
Edition)
aws

About Me

- 3rd Year Computer Science
- Clubs:
  - CPSEC: President
  - CPLUG: President
- Security Engineering Intern @ Fortune 50
- Favorite Linux Distro: Arch

Table of Contents

- Brief history of *NIX
- UNIX philosophy & file structure
- Security tools for Linux
- Recent vulnerabilites

Seems like everyone was writing operating systems back then

History of Unix

- 1960s Multics
- 1970 Unics (UNIX)
  - Written in assembly for PDP 11
  - Written by Ken Thompson, Dennis Ritchie, Brian Kernighan, Douglas McIlroy, and Joe Ossanna at Bell Labs
  - Not Open Source
- 1978 BSD
  - Ken Thompson went to Berkeley in 1975

Unix Philosophy

- Write programs that do one thing and do it well.
- Write programs to work together.
- Write programs to handle text streams, because that is a universal interface.

You'll see this again in CPE 453 with Dr. Nico

Minix

- Released in 1987 by Andrew S. Tanebaum
- Small microkernel architecture
- Primarily used for teaching UNIX*
- Minix 3 is used in millions of devices daily

Did you mean *Freax*?

History of Linux

- 1991 Linus Torvalds begins work on the Linux Kernel & releases version 0.1
- 1994 version 1.0 is released
- 1996 version 2.0 is released
- 2011 version 3.0 is released
- 2013 Android makes up 75% of global smartphone market share
- 2015 version 4.0 is released
- 2019 version 5.0 is released

Did you mean *Linyos Torovoltos*, the Soviet computer hacker?

Linus Torvalds

Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torvalds@kruuna.helsinki.fi)

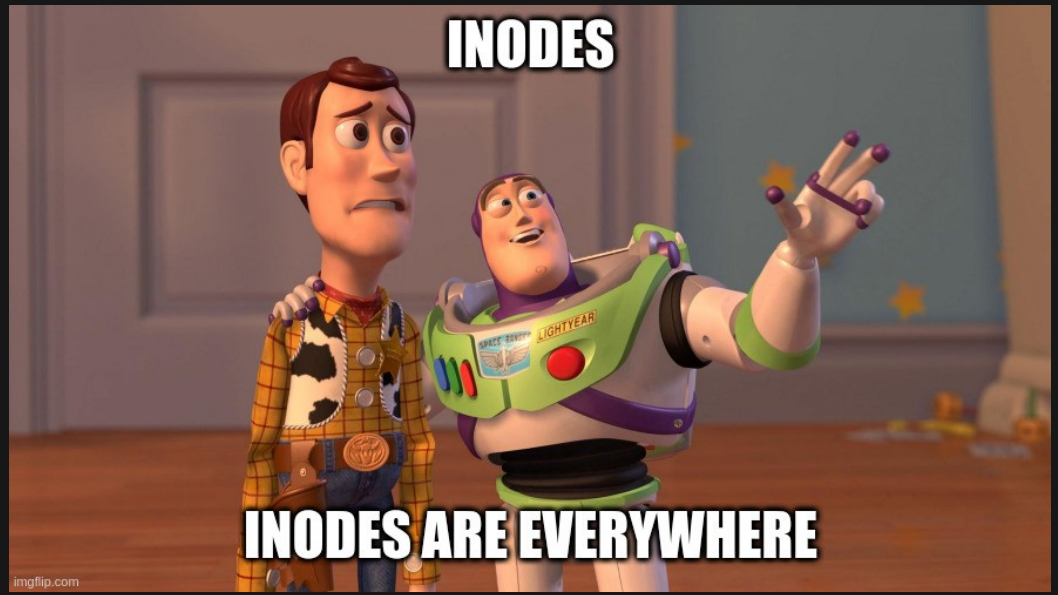
PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT portable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

— Linus Torvalds[15]

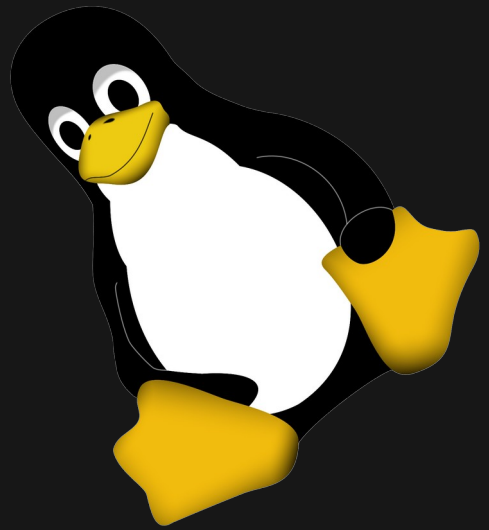
Try *echo 15000 > sys/class/backlight/intel_backlight/brightness* as root

File System Structure

- Everything is a file
- Inodes
- /
- /bin, /boot, /dev, /etc, /home, /lib, /mnt, /opt, /proc, /root, /sbin, /srv, /sys, /run, /tmp, /usr, /var



I'd like to just interject for a moment...

