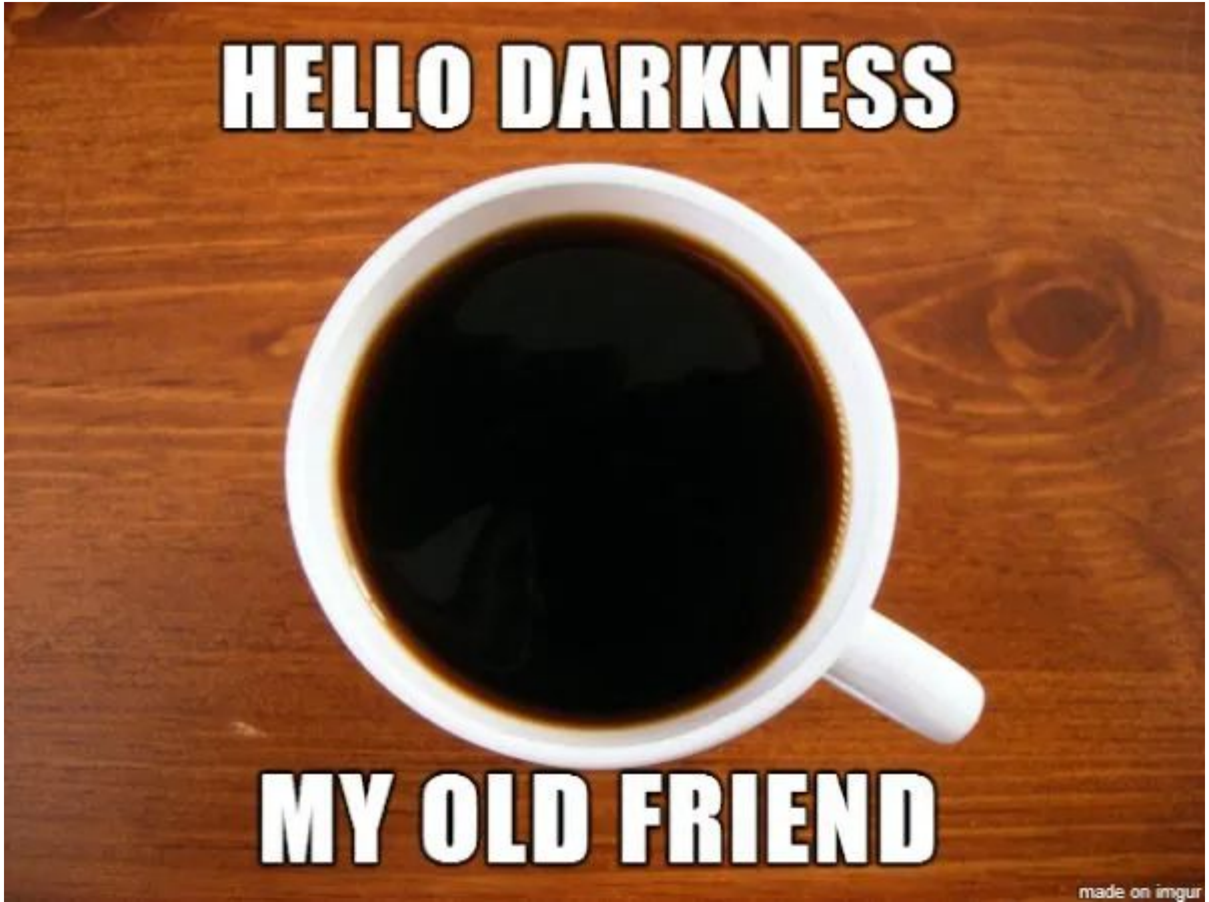
Protecting Yourself From Supply Chain Attacks - Trust Is Overrated

Me reading the list of hardware/software I trust.

Paul Asadoorian - Bsides Charm 2023

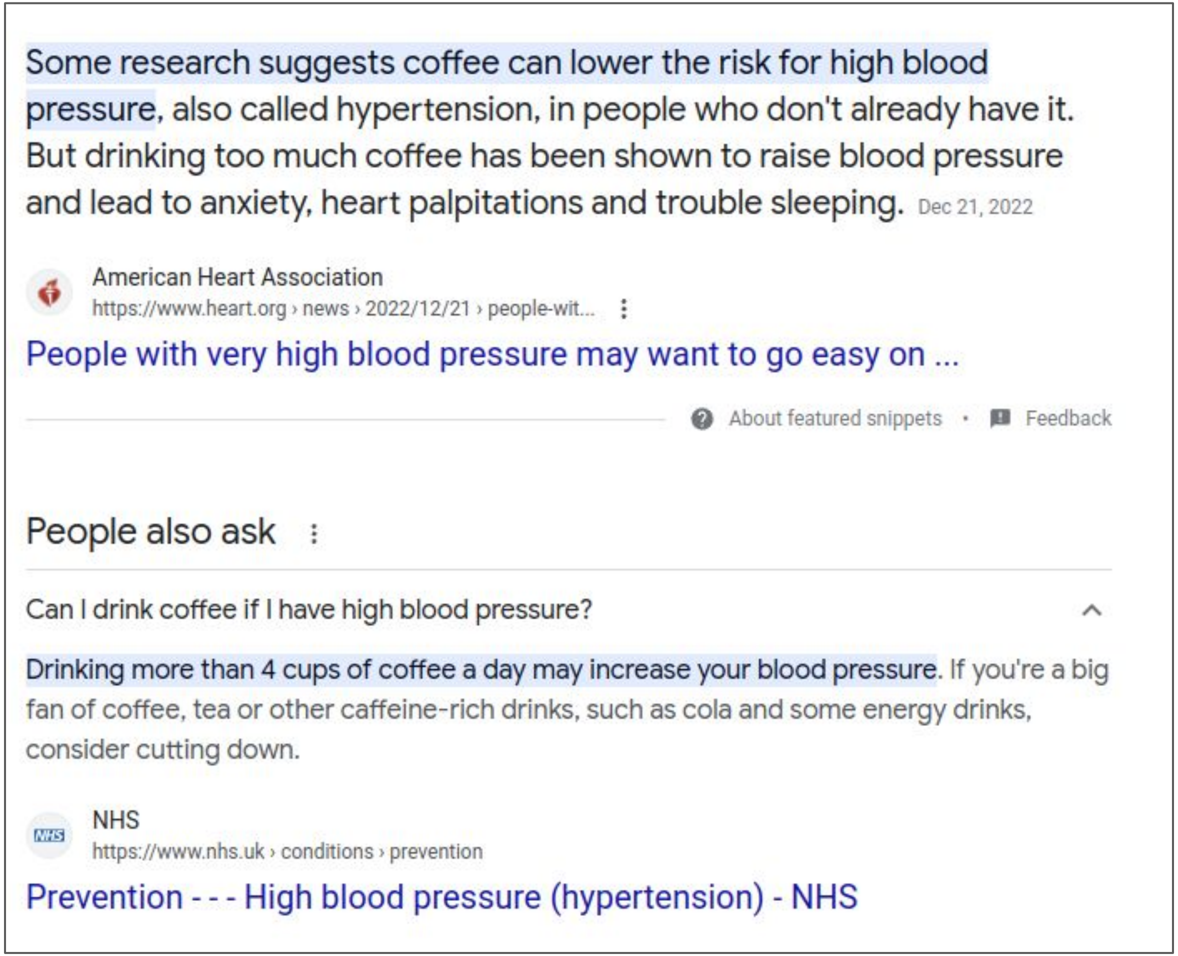
Do you have high blood pressure?

Do you love coffee?



EVERY MORNING, I TAKE MY HIGH
BLOOD PRESSURE PILL AND 12 CUPS OF COFFEE
NEITHER WORKS!
imgflip.com

If you search the Internet long enough, anything can be true…



Some research suggests coffee can lower the risk for high blood pressure, also called hypertension, in people who don't already have it. But drinking too much coffee has been shown to raise blood pressure and lead to anxiety, heart palpitations and trouble sleeping. Dec 21, 2022

American Heart Association
https://www.heart.org › news › 2022/12/21 › people-wit...

People with very high blood pressure may want to go easy on ...

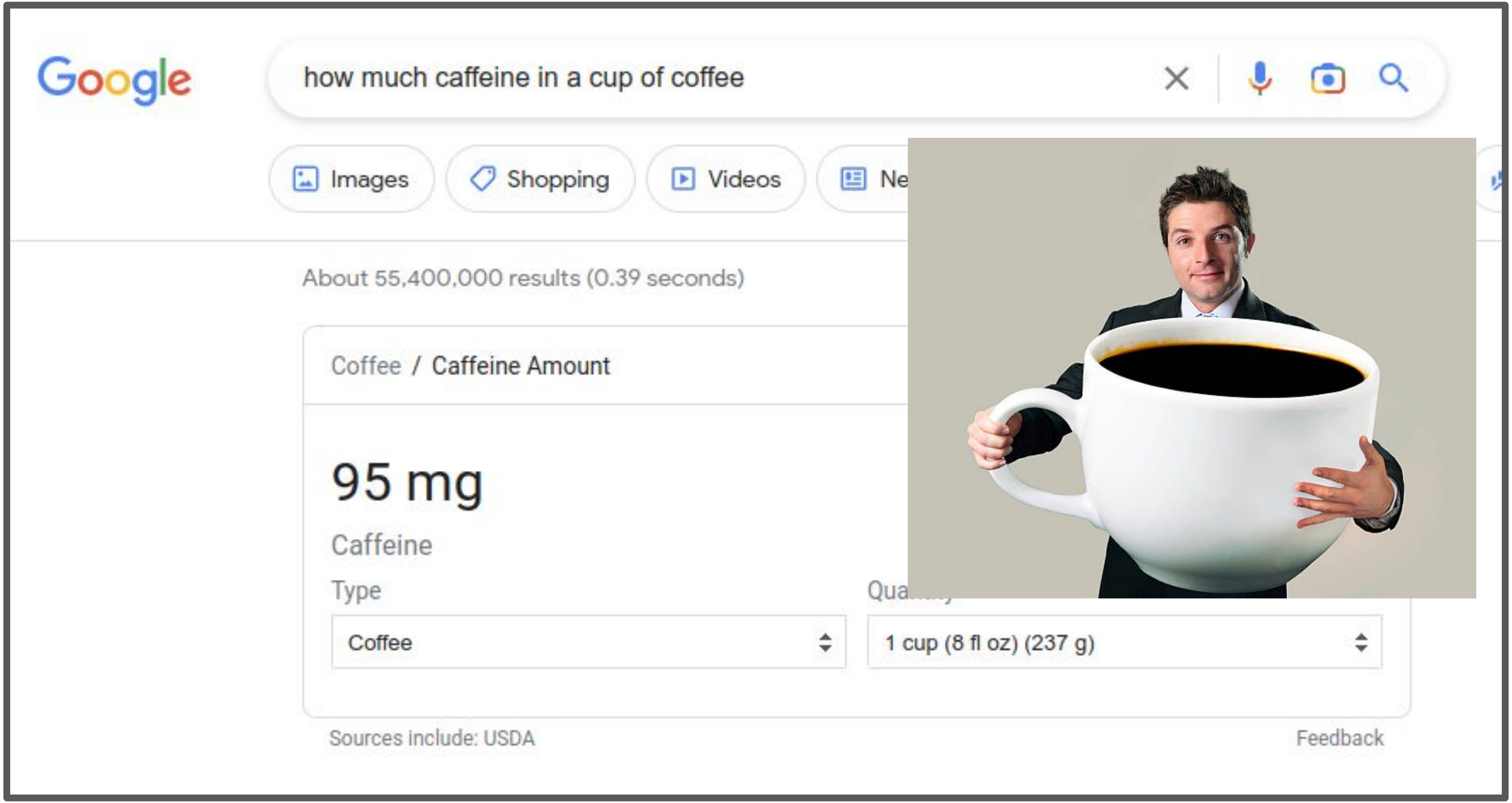
People also ask

Can I drink coffee if I have high blood pressure?

