# **Information Security:** Concepts, Terminology and Real-world Cases

Antti Hietaniemi & Markku Reunanen
ARTX-C1013 Thematic Studio II

# Outline

Definition

Warming up

Technically oriented challenges

Human factors

Conclusion

Readings and links

# What *is* information security?

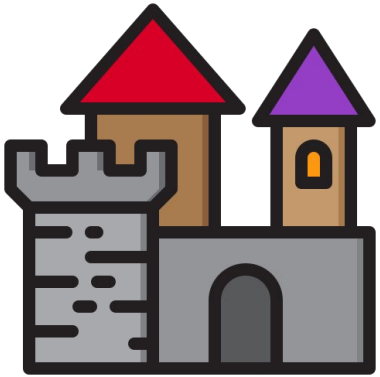
According to ISO/IEC Standard 27000:2009:

"The preservation of confidentiality, integrity and availability of information."

What are:

- Confidentiality?
- Integrity?
- Availability?

# Ancient safety & security



Political and military messages were delicate secrets also historically.

Couriers and their messages could be captured by enemies.

Early encryption, the *Caesar cipher* was based on shifting the alphabet some amount of steps backward or forward.

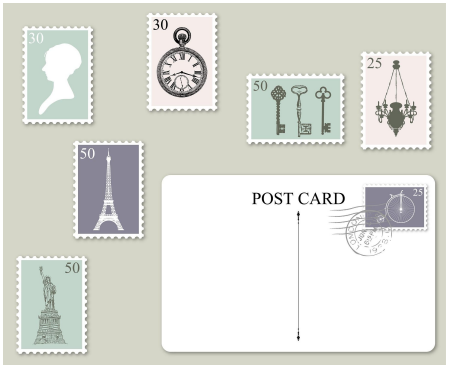
Another modern example is ROT-13, where all the latin alphabet are rotated forward by 13 steps.

## Try to crack this secret:

# Uifnbujd Tuvejp

Hint: it’s Caesar cipher

# From early positivism to today




The early Internet was built for reliability, but not security

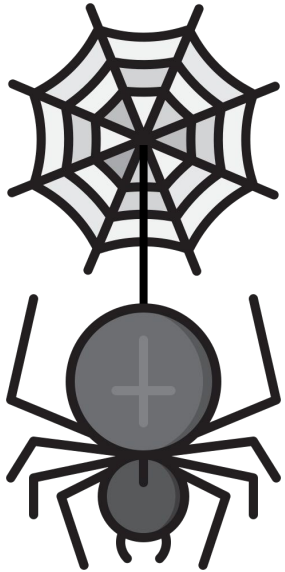
Email for example, by default, is as secure as sending a postcard in mail: anyone who relays or intercepts the message can read it in plaintext.

Early communication applications and *protocols*, such as *http*, *ftp* and *telnet*, sent everything as is over the network

… including **usernames** and **passwords**

Eventually replaced by their secure counterparts, such as *https*, *sftp* and *ssh*

# Why do we need security?



There are many motivations of bad actors:

**Cybercrime:** Make money through identity theft or fraud, infecting computers to create botnets for DDoS attacks etc.

**Black hat hackers:** money, power, access to sensitive information, media visibility, revenge, harassment – range all the way from unskilled individuals to national agents.

**State surveillance:** controlling and monitoring the free speech and public discourse to suppress dissidents.

# Examples of technological and human actors

**Hardware:** personal computers, mobile devices, servers, networking hardware, storage media, cameras, even trashes and physical locks

**Software:** operating systems, drivers, browsers, apps, games, viruses, virus scanners, spyware, server software, encryption

**People:** motivations, knowledge, awareness, skills, practices, trends, individuals, groups and organizations

*Software* runs on *hardware*, but both are made by *people*. And people make mistakes…

# Task: Warming up

1. Think of a moment when you realized your information security was in danger
2. Join your neighboring student or two
3. Share your experiences and try to think of the reasons behind the situation

