(2891457\)](#) | about 7 months ago | ([#44891375](#))

What is best however is the never-ending rotational head movement that some people from the Indian subcontinent use.

Yes indeed, i t is initially very puzzling.

Eventually I learned that it does not mean yes or no or maybe; but simply "I understand you" (this does not imply agreement).

[↩ Reply](#)

▼ Some people ... (4, Insightful)

[daveime \(1253762\)](#) | about 7 months ago | ([#44891321](#))

... can't tell the difference between humour and reality.

Torvalds said no while nodding his head yes is a JOKE people, not a fucking admission. Please, save the tinfoil paranoia for Reddit, and keep the serious tech discussions here.

[↩ Reply](#)[5 hidden comments](#)

▼ Re:Some people ... (4, Insightful)

[Anonymous Coward](#) | about 7 months ago | ([#44891441](#))

... can't tell the difference between humour and reality.

Torvalds said no while nodding his head yes is a JOKE people, not a fucking admission. Please, save the tinfoil paranoia for Reddit, and keep the serious tech discussions here.

I don't know if you've been following the news lately, but when it comes to backdoors a lot of the "tinfoil paranoia" of years past has turned out to actually be true. Statistically speaking it is no longer such a certainty that it's just paranoia anymore. The true tinfoil cynic might say that agencies like the NSA are actually depending on "serious tech people" discounting stuff like this as tinfoil paranoia.

[↩ Reply](#)

▼ The Pragmatics of the Truth (5, Insightful)

[Zanadou \(1043400\)](#) | about 7 months ago | ([#44891337](#))

One question he was asked was whether a government agency had ever asked about inserting a back-door into Linux. Torvalds responded 'no' while shaking his head 'yes,'

That's actually quite a cunning answer: possibly, regardless of his answer to the back-door request (I hope the answer was something like "No, fuck you"), like others in comparable situations have hinted at, maybe he's being held accountable to some kind of on-going government "Non-disclosure clause" concerning such a request/conversation.

But can body language and gestures be held up to the same legal gagging? I'm sure no legal precedent been held for that yet, and Linus probably is aware of that.

A cunning, cunning way of answering the question.

↩ Reply

▼ Slip the backdoor into a precompiled GCC instead (5, Interesting)

[Gautel \(29207\)](#) | about 7 months ago | ([#44891363](#))

Seems we need reminding of [this classic](#) [bell-labs.com] by Ken Thompson.

Slip a backdoor into a RHEL 6.x (or any other major Linux distribution) version of GCC and make it do two major things:

1. Slip a backdoor into any Linux kernel it compiles.
2. Replicate itself in any version of GCC it compiles.

Choose some entry point which changes very rarely so the chances of incompatibility with new code is small.

This would probably keep RHEL with any kernel version tainted for generations of releases without very little chance of being spotted, because there are ☐ no changes in the distributed source code of either project

↩ Reply

[2 hidden comments](#)

▼ Re:Expect to be deported (2)

[Nutria \(679911\)](#) | about 7 months ago | ([#44891631](#))

No matter if they had bank accounts, 401K, houses, they were put on the plane and sent home.

Right. Because somewhere else is their home, and they're here illegally (whether by crossing the southern border or overstaying a visa).

If they really want to be here, there are multiple well-defined sets of rules which hundreds of thousands of people use every year to get here legally,

↩ Reply

▼ if Linux was asked, the MS were asked (5, Insightful)

[Anonymous Coward](#) | about 7 months ago | ([#44891695](#))

If the Government asked for Linux, then certainly they asked for Windows, and whereas I trust Torvalds, I don't trust Microsoft - not in a nasty way, just in the sense that they're a very large company over whom the Government has a great deal of power and where very

large companies typically are not morally motivated. I don't mean that in a nasty sense, I just mean there's so many people, taking a moral stance - e.g. accepting a cost for a benefit you personally do not see - is in practical terms very, very unlikely.

So I think I have to assume there is a backdoor in Windows. In fact, it's hard to imagine anything anyone could say to reassure me. If the NSA said it was not so, I'd laugh. They twist words with the pure purpose of deception. If MS said so, I'd be thinking they were legally compelled, such that they could not even say that such a request had occurred. The NSA surely now have a problem, in that I absolutely cannot trust their word - and indeed I cannot see how that trust can be re-established. If there was a full disclosure, that would be a start, followed by a credible reform programme. I don't think either even remotely likely; and by that, I rather think the NSA has either sealed its doom, or *our* doom. The NSA has gone too far. Either they will be replaced, in which case the problem is addressed, or, if they are not replaced, then *we* have a problem, because the NSA is too powerful to remove (and violates all privacy and security).

So, what do you know? turns out this *will* hurt MS sales, because now I *have* to move to Linux. I've been thinking about it for a while, but the cost of learning a new system to do only exactly what you can do already means where I'm very busy, it hasn't happened; but now there is a *need* for me to do, privacy.

[↩ Reply](#)

▼ I couldn't imagine filling the void in my life if (3, Funny)

[TheGratefulNet \(143330\)](#) | about 7 months ago | [\(#44891803\)](#)

yeah, he's a "char star" alright. yup.

if you have char-stars you don't care about voids, really.

[↩ Reply](#)[load all](#)

Slashdot
News for Nerds

You see but you do not observe. Sir Arthur Conan Doyle, in "The Memoirs of Sherlock Holmes"

Trademarks property of their respective owners. Comments owned by the poster.

Copyright © 2014 Dice. All Rights Reserved. Slashdot is a Dice Holdings, Inc. service

