

Become a fan of Slashdot on Facebook

Nickname:

Password: 6-1024 characters long

Public Terminal

[Forgot your password?](#)

Sign in with

[Close](#)

#NetNeutrality is STILL in danger - [Click here to help.](#) **DEAL:** For \$25 - [Add A Second Phone Number To Your Smartphone for life!](#) Use promo code **SLASHDOT25**. Check out the new [SourceForge HTML5 Internet speed test.](#)

Security Problems Are Primarily Just Bugs, Linus Torvalds Says (tu.edu)

Posted by msmash on Monday November 20, 2017 @10:20AM from the things-Linus-says dept.

Linus Torvalds, in his signature voice: *Some security people have scoffed at me when I say that security problems are primarily "just bugs." Those security people are f*cking morons. Because honestly, the kind of security person who doesn't accept that security problems are primarily just bugs, I don't want to work with.* Security firm Errata Security has [defended Linus's point of view.](#)

[f](#) [t](#) [in](#) [g+](#) [v](#)

[security bugs](#) [linus](#)

From The Web Sponsored Links

He Flew His Drone Into Strange Hole In Lake, But When He Sees The Footage
Travelwhip

17 Photos of Melania That Donald Trump Wishes We'd Forget
LifeDaily.com

Body Gestures You Should Avoid in the Workplace
Work + Money

Think Twice Before Visiting These Most Dangerous Beaches In The World
Frank151

by Taboola

[We Can't Trust Facebook To Regulate Itself, Says Former Operations Manager](#)
[Google Engineer's Leaked 'Gender Diversity' Essay Draws Massive Response](#)
[Developer Accidentally Deletes Three-Month of Work With Visual Studio Code](#)
[The Working Dead: Which IT Jobs Are Bound For Extinction?](#)
[After Healthcare Defeat, Can The Trump Administration Fix America's H-1B Visa Program?](#)
[20,000 Worldclass University Lectures Made Illegal. So We Irrevocably Mirrored Them](#)

This is the most recent story. Help us pick the next by [voting on submissions](#), or [submit your own](#).

The Authority on Asterisk and VoIP

Posted by Slashdot



Voip-Info.org is the premier VoIP and Asterisk wiki on the web. Compare and contribute VoIP resources.
 Voip-Info.org is the premier VoIP and Asterisk wiki on the web. Compare VoIP resources, collaborate with IP telephony developers, and use Voip-Info.org as a resource for all things Asterisk documentation, business VoIP, PBX, and more.

[Learn More](#)

Security Problems Are Primarily Just Bugs, Linus Torvalds Says More | [Reply](#) [Login](#)
[Security Problems Are Primarily Just Bugs, Linus Torvalds Says](#)

[2411350 Abbreviated & Hidden Generate an Account](#)

Comments Filter:

- Score:
- [Insightful](#)
- [Informative](#)
- [Interesting](#)
- [Funny](#)

The Fine Print: The following comments are owned by whoever posted them. We are not responsible for them in any way.

They're bugs, unless they're not (Score:3)
 by [DontBeAMoran \(4843879\)](#) on Monday November 20, 2017 @10:24AM (#55587017)
 Security by obscurity, government backdoors, etc. Those are not bugs.

Nickname:

Password: 6-1024 characters long

Re: (Score:2)
 by [DontBeAMoran \(4843879\)](#)
 If your OS is not open-source, forget release/review processes. If the NSA tells you to add this black box of code, you fucking do it.

Re: (Score:2)
 by [retchdog \(1319261\)](#)
 that works for open source too, it's just trickier.

Re: (Score:2)
 by [retchdog \(1319261\)](#)
 yeah, but it probably isn't. there would be much smarter, more widely-deployed, and more cost-effective ways to do it.
 selinux is just easy for people to think of because it was designed by the NSA to scratch their particular bureaucratic itch. but, sure, anything is possible.

Re: (Score:1)
 by [Narcocide \(102829\)](#)
 The backdoor in SELinux isn't in the code, it's in the setup documentation.

All data security is through obscurity (Score:2)
 by [sibe \(173966\)](#)
 Security by obscurity
 All data security is essentially security through obscurity. Vault combinations, cryptography, keys, etc are all rely on various forms of information that is not widely known. The security comes through obscure information. Now there are forms of "security" through obscurity which are trivial to figure out and thus effectively worthless but even the most robust cryptography is still security through obscurity at its core.

True, but. (Score:2)
 by [XXongo \(3986865\)](#)
 It's true, security problems usually exploit a bug. BUT, in general, there is a systematic problem underneath the bug, which allows a bug in a program to escalate to gain access to root-level systems. So, it's not *just* a bug, but a bug that is built on a system that does not have security built in.