Drinking more than 4 cups of coffee a day may increase your blood pressure. If you're a big fan of coffee, tea or other caffeine-rich drinks, such as cola and some energy drinks, consider cutting down.

NHS
https://www.nhs.uk › conditions › prevention

Prevention - - - High blood pressure (hypertension) - NHS



how much caffeine in a cup of coffee

About 55,400,000 results (0.39 seconds)

Coffee / Caffeine Amount

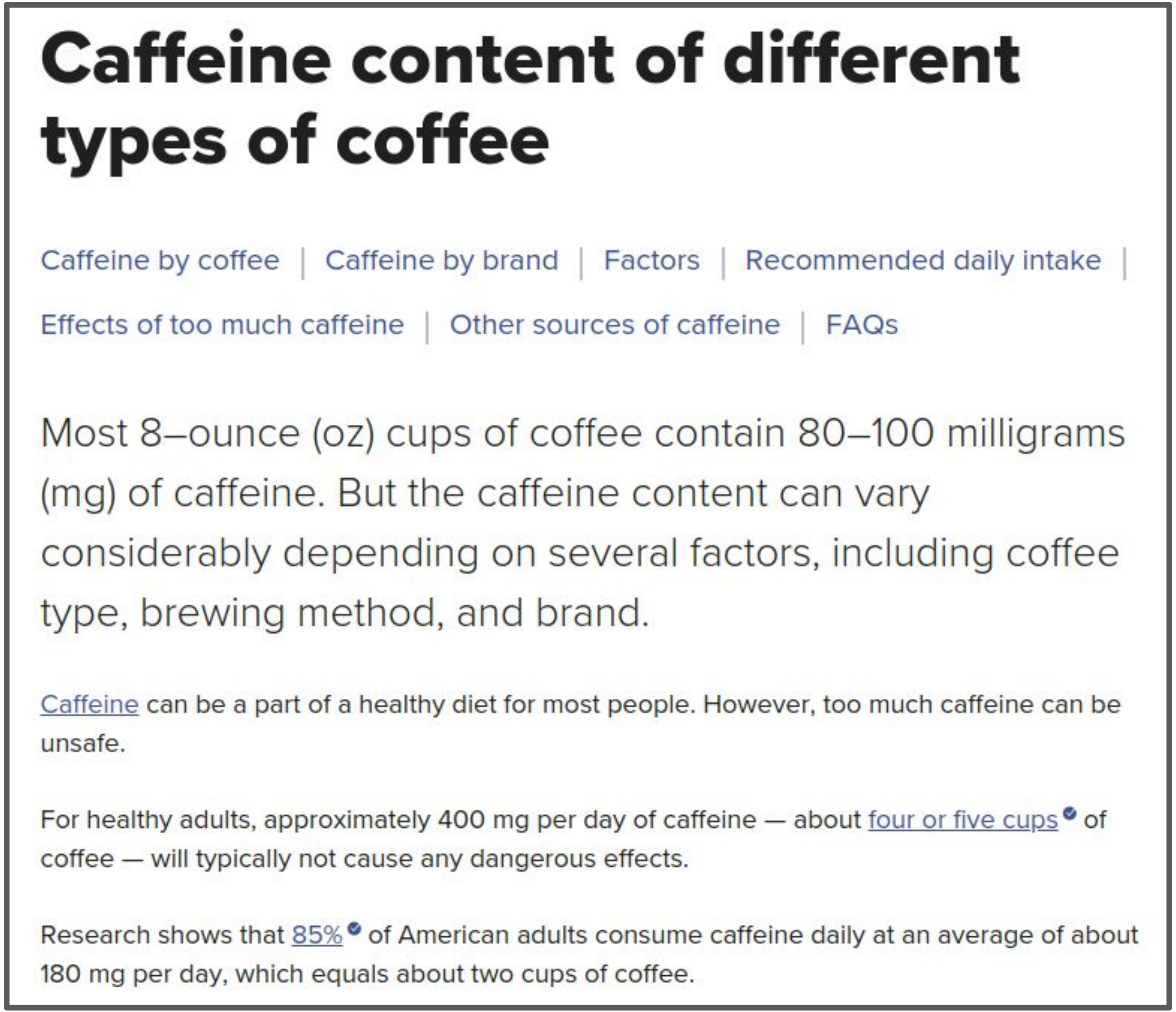
95 mg

Caffeine

Type: Coffee

Qua: 1 cup (8 fl oz) (237 g)

Sources include: USDA



Caffeine content of different types of coffee

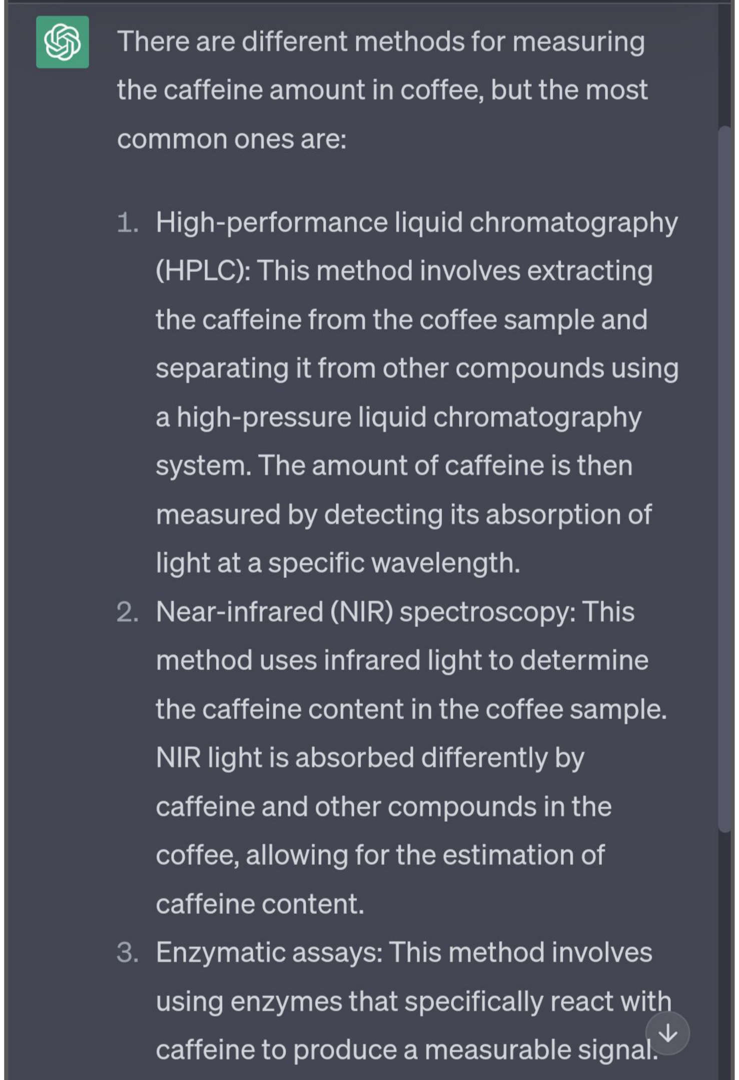
Caffeine by coffee | Caffeine by brand | Factors | Recommended daily intake | Effects of too much caffeine | Other sources of caffeine | FAQs

Most 8–ounce (oz) cups of coffee contain 80–100 milligrams (mg) of caffeine. But the caffeine content can vary considerably depending on several factors, including coffee type, brewing method, and brand.

Caffeine can be a part of a healthy diet for most people. However, too much caffeine can be unsafe.

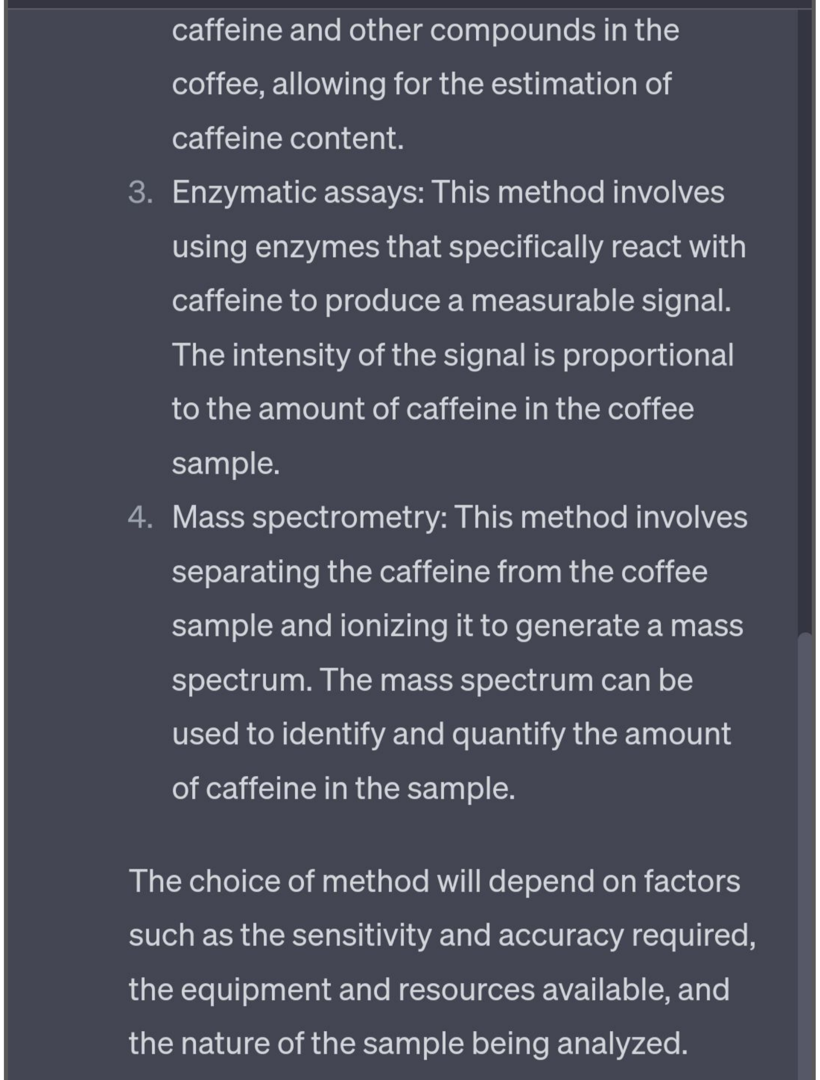
For healthy adults, approximately 400 mg per day of caffeine — about four or five cups of coffee — will typically not cause any dangerous effects.

Research shows that 85% of American adults consume caffeine daily at an average of about 180 mg per day, which equals about two cups of coffee.



