

Thorsten Leemhuis

Aktuelle Entwicklungen
beim Linux-Kernel

1 <https://etherpad.net/p/kltuebix19>

2
3
4 **Aktuelle Entwicklungen beim Linux-Kernel – Tuebix 2019**

5
6 **Fragen zum Vortrag hier reinschreiben! Setzt bitte ein "+" vor Fragen anderer, die euch auch interessieren!**

7
8 Nach 2/3 des Vortrags werde ich dies Dokument öffnen und Fragen live beantworten. Ansatz ist anderswo bislang immer gut angekommen (siehe etwa <https://etherpad.net/p/klclt18> oder <https://etherpad.net/p/klclt19>). Zwei Beispiele für Fragen:

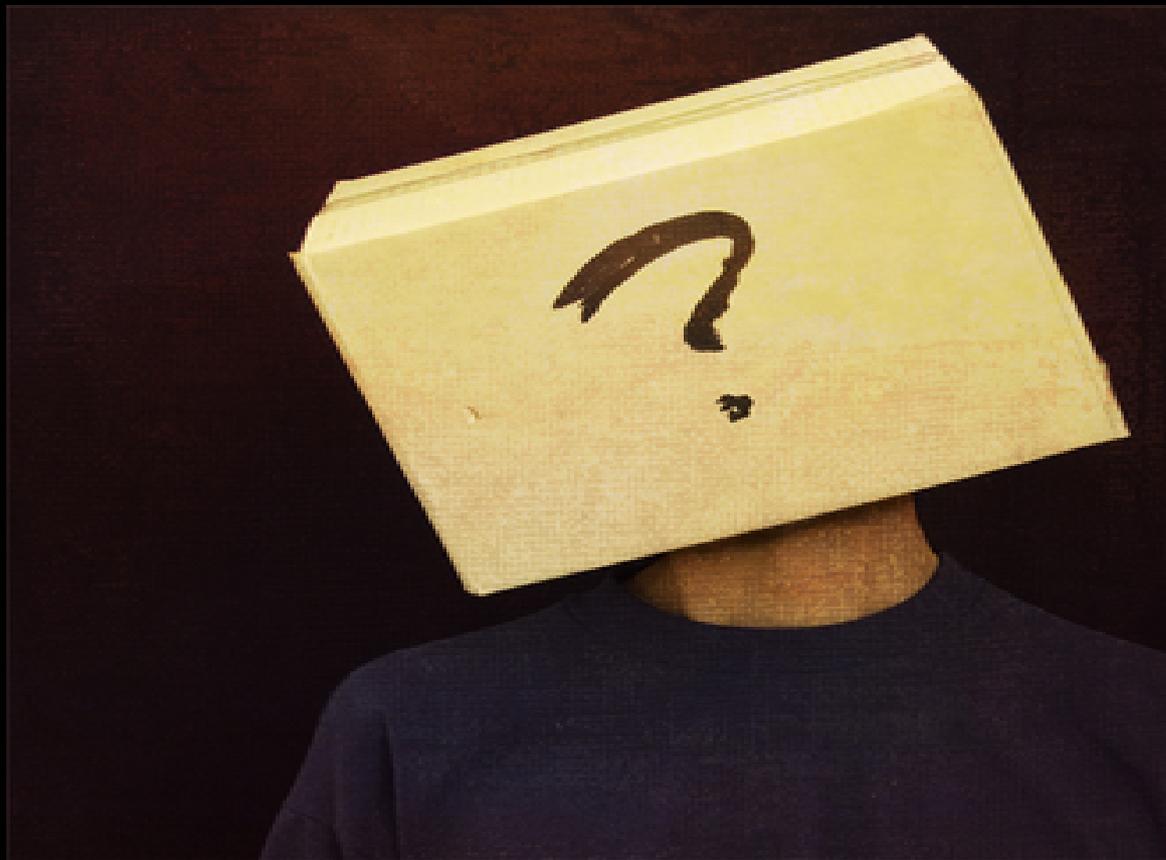
- 9
10 +++ Warum reitest du in c't und auf Social Media immer so auf der Mehrdeutigkeit des Begriffs "Linux" rum?
11 ++ Warum arbeiten die Linux-Entwickler manchmal an exotischen Dingen, statt sich auf wichtigere Dinge wie Grafiktreiber, WLAN oder Lüfterregelung zu konzentrieren, wo es häufiger mal hakt?

12
13 **Fragen hier eintragen:**

- 14
15 •
16 •

17
18 **Feedback zum Vortrag:**

19
Hier könnt ihr Feedback zum Vortrag hinterlassen, wenn ihr wollt:



*"Ist der Typ da vorne eine
verlässliche Quelle?"*



index : kernel/git/torvalds/linux.git

Linux kernel source tree

master ▾

switch

Linus Torvalds

[about](#) [summary](#) [refs](#) **[log](#)** [tree](#) [commit](#) [diff](#) [stats](#)

author ▾

leemhuis

search

Age	Commit message (Expand)	Author	Files	Lines
2019-01-08	docs: Revamp tainted-kernels.rst to make it more comprehensible	Thorsten Leemhuis	2	-55/+154
2019-01-08	tools: add a kernel-chktaint to tools/debugging	Thorsten Leemhuis	3	-6/+226
2017-04-18	Input: elantech - add Fujitsu Lifebook E547 to force crc_enabled	Thorsten Leemhuis	1	-0/+8
2016-01-24	hwmon: (dell-smm) Blacklist Dell Studio XPS 8000	Thorsten Leemhuis	1	-0/+11



Smartwatches im Test

Richtig einstellen mit wenig Aufwand

Die Sicherheits-Checkliste

Handy, Router, NAS, Smart-TV, Server, Browser, Facebook ...

Upgrade auf Windows 10 stoppen
VR-Brille Samsung Gear
USB-Sticks mit Typ C
Fairphone 2 im Test
Spiele-Highlights 2015

Audi macht Ernst mit VR

Die Kabel-Deutschland-Lücke
Web-Typographie
Linux-Prozessmanagement
GUI mit Python
Skylake übertakten

Alte und billige Tablets sinnvoll nutzen

Cooler Tablet-Projekte

Second Screen, Notenständer, Info-Display, Auto-Infotainment ...

€ 4,50

Thorsten Leemhuis

Linux-Kernel 4.4

3D-Grafiktreiber für virtuelle Maschinen und mehr Sicherheit bei RAID 5



Der Linux-Kernel 4.4 wird einen Grafiktreiber für den Raspi mitbringen. Performance-Verbesserungen im Netzwerkkernel sollen SSD-5-Aktivitäten erleichtern. Zwei neue Ansätze versprechen High-End-SSDs mehr Leistung zu entlocken.