Re: (Score:2)
 by [ranton \(36917\)](#)
 It's true, security problems usually exploit a bug. BUT, in general, there is a systematic problem underneath the bug, which allows a bug in a program to escalate to gain access to root-level systems. So, it's not *just* a bug, but a bug that is built on a system that does not have security built in.
 I am assuming Torvalds considers not building security into a system is a bug. Consider software which does not prevent SQL injection attacks. If there was no attempt to prevent these attacks, technically the code is working as intended. Security simply was not a consideration. But in practice I believe it is still fair to consider that a bug.

Re: (Score:2)
 by [DontBeAMoran \(4843879\)](#)
 Aren't SQL injection attacks usually queued commands? Isn't the ability to queue multiple SQL commands in one string a flaw in itself? Ex: what possible harm would it do to require a "drop table" command to be called on its own,etc ?

Re: True, but. (Score:2, Insightful)
 by Anonymous Coward
 Theyâ(TM)re usually someone passing unescaped user data to an sql query. So the end user is able to break out of a string and change the functionality of the query. Incredibly basic stuff.

Re: (Score:2)
 by [magarity \(164372\)](#)
 Aren't SQL injection attacks usually queued commands? Isn't the ability to queue multiple SQL commands in one string a flaw in itself? Ex: what possible harm would it do to require a "drop table" command to be called on its own,etc ?
 The real flaw is giving out ddl grants to a service account that's supposed to be doing dml.

Re: (Score:2)
 by [next_ghost \(1868792\)](#)
 Aren't SQL injection attacks usually queued commands? Isn't the ability to queue multiple SQL commands in one string a flaw in itself? Ex: what possible harm would it do to require a "drop table" command to be called on its own,etc ?
 You won't be able to execute non-trivial installation SQL scripts directly through your code. You'll either have to chop the script into individual queries and run each separately, or run the SQL script e.g. from command line. Also, SQL injection can be useful even without adding extra query. For example, if the login form uses this kind of SQL query: "SELECT * FROM users WHERE username='username' AND password='\$password_hash';", you can log in as arbitrary user without knowing the password just by typing t

Re: (Score:2)
 by [sinij \(911942\)](#)
 I disagree that you can view lack of security as a bug. Using your example, lets say a novel way to attack databases developed in 2018. Lets call it relationship mutations. Today we have no idea how it works and how to defend against it, because it isn't invented yet. Are all databases released today buggy as a result? Do they become buggy,

without any code change whatsoever, at the time this new exploit is invented?

[1 hidden comment](#)

Re: (Score:2)

by [Junta \(36770 \)](#)

The same can be said of functional bugs, they are buggy, but you don't know it until discovered. The discovery of the bug does not mean the code changed, it means that bug hadn't been caught yet.

So yes, a system that is vulnerable to an as-yet unknown attack is buggy.

Re: (Score:2)

by [ranton \(36917 \)](#)

I disagree that you can view lack of security as a bug. Using your example, lets say a novel way to attack databases developed in 2018. Lets call it relationship mutations. Today we have no idea how it works and how to defend against it, because it isn't invented yet. Are all databases released today buggy as a result? Do they become buggy, without any code change whatsoever, at the time this new exploit is invented?

I am not sure why you don't consider that a bug. If a new way of attacking any SQL command was discovered tomorrow, that would simply mean that 100% of existing SQL commands have a bug in them. It was a previously undiscovered bug, but a bug which needs to be fixed none the less. Perhaps the bug is in the SQL syntax or ODBC interface, but it is still a bug in need of fixing.

Re: (Score:2)

by [ShanghaiBill \(739463 \)](#)

I am assuming Torvalds considers not building security into a system is a bug.

By that measure, the code with the most bugs is the program that hasn't been written yet.

Security problems are NOT just bugs (Score:2)

by [sinij \(911942 \)](#)

He is demonstrably wrong. True, some security problems are bugs, but there are also security problems that are bad design choices, that are misconfigurations, that are counting use of old technology (e.g. RSA 1024), that are poor use cases (nobody follows policy, because it is too complex and/or convoluted). You can't secure systems with just code reviews and patching. No way, no how.

[1 hidden comment](#)

Re: Security problems are NOT just bugs (Score:4, Informative)

by [Dog-Cow \(21281 \)](#) on Monday November 20, 2017 @10:38AM (#55587131)

Linus's context is entirely in terms of the kernel. If you ignore that, you write comments that are complete non-sequiturs.