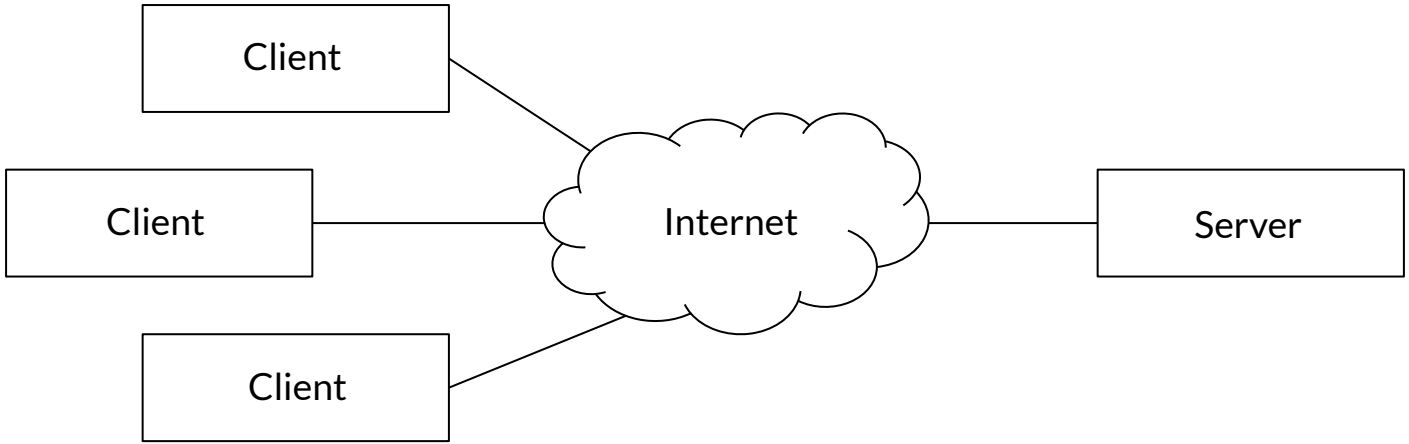
Let's try to discover patterns together!

Thinking of a moment when you realized your information security was in danger, **what patterns did you discover? Can we make a bingo card?**

# BINGO

| | | | | |
|---|---|---|---|---|
| Laptop with no password stolen | Reused password included in a data breach | Gave personal security ID number to scam callers | Unknown devices appeared in iCloud | Sketchy pop-ups and links on websites |
| Using public WiFi to handle private info | "Microsoft" calling: There's problem with your computer... | Work phone stolen, no tracking on | WhatsApp msg from friend = phishing for 2-factor auth | SMS about customs = phishing for credit card info |
| Email from boss = social engineering to sell gift cards | "Know Your Customer" ID photo uploaded via web form |  | "2-factor auth" email as phishing | "Urgent meeting with CEO" email |
| "Hi Mom, lost my phone, msg me on WA" | Online marketplace scams | "Cryptoguru" calling on phone | "Nigerian prince" want's you to help him | Financial institution mishandles your data |
| iOS and Google calendar spam | Ask toolbar and other bloatware | Health information in hacks | Losing your debit card | Online banking glitches |

# Clients and servers




Multiple *clients* (such as your Web browser) connect to a *server* over the Internet. This is basically how Internet-based services work.

# A complex unsecure network (1)

```
marq@vaari:~$ traceroute www.mit.edu
traceroute to www.mit.edu (2.21.200.165), 30 hops max, 60 byte packets
 1  _gateway (10.100.0.1)  1.419 ms  1.944 ms  4.040 ms
 2  jgw-2-v100.aalto.fi (130.233.231.19)  4.545 ms  4.439 ms  4.879 ms
 3  funet-100g-aalto-a.aalto.fi (130.233.231.189)  4.768 ms  4.656 ms  4.514 ms
 4  espoo1.ip.funet.fi (86.50.255.232)  5.530 ms  5.856 ms  5.237 ms
 5  fi-csc.nordu.net (109.105.102.168)  5.582 ms  5.462 ms  5.641 ms
 6  109.105.101.10 (109.105.101.10)  16.341 ms  22.513 ms  22.689 ms
 7  se-brm.nordu.net (109.105.97.47)  14.941 ms  14.768 ms  14.018 ms
 8  as20940-100g-ix1.sthix.net (192.121.80.57)  16.013 ms  15.814 ms  15.485 ms
 9  a2-21-200-165.deploy.static.akamaitechnologies.com (2.21.200.165)  15.348 ms
  15.148 ms  15.005 ms
marq@vaari:~$
```

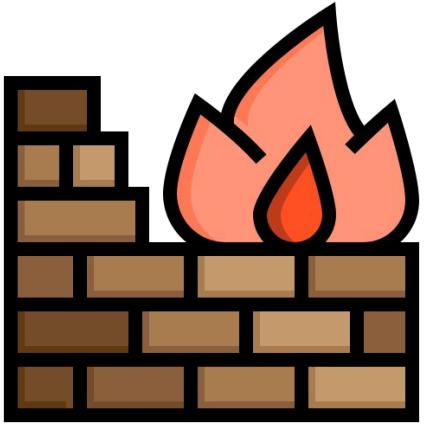
… except it's far more complicated than that.