Das in der ersten Annäherung an Linux 4.4 erwartete die Fähigkeiten des Treibers. Virtuelle GPU. Dadurch sollen Linux-Distributionen, die in einer mit KVM betriebenen virtuellen Maschine (VM) laufen, in Zukunft die 3D-Beschleunigung des Betriebssystemes nutzen können. Bei diesem über mehrere Jahre ak „Virtgl 3D“ entwickelten Ansatz reicht ein Guest-3D-Treiber die OpenGL-Befehle zur Ausführung an den Host weiter. Das Verfahren ermöglicht selbst Linux 4.4 die Grafikbibliothek Mesa 11.1 und den Systememulator Qemu 2.5, beide sollen noch im Dezember erscheinen. Virtualisierung-Software von VMware oder VirtualBox ermöglicht schon länger eine Nutzung der 3D-Beschleunigung in Linux-VMs. Die VMware-Produkte sind allerdings proprietär und VirtualBox erfordert oft die mühsame Einrichtung passender 3D-Gasttreiber. Anders als Virtgl 3D konzentriert die 3D-Support-Team Virtualisierungslösungen allerdings auch in VMs mit Windows. Selbigen gilt auch für das noch unfertige „Virtgl“ von Intel, bei dem die Guest-Treiber direkt auf Funktionen von Intel-GPUs aufbauen.

Das Log kann auch die Geschwindigkeiten hinwegdrehen, die es Änderungen kurz prüfen. Das Log-Verfahren für RAID ist ein wenig anders als RAID-5, die bereits an Erweiterungen arbeiten, die das Log zu einem vollwertigen Writeback-Cache machen. Dabei juffend das Log länger und mehr, was der Geschwindigkeit zugutekommt.

Raspi-Treiber

Linux bringt mit Version 4.4 erstmals einen Kernel-Grafiktreiber für die Broadcom-Prozessoren mit, die auf den verschiedenen Ausführungen des Raspberry Pi stehen. Dieser Treiber funktioniert weitgehend autark und ist nicht auf den Grafiktreiber in der jeweiligen Firmware angewiesen, wie es bei dem derzeit am weitesten entwickelten Treiber der Fall ist. Der in 4.4 enthaltene und von Broadcom selbst vorangestellte Treiber beherrscht aber bislang keine 3D-Beschleunigung, die in Linux 4.5 einfließen sollen.

soll die Geschwindigkeit steigern, denn das vermeidet nicht nur Overhead, sondern auch unnötige Wechselwirkungen zwischen SSD-Firmware und Betriebssystem. Derzeit gibt es aber nur eine Handvoll SSDs, mit denen das Ganze gelingt. Geschwindigkeitsoptimierungen bei High-End-SSDs für Server verspricht auch eine neue, noch experimentelle Architektur bei ihr nutzt der Kernel Paging, wenn es große Datenmengen mit besonders schnellen Datenströmen auszuwahlt. Dieses Trick nutzen viele Netzwerk-Treiber im Kernel schon länger, denn bei der Verarbeitung häufiger Datenmengen macht das regelmäßige Abrufen neuer Daten beim Controller weniger Arbeit als die Abarbeitung der vielen Intergaps, die sonst auffallen.

Linux 4.4 wird TOP-Handshakes schneller verarbeiten. Das reduziert Latenzen und erhöht zugleich SSDs-Anfragen, denn der Kernel kann nun mehr Anfragen bedienen, bevor er unter hoher Last ins Straucheln gerät. Die bessere Performance ist unter anderem einigen Optimierungen, die Locking-Mechanismen im TCP-Code zu verdanken. Bei Treibern durch den ausübenden Entwickler eingetragene diese Änderungen die Zahl der per SYN-ACK hergestellten TCP-Verbindungen um die Zwei- bis Dreifache. Der Entwickler hat zudem noch einige Umbauten an Codepfaden für das SO_REUSEPORT-Flag vorgenommen, über die es mehrere Anwendungen auf einem Port zulassen können, die konnte die Zahl der TCP-Handshakes noch mehr als verdoppeln.

Der neue Package-Layout-Algorithmus RACK (Recently ACK) soll die Geschwindigkeit von TCP-Verbindungen steigern, bei denen häufiger Netzwerkpakete verloren gehen. Dazu versucht RACK einige Paketverluste anhand der Übergangsraten anderer Pakete zu erkennen, und nicht anhand der Reihenfolge, in der sie eintrifft, wie es bisher-

ge Algorithmen meist tun. RACK ist zuerst experimentell und stammt von Google. Das Unternehmen setzt den Algorithmus offenbar schon eine Weile ein und hat ihn bei der IETF zur Standardisierung eingereicht.

Ungefragte Anwendungen können erstmals mit dem ebpf (entworfene Berkeley Packet Filter) ausgeführte Programme in den Kernel laden, um damit Datenströme zu verarbeiten, die durch den Kernel fließen. Zudem können beispielsweise ein nicht von Root ausgeführtes Topdown in Zukunft ebpf-Filter beim Kernel herunterladen, damit der nur die Netzwerkpakete an den Sniffer weitergibt, die der Nutzer untersuchen will. Von unangelegten Anwendungen stammende ebpf-Programme unterliegen allerdings einigen Einschränkungen, damit Angreifer den ebpf-Interpreter nicht manipulieren können. Unabhängig davon haben die Entwickler das Performance-Analyse-Werkzeug perf erweitert, damit es ebpf-Programme automatisch bauen, prüfen und in den Kernel laden kann. Der Kernel kann mit solchen Programmen individuelle Events Instruktion ausfüllen, um Overhead und den Datenfluss der Analyse zu reduzieren.

Langzeit-Kernel

Facebook-Entwickler haben die Prozessoren beim Einsatz der Befehlsreihenfolge reduziert. Zwar hatten sie festgelegt, dass die darüber aktivierte Datenparallelisierung (die Befehlsreihenfolge beim überlappenden RAID der Level 5 und 6 erheblich verbessert).

Zu den neu zum Kernel standardisierten Treibern gehört einer für USB-WLAN-Chips von Realtek, für die es bislang nur einen Übergangstreiber gab, der größere Qualitätsanforderungen aufweist. Der Kernel 4.4 wird zudem einige per Firmware angesprochene Sound-Chips besser unterstützen und spricht per I.S. angebundenen Audio-Chips von Skylake-Narrativen an. Der Webcam-Treiber ersetzt jetzt vier weitere Grafiktablets der Intel-Note an. Linux 4.4 wurde zudem vorab zu einem Langzeit-Kernel erklärt. Dabei sind es nicht nur die IETF, sondern bis mindestens Januar 2016 mit Fehlerkorrekturen und kleineren Verbesserungen versorgt werden. (DhH/ct.de)



Infos zum Artikel

Kapitel

- 01 **Linux 5.0 ist da: Geschwindigkeit zurückerobern und moderner speichern**
- 02 Versionsnummer, Geschwindigkeit und Lizenzdurchsetzungstechnik
- 03 Größere Schrift, russischer Hash-Algorithmus, Umstieg beim Block-Layer
- 04 Schneller netzwerken, Sicherheitsentscheidungen auslagern, Support für neue Boards und SoCs
- 05 Viele neue Treiber, endlich Support für big.LITTLE im Prozess-Scheduler

> Auf einer Seite lesen

320 Kommentare

Re: In diesem Kontext: Nein, nicht wirklich (Was: Hat der Stinkefinger also doch

von charlemagne Donnerstag, 08:18

Re: Danke für den wie immer informativen Kernel Log...

Linux 5.0 ist da: Geschwindigkeit zurückerobern und moderner speichern

UPDATE



TRENDS & NEWS | KERNEL-LOG

Linux-Kernel:
5.0

Thorsten Leemhuis zuletzt geändert 04.03.2019

Adiantum, BFO, BLK-MQ, FreeSync, Kernel, Kernel-Log, Linux, Linux 5.0

Der endgültige Umstieg auf die modernere Block-Layer-Infrastruktur zwingt Storage-Admins zum Umdenken. Gamer dürfen sich über Support für AMDs FreeSync freuen.

Kernel regression tracking, part 2

By **Jonathan Corbet**
November 6, 2017

[2017 Maintainers Summit](#)

The tracking of kernel regressions was [discussed at the 2017 Kernel Summit](#); the topic made a second appearance at the first-ever Maintainers Summit two days later. This session was partly a repeat of what came before for the benefit of those (including Linus Torvalds) who weren't at the first discussion, but some new ground was covered as well.

Thorsten Leemhuis started with a reprise of the Kernel Summit discussion, noting that he has been doing regression tracking for the last year and has found it to be rather harder than he had expected. The core of the problem, he said, is that nobody tells him anything about outstanding regressions or the progress that has been made in fixing them, forcing him to dig through the lists to discover that information on his own. He had, though, come to a few conclusions on how he wants to proceed.

First, he will try again to establish the use of special tags to identify regressions. His first attempt had failed to gain traction, but he agreed that he perhaps had not tried hard enough to publicize the scheme and get developers to use it. He will be looking into using the kernel Bugzilla again, even though it still seems like unpleasant work to him. He'll try to improve the documentation of how regressions should be tracked and handled. There is a plan to create a new mailing list on vger.kernel.org, with the idea that regression reports would be copied there. He will put more effort into poking maintainers about open regressions.

The discussion quickly turned to the problem (as seen by some) of the many kernel subsystems that do not use the kernel.org Bugzilla instance for tracking bugs. Peter Anvin said that many developers don't see much value in that system. Reported bugs tend to say something like "my laptop doesn't boot" with no further information; that tends not to be useful for the identification of any actual bugs. Beyond that, many bugs reported against the core kernel or x86 architecture turn out to be driver bugs in the end.

Users, it was suggested, should be explicitly directed to the mailing lists when



intro

kein (richtiger)
Kernel-Entwickler!

aber irgendwie trotzdem Ahnung ;-)

=kurze Orientierung=

Kurzüberblick

warum ist der Kernel
überhaupt wichtig?

Kurzüberblick

egal was man mit dem System macht

**Der Kernel ist
immer involviert**

*es reicht schon, den Finger
aufs Touchpad zu legen*

Kurzüberblick

nahezu alle Treiber
stecken im Kernel



Kurzüberblick

neues Modell ungefähr
alle ~ 12 Monate

eine ganze Reihen
verschiedener Ausführungen

Kurzüberblick

selbst Prozessoren
brauchen dieser Tage
Dutzende Treiber

**kernel, cpu core: DRM, intel_idle, pstat hwp, Power Management Controller (PMC), Powercap, EDAC, Trace Hub, perf (RAPL, CSTATE and UNCORE), perf MSR, hwmon, ...*

** kernel, PCH: MEI, thermalctl, SPI, MFD, ASoC/I2C, Audio, USB DWC3, I2S, SATA, ...*

**userland: libdrm, opengl, vulkan, video decoding, video encoding, OpenCL, ...*

Kurzüberblick

Mein Problem:

Könnte hier 6 - 8 Stunden reden

*Themen: #Storage, #Dateisysteme, #Netzwerk,
#Treiber, #Architektur, #Infrastruktur, ...*

*Audienz: #Admins, #Software-Entwickler, #Gamer,
#Desktop-User, #Embedded-Entwickler, #HPC, ...*



zuerst

ich erzähle,
was ich will

und dann

ich erzähle,

wozu ihr was wissen wollt

(im Rahmen meiner Möglichkeiten...)

1 <https://etherpad.net/p/kltuebix19>

2
3
4 **Aktuelle Entwicklungen beim Linux-Kernel – Tuebix 2019**

5
6 **Fragen zum Vortrag hier reinschreiben! Setzt bitte ein "+" vor Fragen anderer, die euch auch interessieren!**

7
8 Nach 2/3 des Vortrags werde ich dies Dokument öffnen und Fragen live beantworten. Ansatz ist anderswo bislang immer gut angekommen (siehe etwa <https://etherpad.net/p/klclt18> oder <https://etherpad.net/p/klclt19>). Zwei Beispiele für Fragen:

- 9
10 +++ Warum reitest du in c't und auf Social Media immer so auf der Mehrdeutigkeit des Begriffs "Linux" rum?
11 ++ Warum arbeiten die Linux-Entwickler manchmal an exotischen Dingen, statt sich auf wichtigere Dinge wie Grafiktreiber, WLAN oder Lüfterregelung zu konzentrieren, wo es häufiger mal hakt?

12
13 **Fragen hier eintragen:**

- 14
15 •
16 •

17
18 **Feedback zum Vortrag:**

19
Hier könnt ihr Feedback zum Vortrag hinterlassen, wenn ihr wollt:

etherpad.net/p/kltuebix19

*brauche einen Freiwilligen, der ein Auge
drauf hält und einmal umsortiert*

= Statusüberblick =

Kurzüberblick

Entwicklung läuft wie
ein gut geschmierter
und optimierter Motor

Kurzüberblick

neue Versionen alle
9 oder 10 Wochen

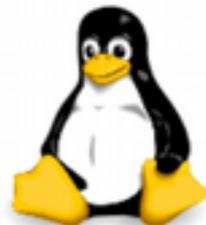
Kurzüberblick

jede ~13.500
Änderungen

Kurzüberblick

durchschnittlich
+300.000 Zeilen

The Linux Kernel Archives

[About](#)[Contact us](#)[FAQ](#)[Releases](#)[Signatures](#)[Site news](#)

Protocol	Location
HTTP	https://www.kernel.org/pub/
GIT	https://git.kernel.org/
RSYNC	rsync://rsync.kernel.org/pub/

Latest Stable Kernel:



5.1.16

mainline:	5.2-rc7	2019-06-30	[tarball]	[patch]	[inc. patch]	[view diff]	[browse]	
stable:	5.1.16	2019-07-03	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
stable:	5.0.21 [EOL]	2019-06-04	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
longterm:	4.19.57	2019-07-03	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
longterm:	4.14.132	2019-07-03	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
longterm:	4.9.184	2019-06-27	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
longterm:	4.4.184	2019-06-27	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
longterm:	3.16.69	2019-06-20	[tarball]	[pgp]	[patch]	[inc. patch]	[view diff]	[browse] [changelog]
linux-next:	next-20190703	2019-07-03						[browse]

Kurzüberblick

4.19 der aktuelle
Longterm-Kernel

*mind. 2 Jahre Support,
manche 6 Jahre*

Kurzüberblick

5.1 aktuell, 5.2
erscheint diesen oder
nächsten Montag

Kurzüberblick

Highlights von 5.2:

**Case Insensitivity
bei Ext4**

Kurzüberblick

Highlights von 5.2:

BFQ aufgebohrt

Kurzüberblick

Highlights von 5.2:

> 30.000 Dateien
verändert (fast 50%)

SPDX-Tags

Kurzüberblick

Highlights von 5.2:

**Treiber für ARM Mali und
neue Intel-GPUs**

#lima #panfrost #i915

Mehr Details im Kernel-
Log zu Linux 5.2:
heise.de/-4424484

Kurzüberblick

direkt nach Freigabe 5.2:

heiße Entwicklungs-
Phase von 5.3 in Kürze

Kurzüberblick

Highlights von 5.3 (wahrscheinlich):

AMD Navi Support

aka Radeon RX 5700

Kurzüberblick

Highlights von 5.3 (wahrscheinlich):

HDR Support in i915

Kurzüberblick

Highlights von 5.3 (wahrscheinlich):

bye bye ISDN4Linux,
Hisax & später auch Capi

mISDN bleibt

Kurzüberblick

Highlights von 5.3 (wahrscheinlich):

Adreno 540

Snapdragon-Notebooks

Kurzüberblick

Highlights von 5.3 (wahrscheinlich):

kleiner Performance-
Gewinn Dank FSGSBASE

=aktuelle Ereignisse=

aktuelles

ein wenig Unruhe jüngst

so weit zum "rund laufenden Motor"... ;-)

aktuelles

ZOL (ZFS on Linux)

ging bei 5.0-rc1 kaputt

#Januar #!Kernel #Kernelnah

aktuelles - ZoL

ZoL hat Workaround
implementiert

CPU-Overhead steigt dadurch

aktuelles - ZoL

Situation guter Reminder:

ZoL hat seine Tücken

(Lizenzproblematik ist nur eine!)

aktuelles

ein wenig Unruhe jüngst

so weit zum "rund laufenden Motor"... ;-)

aktuelles - spectre v2

Immer mal wieder

Flicken für Sicherheits-
Lücken von CPUs

manche davon drücken Performance :-/

aktuelles - spectre v2

Alles im grünen Bereich

*muss halt sein; und ja, durch Zeitdruck
hat es manchmal etwas geholpert;*

aktuelles - spectre v2

Performance zurückgewinnen:

mitigations=off

*deaktiviert PTI, L1TF, MDS, SSBD,
Spectre v1 & V2, ...*

aktuelles

ein wenig Unruhe jüngst

so weit zum "rund laufenden Motor"... ;-)

aktuelles

Linus-Auszeit & Code of Conduct (COC)

#September #Oktober

aktuelles - Linus break

viel Bikeshedding &
Besorgnis online

aktuelles - Linus break

COC wird fürs Erste so
bleiben, wie er ist

aktuelles - Linus break

Letztlich signalisiert er
"wir sind offen und
freundlich hier"

#wichtig

aktuelles - Linus break

überfällig, um
schlechtem Ruf zu
begegnen

```
> >> I fart in your general  
> >> direction and call your mother a hamster.
```

```
>  
> >> I fart in your general  
> >> direction and call your mother a hamster.  
>  
> That is plain harassment. I ask to *stop* it!
```

From Linus Torvalds <>
Date Wed, 15 Aug 2018 14:33:10 -0700
Subject Re: [GIT PULL] gcc-plugin updates for v4.19-rc1

On Wed, Aug 15, 2018 at 2:19 PM Alexander Popov <alex.popov@linux.com> wrote:
>

> >> I fart in your general
> >> direction and call your mother a hamster.

>
> That is plain harassment. I ask to *stop* it!

The correct reply is

"Is there someone else up there we can talk to?"

just google for it if you haven't seen the Holy Grail.

(And I got the quote wrong too. I forgot about how your father smelt of elderberries)