[Reply to This](#) [Parent](#) [Share](#)

[twitter](#) [facebook](#) [linkedin](#)

[Flag as Inappropriate](#)

Re: (Score:2)

by [burhop \(2883223 \)](#)

he said they were "primarily" bugs. By "problem", I would guess he is talking about issues in properly set up software.

You are right about there being other issues in practice but you might argue better without using a strawman.

Re: (Score:1)

by Anonymous Coward

He is demonstrably wrong. True, some security problems are bugs, but there are also security problems that are bad design choices, that are misconfigurations, that are counting use of old technology (e.g. RSA 1024), that are poor use cases (nobody follows policy, because it is too complex and/or convoluted). You can't secure systems with just code reviews and patching. No way, no how.

Considering that he is a kernel maintainer and that his was responding to a guy trying to push code into the kernel, it is pretty clear that he was talking about kernel code. So he is demonstrably right, if you understand that he is talking about the kernel code.

Re: (Score:3)

by [ranton \(36917 \)](#)

He is demonstrably wrong. True, some security problems are bugs, but there are also security problems that are bad design choices, that are misconfigurations, that are counting use of old technology (e.g. RSA 1024), that are poor use cases (nobody follows policy, because it is too complex and/or convoluted). You can't secure systems with just code reviews and patching. No way, no how.

[A software bug is an error, flaw, failure or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways.](#) [wikipedia.org] You may disagree with this

definition of a software bug from Wikipedia, but I think it lines up with what I consider a bug. The bad design choices you mention are merely another potential cause of a bug.

The context of Linus's statements must also be considered. He is talking about product level security (Linux kernel in this case),

Re: (Score:1)

by [Nutria \(679911 \)](#)

Bad design choices

Like choosing to use insecure-by-design languages.

The vast majority of security **bugs** would disappear if languages like Ada, PL/1, FORTRAN and COBOL were used instead.

Re: (Score:2)

by [mean pun \(717227 \)](#)

He is demonstrably wrong. True, some security problems are bugs, but there are also security problems that are bad design choices, that are misconfigurations, that are counting use of old technology (e.g. RSA 1024), that are poor use cases (nobody follows policy, because it is too complex and/or convoluted). You can't secure systems with just code reviews and patching. No way, no how.

You are completely missing Linus' point. He is saying *in the context of kernel development* that security issues don't get privileged treatment. There is one set of rules for all issues, be they outright bugs, bad design choices in any aspect, misconfiguration in any aspect, etc.

Re: (Score:1)

by [NicknameUnavailable \(4134147 \)](#)

Bad development choices and programs which are able to be misconfigured are bugs. Examples of this are choices not to use https for a login page - it's a bug in the implementation, or a config file which allows you to forgo a certification+keypair - which implies the underlying program lacks the means to prevent you from running it with that setting in place or is too lazy to generate some on the fly as needed. All security holes are bugs, they mostly revolve around imparting some degree of trust to the e

Re: (Score:1)

by [TexasDiaz \(4256139 \)](#)

True, but I can think of many developers who build in security problems due to ineptitude. Ignorance is not an excuse.

Re: (Score:1)

by [NicknameUnavailable \(4134147 \)](#)

True, but I can think of many developers who build in security problems due to ineptitude. Ignorance is not an excuse.

Ineptitude is a bug. The resolution just involves a hammer to the face instead of an IDE.

Bug or feature? (Score:2)

by [BKDotCom \(542787 \)](#)

The alternative would be "features"

Re: (Score:2)

by [Junta \(36770 \)](#)

The question was *how* equifax was hacked. Was it through a measure that this would have prevented? Probably not, it was probably much more mundane.

The patch may be a nice improvement and ultimately a good idea, but it's a hardening improvement, not a fix for a specific vulnerabilty, so caution must be taken. You can't just invoke the 'security' card as a 'nothing else matters' when dealing with adding security features.

Security vulnerabilities are urgent, security mitigation features are important, but

Linus is mostly right (Score:2)

by [gweihir \(88907 \)](#)

At least when you take into account that people should design security in today. So from the coding angle, pretty much "just bugs". From the testing angle often vastly different, as in functionality testing you check for the presence of functionality, but in security testing you check for the absence of functionality. Individual tests are still pretty similar, but getting test-coverage is very different and a lot more difficult.

Of course, the "just bugs" view also requires that the developers actually under

Re: (Score:2)

by [DontBeAMoran \(4843879 \)](#)

We will NEVER, EVER have 100% of all developers understand security at the level required to make 100% secure programs.