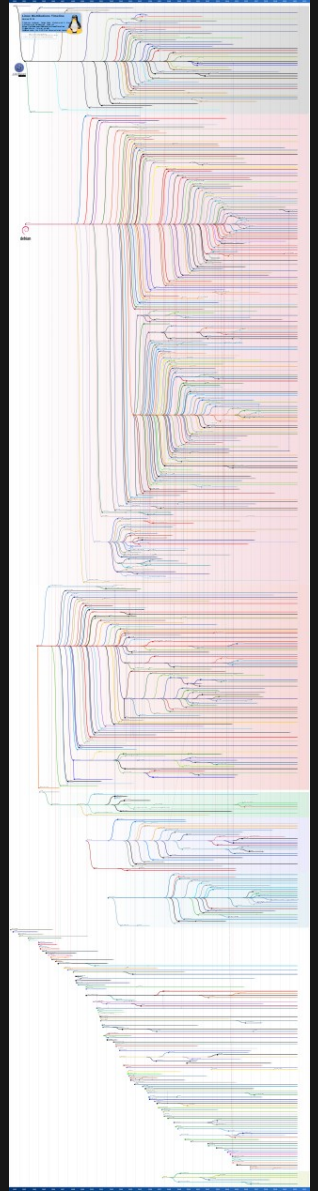


GNU/Linux copypasta

- I'd just like to interject for a moment. What you're refering to as Linux, is in fact, GNU/Linux, or as I've recently taken to calling it, GNU plus Linux. Linux is not an operating system unto itself, but rather another free component of a fully functioning GNU system made useful by the GNU corelibs, shell utilities and vital system components comprising a full OS as defined by POSIX.
- Many computer users run a modified version of the GNU system every day, without realizing it. Through a peculiar turn of events, the version of GNU which is widely used today is often called Linux, and many of its users are not aware that it is basically the GNU system, developed by the GNU Project.
- There really is a Linux, and these people are using it, but it is just a part of the system they use. Linux is the kernel: the program in the system that allocates the machine's resources to the other programs that you run. The kernel is an essential part of an operating system, but useless by itself; it can only function in the context of a complete operating system. Linux is normally used in combination with the GNU operating system: the whole system is basically GNU with Linux added, or GNU/Linux. All the so-called Linux distributions are really distributions of GNU/Linux!

Distros

- Primary forks:
  - Slackware
  - Debian
  - Red Hat
  - Jurix/SuSE
  - Enoch
  - Arch
  - Android Open Source Project (AOSP)