There are different methods for measuring the caffeine amount in coffee, but the most common ones are:

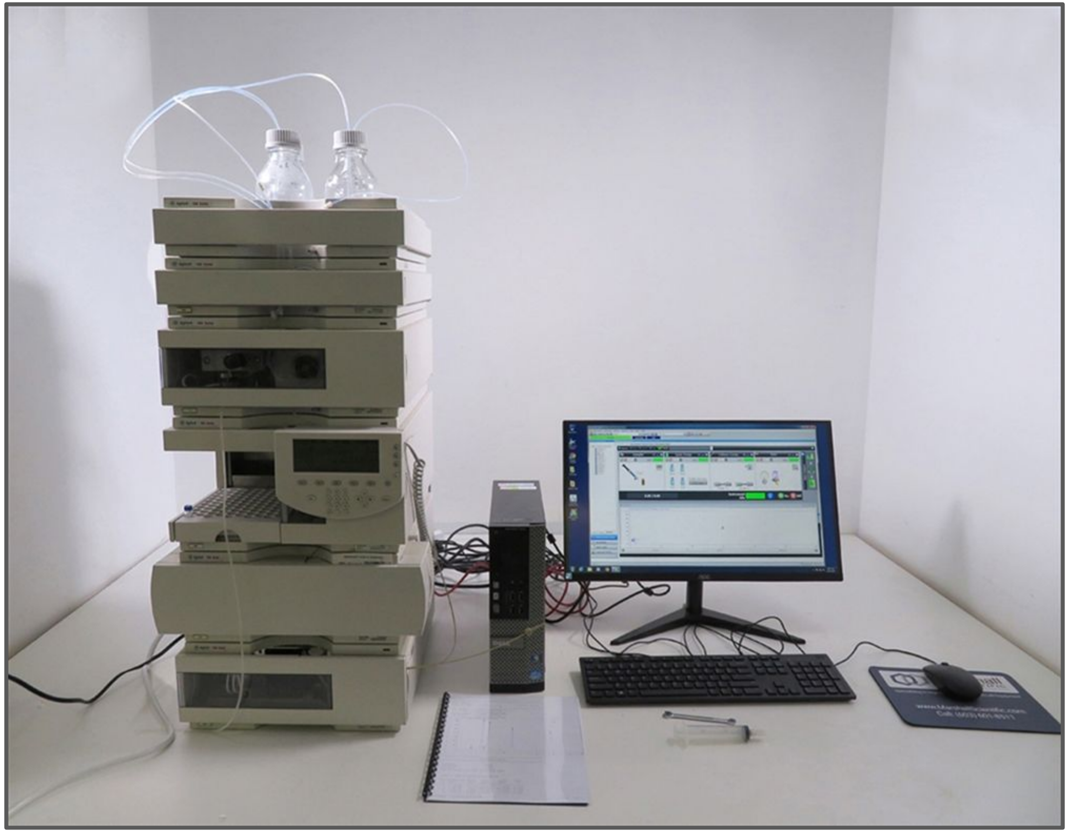
1. High-performance liquid chromatography (HPLC): This method involves extracting the caffeine from the coffee sample and separating it from other compounds using a high-pressure liquid chromatography system. The amount of caffeine is then measured by detecting its absorption of light at a specific wavelength.
2. Near-infrared (NIR) spectroscopy: This method uses infrared light to determine the caffeine content in the coffee sample. NIR light is absorbed differently by caffeine and other compounds in the coffee, allowing for the estimation of caffeine content.
3. Enzymatic assays: This method involves using enzymes that specifically react with caffeine to produce a measurable signal.



caffeine and other compounds in the coffee, allowing for the estimation of caffeine content.

3. Enzymatic assays: This method involves using enzymes that specifically react with caffeine to produce a measurable signal.
The intensity of the signal is proportional to the amount of caffeine in the coffee sample.
4. Mass spectrometry: This method involves separating the caffeine from the coffee sample and ionizing it to generate a mass spectrum. The mass spectrum can be used to identify and quantify the amount of caffeine in the sample.

The choice of method will depend on factors such as the sensitivity and accuracy required, the equipment and resources available, and the nature of the sample being analyzed.



High-performance liquid chromatography (HPLC) is a technique used to separate molecules based on size and surface charge, among other properties. The incorporation of ultra-violet (UV) spectroscopy with HPLC allows the concentration of molecules to be determined following separation.

Cost: $15,000-$50,000+

Checking the supply chain of my coffee…

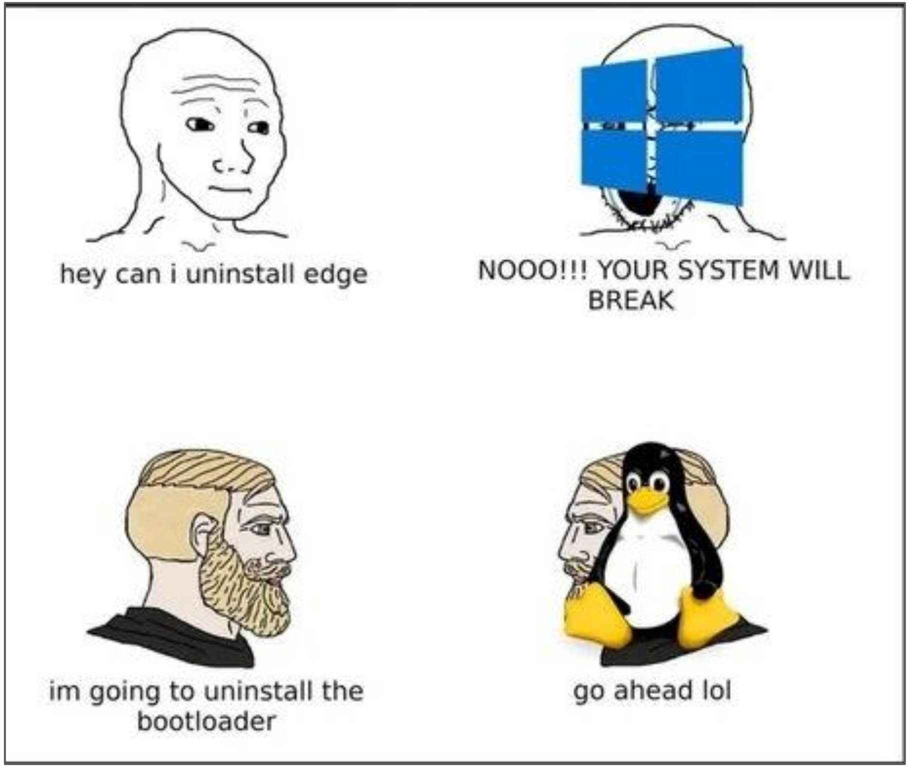
How do we minimize supply chain risks?

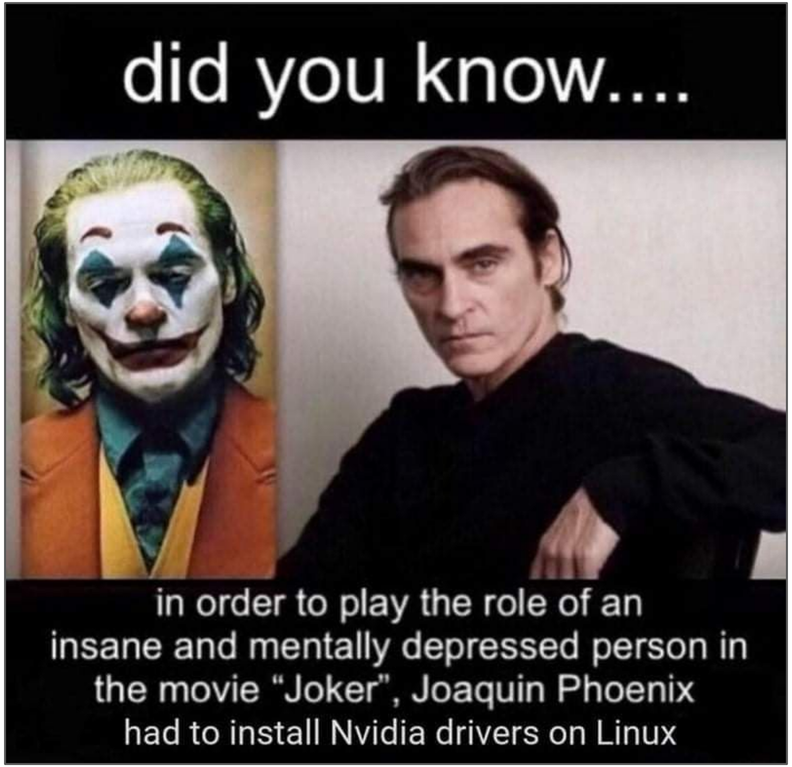
Create everything myself

Verify, then trust. Make attackers lives more difficult.

Create nothing and do no verification

I use Linux as my daily driver


hey can i uninstall edge
NOOO!!! YOUR SYSTEM WILL BREAK
im going to uninstall the bootloader
go ahead lol


did you know....
in order to play the role of an insane and mentally depressed person in the movie "Joker", Joaquin Phoenix had to install Nvidia drivers on Linux

I am obligated to tell you that. I'll use many Linux-related examples.

The Digital Supply Chain Attack Surface

← Reduced Visibility = Validation Challenges

PHYSICAL

"Hunting for backdoors in Counterfeit Cisco devices"

PRE-INSTALLED

CPU
BIOS/UEFI
ME/AMT
BMC
NIC
Storage

Components

- Firmware
- Bootloaders
- Kernels
- Operating Systems

3RD-PARTY APPLICATIONS

slack
zoom
Ps
W
P

SOFTWARE DEVELOPED IN-HOUSE

python™ Package Index

npm

docker

Increased Customization & Control →

Never trust HW/SW vendors whose name starts with

A,B,C,D,E,F,G,H,I,J,K,L,M,N,
O,P,Q,R,S,T,U,V,W,X,Y,Z

Real-world Supply Chain Attack Examples

Reduced Visibility = Validation Challenges

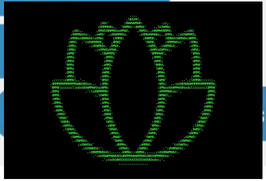
PHYSICAL

"Hunting for backdoors in Counterfeit Cisco devices"

PRE-INSTALLED

Firmware

Bootloaders

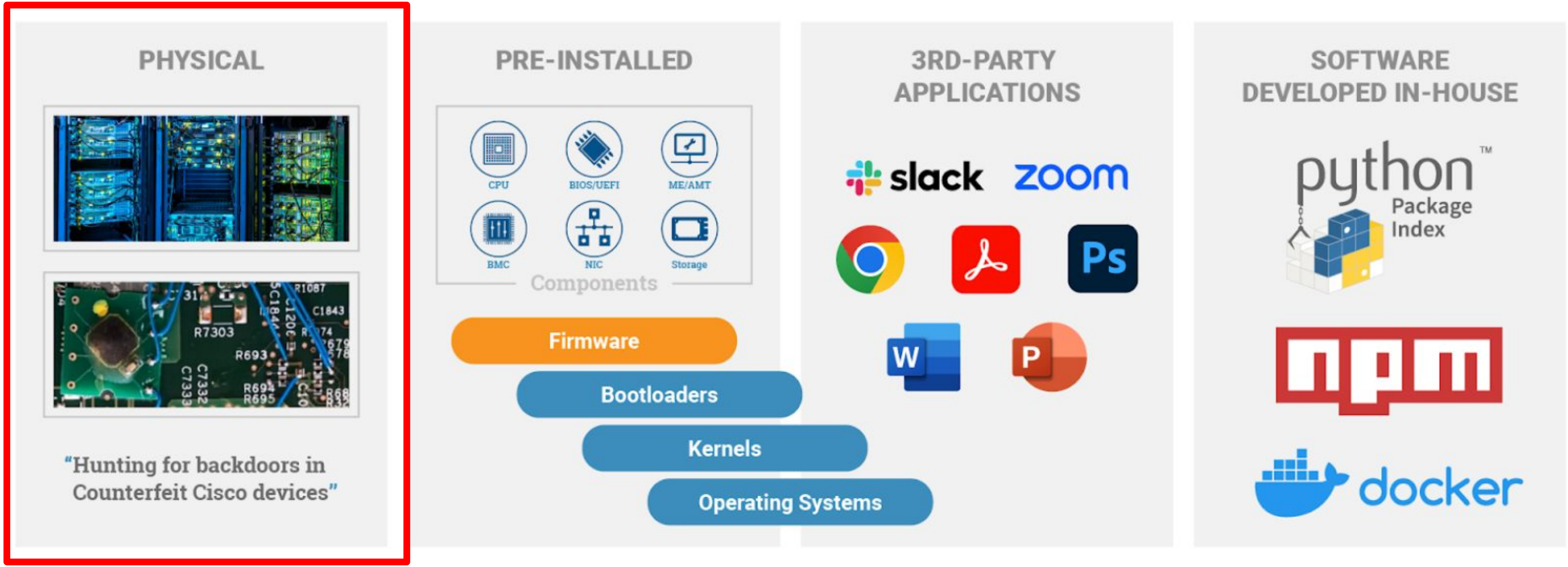


3RD-PARTY APPLICATIONS

SOFTWARE DEVELOPED IN-HOUSE

docker

Increased Customization & Control



PHYSICAL

“Hunting for backdoors in Counterfeit Cisco devices”

PRE-INSTALLED

Firmware

Bootloaders

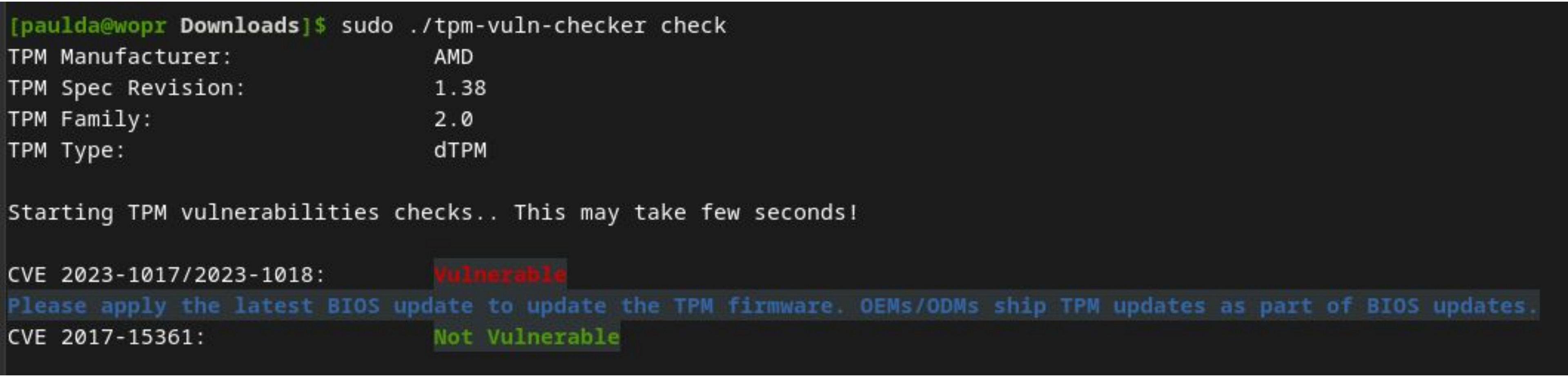
Kernels

Operating Systems

3RD-PARTY APPLICATIONS

SOFTWARE DEVELOPED IN-HOUSE

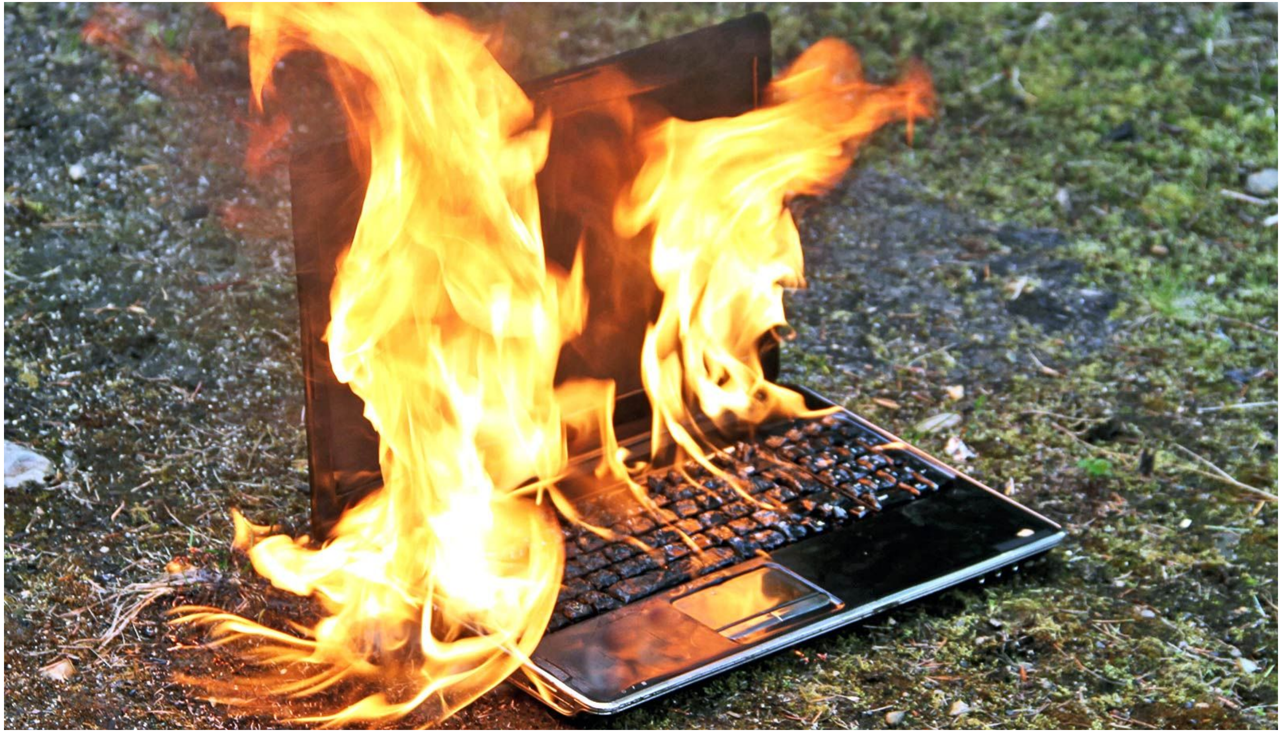
Checking Your TPM



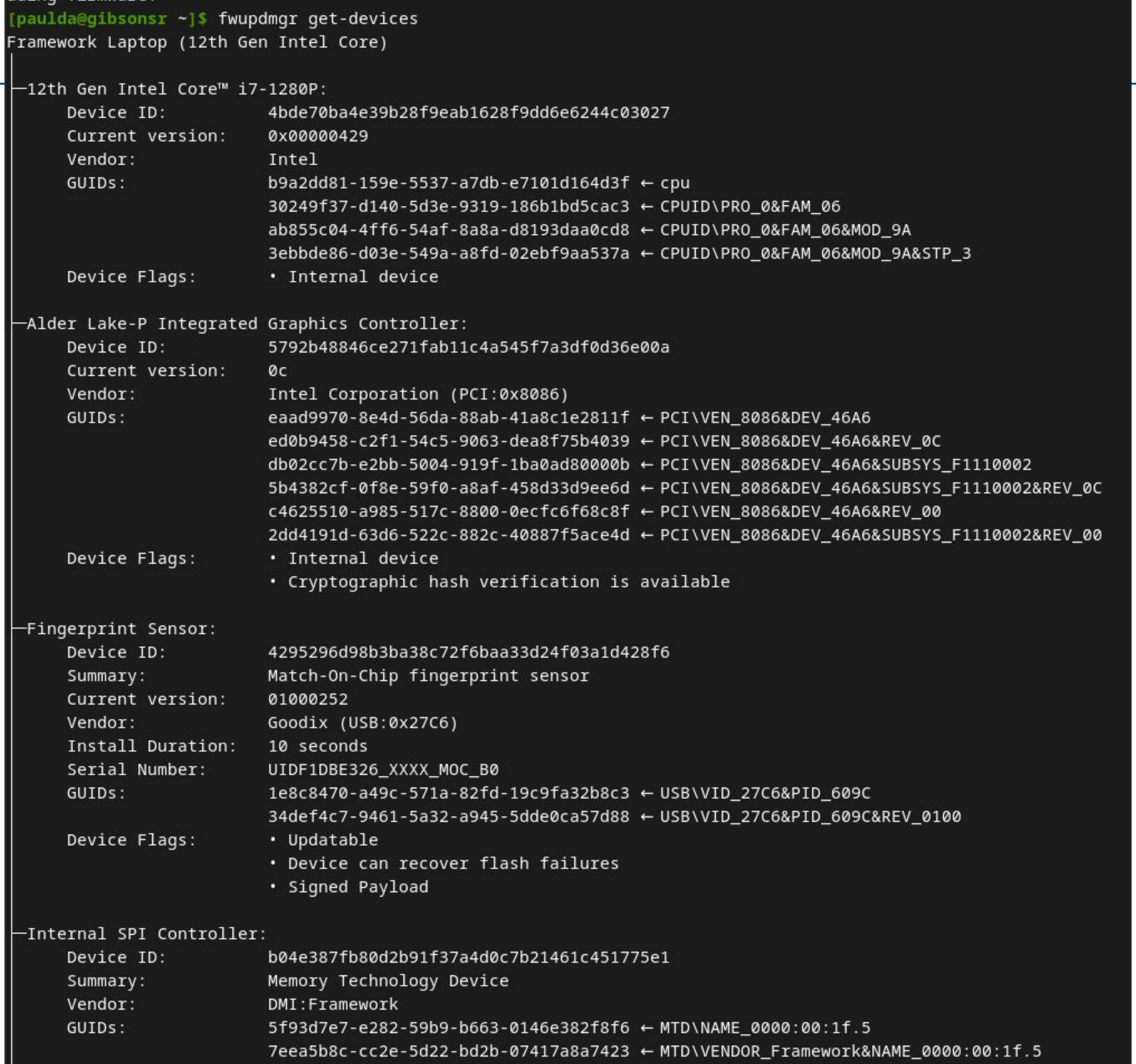
```
[paulda@wopr Downloads]$ sudo ./tpm-vuln-checker check
TPM Manufacturer:               AMD
TPM Spec Revision:              1.38
TPM Family:                     2.0
TPM Type:                       dTPM

Starting TPM vulnerabilities checks.. This may take few seconds!

CVE 2023-1017/2023-1018:        Vulnerable
Please apply the latest BIOS update to update the TPM firmware. OEMs/ODMs ship TPM updates as part of BIOS updates.
CVE 2017-15361:                 Not Vulnerable
```

https://github.com/immune-gmbh/tpm-vuln-checker

What To Do?

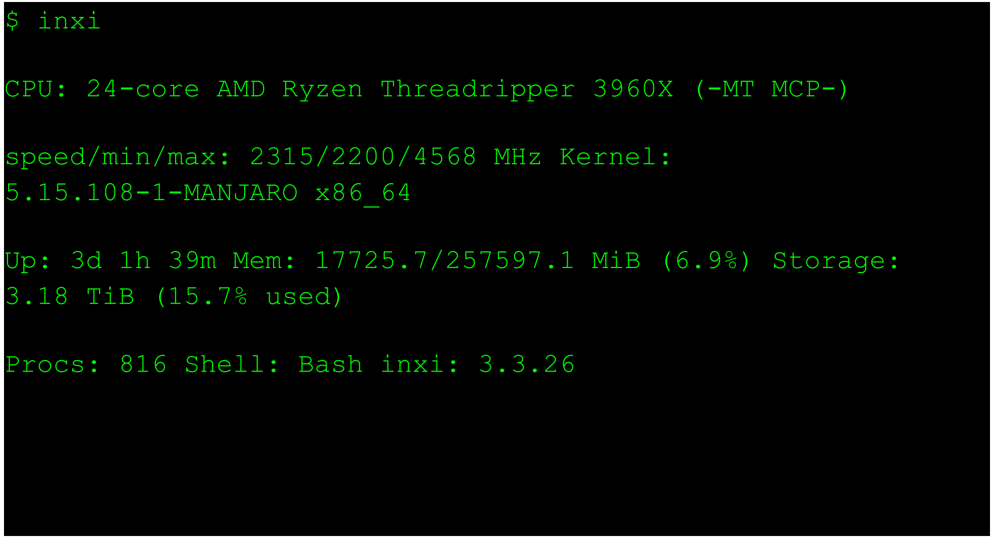


https://blog.quarkslab.com/vulnerabilities-in-the-tpm-20-reference-implementation-code.html



```
[paulda@gibsonsr ~]$ fwupdmgr get-devices
Framework Laptop (12th Gen Intel Core)
│
├─12th Gen Intel Core™ i7-1280P:
│     Device ID:          4bde70ba4e39b28f9eab1628f9dd6e6244c03027
│     Current version:    0x00000429
│     Vendor:             Intel
│     GUIDs:              b9a2dd81-159e-5537-a7db-e7101d164d3f ← cpu
│                         30249f37-d140-5d3e-9319-186b1bd5cac3 ← CPUID\PRO_0&FAM_06
│                         ab855c04-4ff6-54af-8a8a-d8193daa0cd8 ← CPUID\PRO_0&FAM_06&MOD_9A
│                         3ebbde86-d03e-549a-a8fd-02ebf9aa537a ← CPUID\PRO_0&FAM_06&MOD_9A&STP_3
│     Device Flags:       • Internal device
│
├─Alder Lake-P Integrated Graphics Controller:
│     Device ID:          5792b48846ce271fab11c4a545f7a3df0d36e00a
│     Current version:    0c
│     Vendor:             Intel Corporation (PCI:0x8086)
│     GUIDs:              eaad9970-8e4d-56da-88ab-41a8c1e2811f ← PCI\VEN_8086&DEV_46A6
│                         ed0b9458-c2f1-54c5-9063-dea8f75b4039 ← PCI\VEN_8086&DEV_46A6&REV_0C
│                         db02cc7b-e2bb-5004-919f-1ba0ad80000b ← PCI\VEN_8086&DEV_46A6&SUBSYS_F1110002
│                         5b4382cf-0f8e-59f0-a8af-458d33d9ee6d ← PCI\VEN_8086&DEV_46A6&SUBSYS_F1110002&REV_0C
│                         c4625510-a985-517c-8800-0ecfc6f68c8f ← PCI\VEN_8086&DEV_46A6&REV_00
│                         2dd4191d-63d6-522c-882c-40887f5ace4d ← PCI\VEN_8086&DEV_46A6&SUBSYS_F1110002&REV_00
│     Device Flags:       • Internal device
│                         • Cryptographic hash verification is available
│
├─Fingerprint Sensor:
│     Device ID:          4295296d98b3ba38c72f6baa33d24f03a1d428f6
│     Summary:            Match-On-Chip fingerprint sensor
│     Current version:    01000252
│     Vendor:             Goodix (USB:0x27C6)
│     Install Duration:   10 seconds
│     Serial Number:      UIDF1DBE326_XXXX_MOC_B0
│     GUIDs:              1e8c8470-a49c-571a-82fd-19c9fa32b8c3 ← USB\VID_27C6&PID_609C
│                         34def4c7-9461-5a32-a945-5dde0ca57d88 ← USB\VID_27C6&PID_609C&REV_0100
│     Device Flags:       • Updatable
│                         • Device can recover flash failures
│                         • Signed Payload
│
├─Internal SPI Controller:
│     Device ID:          b04e387fb80d2b91f37a4d0c7b21461c451775e1
│     Summary:            Memory Technology Device
│     Vendor:             DMI:Framework
│     GUIDs:              5f93d7e7-e282-59b9-b663-0146e382f8f6 ← MTD\NAME_0000:00:1f.5
│                         7eea5b8c-cc2e-5d22-bd2b-07417a8a7423 ← MTD\VENDOR_Framework&NAME_0000:00:1f.5
```

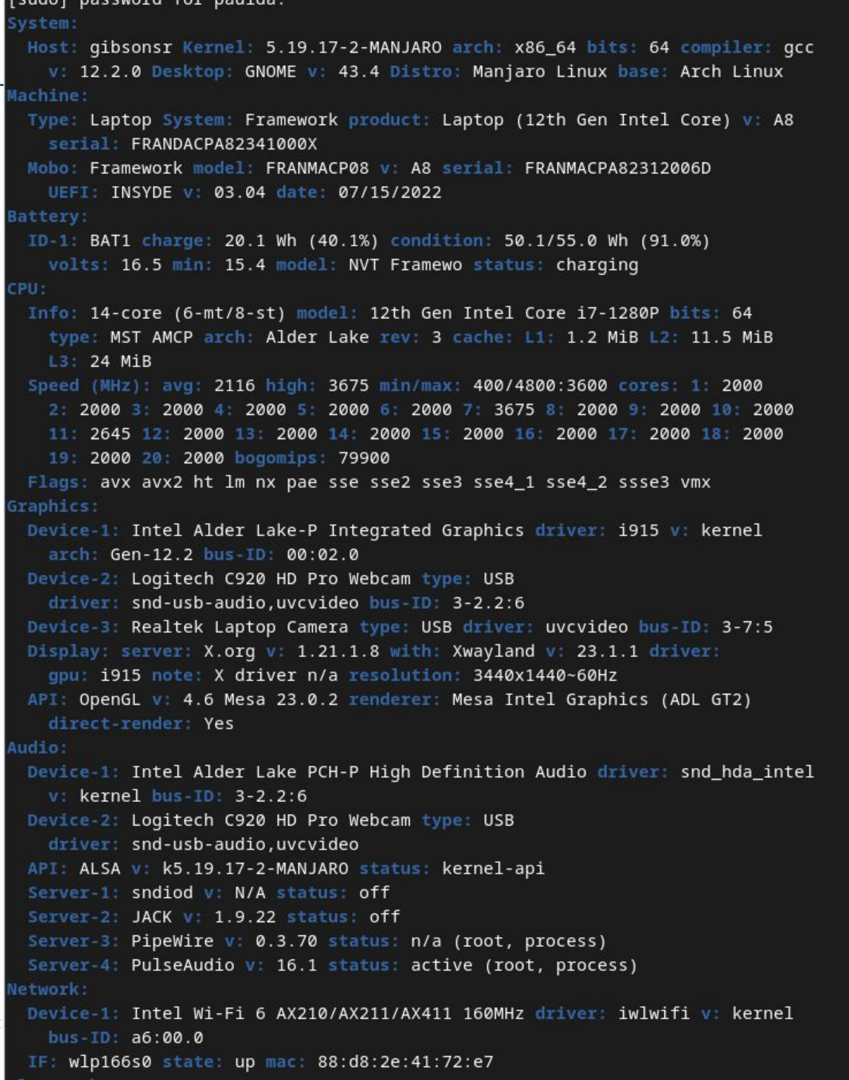
Which hardware do I have?



```
$ inxi

CPU: 24-core AMD Ryzen Threadripper 3960X (-MT MCP-)

speed/min/max: 2315/2200/4568 MHz Kernel:
5.15.108-1-MANJARO x86_64

Up: 3d 1h 39m Mem: 17725.7/257597.1 MiB (6.9%) Storage:
3.18 TiB (15.7% used)

Procs: 816 Shell: Bash inxi: 3.3.26
```

My HW may be around for a while.

https://github.com/smxi/inxi



```
[sudo] password for paulda:
System:
  Host: gibsonsr Kernel: 5.19.17-2-MANJARO arch: x86_64 bits: 64 compiler: gcc
    v: 12.2.0 Desktop: GNOME v: 43.4 Distro: Manjaro Linux base: Arch Linux
Machine:
  Type: Laptop System: Framework product: Laptop (12th Gen Intel Core) v: A8
    serial: FRANDACPA82341000X
  Mobo: Framework model: FRANMACP08 v: A8 serial: FRANMACPA82312006D
    UEFI: INSYDE v: 03.04 date: 07/15/2022
Battery:
  ID-1: BAT1 charge: 20.1 Wh (40.1%) condition: 50.1/55.0 Wh (91.0%)
    volts: 16.5 min: 15.4 model: NVT Framewo status: charging
CPU:
  Info: 14-core (6-mt/8-st) model: 12th Gen Intel Core i7-1280P bits: 64
    type: MST AMCP arch: Alder Lake rev: 3 cache: L1: 1.2 MiB L2: 11.5 MiB
    L3: 24 MiB
  Speed (MHz): avg: 2116 high: 3675 min/max: 400/4800:3600 cores: 1: 2000
    2: 2000 3: 2000 4: 2000 5: 2000 6: 2000 7: 3675 8: 2000 9: 2000 10: 2000
    11: 2645 12: 2000 13: 2000 14: 2000 15: 2000 16: 2000 17: 2000 18: 2000
    19: 2000 20: 2000 bogomips: 79900
  Flags: avx avx2 ht lm nx pae sse sse2 sse3 sse4_1 sse4_2 ssse3 vmx
Graphics:
  Device-1: Intel Alder Lake-P Integrated Graphics driver: i915 v: kernel
    arch: Gen-12.2 bus-ID: 00:02.0
  Device-2: Logitech C920 HD Pro Webcam type: USB
    driver: snd-usb-audio,uvcvideo bus-ID: 3-2.2:6
  Device-3: Realtek Laptop Camera type: USB driver: uvcvideo bus-ID: 3-7:5
  Display: server: X.org v: 1.21.1.8 with: Xwayland v: 23.1.1 driver:
    gpu: i915 note: X driver n/a resolution: 3440x1440~60Hz
  API: OpenGL v: 4.6 Mesa 23.0.2 renderer: Mesa Intel Graphics (ADL GT2)
    direct-render: Yes
Audio:
  Device-1: Intel Alder Lake PCH-P High Definition Audio driver: snd_hda_intel
    v: kernel bus-ID: 3-2.2:6
  Device-2: Logitech C920 HD Pro Webcam type: USB
    driver: snd-usb-audio,uvcvideo
  API: ALSA v: k5.19.17-2-MANJARO status: kernel-api
  Server-1: sndiod v: N/A status: off
  Server-2: JACK v: 1.9.22 status: off
  Server-3: PipeWire v: 0.3.70 status: n/a (root, process)
  Server-4: PulseAudio v: 16.1 status: active (root, process)
Network:
  Device-1: Intel Wi-Fi 6 AX210/AX211/AX411 160MHz driver: iwlwifi v: kernel
    bus-ID: a6:00.0
  IF: wlp166s0 state: up mac: 88:d8:2e:41:72:e7
```

PHYSICAL

“Hunting for backdoors in Counterfeit Cisco devices”

PRE-INSTALLED

CPU BIOS/UEFI ME/AMT

BMC NIC Storage

Components

Firmware

Bootloaders

Kernels

Operating Systems

3RD-PARTY APPLICATIONS

slack zoom

Ps

W P

SOFTWARE DEVELOPED IN-HOUSE

python™ Package Index

npm

docker

MSI Breach and the Supply Chain

- Ransomware operator known as Money Message has ~~***likely***~~ stolen 1.5TB of data including MSI source code, BIOS development framework, and private keys needed to sign modules.

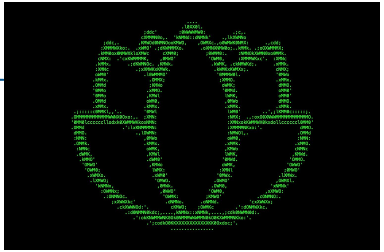
- Attackers will be able to **develop malicious UEFI firmware, insert backdoors into source code, or compromise infrastructure** used by many people around the world.

- The extreme risk already present on MSI systems due to a **lack of signatures on updates**. Without these signatures, enterprises and consumers have no way to verify known-good firmware binaries before installing them, creating a scenario ripe for abuse by any supply chain attacker.

https://eclypsium.com/blog/analyzing-your-risk-from-the-msi-breach/

https://eclypsium.com/blog/msi-incident-part-2-binary-analysis/

Black Lotus

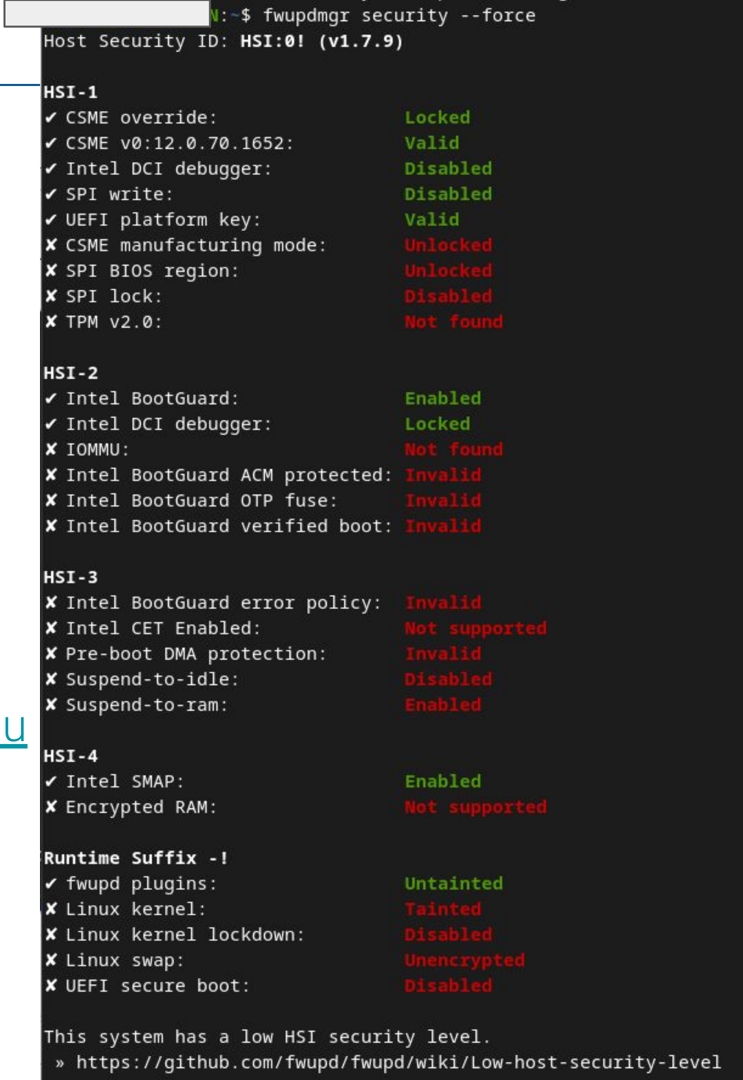


- News in late 2022 of a new UEFI bootkit being sold for $5,000 on hacking forums called BlackLotus.
- The rootkit bypasses UEFI Secure Boot by exploiting a vulnerability in the Windows bootloader (CVE-2022-21894, AKA “Baton Drop”).
- An attacker with administrator privileges (and the ability to bypass UAC) can install an older, still-vulnerable boot manager version.
- With the vulnerable code in place, the attacker can install a signing key using the same MOK/Shim toolset used to enable UEFI Secure Boot on Linux. This allows boot-time persistence for a payload that alters the Windows kernel behavior, disabling multiple security protections

https://eclypsium.com/blog/blacklotus-a-threat-coming-to-a-system-near-you/

FWUPD and LVFS

- LVFS - Vendors submit firmware updates
- Fwupd - Linux software package to check and update firmware
- It’s free and open-source software
- I interviewed the maintainer of this project, Richard Hughes here: https://eclypsium.com/podcasts/bts-8-richard-hughes/



```
[redacted]N:~$ fwupdmgr security --force
Host Security ID: HSI:0! (v1.7.9)

HSI-1
✔ CSME override:                 Locked
✔ CSME v0:12.0.70.1652:          Valid
✔ Intel DCI debugger:            Disabled
✔ SPI write:                     Disabled
✔ UEFI platform key:             Valid
✘ CSME manufacturing mode:       Unlocked
✘ SPI BIOS region:               Unlocked
✘ SPI lock:                      Disabled
✘ TPM v2.0:                      Not found

HSI-2
✔ Intel BootGuard:               Enabled
✔ Intel DCI debugger:            Locked
✘ IOMMU:                         Not found
✘ Intel BootGuard ACM protected: Invalid
✘ Intel BootGuard OTP fuse:      Invalid
✘ Intel BootGuard verified boot: Invalid

HSI-3
✘ Intel BootGuard error policy:  Invalid
✘ Intel CET Enabled:             Not supported
✘ Pre-boot DMA protection:       Invalid
✘ Suspend-to-idle:               Disabled
✘ Suspend-to-ram:                Enabled

HSI-4
✔ Intel SMAP:                    Enabled
✘ Encrypted RAM:                 Not supported

Runtime Suffix -!
✔ fwupd plugins:                 Untainted
✘ Linux kernel:                  Tainted
✘ Linux kernel lockdown:         Disabled
✘ Linux swap:                    Unencrypted
✘ UEFI secure boot:              Disabled

This system has a low HSI security level.
 » https://github.com/fwupd/fwupd/wiki/Low-host-security-level
```

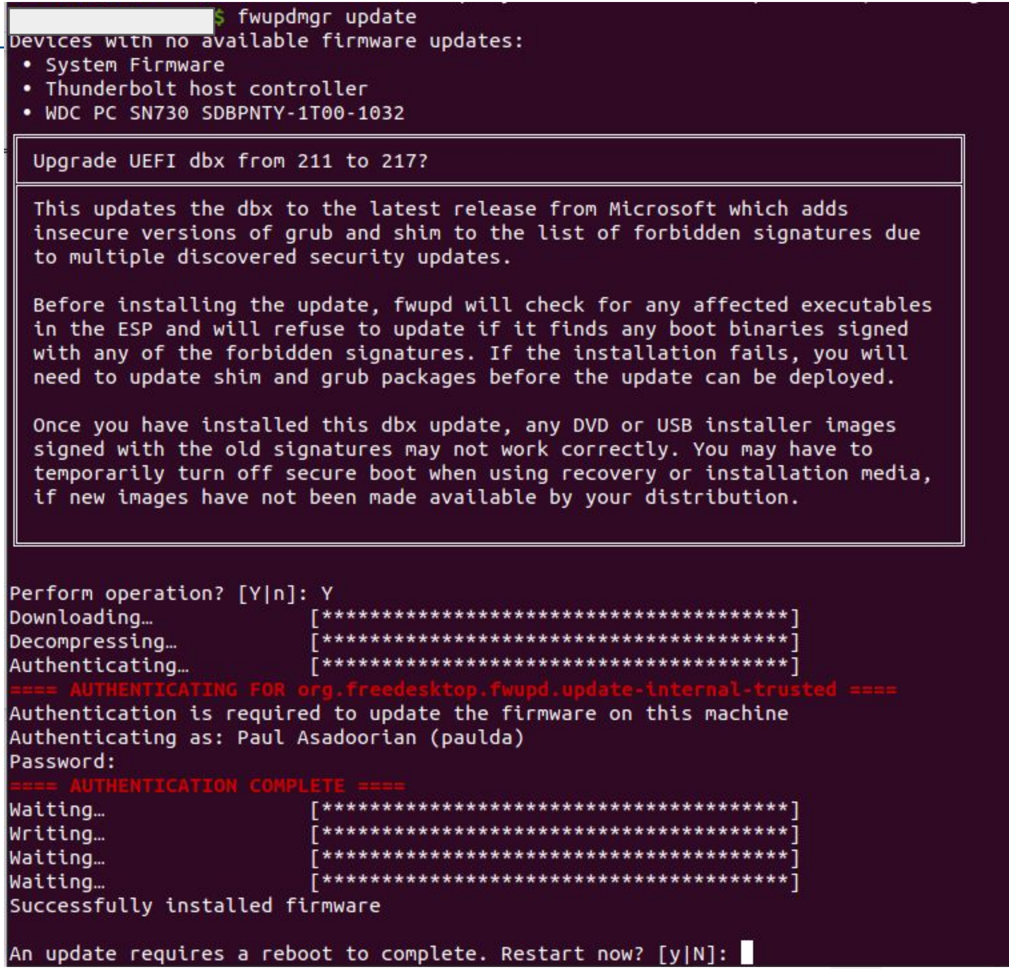
Secure Boot

- You should enable it

- You should also keep the DBX up-to-date

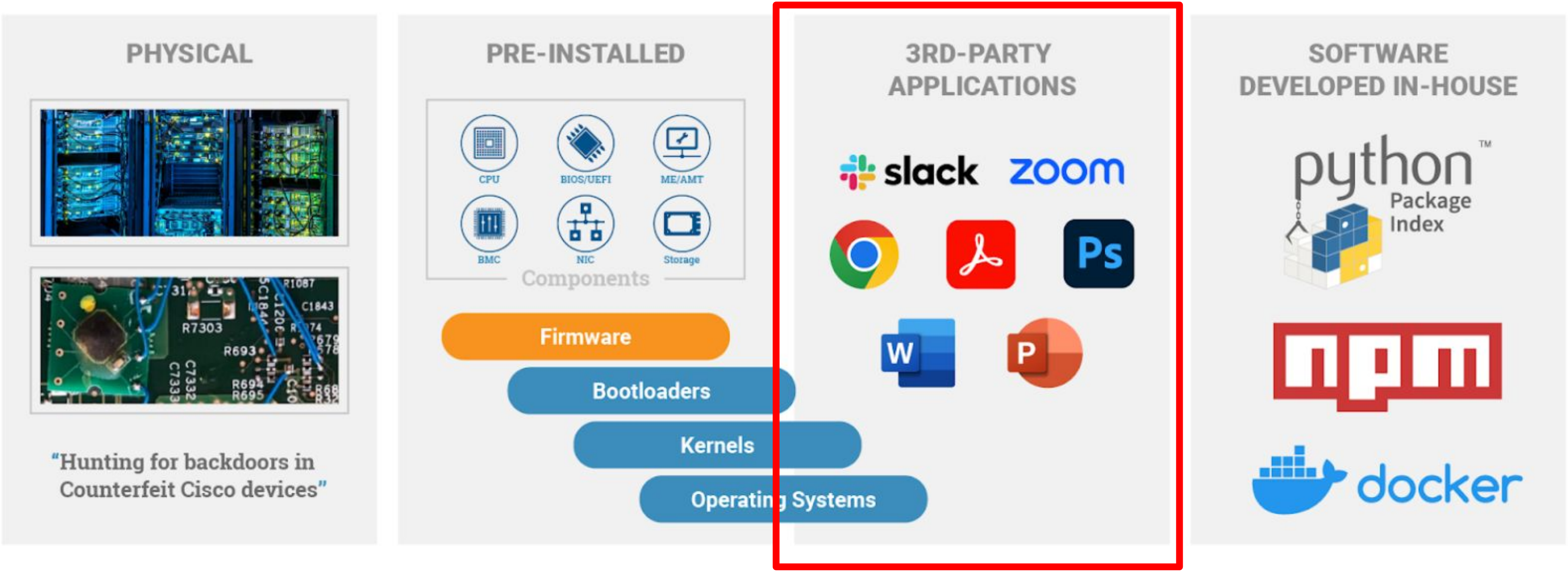
- Fwupd can detect dangerous situations (e.g. a DBX update that includes a hash for the existing bootloader)

- https://twitter.com/esetresearch/status/1641008260487471106 - Vulnerable UEFI binaries Revoked in August 2022 DBX update were revoked incorrectly



```
[redacted]$ fwupdmgr update
Devices with no available firmware updates:
 • System Firmware
 • Thunderbolt host controller
 • WDC PC SN730 SDBPNTY-1T00-1032
╔══════════════════════════════════════════════════════════════════════════════╗
║ Upgrade UEFI dbx from 211 to 217?                                            ║
╠══════════════════════════════════════════════════════════════════════════════╣
║ This updates the dbx to the latest release from Microsoft which adds         ║
║ insecure versions of grub and shim to the list of forbidden signatures due   ║
║ to multiple discovered security updates.                                     ║
║                                                                              ║
║ Before installing the update, fwupd will check for any affected executables  ║
║ in the ESP and will refuse to update if it finds any boot binaries signed    ║
║ with any of the forbidden signatures. If the installation fails, you will    ║
║ need to update shim and grub packages before the update can be deployed.     ║
║                                                                              ║
║ Once you have installed this dbx update, any DVD or USB installer images     ║
║ signed with the old signatures may not work correctly. You may have to       ║
║ temporarily turn off secure boot when using recovery or installation media,  ║
║ if new images have not been made available by your distribution.             ║
║                                                                              ║
╚══════════════════════════════════════════════════════════════════════════════╝

Perform operation? [Y|n]: Y
Downloading…             [***************************************]
Decompressing…           [***************************************]
Authenticating…          [***************************************]
==== AUTHENTICATING FOR org.freedesktop.fwupd.update-internal-trusted ====
Authentication is required to update the firmware on this machine
Authenticating as: Paul Asadoorian (paulda)
Password:
==== AUTHENTICATION COMPLETE ====
Waiting…                 [***************************************]
Writing…                 [***************************************]
Waiting…                 [***************************************]
Waiting…                 [***************************************]
Successfully installed firmware

An update requires a reboot to complete. Restart now? [y|N]:
```

NPM



PHYSICAL

“Hunting for backdoors in Counterfeit Cisco devices”

PRE-INSTALLED

Components

Firmware

Bootloaders

Kernels

Operating Systems

3RD-PARTY APPLICATIONS

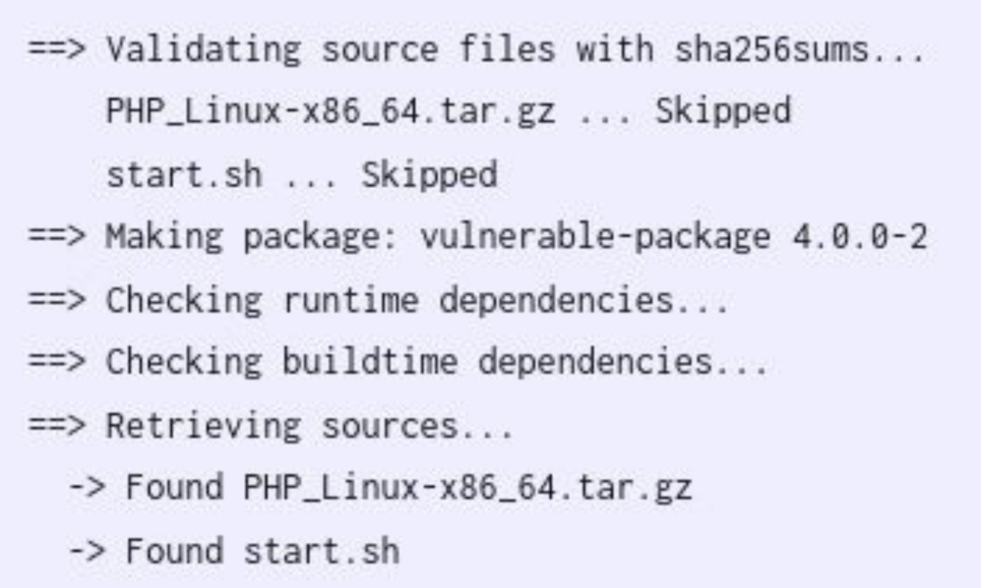
SOFTWARE DEVELOPED IN-HOUSE

3CX

- This was a nested supply chain attack - Trading Technologies X_TRADER -> 3CX build systems where 3CX was backdoored
- Attackers exploited old bugs (https://www.bleepingcomputer.com/news/microsoft/10-year-old-windows-bug-with-opt-in-fix-exploited-in-3cx-attack/) allowing them to bypass code signing.
- The vendor handled the situation very poorly
- We still do not know the extent of the damages

A Linux Example

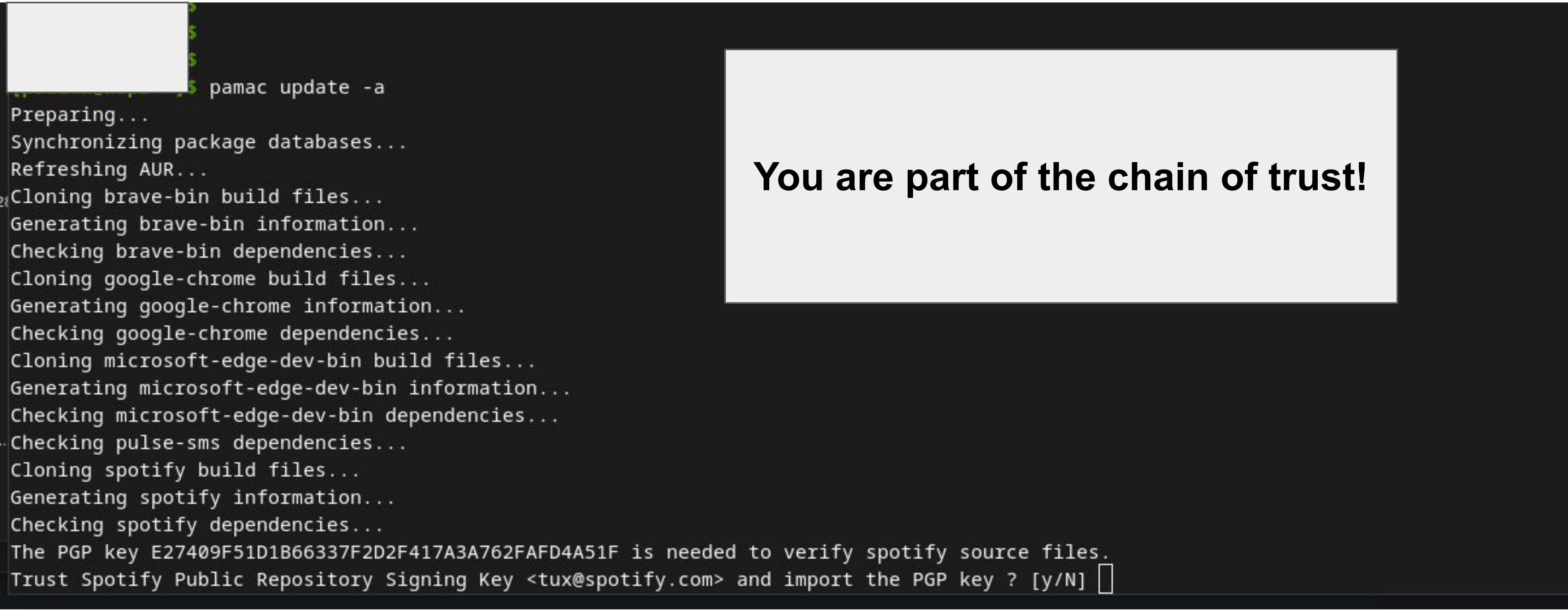
- The Arch team is working to make this better
- Package maintainers in AUR can select which files are validated and which ones are not
- Pay attention when you are updating systems!



```
==> Validating source files with sha256sums...
    PHP_Linux-x86_64.tar.gz ... Skipped
    start.sh ... Skipped
==> Making package: vulnerable-package 4.0.0-2
==> Checking runtime dependencies...
==> Checking buildtime dependencies...
==> Retrieving sources...
  -> Found PHP_Linux-x86_64.tar.gz
  -> Found start.sh
```

https://blog.nietaanraken.nl/posts/aur-packages-expired-domains/

Verify Then Trust



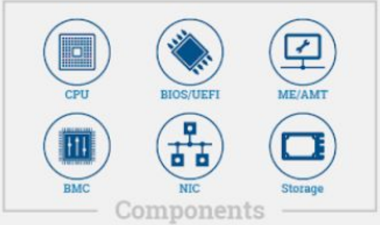
```
[redacted]$
$
$
$ pamac update -a
Preparing...
Synchronizing package databases...
Refreshing AUR...
Cloning brave-bin build files...
Generating brave-bin information...
Checking brave-bin dependencies...
Cloning google-chrome build files...
Generating google-chrome information...
Checking google-chrome dependencies...
Cloning microsoft-edge-dev-bin build files...
Generating microsoft-edge-dev-bin information...
Checking microsoft-edge-dev-bin dependencies...
Checking pulse-sms dependencies...
Cloning spotify build files...
Generating spotify information...
Checking spotify dependencies...
The PGP key E27409F51D1B66337F2D2F417A3A762FAFD4A51F is needed to verify spotify source files.
Trust Spotify Public Repository Signing Key <tux@spotify.com> and import the PGP key ? [y/N]
```

You are part of the chain of trust!

PHYSICAL

“Hunting for backdoors in Counterfeit Cisco devices”

PRE-INSTALLED



Firmware

Bootloaders

Kernels

Operating Systems

3RD-PARTY APPLICATIONS

slack zoom

SOFTWARE DEVELOPED IN-HOUSE

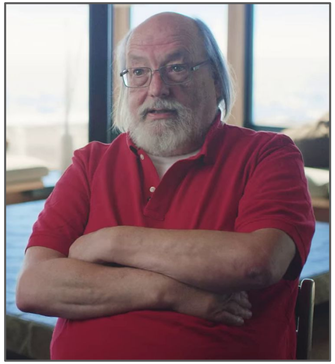
python™ Package Index

npm

docker

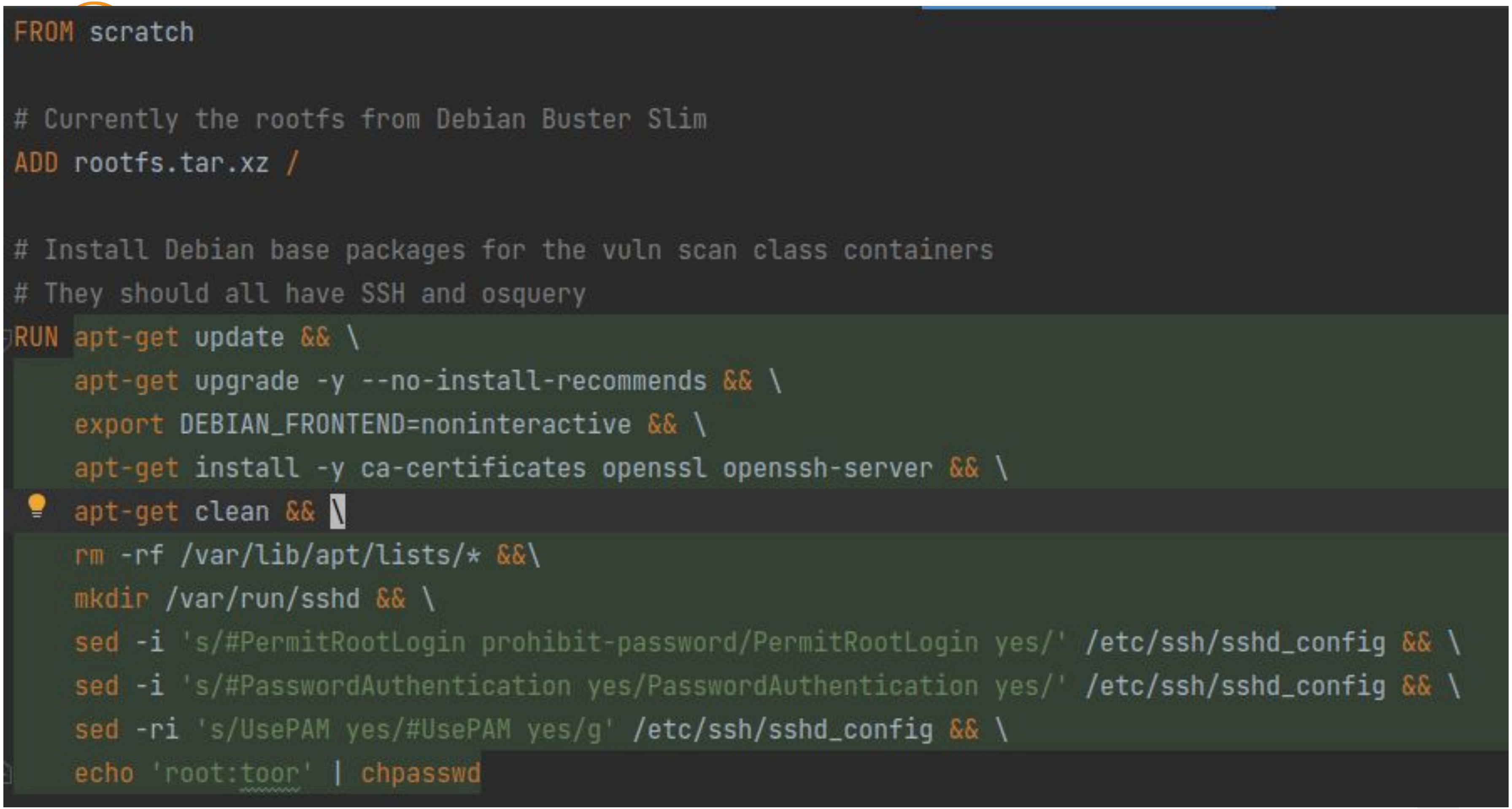
“You can't trust code that you did not totally create yourself.”

“No amount of source-level verification or scrutiny will protect you from using untrusted code.”



“Reflections on Trusting Trust” - Ken Thompson, August 1984, Volume 27 Number 8, Communications of the ACM

https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf

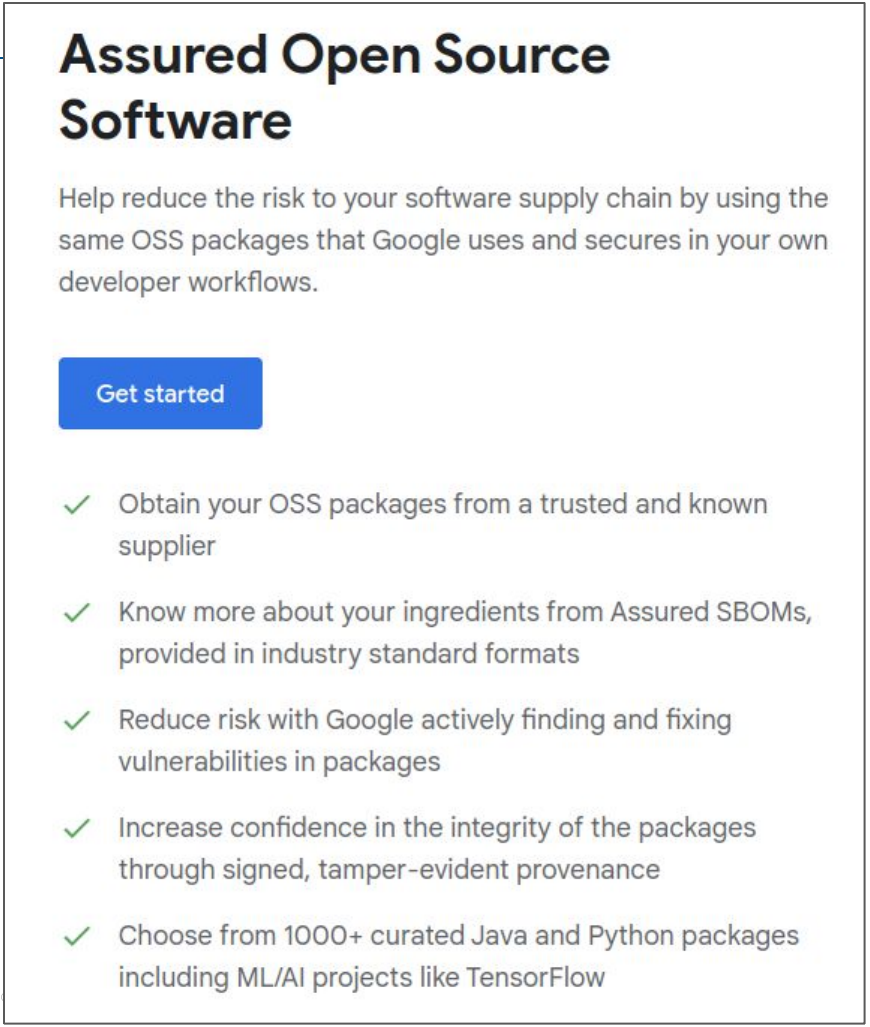


```
FROM scratch

# Currently the rootfs from Debian Buster Slim
ADD rootfs.tar.xz /

# Install Debian base packages for the vuln scan class containers
# They should all have SSH and osquery
RUN apt-get update && \
    apt-get upgrade -y --no-install-recommends && \
    export DEBIAN_FRONTEND=noninteractive && \
    apt-get install -y ca-certificates openssl openssh-server && \
    apt-get clean && \
    rm -rf /var/lib/apt/lists/* &&\
    mkdir /var/run/sshd && \
    sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config && \
    sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config && \
    sed -ri 's/UsePAM yes/#UsePAM yes/g' /etc/ssh/sshd_config && \
    echo 'root:toor' | chpasswd
```

Use The Google?

- Only Java and Python (For now)
- SBOMs - SPDX and VEX
- Verifiable SLSA (Supply Chain Levels for Software Artifacts) compliance

https://cloud.google.com/assured-open-source-software



Assured Open Source Software

Help reduce the risk to your software supply chain by using the same OSS packages that Google uses and secures in your own developer workflows.

✓ Obtain your OSS packages from a trusted and known supplier

✓ Know more about your ingredients from Assured SBOMs, provided in industry standard formats

✓ Reduce risk with Google actively finding and fixing vulnerabilities in packages

✓ Increase confidence in the integrity of the packages through signed, tamper-evident provenance

✓ Choose from 1000+ curated Java and Python packages including ML/AI projects like TensorFlow

Conclusions

In the areas of hardware, firmware, 3rd party software and application software - Develop a strategy and plans for validating the supply chain

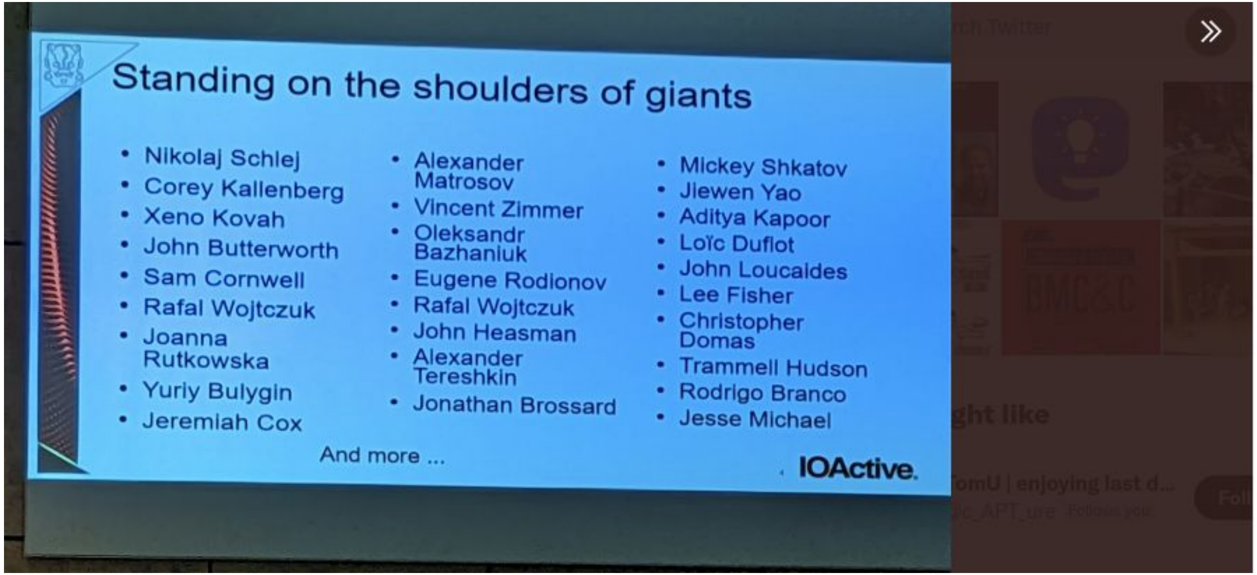
Monitor for changes - Look for changes in BMC firmware, UEFI, bootloaders and kernel drivers - If they happen independent of a known update, something is wrong.

Compare SBOMs - Continuously verify and validate firmware and software. Has it changed? Does it match what is intended to be installed?

Huge Thanks!

My Co-workers: Alex Bazhaniuk, Yuriy Bulygin, John Loucaides, Federico “Fede” Perez, Mickey Shkatov, Jesse Michael, Vladyslav Babkin, Nate Warfield and more!

About Me: Podcast host for Paul’s Security Weekly (https://securityweekly.com), Principal Security Evangelist for Eclypsium, and Eclypsium Podcast host (new!)

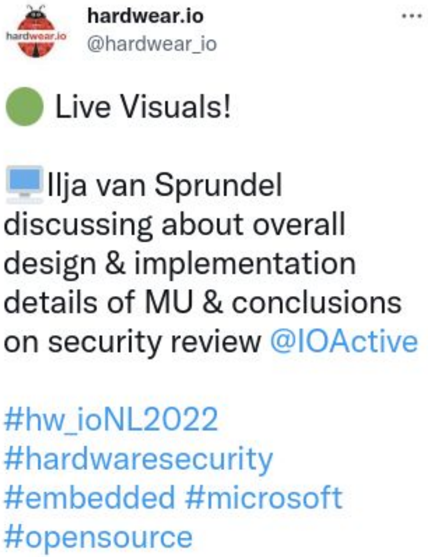


Standing on the shoulders of giants

- Nikolaj Schlej
- Corey Kallenberg
- Xeno Kovah
- John Butterworth
- Sam Cornwell
- Rafal Wojtczuk
- Joanna Rutkowska
- Yuriy Bulygin
- Jeremiah Cox
- Alexander Matrosov
- Vincent Zimmer
- Oleksandr Bazhaniuk
- Eugene Rodionov
- Rafal Wojtczuk
- John Heasman
- Alexander Tereshkin
- Jonathan Brossard
- Mickey Shkatov
- Jiewen Yao
- Aditya Kapoor
- Loïc Duflot
- John Loucaides
- Lee Fisher
- Christopher Domas
- Trammell Hudson
- Rodrigo Branco
- Jesse Michael

And more ...

IOActive.



hardwear.io
@hardwear_io

🟢 Live Visuals!

💻Ilja van Sprundel discussing about overall design & implementation details of MU & conclusions on security review @IOActive

#hw_ioNL2022 #hardwaresecurity #embedded #microsoft #opensource

Resources

Firmware Enumeration with Open Source Tools (Video/Webinar)

BHIS | Firmware Enumeration Using Open Source Tools | Paul Asadoorian | 1-Hour (Video/Webinar)

Firmware Security Realizations – Part 1 – Secure Boot And Dbx (Blog post)

Firmware Security Realizations – Part 2 – Start Your Management Engine (Blog Post)

Firmware Security Realizations – Part 3 – Spi Write Protections (Blog Post)

UEFI & SMM Vulnerabilities - Jesse Michael - PSW #764 (Video/Podcast)

Not-So-Secure Boot - Jesse Michael, Mickey Shkatov - PSW #751 (Video/Podcast)