# **A complex unsecure network** (2)

Along the way we meet: *local area networks*, *wide area networks* and *backbone networks* (what are these?) consisting of *cables*, *wireless and satellite links*, *switches* and *routers* (what are these?)

We can't ensure the security of each, so the problem becomes: *How to communicate securely over an unsecure network?*

# Partial solution: the firewall



A physical device, or software running on a computer, mobile or other general-purpose device

Filters outgoing and especially incoming traffic, stops unwanted connection attempts

For example your home router contains one

However, a firewall does not provide a secure connection in itself

# A firewall *is* useful

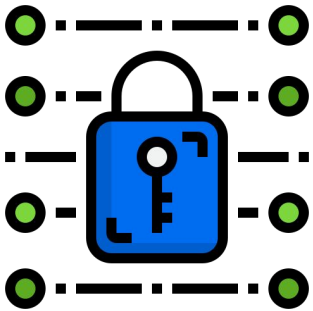
```
Jan 18 08:55:01        CRON[31707]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 18 08:55:01        CRON[31707]: pam_unix(cron:session): session closed for user root
Jan 18 08:56:05        sshd[31727]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
.0.190  user=root
Jan 18 08:56:08        sshd[31727]: Failed password for root from 218.92.0.190 port 17572 ssh2
Jan 18 08:56:09        sshd[31727]: Failed password for root from 218.92.0.190 port 17572 ssh2
Jan 18 08:58:42        sshd[31743]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
144.25  user=root
Jan 18 08:58:44        sshd[31743]: Failed password for root from 14.49.144.25 port 46822 ssh2
Jan 18 08:58:46        sshd[31743]: Failed password for root from 14.49.144.25 port 46822 ssh2
Jan 18 08:58:47        sshd[31743]: Connection reset by authenticating user root 14.49.144.25 port 4
Jan 18 08:58:47        sshd[31743]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh
er=root
Jan 18 09:05:01        CRON[31759]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 18 09:05:01        CRON[31759]: pam_unix(cron:session): session closed for user root
Jan 18 09:05:07        sshd[31766]: Invalid user admin from 59.126.160.245 port 42693
Jan 18 09:05:07        sshd[31766]: pam_unix(sshd:auth): check pass; user unknown
Jan 18 09:05:07        sshd[31766]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
.160.245
Jan 18 09:05:09        sshd[31766]: Failed password for invalid user admin from 59.126.160.245 port
Jan 18 09:05:10        sshd[31766]: Failed password for invalid user admin from 59.126.160.245 port
Jan 18 09:05:11        sshd[31766]: pam_unix(sshd:auth): check pass; user unknown
Jan 18 09:05:13        sshd[31766]: Failed password for invalid user admin from 59.126.160.245 port
Jan 18 09:07:00        sshd[31783]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
.0.190  user=root
Jan 18 09:07:02        sshd[31783]: Failed password for root from 218.92.0.190 port 33801 ssh2
Jan 18 09:07:06        sshd[31783]: message repeated 2 times: [ Failed password for root from 218.92
Jan 18 09:07:07        sshd[31783]: Received disconnect from 218.92.0.190 port 33801:11:  [preauth]
Jan 18 09:07:07        sshd[31783]: Disconnected from authenticating user root 218.92.0.190 port 338
Jan 18 09:07:07        sshd[31783]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ss
ser=root
Jan 18 09:08:37        sshd[31813]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid
.0.190  user=root
Jan 18 09:08:39        sshd[31813]: Failed password for root from 218.92.0.190 port 62536 ssh2
Jan 18 09:08:41        sshd[31813]: Failed password for root from 218.92.0.190 port 62536 ssh2
Jan 18 09:09:01        CRON[31821]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 18 09:09:01        CRON[31821]: pam_unix(cron:session): session closed for user root
```

Unwanted connection attempts from just this morning

# Risks of turning off the firewall

- Connection attempts from the outside can try to  access your operating system and running applications
- Inbound connections a major problem only if there is something on your computer that can be compromised
- … but do you know everything that's running on your computer?