Linus

aktuelles - Linus break

überfällige
Anpassungen an
moderne Zeit



**From now on, I want you
all to call me Loretta.**

aktuelles - Linus break

COC kann überarbeitet
werden, falls nötig

= was tut sich so? =

zeige euch, was sich in
der Linux-Welt so tut



China

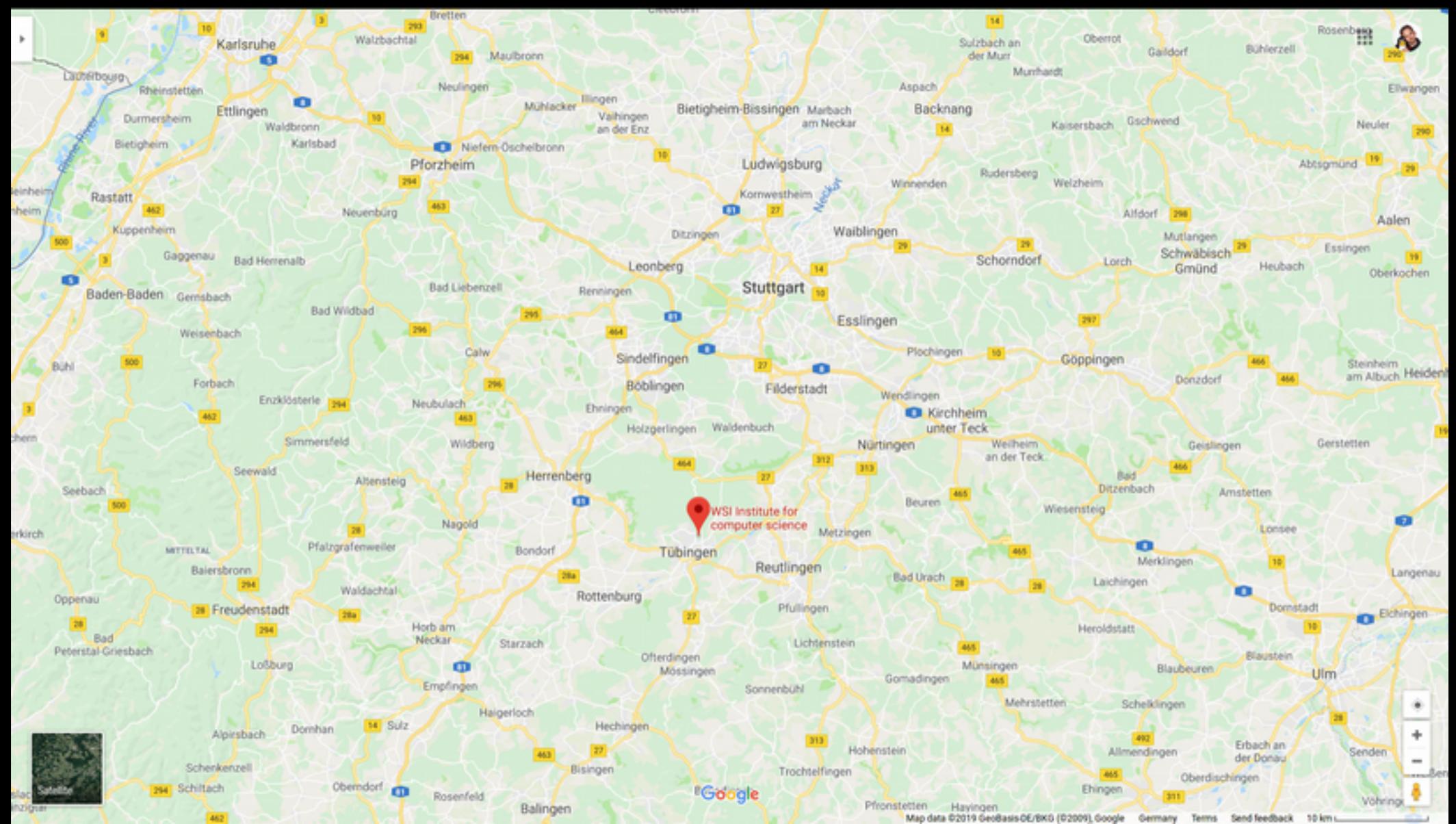


Zoom
Show slider



STATE OF

und wo es sich vielleicht
lohnt, näher hinzusehen



WSI Institute for computer science

Google

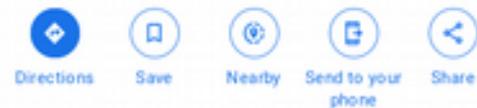


WSI Institute for computer science

Wilhelm-Schickard-Institut

4.0 ★★★★★ (1)

University department

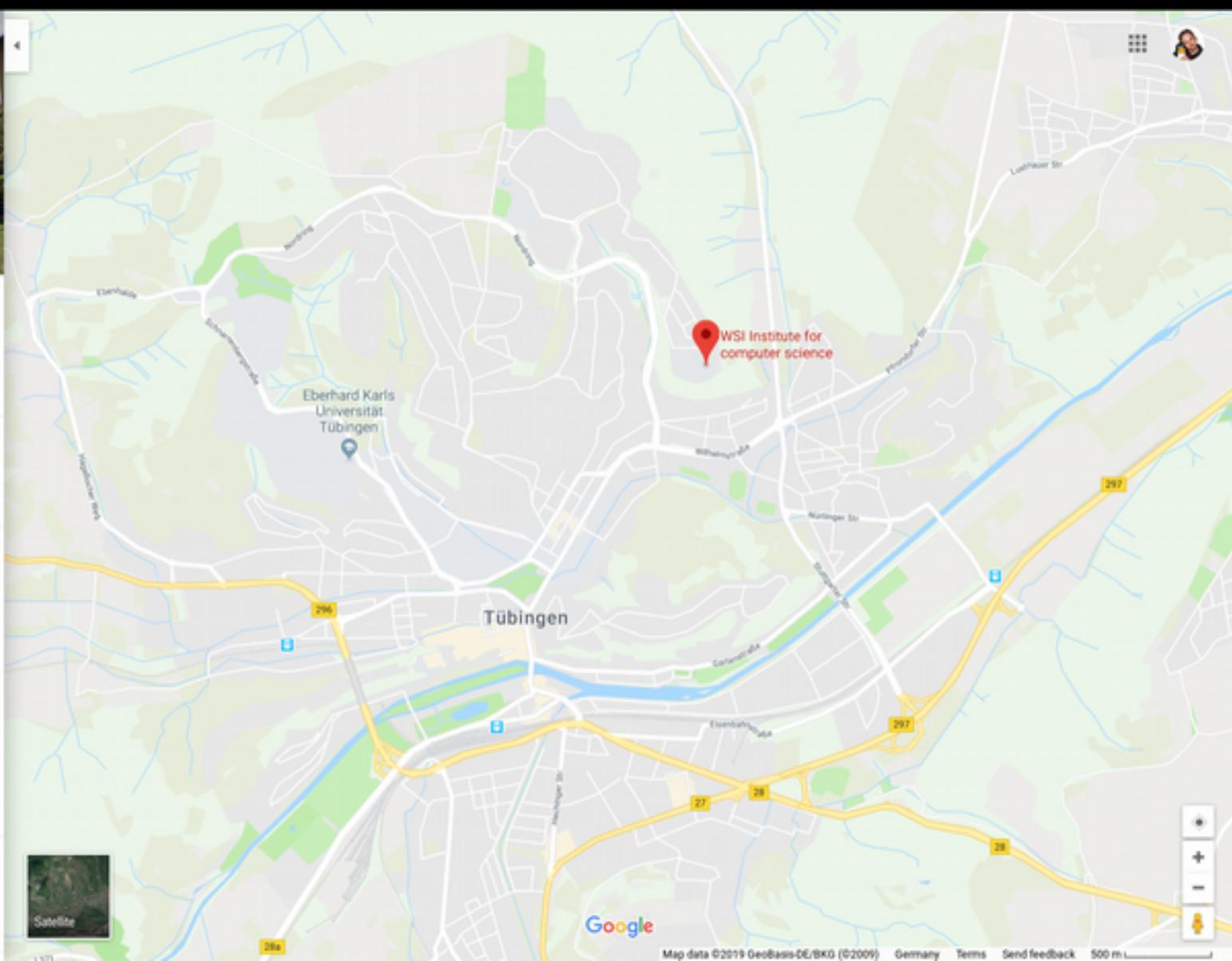


- 📍 Sand 13, 72076 Tübingen
- 📍 G3MC+QP Tübingen
- 🌐 wsi.uni-tuebingen.de
- ☎ 07071 295460
- 👤 Claim this business
- 🏷 Add a label

📝 Suggest an edit

Add missing information

🕒 Add hours



schaue zurück,
schaue nach vorne

das spannendste zuerst

*IOW: keine Sortierung nach
Themengebieten oder Wichtigkeit*

= Dateisysteme =

Bcachefs

Bcachefs

Neuer Mitbewerber

"The COW filesystem for Linux that won't eat your data".

Bcachefs is an advanced new filesystem for Linux, with an emphasis on reliability and robustness. It has a long list of features, completed or in progress:

- Copy on write (COW) - like zfs or btrfs
- Full data and metadata checksumming
- Multiple devices, including replication and other types of RAID
- Caching
- Compression
- Encryption
- Snapshots
- Scalable - has been tested to 50+ TB, will eventually scale far higher
- Already working and stable, with a small community of users

We prioritize robustness and reliability over features and hype: we make every effort to ensure you won't lose data. It's building on top of a codebase with a pedigree - bcache already has a

Bcachefs

Vielversprechend?

Vielleicht...

Bcachefs

Dauert Jahre, ein Dateisystem zu stabilisieren

Das wird bei Bcachefs nicht anders sein

Bcachefs

Oder noch länger...

- *keine Rückdeckung eines großen Players
& weitgehend eine One-Man-Show*
- *viel Code durch großen Funktionsumfang
& daher viele Bugs*

Bcachefs

Erstmal:

in den Kernel schaffen...

gerade im Gange

Bcachefs

Vielleicht besser, bei
Btrfs zu helfen?

#schwerZuSagen

= Netzwerk =

Wireguard

Wireguard

vielversprechende neue
VPN-Technik

Wireguard

stateless,

einfache Konfiguration,

schneller reconnect, ...

From Linus Torvalds <>
Date Thu, 2 Aug 2018 10:15:40 -0700
Subject Re: [GIT] Networking

On Wed, Aug 1, 2018 at 9:37 PM David Miller <davem@davemloft.net> wrote:
>
> Fixes keep trickling in:

Pulled.

Btw, on an unrelated issue: I see that Jason actually made the pull request to have wireguard included in the kernel.

Can I just once again **state my love for it** and hope it gets merged soon? Maybe the code isn't perfect, but I've skimmed it, and compared to the horrors that are OpenVPN and IPsec, it's a work of art.

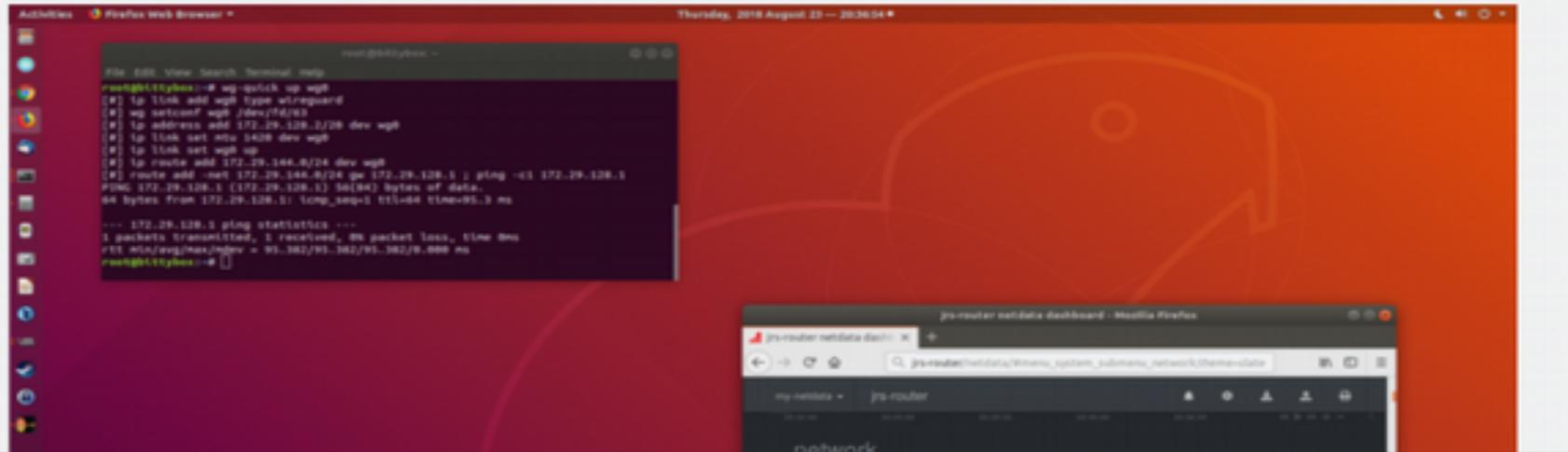
Linus

VPN —

WireGuard VPN review: A new type of VPN offers serious advantages

Fewer lines of code, simpler setup, and better algorithms make a strong case.

JIM SALTER - AUG 26, 2018 3:00 PM UTC



<https://arstechnica.com/gadgets/2018/08/wireguard-vpn-review-fast-connections-amaze-but-windows-support-needs-to-happen/>



Besser tunneln

Sichere VPN-Verbindungen mit WireGuard

Die neue VPN-Technik WireGuard soll einfacher als IPsec und performanter als OpenVPN sein. Daten auf dem Weg durchs Internet genauso gut schützen und auf mobilen Clients Netzwerk- oder Adresswechsel ohne Tunnelabriss überstehen. Wir beleuchten die Hintergründe und zeigen, wie leicht sich WireGuard unter Windows, Linux und Android aufsetzen lässt.

Von Carsten Strotmann

Linux-Vater Linus Torvalds lobt WireGuard über den grünen Klee: „... verglichen mit [...] IPsec und OpenVPN ist es ein Kunstwerk“ [1]. Die Einschätzung könnte daran liegen, dass der Entwickler Jason A. Donenfeld WireGuard von Grund auf neu und mit moderneren Krypto-Algorithmen als schnelle und sichere VPN-Lösung entworfen hat. Es lackt mit simpler Konfiguration, festem Verbindungsaufbau und abisolierten Tunneln, auch wenn mobile Clients das Netzwerk wechseln.

WireGuard ist sowohl VPN-Protokoll als auch VPN-Software. Manche Dienstleister betten parallel zu anderen Proto-

kollen auch schon auf WireGuard basierende Tunnel an. Das experimentelle, gratis nutzbare TunSafe (www.zumafz.com) wurde nur zu dem Zweck aufgesetzt, das neue Protokoll zu testen.

Donenfeld hat bei WireGuard darauf geachtet, dass der Programmcode gut zu lesen und zu verstehen ist, eine wichtige Eigenschaft für sicherheitskritische Software, erlaubt sie doch eine einfache Überprüfung des Programms. Für das Protokoll wurden wesentliche Krypto-Eigenschaften schon formal bestätigt (https://doi.org/10.1007/978-1-4939-9832-1_10), unter anderem bezüglich Correctness, Strong Key Agreement and Authenticity und Forward Secrecy.

Wireguard

braucht eigene Crypto-
Infrastruktur "ZINC"

Wireguard

hakt bei Begutachtung
(Review) von ZINC

<https://lwn.net/Articles/761939/>

Wireguard

Verdächtig ruhig in den
letzten Monaten :-/

= Paketfilter =

aka Firewall

packet filtering

nftables/nft starten
gerade durch

langsam und ziemlich unbemerkt

nftables == Kernel-Technik im Netfilter-Subsystem

nft == Userspace-Tool für eben diese Kernel-Technik

packet filtering

```
[th1@th1 ~]$ which iptables
/usr/sbin/iptables

[th1@th1 ~]$ ll /usr/sbin/iptables
lrwxrwxrwx. 1 root root 26 13. Nov 09:55 /usr/sbin/iptables -> /etc/alternatives/iptables

[th1@th1 ~]$ ll /etc/alternatives/iptables
lrwxrwxrwx. 1 root root 22 13. Nov 09:55 /etc/alternatives/iptables -> /usr/sbin/iptables-nft

[th1@th1 ~]$ iptables --version
iptables v1.8.0 (nf_tables)

[th1@th1 ~]$ /usr/sbin/iptables-legacy --version
iptables v1.8.0 (legacy)

[th1@th1 ~]$
```

packet filtering

firewalld 0.6 sowie
RHEL8, Debian 10,
Fedora 31, ...

packet filtering

wer stärker von Vorteilen
profitieren will, muss
Regeln portieren

*Von Iptables- auf Nft-Syntax;
lohnt sich bei komplexeren Firewalls*

= storage =

Asynchronous I/O (AIO)

*(unter Windows der Normalfall,
unter Linux eher die Ausnahme)*

AIO

5.1: io_uring

(IO userspace ring buffer)

AIO

endlich ordentliches,
zeitgemäßes AIO

*schneller, geringere Latenz,
simpleres API*



[knurd](#) | [Log out](#) | (Subscriber)

Ringling in a new asynchronous I/O API

By **Jonathan Corbet**
January 15, 2019

While the kernel has had support for asynchronous I/O (AIO) since the 2.5 development cycle, it has also had people complaining about AIO for about that long. The current interface is seen as difficult to use and inefficient; additionally, some types of I/O are better supported than others. That situation may be about to change with the introduction of a proposed new interface from Jens Axboe called "io_uring". As might be expected from the name, io_uring introduces just what the kernel needed more than anything else: yet another ring buffer.