What we need is OS and languages that have security built-in, the same way programmers don't know assembly and UEFI and yet can still code and make programs.

Re: (Score:1)

by [NicknameUnavailable \(4134147 \)](#)

Linus is usually right, it's just he says the right thing in the way which makes him sound like the largest asshole possible. Personally I find it refreshing.

Re: (Score:3)

by [Junta \(36770 \)](#)

The patch submitter agreed with him, don't know why everyone is jumping to white knight for him.

Torvalds point is that it can wait, and that it can be phased in. The proposal is a hardening scheme and there's a long history of hardening schemes breaking valid usage inadvertently. Torvalds perspective is that it can be done carefully, it's a nice to have, but it's not going to save the world and it's not so terrible for it to wait a little while to make sure it is right. The patch submitter said that he d

Assuming he has a clear requirement for security (Score:2)

by [Chrisq \(894406 \)](#)

Assuming he has a requirement for security then of course he's right

Doesn't matter (Score:2)

by [SCVonSteroids \(2816091 \)](#)

You can word it the way you want. If it's not secure, it's not secure.

Here's a more complete discussion of the issue. (Score:2)

by [mspohr \(589790 \)](#)

<https://www.theregister.co.uk/...> [theregister.co.uk]

Didn't Linus approve this? (Score:2)

by [Hrrrg \(565259 \)](#)

I thought that Linus personally approves all the changes to the kernel. So didn't he approve the changes he is complaining about?

I agree... with certain assumed contexts (Score:2)

by [adosch \(1397357\)](#)

I couldn't agree more with Linus. It's not like we know each other or have Thanksgiving together; he's right in his own non-PC way. As long as we're talking about a bug not being: 1) maliciously intended code or put there 'on purpose', 2) functionality or operability that falls into as not-as-advertised, or blatantly didn't follow an RFP or standard or 3) hell, stuff that was just overlooked, seemingly over/under-engineered or ego-over-good-code. ...I'm sure there's a few more mental dice-up catalogs to

- o
-
- o
-
-

Related Links Top of the: [day](#), [week](#), [month](#).

- 1122 comments [Google Engineer's Leaked 'Gender Diversity' Essay Draws Massive Response](#)
- 765 comments [Developer Accidentally Deletes Three-Month of Work With Visual Studio Code](#)
- 581 comments [The Working Dead: Which IT Jobs Are Bound For Extinction?](#)
- 566 comments [After Healthcare Defeat, Can The Trump Administration Fix America's H-1B Visa Program?](#)
- 555 comments [20,000 Worldclass University Lectures Made Illegal, So We Irrevocably Mirrored Them](#)


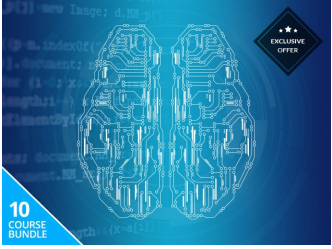




This is the most recent story. Help us pick the next by [voting on submissions](#), or [submit your own](#). [previous](#)



[We Can't Trust Facebook To Regulate Itself, Says Former Operations Manager](#)

36 comments

- **Check if you are eligible for a U.S Green Card**
(The United States Green Card Organization)
- **Uncommonly Dangerous Creatures You Should Be Aware Of**
(Frank151)
- **Bill Gates Lives In A House That Goes Beyond Human Imagination** (Credit Tips Today)
- **Discover the data gaps that many financial institutions are struggling to plug before the IFRS 9 implementation.**
(S&P Global Market Intelligence)
- **See How The "Perfect" Female Body Has Changed Over 100 Years** (Lifebru)

Slashdot Top Deals					
 Pay What You Want: The Big Data \$1	 The Complete Machine Learning Bundle \$39	 Quant Trading Using Machine Learning \$15	 Pay What You Want: The Full Stack Web \$1	 IT Security & White Hat Hacking \$29	 Skechers Heart Rate Monitor Watch \$17

[Slashdot](#)

[Post](#)

[Get more comments](#)

50 of 50 loaded

[Submit Story](#)

What the gods would destroy they first submit to an IEEE standards committee.

[FAQ](#)

[Story Archive](#)

[Hall of Fame](#)

[Advertising](#)

[Terms](#)

[Privacy](#)

[Cookie Preferences](#)

[Opt Out Choices](#)

[About](#)

[Feedback](#)

[Mobile View](#)

[Blog](#)

Trademarks property of their respective owners. Comments owned by the poster. Copyright © 2017 SlashdotMedia. All Rights Reserved.

[Close](#)

[Slashdot](#)

Working...