# Virtual Private Networks



Virtual Private Network (VPN) connects a client to a server securely over an unsecure connection through a virtual tunnel between the two networks. This enables for example safe remote work from any location, such as internet cafes with public WiFis.

Often used for home–workplace connections, but also for hiding your traffic from a *surveillance state* or faking your country of origin to bypass regional restrictions.

A practical nearby example: Aalto VPN - when you log in, your network connection appears to originate from inside Aalto campus. Your network traffic between your actual location and Aalto servers is encrypted.

Warning: **VPN providers can monitor all your traffic and metadata. You cannot know 100% reliably if they do or do not.** There are independent audits available, but you should never assume that your identity or your data stays absolutely secret over a VPN.

Again, VPN alone is not enough, as most of the services you use daily are located elsewhere and possibly unsecure.

**Some popular VPN providers:**
NordVPN
SurfShark
F-Secure FreeDome
OpenVPN
Mullvad

# Encryption


Secure network traffic requires encryption

*Encryption* refers to making information unreadable – using computationally heavy mathematical methods – for an unwanted party even if they could get hold of it.

*Decryption* reverses the process and requires a *key* (typically a number sequence).

Not just for communications, for example computer data storage can be encrypted to counter data theft.

# Malware

*Malware* is an umbrella term for malicious software, such as *viruses*, *spyware* and *trojan horses* (what are these?).

At times malware, such as *worms* may spread proactively from computer to computer, but very typically malware requires some human assistance:

- Visiting the wrong website
- Opening the wrong email attachment
- Installing a game or utility from a shady source etc.

# Old-timer's memoir from Markku:


*Around 1991 I took some pirate games on floppy disks with me to play on my cousins' Amiga 500 home computer. Unfortunately one of the floppies contained the infamous SCA virus which spread like wildfire and infected other non write-protected diskettes, including original games. The virus displayed its signature slogan "Something wonderful has happened – Your AMIGA is alive!!!" Later on I found an SCA killer tool which let me rescue the games, but my reputation as a computer whizz-kid surely was damaged for a while.*

# Ransomware


*Ransomware* is a particularly vicious kind of malware which may lock the victim's computer or encrypt the files

The attackers then demand a payment to release the computer, usually in a hard to trace cryptocurrency

*WannaCry* in 2017 was one of the worst epidemics affecting various Windows versions

Hit as many as 200 000 computers in 150 countries, several companies included

# What to do with intrusions?

The SANS Institute six-step model:

1. **Preparation** – planning, testing
2. **Identification** – identifying the breach
3. **Containment** – minimizing damage
4. **Eradication** – removing the issue
5. **Recovery** – restoring systems to use
6. **Lessons learned** – post-analysis of what happened

Q: If I get hit, should I pay?

A: You should have backups! Anyway, who's responsible for the ransomware? Yes, people who pay, but also...

"North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs." https://www.cisa.gov/uscert/northkorea

# Does it matter?

"Why bother? I don't have anything to hide."

It's a relevant question, but…

*What about some other service that you also use?*

→ **Access to your account here helps to crack another elsewhere**

*What about other users?*

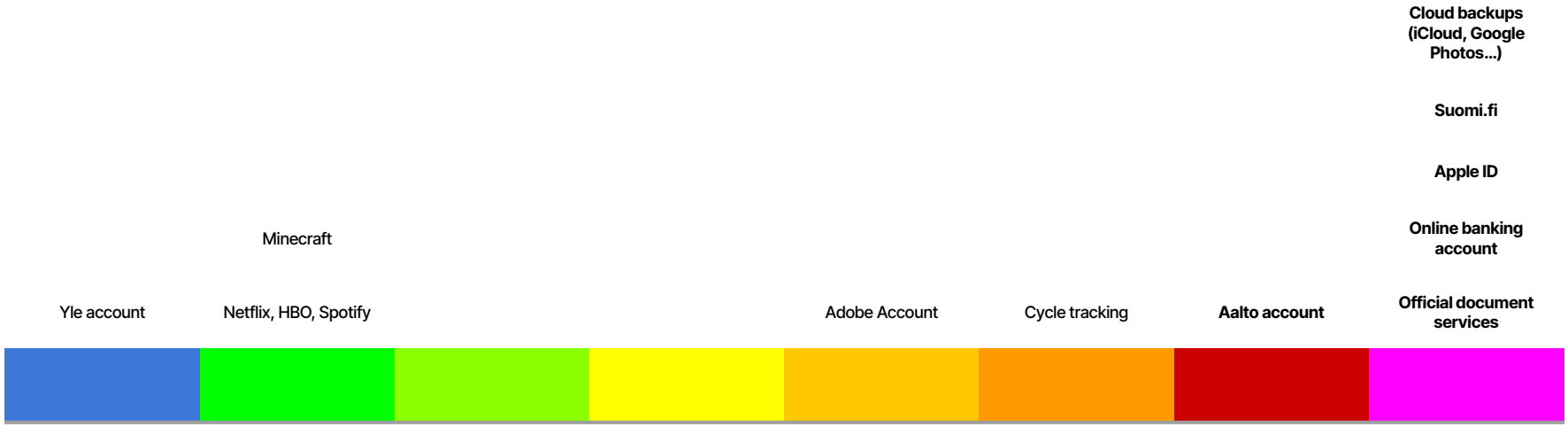
→ **Even a seemingly innocent breach opens attackers new doors**

# Task: What matters and what not?

1. **Think of some online services you use regularly.**
   If there was a security breach, which of them would matter and which not?
2. Join your neighbor(s) again and compare

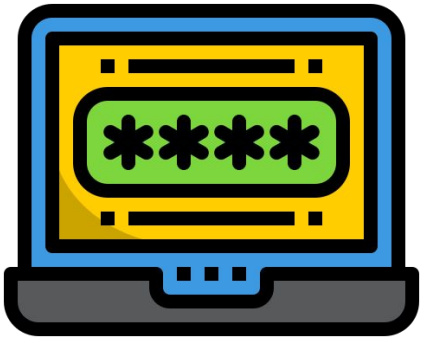
Together let's place some examples on a security continuum ranging from *irrelevant* to *crucial*

# Impact mapping




If there was a security breach, which services would matter and which not?

# Passwords, passwords




Still the main method of *authentication* on the majority of services and systems

General weaknesses: easy and short passwords easy to crack, reusing the same password across services

They're just too many to manage and remember

Alternatives and improvements: fingerprints, facial recognition, multi-factor authentication, password managers

# Password *cracking*

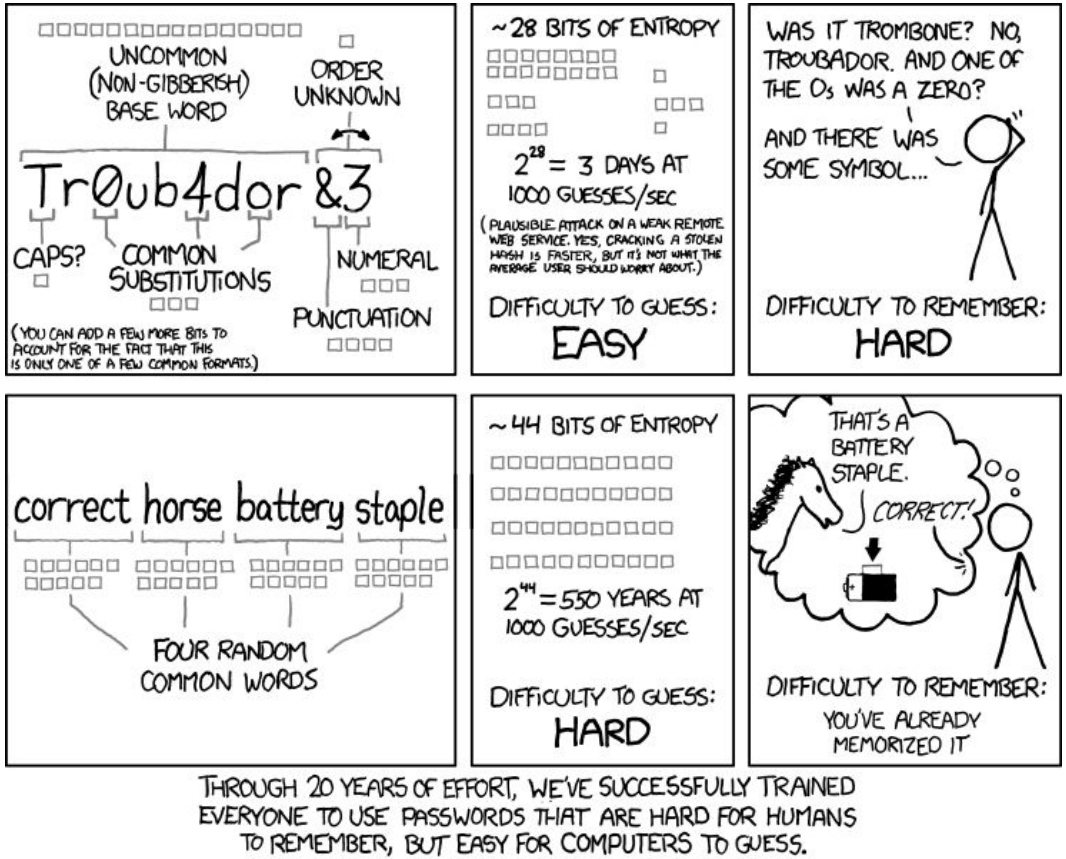
Cracking SHA-512 encrypted user passwords using *John the Ripper* tool:

**pass** – 0.811 seconds

**Pass2** – 9 seconds

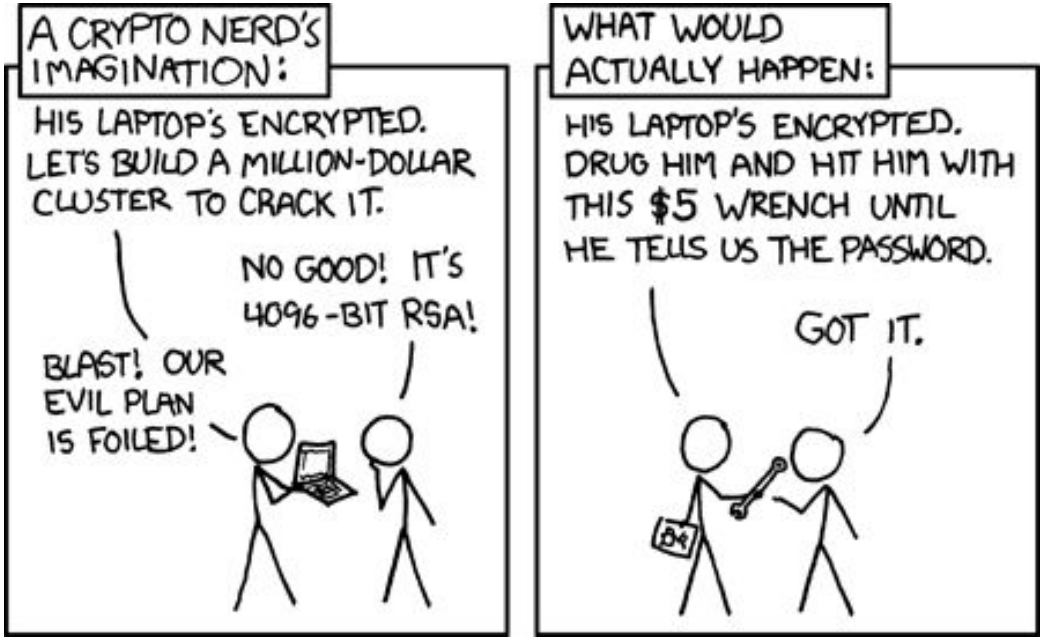
**pass123** – 3 minutes 36 seconds

**P!"#w0rd** – not cracked in 30 minutes, had to stop




https://xkcd.com/936/ & https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength

# Physical access is critical




https://xkcd.com/538/ & https://www.explainxkcd.com/wiki/index.php/538:_Security

# Password breaches

**847,223,402**

passwords have been exposed in password breaches between 2017–2021 and searchable through the free service **Have I Been Pwned** created by Troy Hunt, Microsoft Regional Director. Try your old passwords on it here: https://haveibeenpwned.com/Passwords

# Passwords: case Vastaamo (1)


One of the highest visibility data breaches in Finland ever

Took place in 2018/2019 and became known in 2020

About 33 000 patients' information leaked

Highly sensitive data, *Vastaamo* was a psychotherapy provider – went bankrupt shortly thereafter

Ransom demands in Bitcoin

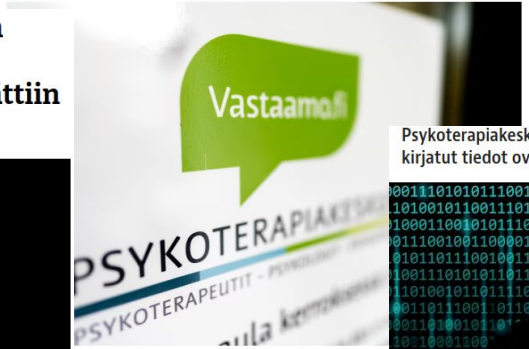
Causes: no firewall and using default password for the database server

# Passwords: case Vastaamo (2)

Psykoterapiakeskus Vastaamon potilastietojen varastamisesta epäilty mies tunnetaan kansainvälisesti tietomurroista.


**Vastaamo-tutkinnassa saatu dataa ulkomailta takavarikkoon, syytteennoston määräpäivä määrättiin vuoden päähän**

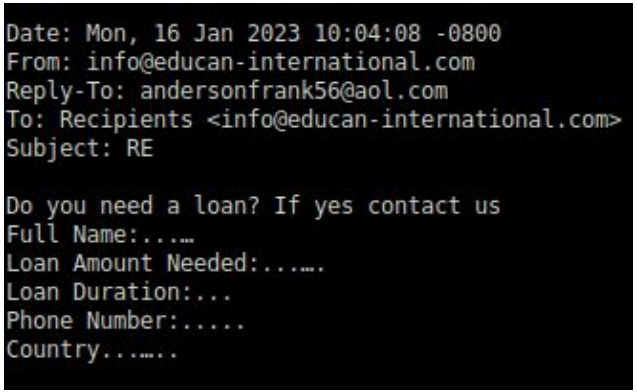

Teosta epäillyn nimi nousi esiin jo aivan tutkinnan alussa hänen rikostaustansa ja osaamisensa takia.




Psykoterapiakeskus Vastaamon mukaan marraskuun 2018 jälkeen kirjatut tiedot ovat turvassa.


Plenty of media coverage, including rumors and speculation

# Social engineering




An umbrella term for attacks based on psychological means

One of the oldest kinds of online fraud

Some types: *tailgating* to access protected spaces, *phishing* by spam email or phone calls to obtain confidential information, *baiting* to install malware

People are creative when exploiting others' gullibility, ignorance, greed, helpfulness, curiosity and other human traits

# Social engineering case: vishing

How many of you have received suspicious phone calls from a British number? Country code +44

"Hello, we are calling from Microsoft Technical Support …"

*Spoofed* numbers look like they came from another country

Trying to get the victim to install remote access software, such as *TeamViewer*

Largely India-based call centers

Humorous countermeasures: scambaiting

# Best practices to keep yourself safe (1)

Aalto users:

- Do the Student's information security training.
- Are you using Multifactor Authentication?
- Multifactor authentication is less painful and your Wifi security is better using Aalto VPN.

Windows users:

- Keep your Microsoft Defender Antivirus always on and updated.

# Best practices to keep yourself safe (2)

- **Take care of your mobile phone!** It's the most important verification tool but also a single point of failure. Learn how to sign into important services without your phone (it's possible).
- Use 2-Step Verification for important services. Use more than one account with overlapping recovery options.
- **Make backups.** Best backups are automatic.
- Don't run very old and unsupported versions of the operating system or Web browsers.
- Install applications and drivers from reputable sources only.

# Conclusions

- We're dealing with a constantly moving target
- Actors range from hardware to software, and from individuals to large social systems
- High complexity issues generally out of layperson's reach
- Information security isn't an on/off type decision, but a *compromise* involving at least: knowledge, hands-on skills, awareness, resources, convenience, practices, laws, trends and personal liberty

# Readings and links

**Guidelines**

Aalto Cyber Security For Students

Information security at Aalto University – our very own guidelines

Defence in Depth

**Online organizations**

Electronic Frontier Foundation – nonprofit dealing with privacy, freedom and related issues

The Hacker News – news on information security

**Legislation**

GDPR – European privacy and security law

**Historical context**

Steven Levy (1984): *Hackers – Heroes of the Computer Revolution*

# Thank you!

Icons: Flaticon Cyber Security Icon Pack by srip