Setting up

Any AIO implementation must provide for the submission of operations and

Content

[Weekly Edition](#)

[Archives](#)

[Search](#)

[Kernel](#)

[Security](#)

[Distributions](#)

[Events calendar](#)

[Unread comments](#)

[LWN FAQ](#)

[Write for us](#)

Edition

[Return to the](#)

AIO

Antwort auf das
Storage Performance
Development Kit (SPDK)

AIO

brandneu &
vielversprechend

von einem Facebook-Entwickler;

<https://lwn.net/Articles/776703/>

= Diagnose =

4.20: PSI

Pressure-stall Information

PSI

**/proc/loadavg,
nur viel viel besser**
cpu, mem und i/o separiert

```
[th1@th1 ~]$ head /proc/pressure/*
```

```
==> /proc/pressure/cpu <==
```

```
some avg10=3.00 avg60=2.79 avg300=1.45 total=308998108
```

```
==> /proc/pressure/io <==
```

```
some avg10=2.86 avg60=10.78 avg300=7.90 total=1563069450
```

```
full avg10=2.21 avg60=9.52 avg300=7.09 total=1517691815
```

```
==> /proc/pressure/memory <==
```

```
some avg10=0.11 avg60=0.23 avg300=0.19 total=4813833
```

```
full avg10=0.03 avg60=0.11 avg300=0.08 total=3347893
```

```
[th1@th1 ~]$ █
```

PSI

PSI Monitor (5.2)

*Reaktionsgeschwindigkeit bei
Android besser sicher stellen*

= Sicherheit =



- Home
- Cyber Crime
- Cyber warfare
- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivsm
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- EXTENDED COOKIE POLICY
- Contact me

Linux Kernel is affected by two DoS vulnerabilities still unpatched

November 26, 2018 By Pierluigi Paganini

Linux Kernel is affected by two denial-of-service (DoS) flaws, both vulnerabilities are NULL pointer deference issues

Linux Kernel is affected by two denial-of-service (DoS) vulnerabilities, the issues impact Linux kernel 4.19.2 and previous versions



**Dmitry Vyukov**

@dvyukov

Following



"Linux Kernel is affected by two DoS vulnerabilities still unpatched" goo.gl/MeDDDw

HA-HA-HA-HA-HA. Wait... HAAAAH-HA-HA-HA-HA-HA-HA-HA

[@securityaffairs](https://twitter.com/securityaffairs) please don't make inexperienced readers think that 2 DoS in Linux kernel are any significant goo.gl/Gi4Ama

**Linux Kernel is affected by two DoS vulnerabilitie...**

Linux Kernel is affected by two denial-of-service (DoS) flaws, both vulnerabilities are NULL pointer deference issues

securityaffairs.co

9:57 AM - 27 Nov 2018

security

open (528):

Title	Repro	Count	Last	Reported
KASAN: global-out-of-bounds Read in validate_nla	C	8	4h54m	38m
general protection fault in rxrpc_connect_call	C	3	1d12h	1d11h
general protection fault in nf_ct_gre_keymap_flush	syz	12	18m	1d22h
KASAN: use-after-free Read in do_raw_spin_trylock		1	2d19h	1d22h
INFO: rcu detected stall in gc_worker		1	4d16h	1d23h
general protection fault in __bfs (2)	syz	3	15h41m	2d00h
KASAN: use-after-free Read in oom_kill_process		1	7d21h	3d12h
INFO: rcu detected stall in rw_verify_area	C	1	5d07h	5d06h
INFO: rcu detected stall in sys_sendfile64 (2)	C	2	5d07h	5d07h
kernel BUG at mm/page_alloc.c:LINE!		3	7d20h	7d16h
INFO: rcu detected stall in tipc_disc_timeout		1	8d05h	8d02h
KASAN: use-after-free Read in ila_nf_input		1	9d05h	9d02h
KASAN: use-after-free Read in ip_tunnel_lookup		2	34d	10d
general protection fault in hci_uart_write_work	C	22	1d13h	10d
KASAN: slab-out-of-bounds Read in xfrm_policy_insert_1...		1	11d	10d
KASAN: null-ptr-deref Read in ip6_hold_safe		4	1d23h	10d
WARNING in tty_set_termios	C	121	1h55m	11d
WARNING: refcount bug in xfrm_policy_byysel_ctx		1	13d	13d
possible deadlock in genl_rcv (2)		1	13d	13d
general protection fault in gre_cells_destroy		2	13d	14d

<https://syzkaller.appspot.com/#upstream-open>

security

Danke,
syzbot & syzkaller!

**=Kommen gleich zum
interaktiven Teil=**

jetzt noch Grafiktreiber

Vorwarnung

Vortrag hat nichts zu...

= where the magic is ;-) =

BPF (aka eBPF)

XDP, AF_XDP,

Bpfilter, Microkernel-Aspekte,

Bpftrace (aka Dtrace 2.0), Tracing, ...

BTRFS

XFS Revamp

VDO

*Storage-Corruption Bug letzten Herbst,
Bcache-Bug jüngst*

Realtime aka RT-Patch

Kernel live patching

Y2K38

Grsecurity

Multipath TCP (MPTCP)

Stromsparen

D-BUS/Kdbus/BUS1

Wayland

virtio-fs

Lockdown/Secure Boot

WSL/Linux in Windows

Hellwig & VMware

etherpad.net/p/kltuebix19

= Grafiktreiber =

Userspace

Anwendung (Video-Player, Firefox, LibreOffice, Spiel, ...)

Video-Beschleunigung

Bedienoberfläche mit
GTK+, Qt, ...

