SYNACKTIV

Back to the failure

Did your physical security really evolve in the last 40 years ?

hack.lu 2024

whoami

- **Simon Geusebroek** *"WhiteWinterWolf"*
  - Pentester @Synacktiv
  - Physical intrusion specialist
    - Industrial sites and offices
    - Datacenters, upper tier Seveso establishments, luxury logistic, …
- **Synacktiv**
  - Offensive security
  - Based in France
  - 170 Experts
  - Pentest, Reverse Engineering, Development, Incident Response

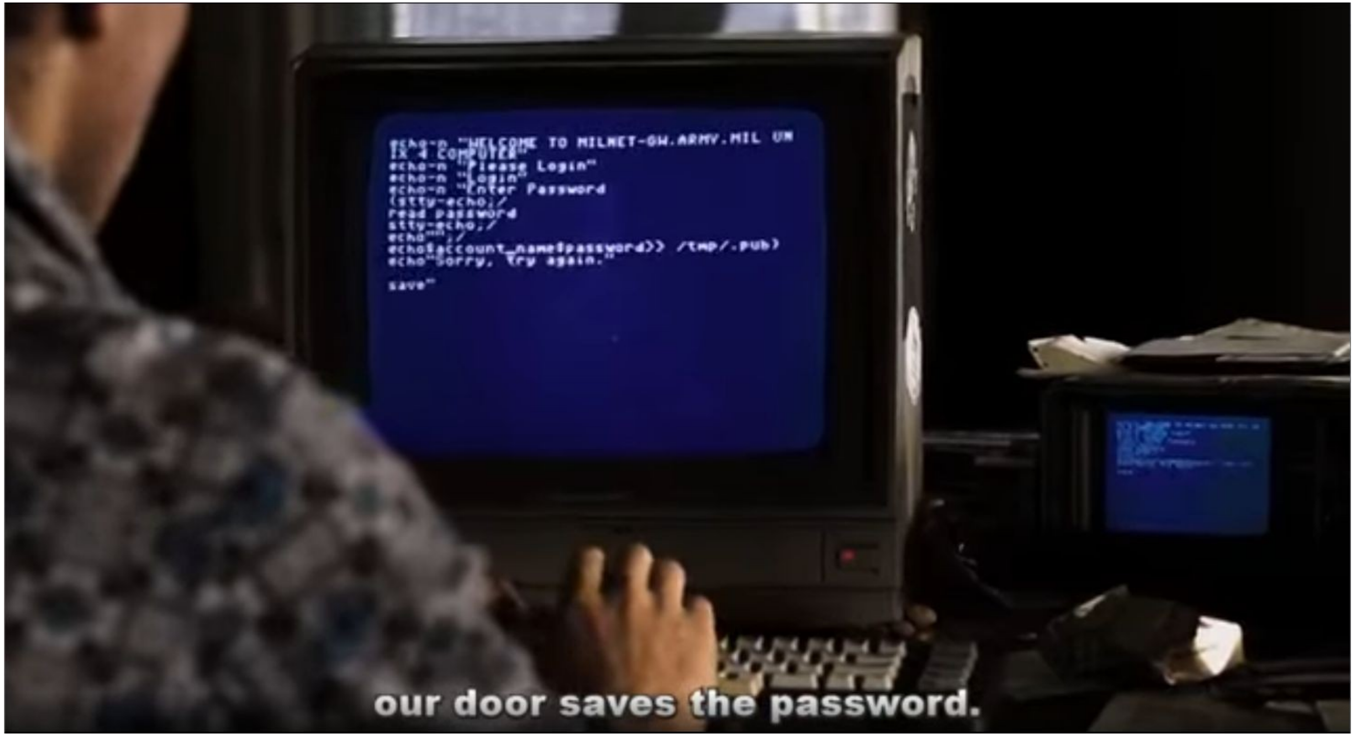
What is a physical pentest? (very broadly)

- **Audit client perspective**
  - Like a classical pentest
  - But instead of entering into your computer, we physically enter into your facilities
    - Similar legal framework
    - Same objective of finding vulnerabilties to improve security
- **Pentester perspective**
  - Like urbex
  - But with people still inside
  - And both legal and helpful!

The history of hacking

SYNACKTIV

- **23 – Nichts ist so wie es scheint**
  - 1998 film, depicting actual events from 1980



```
echo-n "WELCOME TO MILNET-GW.ARMY.MIL UN
IX 4 COMPUTER"
echo-n "Please Login"
echo-n "Login"
echo-n "Enter Password
(stty-echo;/
read password
stty-echo;/
echo"";/
echo$account_name$password>> /tmp/.pub)
echo"Sorry, Try again."

save"
```

our door saves the password.

The history of physical intrusion… oh wait!

- **Sneakers**
  - 1992 film, more comedyish but still some valid background

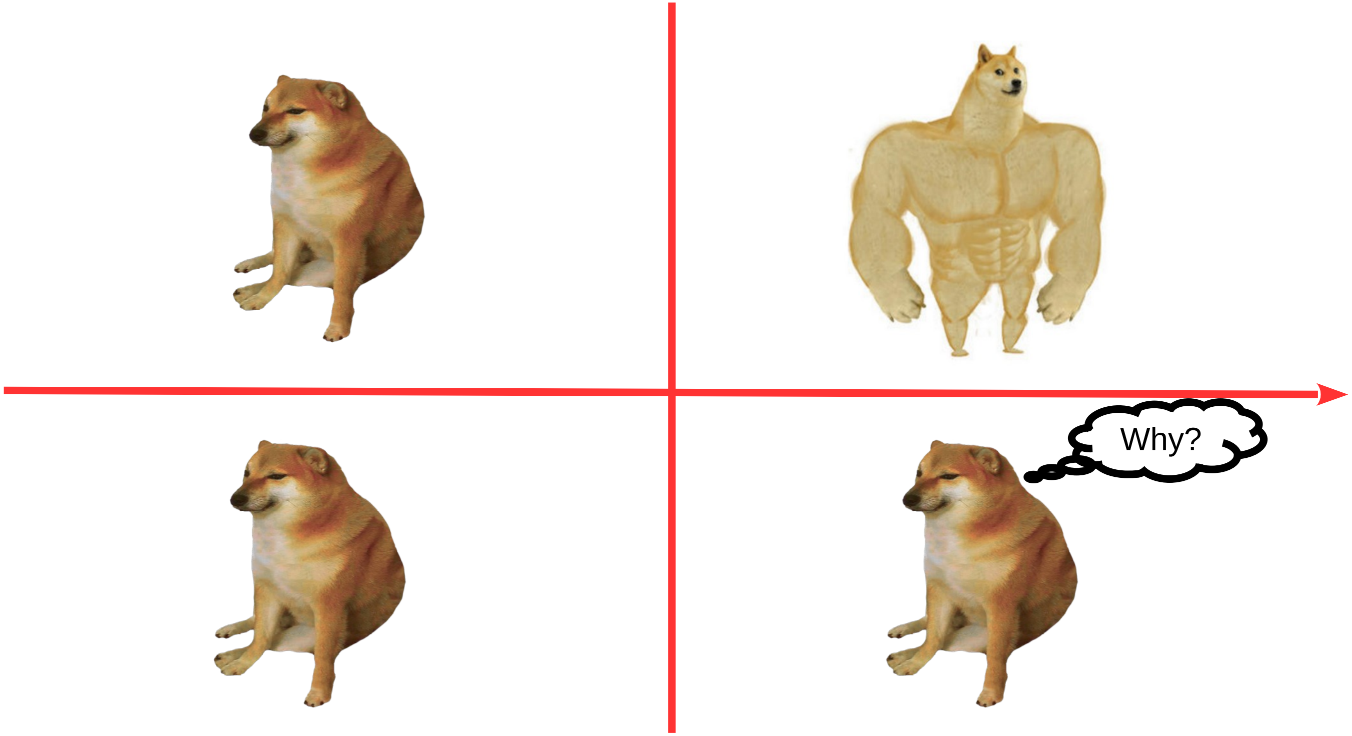
We're late for the party on the
second floor. Push the goddamned buzzer.

Cyber and physical security compared

Internet start era | Now

Cyber security

Physical security



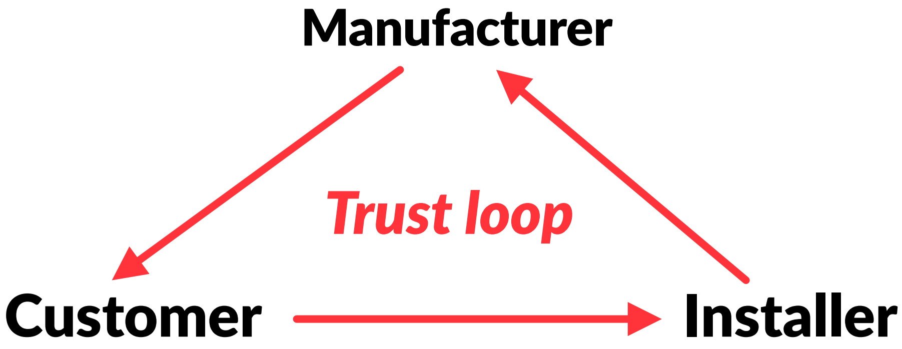
Delegate risk and play ostrich

SYNACKTIV

- **A different approach to “security”**
  - Strict focus on cost, conformity and liability reduction
  - Don’t care about the actual security level
- **But what about…**
  - Brand reputation damage?
  - Intellectual property and industrial knowledge theft?
  - Guarantee that potential intrusions will really be detected (and reported)?

Endless loop of trust

- Everyone assumes that somebody else took the security into account…


Manufacturer

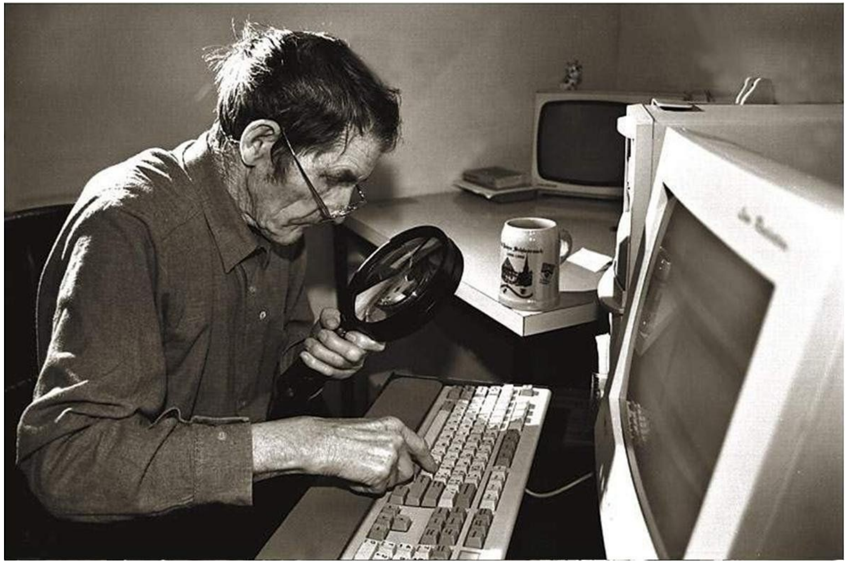
Trust loop

Customer

Installer

- … while in fact nobody did.

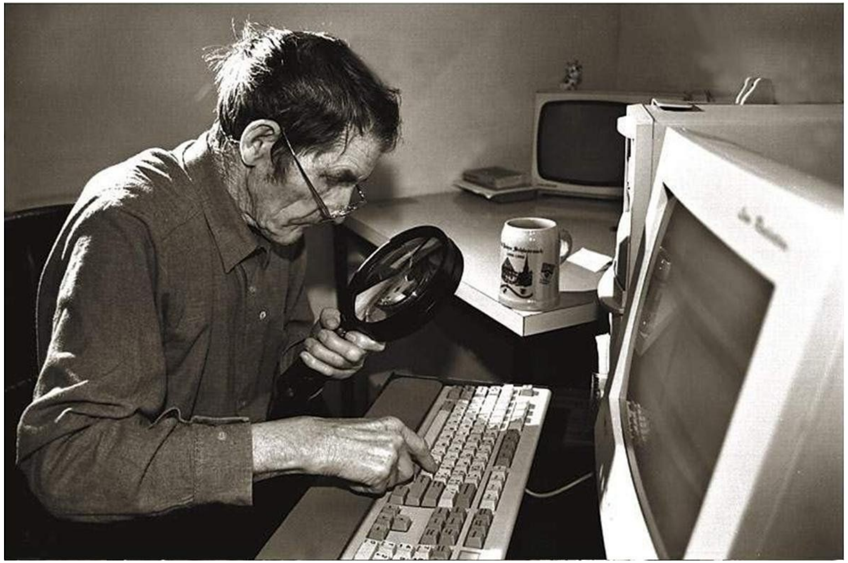
False beliefs



I am the old wisdom of legacy IT security

Feel free to (not) follow my advice!

1/10: Missing lock cylinder

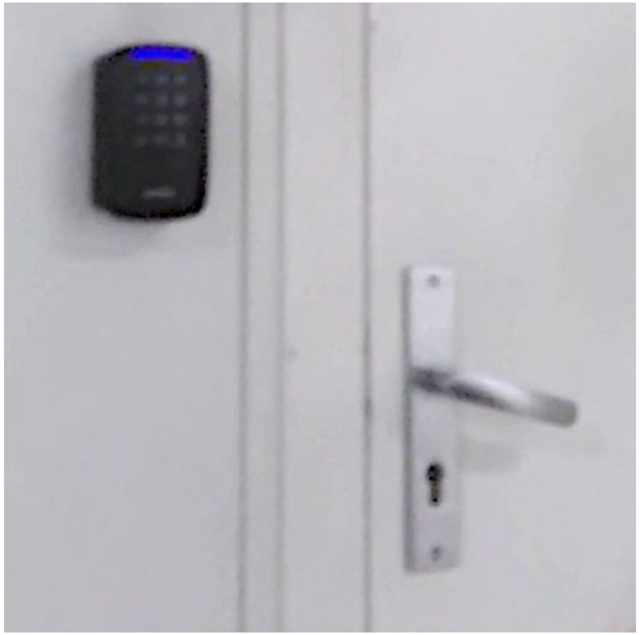


I did not put any ~~password~~ as I use my ~~IP address~~ to authenticate.

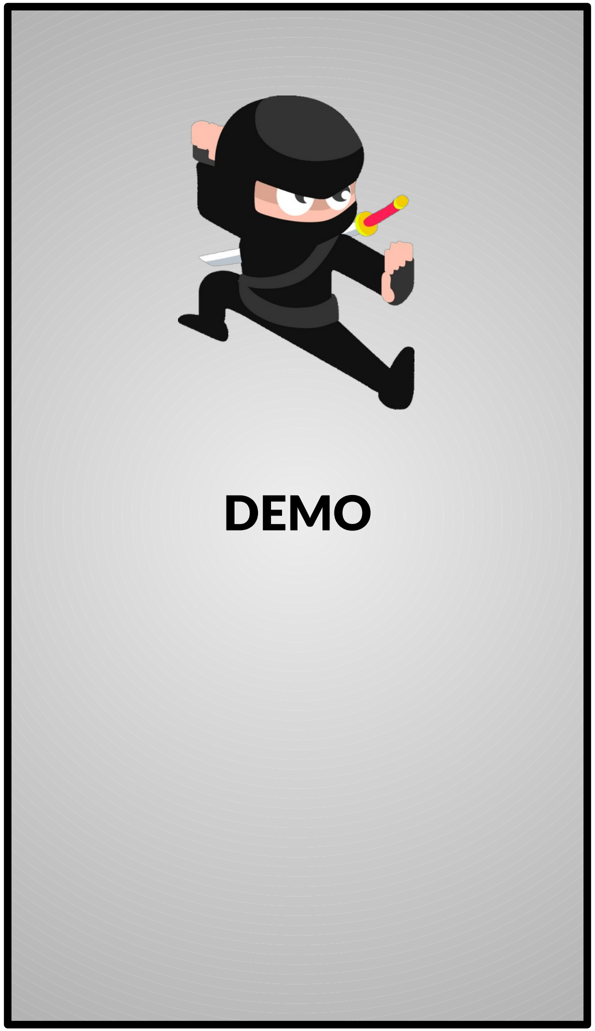
Lock cylinder access badge

1/10: Missing lock cylinder

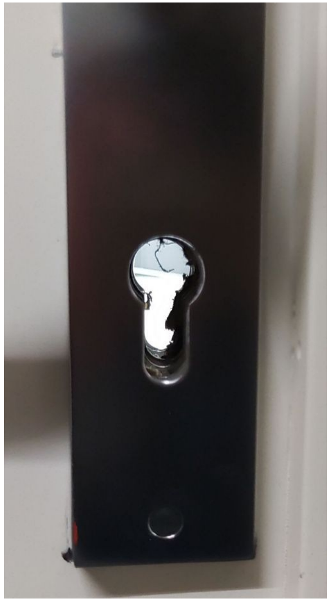
- **Example case**
  - Multifactor authentication
    - Access badge + PIN code
  - But no lock cylinder



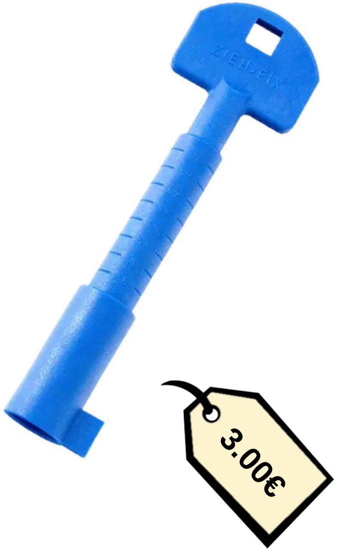
1/10: Missing lock cylinder



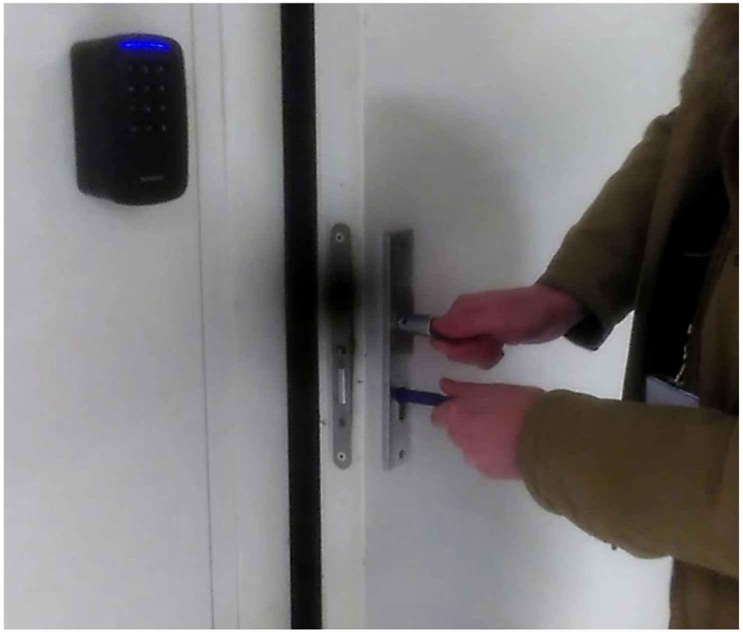
1/10: Missing lock cylinder



+



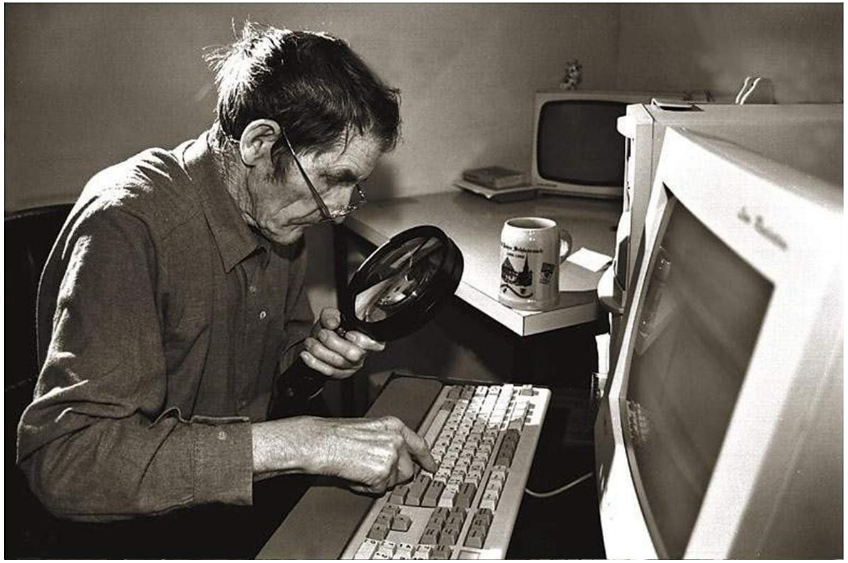
=



1/10: Missing lock cylinder

- **If you need to keep a key-based access**
  - Install a secure cylinder lock
- **If you don’t need to keep a key-based access**
  - Properly condamn the lock cylinder hole
    - For instance using a false cylinder
- **A cosmetic plate is rarely a good solution**

2/10: Default locks



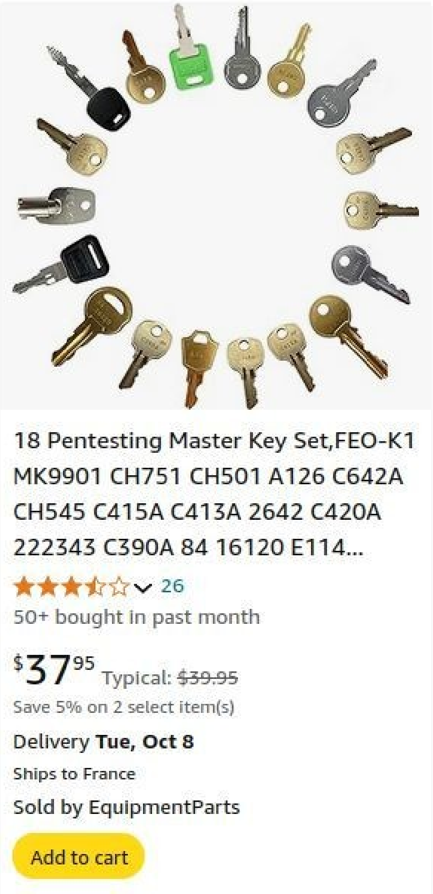
I leave default ~~passwords~~, they are good enough.

locks

2/10: Default locks

- **Some equipment come with well-known default keys**
  - Keys widely available on the Internet
    - Spare and hardware stores

- **A set of default keys: the physical counterpart of a passwords wordlist**
  - Such set is heavily country dependant



18 Pentesting Master Key Set,FEO-K1 MK9901 CH751 CH501 A126 C642A CH545 C415A C413A 2642 C420A 222343 C390A 84 16120 E114...

26

50+ bought in past month

$37 95 Typical: ~~$39.95~~

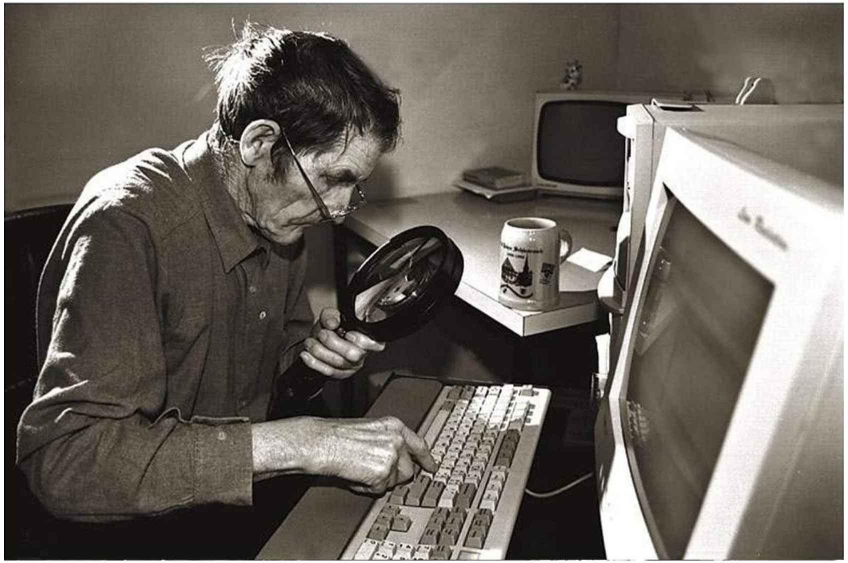
Save 5% on 2 select item(s)

Delivery **Tue, Oct 8**

Ships to France

Sold by EquipmentParts

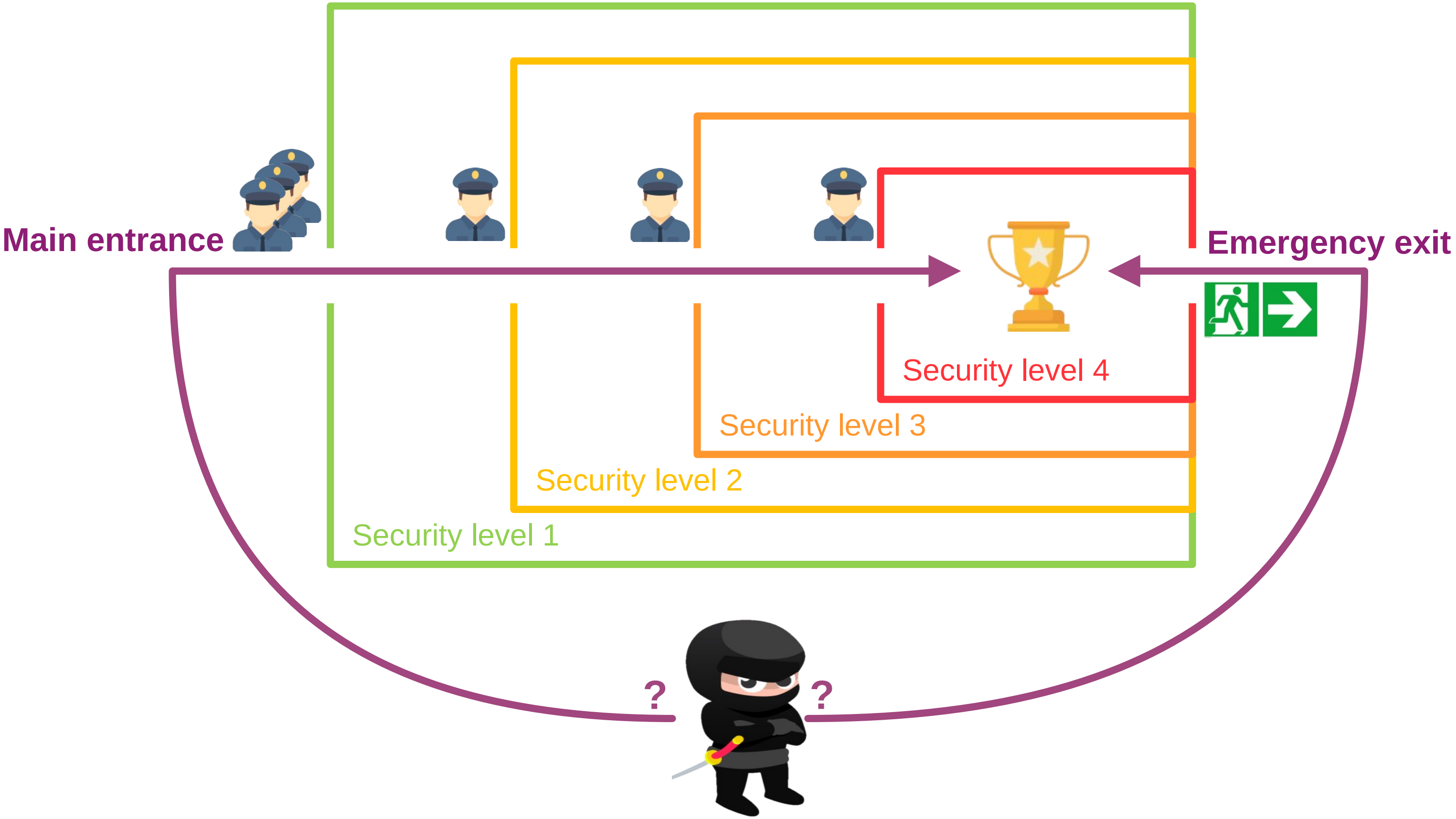
3/10: Weak locks



I left a crappy ~~password~~ lock on this ~~server~~ door, we never use it anyway.

3/10: Weak locks

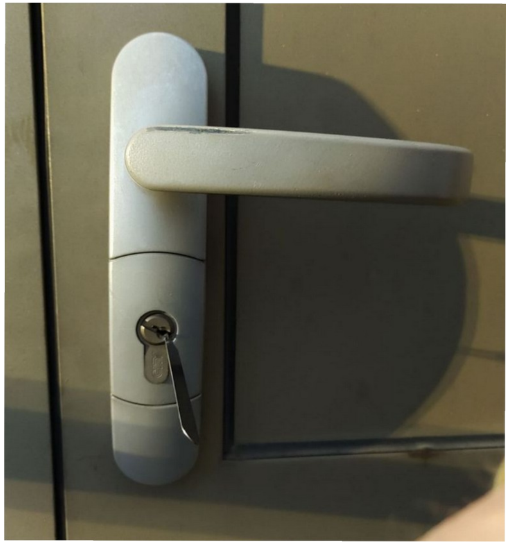
- ***Shall we play a game?***
  Help the ninja to choose a path to access Level 4



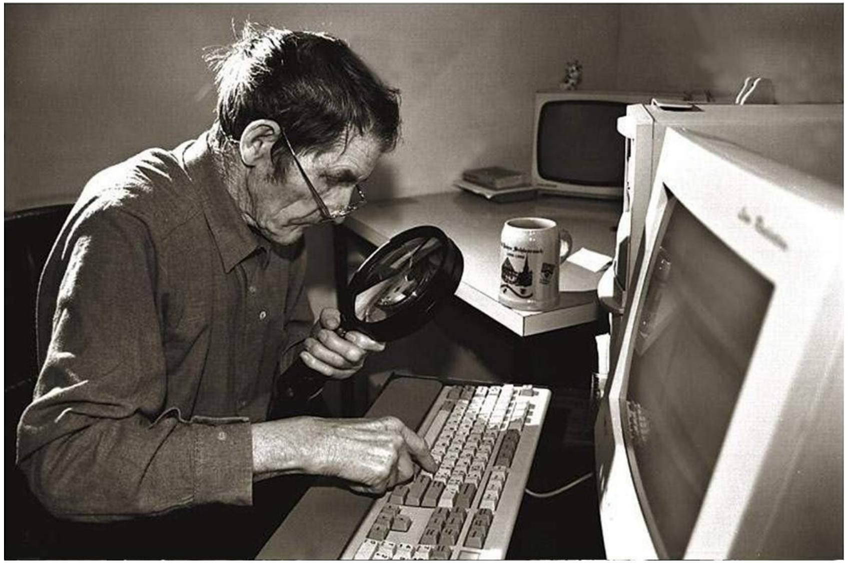
3/10: Weak locks

- ~~Nobody~~ ever need to unlock the emergency exit from the outside

No legitimate person



4/10: Just FUD?



Real life attackers don’t exist, it’s just FUD and marketing

4/10: Just FUD?

SYNACKTIV

- **Quite often, we see we are not the first ones following a path**
  - Normally we are not expected to cut fences… ourselves
    - Every action done during a physical pentest should be reversible
  - But most often others already did it for us!

4/10: Just FUD?

- **Quite often, we see we are not the first ones following a path**
  - Sometimes we encouter proofs of a previous determined forced entry attempt
    - Here using a crowbar

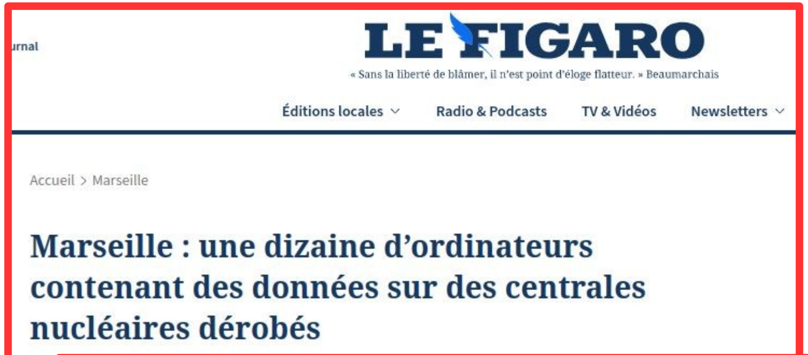
4/10: Just FUD?

- **Customer feedback**
  - Customer warned by a government agency how they would do if they wanted to enter
    - Warning ignored by management: it’s just FUD, not something likely to happen in real life
  - Customer hired us, providing no information
    - We identified as the same path as the most easily exploitable
    - We managed to get in and out, without raising any alert
  - This shows 3 things
    - This path is highly likely to be chosen by anybody wanting to get in
    - It works and effectively allows to bypass all security mechanisms
    - There is no way to determine if somebody previously used this path as it raises no alert

4/10: Just FUD?

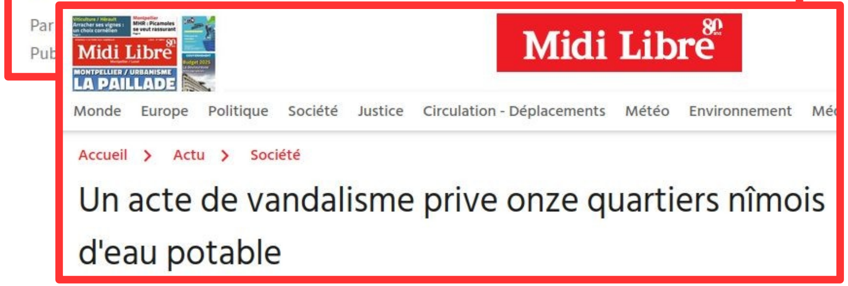
Press news

- Stolen computers (from laptops to mainframes (!)), vandalism, bioterrorism, …
- Espionage, prepositioning, etc. are rarely made public

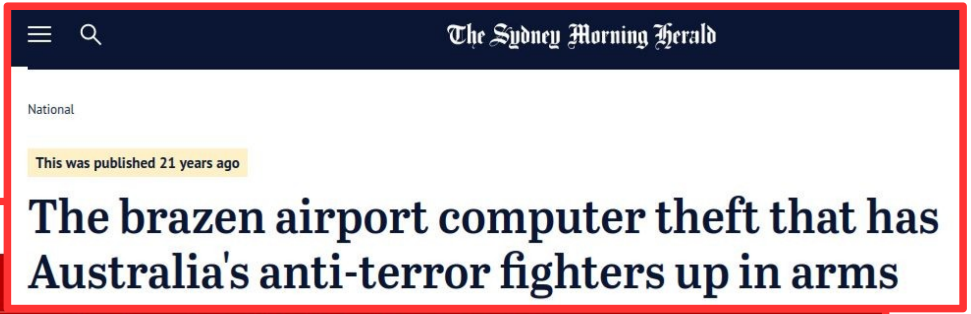


Marseille : une dizaine d'ordinateurs contenant des données sur des centrales nucléaires dérobés

Par
Pub

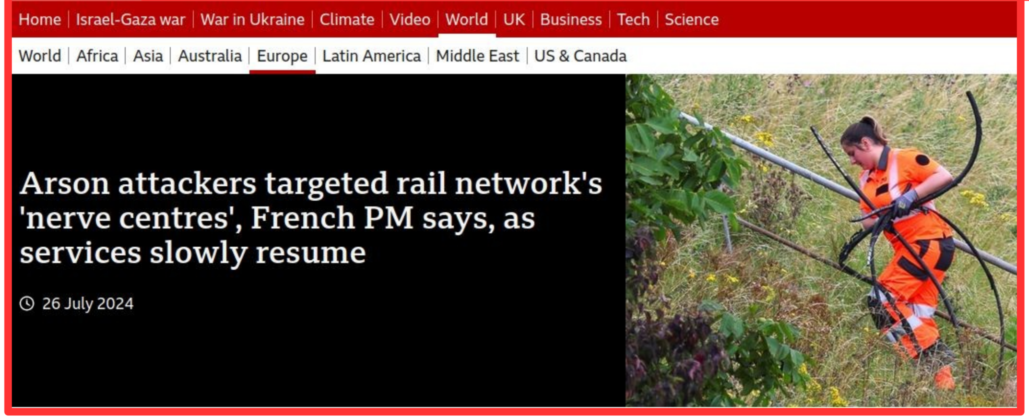


Un acte de vandalisme prive onze quartiers nîmois d'eau potable



This was published 21 years ago

The brazen airport computer theft that has Australia's anti-terror fighters up in arms



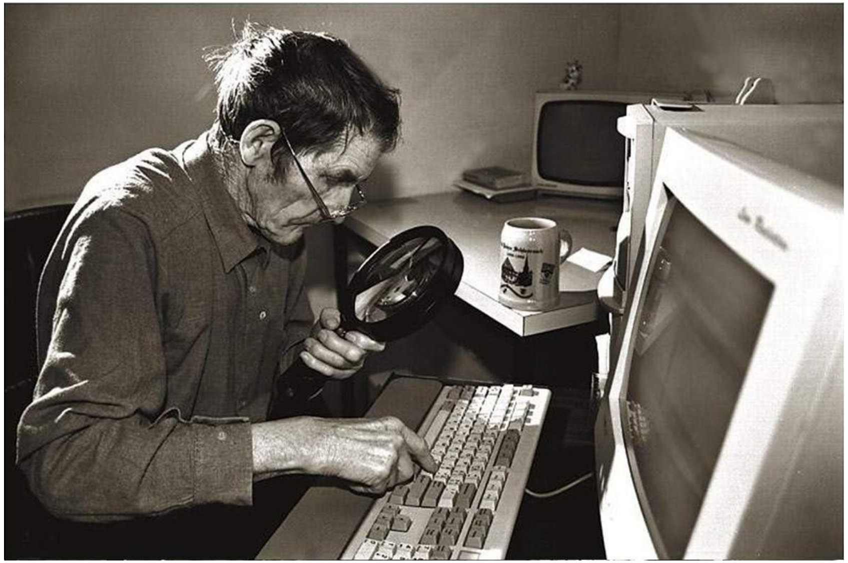
Arson attackers targeted rail network's 'nerve centres', French PM says, as services slowly resume

26 July 2024

4/10: Just FUD?

- **Job interview**
  - A candidate's previous job included intelligence gathering from competing companies
- **False perception due to weak monitoring**
  - The fact of not detecting any intrusion on your site does not mean there are none
  - A successful intrusion is usually meant to not be detected
- **As cybersecurity gains in maturity, physical intrusion may become more and more the weak point in global IT security**
  - Play the *"Help the bad guy to choose a path"* game:
    - Choice A: hardened, tested and heavily monitored cyber
    - Choice B: weak, untested and loosely monitored physical accesses

5/10: Just a reminder for honest people?



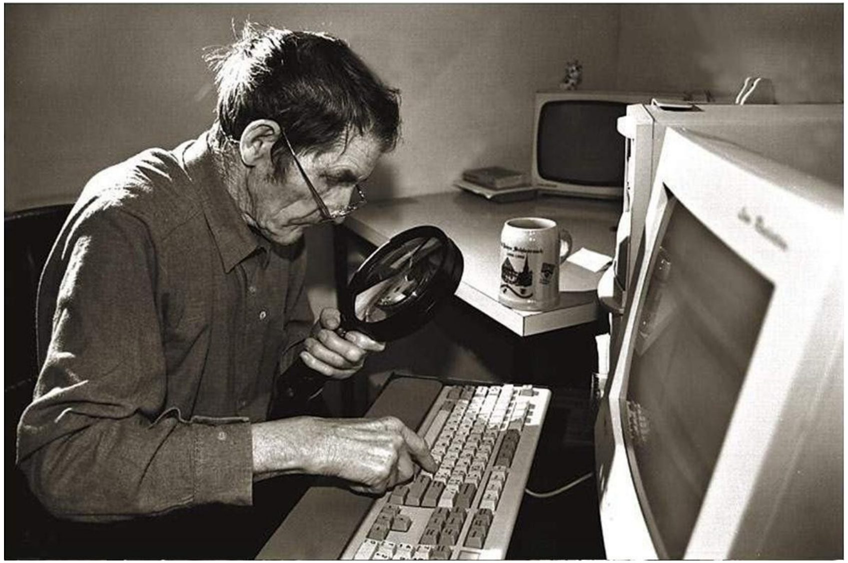
Security systems are just to keep honest people honest.

If an attacker really wants to enter, he will always find a way to get in.

5/10: Just a reminder for honest people?

- **Any intrusion require some effort**
  - Tools
  - Training
  - Time
  - Financement
  - Human ressources
- **The intrusion must worth the effort**
  - Potential gain vs. required effort
  - Comparison with similar targets
- **Security systems allow to raise the required effort to a desired level**
  - The desired level will vary notably depending on the asset to protect

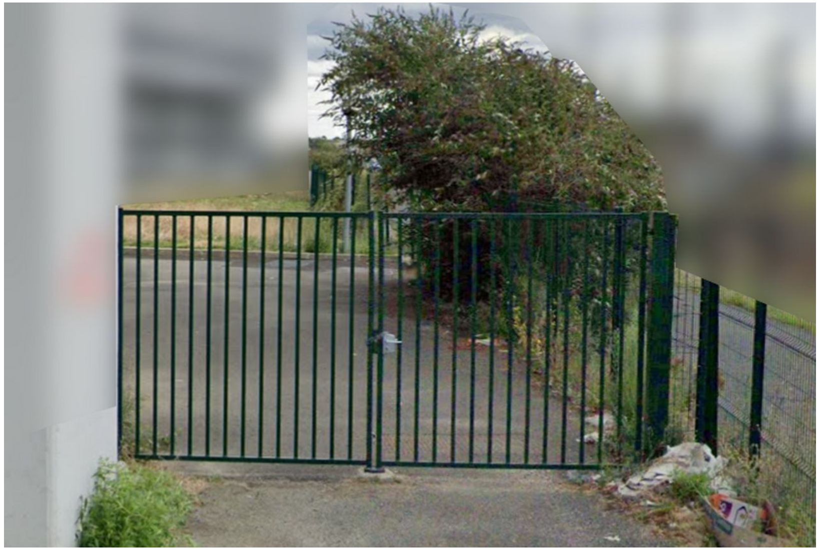
6/10: Physical security cost



Good security is too expensive anyway.

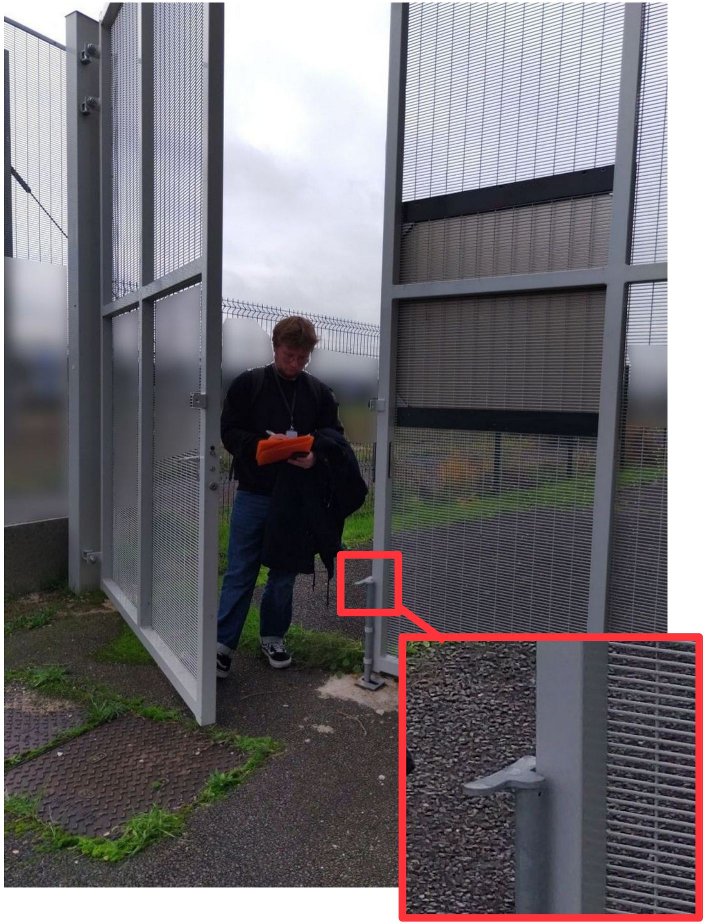
6/10: Physical security cost

- **Before:**
  A small classical portal closed with a padlock and a chain
  - A camera covers the portal
    - With some luck the tree is still there with enough leaves to create a blindspot
  - Portal closed by a chain
    - Risk to attack right in front of the camera
  - Maybe possible to escalade the portal ?
    - Risky idea
    - Only if desperate enough

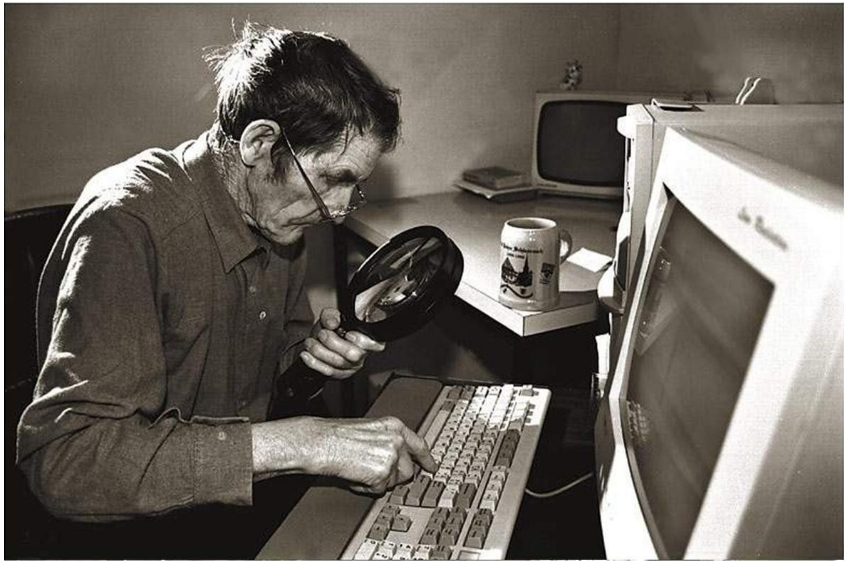


6/10: Physical security cost

- **After:**
  A monumental gate… keyclosed
  - Default key for this manufacturer
    - We already bought it on the Internet !
  - The key is facultative
    - The gate drop down bolt is exposed on the outside
  - A camera covers the portal
    - Cool ! Showing that we have the key will provide even more credibility !
- **Huge relief for the attacker!**
  - No more question on how we as attackers will pass the external perimeter fence
  - Not sure that was the expected result from this investment…



7/10: Certifications value



I installed a certified ~~firewall~~, nobody could enter!

armored door with biometric authentication

7/10: Certifications value

- **Certifications are good, but not sufficient**
  - Generally do not take into account
    - Aging
    - Installation details (the actual one you have)
    - Environment (unexpected entry points, etc.)
  - Rely on standardized attack methods
    - Objectives :
      - Allow to compare similar products
      - Provide a rough idea of a product resistance
    - Do not necessarilly cover the most efficient attack against actually installed product
      - Most bypass tools used during a pentest assessment are not part of standard certification allowed tools

7/10: Certifications value

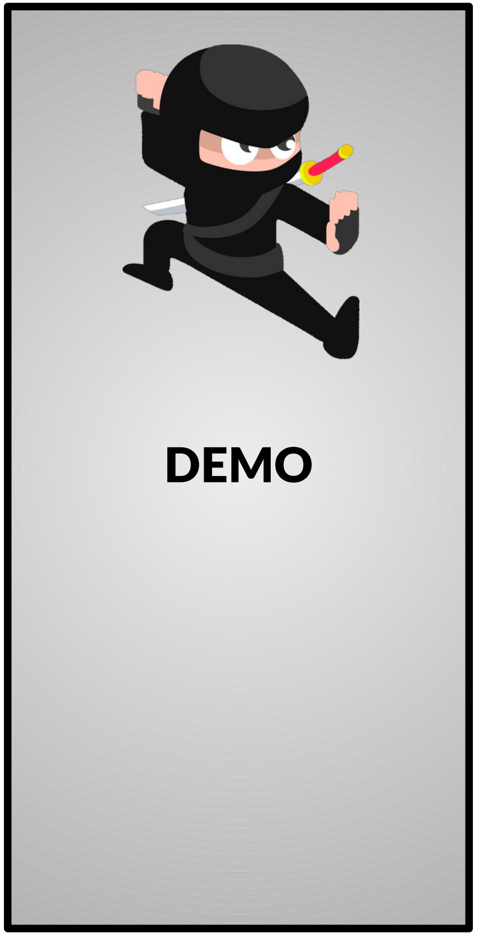
- **Concrete example**
  - 50 000 € armored door
  - 12 000 € biometric MFA access control
  - “Would you manage to open it?”

Be warned, this will go real quick!

7/10: Certifications value

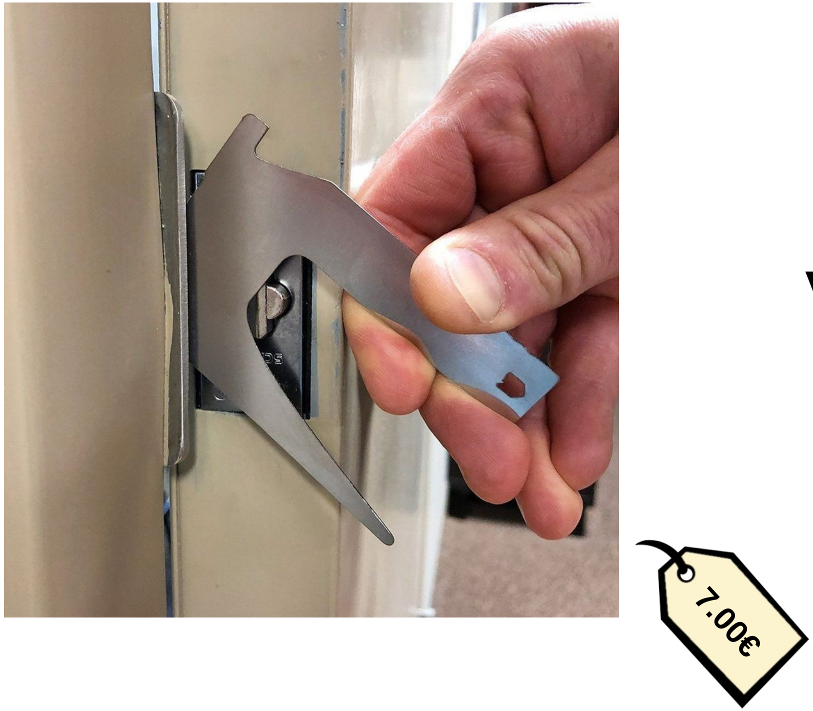
- **Concrete example**
  - 50 000 € armored door
  - 12 000 € biometric MFA access control
  - "Would you manage to open it?"

Be warned, this will go real quick!

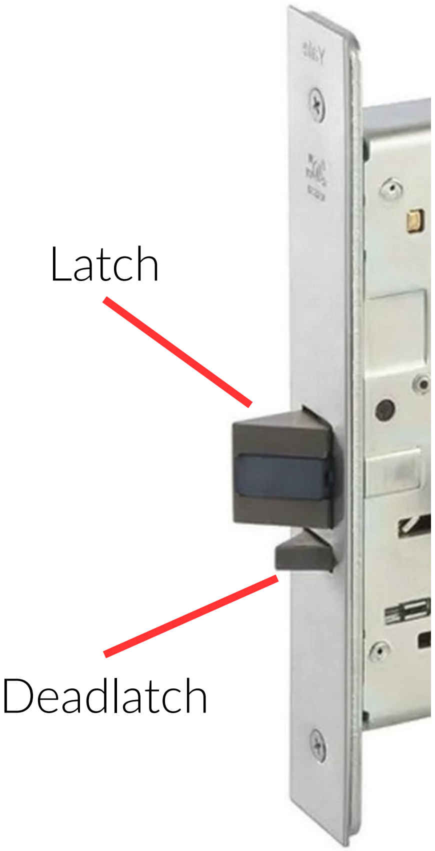


7/10: Certifications value

- **Concrete example**



vs.



7/10: Certifications value

SYNACKTIV

- **Certifications show what a device *can* provide**

- **This is not necessarily what it *actually* provides in your context**
  - Only a formal test can confirm if a device matches your expectations
  - Visual inspection and conformity audits might miss critical aspects

- **Attackers already know what to test**
  - Low-cost, easy and discrete: the exploit here shown is a classical and prime target

8/10: Vendors’ discourse

SYNACKTIV

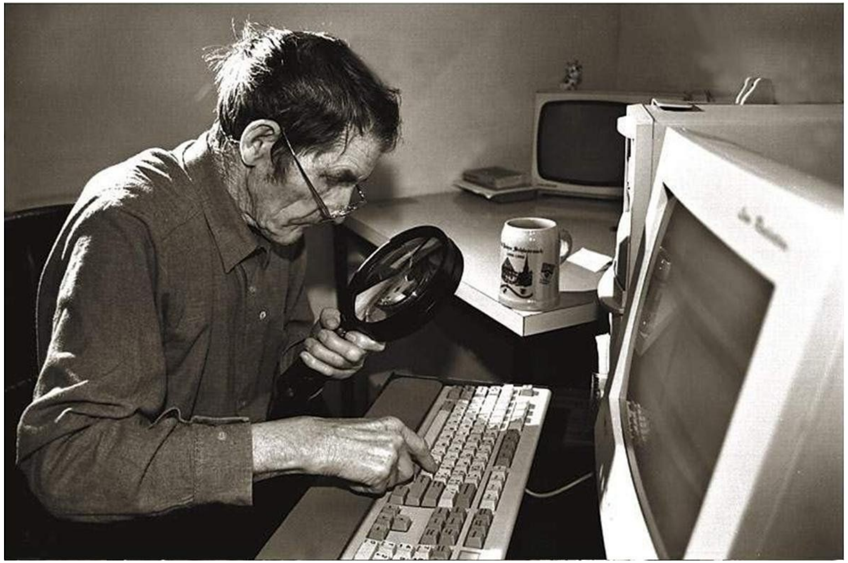
This will protect you against evil intruders. 100 % guaranted!

And we also provide support and maintenance at a very competitive price!

8/10: Vendors' discourse

- **Stacking always more security devices…**
  - … and crossing the fingers that they will prevent intrusions
- **… is not the best solution**
  - If they don't fix the weak point, the weak point will remain the same
    - It is harder to target the weak point when you don't know it
  - Poorly chosen equipment may even noticeably lower the security posture
    - Exact opposite of the expected goal
      - Cf. previous slides about the monumental gate
    - Vendors discourse cannot be blindly trusted
      - May not always propose the most efficient solution in your specific case
      - May be biaised in favor to… "other incentives"

9/10: Intrusion detection systems



I have an IDS and vigilant employees, an intruder will certainly be noticed.

9/10: Intrusion detection systems

- **Actual intruders won't attempt to hide themselves**
  - The best way to not been seen is to act in plain sight
  - There are multiple techniques to…
    - Look legitimate
    - Justify dubious actions
    - Discourage any question or interception
    - Persuade or manipulate people

- **People don't expect an actual intrusion**
  - Intruders just have to show them what they expect to see

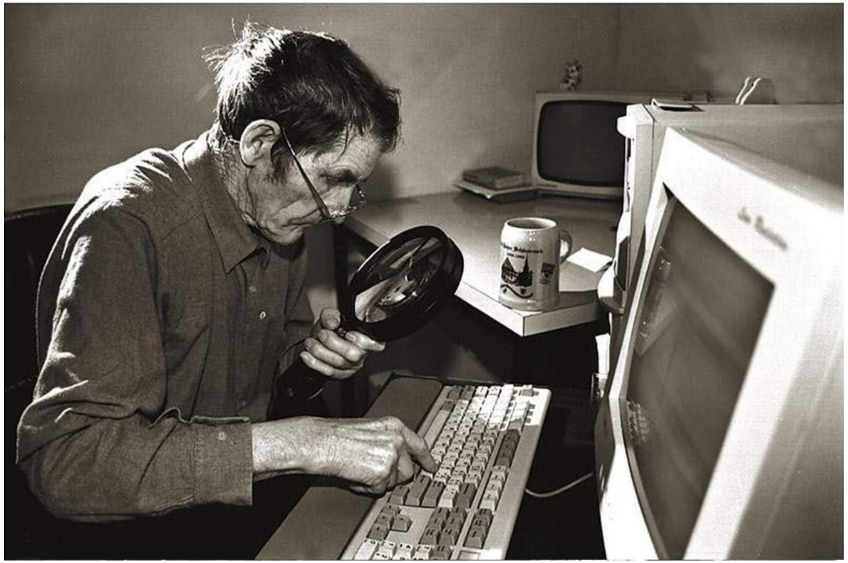
9/10: Intrusion detection systems

SYNACKTIV

- **Cameras are mostly forensic tools, not detection**
  - We passed 1 hour picking a lock right below a camera without being disturbed
- **Alarms are only as good as security agents behind them**
  - A bit of social engineering and you’re good to go!

10/10: The weakest link

SYNACKTIV



We already pay a security company to handle security.

10/10: The weakest link

- **Some actual quotes**

10/10: The weakest link

- **Some actual quotes**

  - “I see them! Don’t intervene, they are normal people!”

    A small site manager

10/10: The weakest link

- **Some actual quotes**
  - “I see them! Don’t intervene, they are normal people!”

    A small site manager
  - Alert closed: “Nobody was there upon my arrival.”

    A large site guard

10/10: The weakest link

- **Some actual quotes**
  - "I see them! Don't intervene, they are normal people!"

    A small site manager
  - Alert closed: "Nobody was there upon my arrival."

    A large site guard
  - "Thank you for your work, you're doing a great job, continue like that!"

    A large site guard

Wrap up

SYNACKTIV

- **Apply same best practices for physical security you already do for decades in cybersecurity**
  - No need to reinvent the wheel!
- **Don’t assume/hope something is secure**
  - Test it!
- **PDCA**
  - Test to check if expectations are fulfilled
    - Identify your worse security weaknesses
  - Fix them
  - Go back to step one

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com