Security tools you should know about

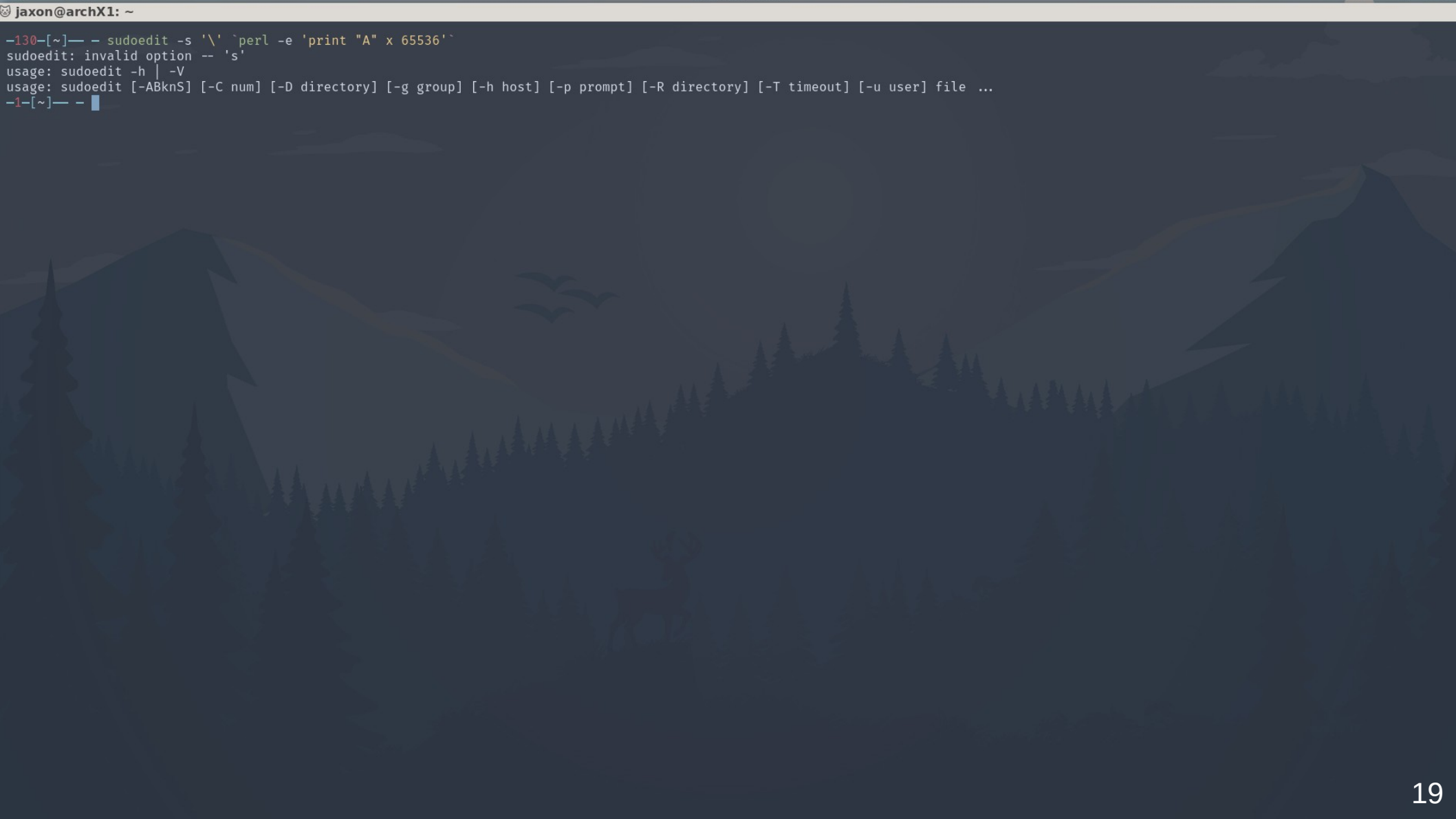
Tools

- Firejail, AppArmor, chroot, containers
- Firewalld, iptables, nftables
- LUKS, dm-crypt
- Sudo, visudo, sudoedit
- USB Guard
- Linux-hardened kernel

Recent Vulns

Sudo

- CVE-2021-3156
- Heap-based buffer overflow
- Affects versions: 1.8.2-1.8.1p2 (legacy) and 1.9.0-1.9.5p1 (stable)
- Bug was introduced in July 2011
- Found January 2021
- sudoedit -s '\' `perl -e 'print "A" x 65536'`


jaxon@archX1: ~
-130-[~]— – sudoedit -s '\' `perl -e 'print "A" x 65536'`
sudoedit: invalid option -- 's'
usage: sudoedit -h | -V
usage: sudoedit [-ABknS] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...
-1-[~]— –

Cinammon 4.2

- December 2020
- Kids find lockscreen bypass by mashing keys
- https://github.com/linuxmint/cinnamon-screensaver/issues/354

ghost commented on Dec 28, 2020 ...

```
* Cinnamon version:  Cinnamon 4.6.7
* Distribution: Fedora 32
* Graphics hardware *and* driver used: 03:00.0 VGA compatible controller: Advanced Micro Devices, Inc. [AMD/AT
* 32 or 64 bit: 64bit
```

Issue
Screensaver lock by-pass. It is possible to crash the screensaver and unlock the desktop via the virtual keyboard.

Steps to reproduce
Lock the system
Click on the virtual keyboard
Type at the real keyboard while typing at the virtual keyboard, both at the same time, as many keys as possible.

Expected behaviour
No crash.

Other information
A few weeks ago, my kids wanted to hack my linux desktop, so they typed and clicked everywhere, while I was standing behind them looking at them play... when the screensaver core dumped and they actually hacked their way in! wow, those little hackers... 💪

I thought it was a unique incident, but they managed to do it a second time. So I'd consider this issue... reproducible... by kids 😄

I tried to recreate the crash on my own with no success, maybe because it required more than 4 little hands typing and using the mouse on the virtual keyboard.

Maybe not the best bug report, but I've seen the screenlock crash twice already with my own eyes, so its pretty real.

One last thing, after the desktop is unlocked, I can't re-lock it again, the screensaver process is pretty dead and requires me to open a shell and run 'cinnamon-screensaver' manually to get it working.

👍 318 😄 667 🎉 36 ❤️ 186 🚀 33 👀 39

Now a word from our sponsor...

Mandatory plug...

CPLUG – Cal Poly Linux Users Group

- Free Your Machine Events
- Resource for all things Linux
- Linux Workshops next quarter!
- Join our discord/email list!
- cplug.org

Additional Resources

- https://wiki.archlinux.org/title/Security
- Advanced Programming in the Unix Environment
- The C Programming Language
- Operating Systems: Design and Implementation
- https://www.gwern.net/docs/cs/2001-12-02-treginaldgibbons-isyoursonacomputerhacker.html
- r/linuxmemes

Memes


I would like to present my client's
~/.bash_history from that evening.
I'd rather just confess to the murder.

Operating systems that use "/" as their path separator

Operating systems that use "\" as their path separator

Linus: Installs Steam through apt because Pop Shop gives an error

Apt:

Ubuntu users looking at Arch linux getting no second release: