Systems 3

OS Security

Marcel Waldvogel

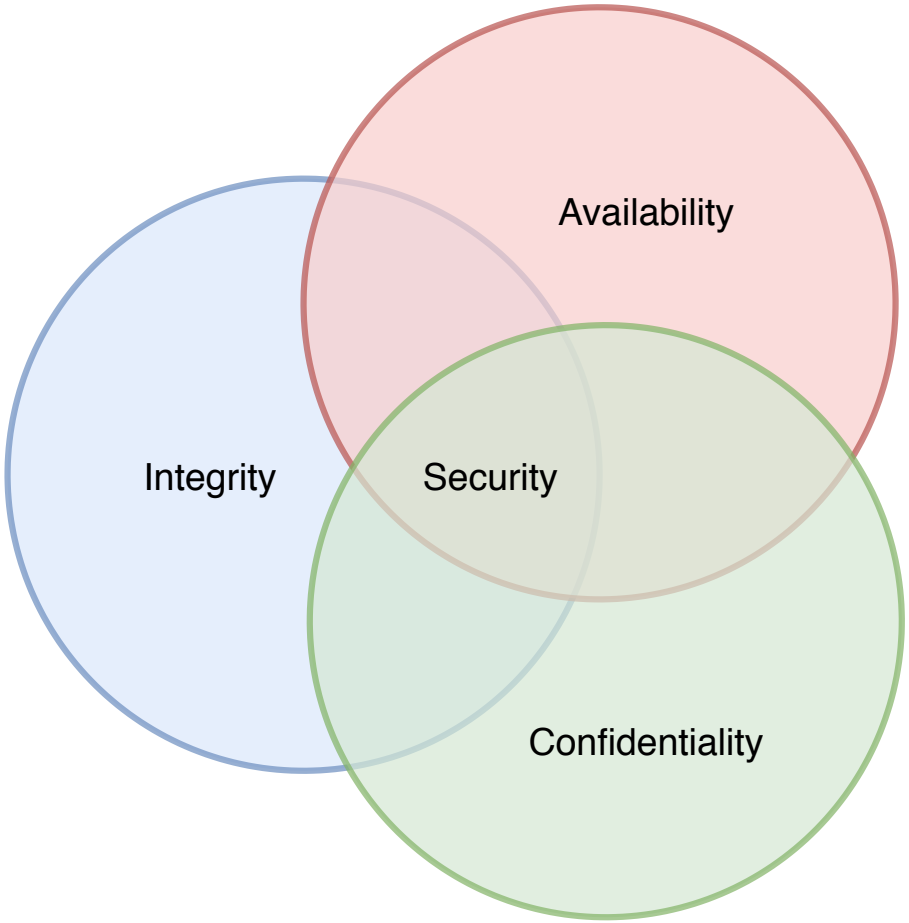
(Handout)

Department of Computer and Information Science
University of Konstanz

Winter 2019/2020

Chapter Goals

Security



Attacks

- Passive
  - Wiretapping
  - Keystroke logging
  - Data harvesting
- Active
  - Denial-of-service
  - Spoofing
  - Man-in-the-middle
  - Ping flood
- Malware
  - Virus
  - Ransomware
  - Trojan horse
  - Worm

Hardware

- Vendor and governments trustworthy?
- Produced in poor countries
- Verification
- Complex
- Many parts
- Firmware

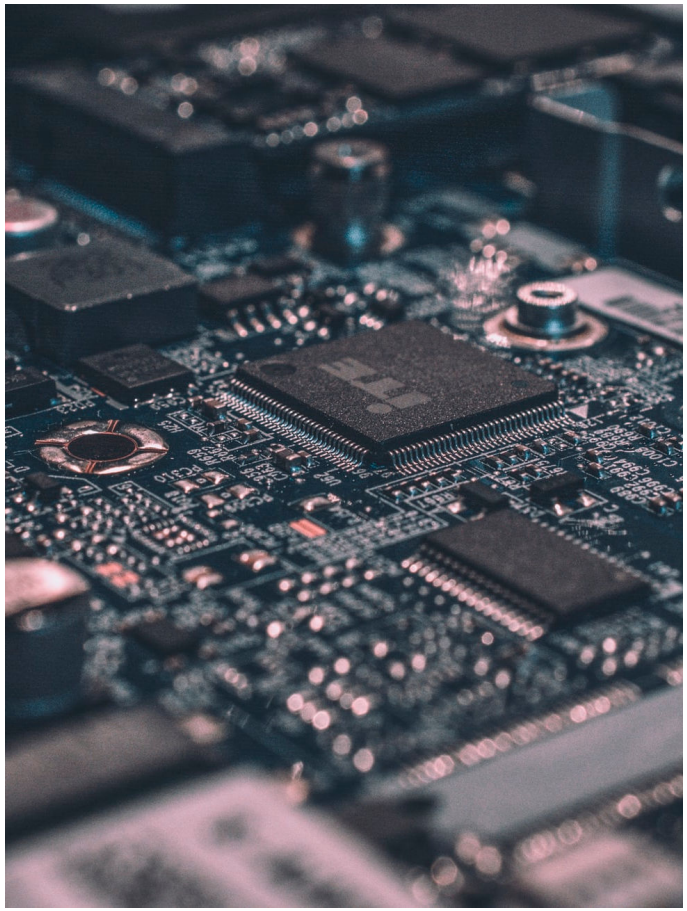


Photo by Alexandre Debiève (Unsplash license)

Randomness

- Keystone in encryption
- Non-trivial task
- Embedded devices
- CSPRNG
- Verifiable?

Photo by Riho Kroll
(Unsplash license)

Trusted Platform Module (TPM)

- International standard
- Random number generator
- Platform integrity
- Generation of cryptographic keys
- Disk encryption

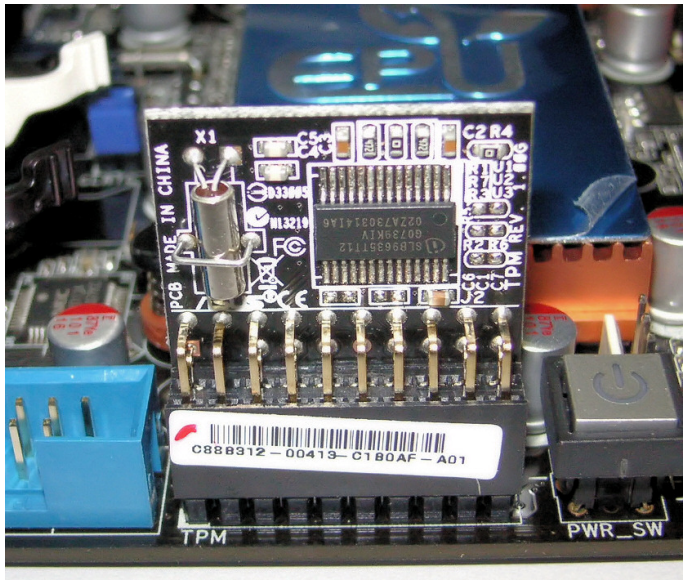


Photo by FxJ (Public Domain)

Smartphones

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft

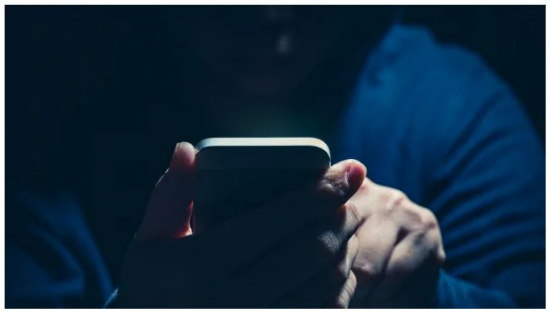
TOPTHEMEN: CES EMOTET QUANTENCOMPUTER E-AUTO WINDOWS 10 RASPI

Security 〉 7-Tage-News 〉 01/2020 〉 US-gefördertes Handy kommt mit Malware aus China

US-gefördertes Handy kommt mit Malware aus China

Ein subventionierter Mobilfunkdienst für arme US-Amerikaner verkauft ein billiges Smartphone. Es enthält Malware ab Werk.

Lesezeit: 1 Min. In Pocket speichern 221



(Bild: Shutterstock.com / weedezign)

12.01.2020 11:52 Uhr | Security

Von Daniel AJ Sokolov

Das chinesische Billig-Smartphone UMX U683CL von Unimax Communications kommt bereits mit Malware in den Handel, die sich nicht entfernen lässt. Verkauft wird dieses Modell von Assurance Wireless, einer Tochterfirma des US-Mobilfunkers Sprint. Assurance Wireless ist ein Angebot an arme US-Amerikaner, das über einen Fonds der Regulierungsbehörde FCC subventioniert wird. Für diese Kunden ist es finanziell eine besondere Belastung, sich ein neues Handy kaufen zu müssen.

Published 2020-01-12 on heise.de
(retrieved on 2020-01-15)

1,442,396 views | Aug 10, 2019, 06:39am

Google Warning: Tens Of Millions Of Android Phones Come Preloaded With Dangerous Malware

Zak Doffman Contributor ⓘ
Cybersecurity
I write about security and surveillance.

GETTY

Millions of shiny new Android smartphones are being purchased with dangerous malware factory-installed, according to Google's own security research team. There have been multiple headlines about the millions of harmful apps being installed from the Play Store, but this is something new. And the danger to unsuspecting users, trusting that new boxed devices are safe and clean, is that some of that preinstalled malware can download other malware in the background, commit ad fraud, or even take over its host device.

Published 2019-08-10 on forbes.com
(retrieved on 2020-01-15)

Spy Chips

ANDY GREENBERG SECURITY 10.10.2019 11:07 AM

Planting Tiny Spy Chips in Hardware Can Cost as Little as $200

A new proof-of-concept hardware implant shows how easy it may be to hide malicious chips inside IT equipment.

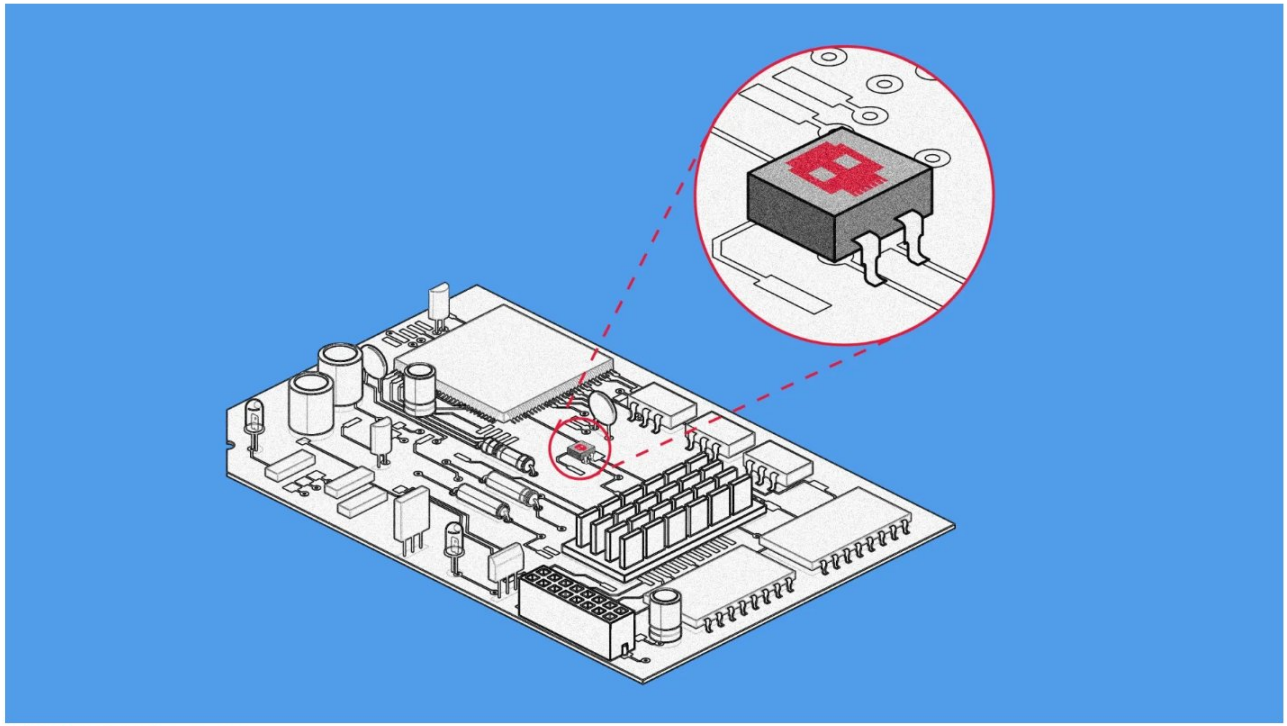


ILLUSTRATION: CASEY CHIN; GETTY IMAGES

More than a year has passed since *Bloomberg Businessweek* grabbed the lapels of the cybersecurity world with a bombshell claim: that Supermicro motherboards in servers used by major tech firms, including Apple and Amazon, had been stealthily implanted with a chip the size of a rice grain that allowed Chinese hackers to spy deep into those networks. Apple

Published 2019-10-10 on wired.com (retrieved on 2020-01-15)

Physical Attack

- Lock the server room
- Set up surveillance
- Protect network devices
- Protect workstations
- Secure chassis
- Protect mobile devices
- Use a safe for your backup
- Prevent data skimming
- Protect your printers

Photo by Annie Gray (Unsplash license)

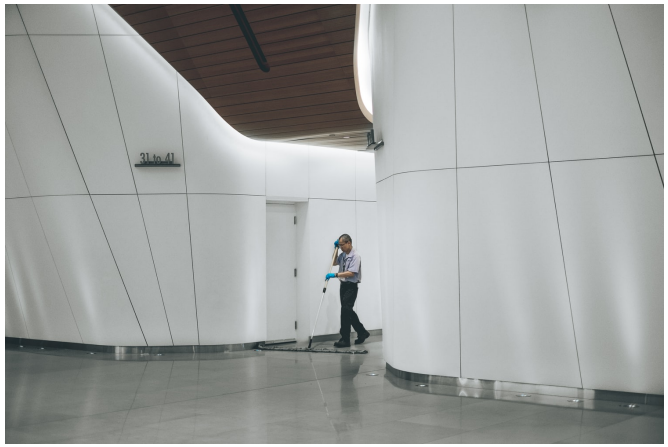


Photo by Verne Ho (Unsplash license)

Software

- Can you write all software by your own? No!
- Can you verify every program? No!

Question: How can you make sure that you will not install any malicious software on your device?

"To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software."[1]

[1] Ken Thompson. Reflections on Trusting Trust. Communications of the ACM 27(8):761–763. August 1984.

Verifiable builds

Even if the source code is publicly available and verifiable, most people will not compile a program from source. How can you make sure that the binary does not contain any backdoor?

Example based on Truecrypt[2]: Challenges and Implications of Verifiable Builds for Security-Critical Open-Source Software.

BTW: Who verifies the correctness of your compiler?

[2] Beware that Truecrypt is no longer maintained. Use veracrypt instead.

Verifiable web applications

Web applications are a security and privacy nightmare, because they

- are volatile
- contain a lot of third-party code
- often require external services
- can be different for every visitor

Hint

You can block most internet advertisements in your network with Pi-hole©

Access control

From the Cambridge Dictionary:

Identification the act of recognizing and naming someone or something

Authentication to prove that something is real, true, or what people say it is[3]

Authorization official permission for something to happen, or the act of giving someone official permission to do something[4]

[3] Can be done via something you know/have/are. There should be always a second factor.

[4] Always check if the authentication result is still valid.

Software updates

Even if software updates are sometimes rough, there is no other way to keep your software secure.[5]

Apropos

Are you still running Windows 7 or Windows Server 2008?

[5] Also printers, faxes(!), IoT devices, ...

Privilege escalation

Privilege escalation is the act of getting access to resources that are normally protected from the user.

- Vertical
  - Cross-zone scripting
  - Jailbreaking
  - ...
- Horizontal
  - former throwaway mail address system at Uni Konstanz
  - Session hijacking
  - Cross-site scripting
  - Password guessing
  - ...

Mitigation strategies

ASLR, Data Execution Prevention, dedicated users, code signing, mandatory access control (e.g. SELinux)

Clean memory

Assume you write an application like `ssh-agent(1)` which handles confidential data. Where is this information stored?

Answer: In memory. Therefore always keep your memory clean and deliberate which data you have to keep in storage.

Not that easy as a study showed: Password Managers: Under the Hood of Secrets Management.

Question: Is your data only stored in RAM?

mlock(2)

As a result of paging, your data will probably also copied to some persistent storage.

- You have no control how long the data will be there
- Even after your machine is off, the data could be readable

To mitigate this issue, you should use mlock(2).

Cold boot attack

Photo by Although (Public Domain)

Heartbleed

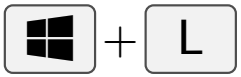
- Buffer over-read in OpenSSL
- "Undiscovered" for 2 years
- At least 66% of all web servers used OpenSSL[6]
- Estimated costs of $500 million[7]

Lesson learned

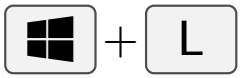
Testing, risk analysis, two developers are not enough

[6] Combined market share of Apache and nginx.
[7] eweek.com

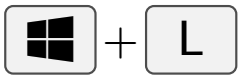
Lock your machine

Always lock your device! 

Let's do it.



Once again.



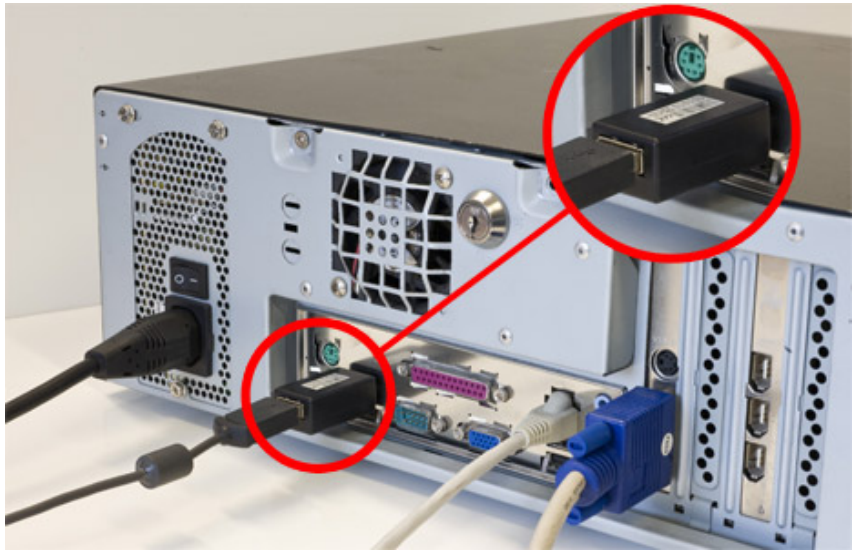
Password policy

- Never ever use the same password for multiple services!
- Passwords should be as long as possible
- Passwords should not contain words
- Just bang your fingers against your keyboard
- Or use `pwgen 20`
- Use a password manager (dedicated or browser based)

Check if your password was compromised:
https://haveibeenpwned.com/Passwords

Side-channel

- key logger
- timing attack
- electromagnetic attack
- acoustic cryptanalysis
- cameras
- shoulder surfing



kingston.ac.uk (CC BY-SA 4.0)

Social engineering

- blackmail
- money 💵 💵 💵 💵
- most of the time just call or visit in a nice suit
- forged mail address or phone number
- leaked information

Counter-measures

- physical access control and badges
- staff training
- guidelines (e.g., verify and call back)

Third-party devices

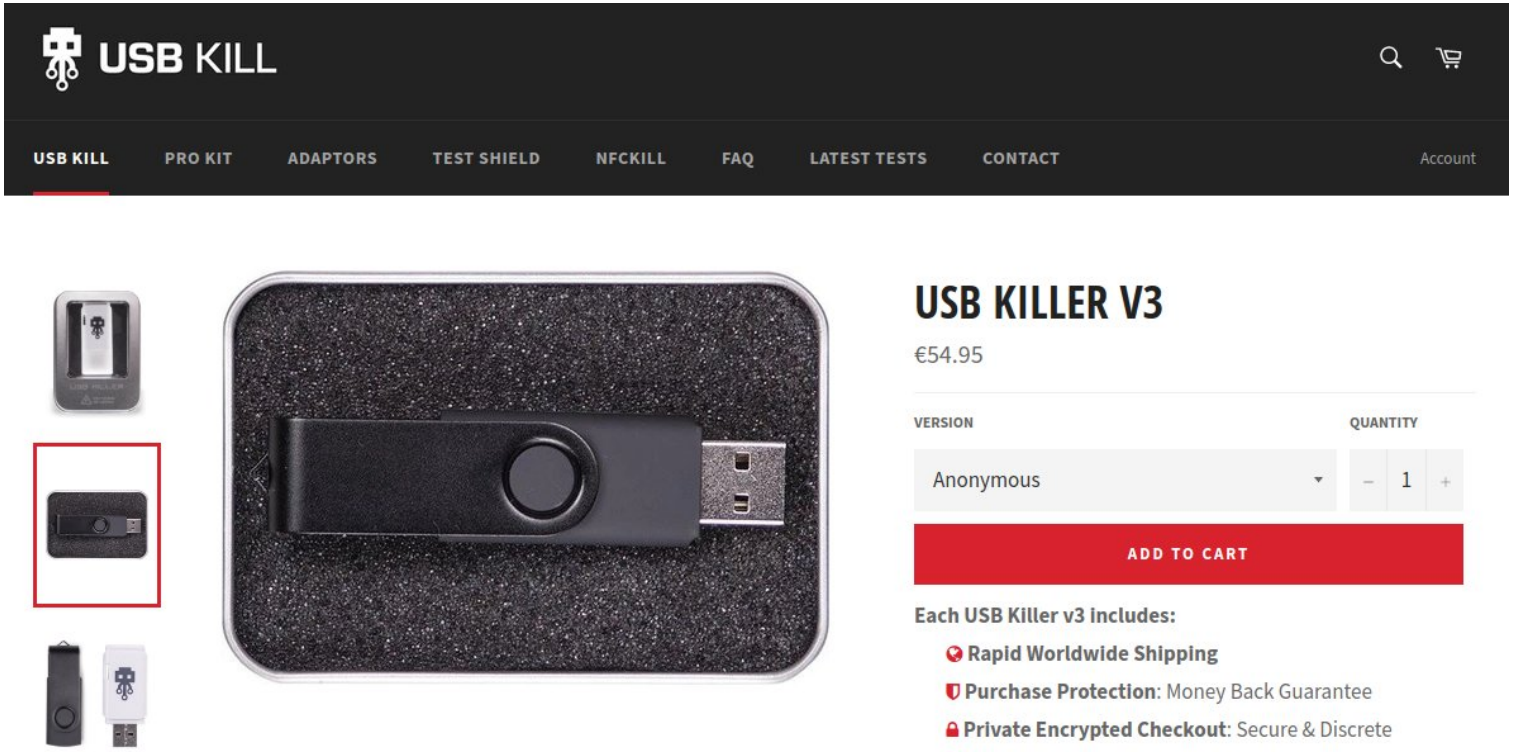
What are you doing if you find a USB stick on the ground?

Photo by Sara Kurfeß (Unsplash license)

Do not insert it into your PC!

Nice presentation from Blackhat 2016: What are malicious usb keys and how to create a realistic one?

Third-party devices



https://usbkill.com/products/usb-killer-v3 (visited 2020-01-16)

Disposal of hardware

There is a bunch of devices which hold important data: HDD, SSD, printer, mobile phone, ...

- Format (ouch!)
- Overwrite (does not work for SSD, printer, mobile phone)
- Destroy (expensive)

There is a better solution on the next slide which also protects against theft and loss.

Full disk encryption

You should use full disk encryption on every device.

- Linux: available for every device (super easy on Ubuntu)
- MacOS: available for every device (FileVault)
- Windows: only available for the Professional edition (or third-party)
- Android: Settings » Security » Encrypt phone or default
- iOS: encryption by default

What should you do after a security incident?

- Create emergency plans beforehand (identifying risks, protection goals, action plans)
- Monitoring and detection
- Prevent spread
- Forensics
- Junk/reinstall all affected devices
- Restore your backup (data only, with care!)
- Inform affected users

No easy task, see IT-Grundschutz-Kompendium (german).

Current example: University Gießen.