3D-Beschleunigung

↓ VA API

↓ X11

↓ OpenGL

libva.so der Libva

X-Server

libGL.so von Mesa

Libva-Treiber:

i965_drv_video.so

X-Treiber:

intel_drv.so

Mesa-Treiber:

i965_dri.so

libdrm.so

Libdrm-Treiber: *libdrm_intel.so*

Linux-Kernel

Direct Rendering Manager
(DRM) im Linux-Kernel

Kernel-/DRM-Treiber: *i915.ko*

Hardware

GPU

= Grafiktreiber =

Intel

Grafiktreiber

nichts besonderes zu
erzählen

Situation ziemlich gut, wie gewohnt

Grafiktreiber

5.1: schöner booten

aka "fastboot"

= Grafiktreiber =
AMD Radeon

hardware

#amdgpu

5.0: Freesync aka VRR

hardware

generell: Amdgpu ist
wirklich gut geworden

hardware

AMDs offene 3D-Treiber
ebenfalls

hardware

**FLOSS-Stack für Gamer
oft der bessere**

meist schneller als der proprietäre

hardware

ROCm bald in den
Distros?

hardware

beim anderen GPGPU-
Stack hakt es noch

hardware

IOW: OOTB-Support bei
AMD ziemlich gut

hardware

IOW: OOTB-Support bei
AMD bald noch besser

= Grafiktreiber =
Nvidia GeForce

hardware

foss-Treiber "nouveau"

Firmware nach wie
vor großes Problem

weder schnellste noch sparsamer

Betriebsmodi ansteuerbar

hardware

Einer der Gründe,
warum der freie Treiber
so hinterher hinkt

hardware

FLOSS-Enthusiasten
sollten daher AMD oder
Intel-Chips kaufen

=Interaktive Teil=

etherpad.net/p/kltuebix19

1 <https://etherpad.net/p/kltuebix19>

2
3
4 **Aktuelle Entwicklungen beim Linux-Kernel – Tuebix 2019**

5
6 **Fragen zum Vortrag hier reinschreiben! Setzt bitte ein "+" vor Fragen anderer, die euch auch interessieren!**

7
8 Nach 2/3 des Vortrags werde ich dies Dokument öffnen und Fragen live beantworten. Ansatz ist anderswo bislang immer gut angekommen (siehe etwa <https://etherpad.net/p/klclt18> oder <https://etherpad.net/p/klclt19>). Zwei Beispiele für Fragen:

- 9
10 +++ Warum reitest du in c't und auf Social Media immer so auf der Mehrdeutigkeit des Begriffs "Linux" rum?
11 ++ Warum arbeiten die Linux-Entwickler manchmal an exotischen Dingen, statt sich auf wichtigere Dinge wie Grafiktreiber, WLAN oder Lüfterregelung zu konzentrieren, wo es häufiger mal hakt?

12
13 **Fragen hier eintragen:**

- 14
15 •
16 •

17
18 **Feedback zum Vortrag:**

19
Hier könnt ihr Feedback zum Vortrag hinterlassen, wenn ihr wollt:

=Zusammenfassend=

takeaways

Netzwerk: Nftables,
Wireguard

takeaways

Storage: AIO

(& Bcachefs vielleicht bald im Kernel)

takeaways

GPU: AMD & Intel fein,
Nvidia problematisch,
ARM Mali im Werden

takeaways

Sicherheit eine nie
endende Geschichte

takeaways

Fürchtet den Code Of
Conduct nicht

takeaways

Entwicklung schreitet

rasant voran

wie gewohnt

takeaways

vieles, vieles mehr

*eBPF, Bpftrace, XDP, AF_XDP, Bpfilter,
Realtime, Tracing, ...*

takeaways

mehr Infos zu
allem im Netz

fragt mich, wenn ihr es nicht findet



News from the source

Content

[Weekly Edition](#)

[Archives](#)

[Search](#)

[Kernel](#)

[Security](#)

[Distributions](#)

[Events calendar](#)

[Unread comments](#)

[LWN FAQ](#)

[Write for us](#)

[LWN.net Weekly Edition for September 29, 2016 \(One big page\)](#)

- [Front](#): GTK+ version numbering; Vulkan driver anatomy; OpenType 1.8 and style attributes.
- [Security](#): The trouble with new TLS version numbers; New vulnerabilities in bash, firefox, imagemagick, openssl, ...
- [Kernel](#): 4.8 development statistics; A low-level hibernation bug hunt.
- [Distributions](#): ARC++; RIP Kristoffer H. Rose, Ubuntu Yakkety Yak, Firefox OS, ...
- [Development](#): Systemd programming, 30 months later; MIT License, ...
- [Announcements](#): KDE Advisory Board, Lenovo laptops, ...

[LWN.net Weekly Edition for September 22, 2016 \(One big page\)](#)

- [Front](#): ATypI font special.
- [Security](#): On the way to safe containers; New vulnerabilities in chromium, graphicsmagick, kernel mozilla, ...
- [Kernel](#): Btrfs encryption; Stable kernel creation; BBR congestion control.
- [Distributions](#): The NTP pool system; Debian 8.6, ...
- [Development](#): Font build chains; Emacs 25.1; CouchDB 2.0; The Python packaging ecosystem; ...
- [Announcements](#): PGConf US cfp, ...

[LWN.net Weekly Edition for September 15, 2016 \(One big page\)](#)

- [Front](#): Automating hinting for every script; Backports and long-term stable kernels.
- [Security](#): Filesystem images & unprivileged containers; Minijail; New vulnerabilities in libarchive

<https://lwn.net/>

folgt mir

@kernellogger bei #twitter

bzw.

kernellogger@fc.leemhuis.info

via ActivePub, Fediverse und

Federation

(also u.a. Diaspora, Friendi.ca, Mastodon, ...)

social media madness ;-)



Following

Thorsten 'Das Leben, das U...

@thleemhuis Follows you

Das Leben, das Universum und der ganz Rest. Account 1/6, für die anderen siehe leemhuis.info/me/ Ansichten sind meine eigenen.



Following

Thorsten 'Gnome & Flatpak'...

@knurd42gnome Follows you

The [#gnome](#) and [#flatpak](#) personality of [@knurd42](#). Account 4/6, for the others see leemhuis.info/me/ Opinions are my own.



Following

Thorsten 'FOSS & Life, The ...

@knurd42 Follows you

Free & Open source software as well as Life, the universe, and everything. Account 3/6, for the others see leemhuis.info/me/ Opinions are my own.



Thorsten 'the Linux kernel I...

@kernellogger

[#Linux](#) [#kernel](#) and related areas like [#xorg](#), [#mesa](#), [#wayland](#), [#qemu](#), and [#mdadm](#). Account 6/6, for the others see leemhuis.info/me/ Opinions are...



Following

Thorsten 'Computer & freie ...

@thleemhuisfoss Follows you

Computerkram & Free and Open Source Software des [@thleemhuis](#). Account 2/6, für die anderen siehe leemhuis.info/me/ Ansichten sind...



Following

Thorsten 'Red Hat, Fedora ...

@knurd42rhfc Follows you

The [#RedHat](#), [#Fedora](#), and [#CentOS](#) personality of [@knurd42](#). Account 5/6, for the others see leemhuis.info/me/ Opinions are my own.

feedback

eins noch

gebt mir Feedback

*redet mir mir! auch negatives Feedback
willkommen, solange es kein Trollen ist ;-)*

(TWIMC: dies ist Slide #153)

mail: linux@leemhuis.info, thl@ct.de

GPG Key: 0x72B6E6EF4C583D2D

social media: see leemhuis.info/me/

#EOF