Computer Safety, Security

… some tips and tricks

for you DESY stay, and hopfully also beyond

Yves Kemp, DESY IT
Beamline4Schools, 23.9.2022

… please connect to ZOOM, presenter is remote

HELMHOLTZ RESEARCH FOR GRAND CHALLENGES

DESY.

(Some) Terminology

- **Security vs. Safety**
  - Safety prevents from internal, unintended, accidental threads
    - “The safety fence around my pool protects my child from falling into the water”
  - Security prevents from external, intended, (criminal) threads
    - “The security fence around my property protects us from burglars”
- **IT security, data security, data protection**
  - IT security and data security is the effort of the organization to secure its functioning and data against threats
  - Data protection is the effort to protect *your* privacy / *your* private data against other users / your organization / the state / …
  - Sometimes these two goals go in line, sometimes they don’t

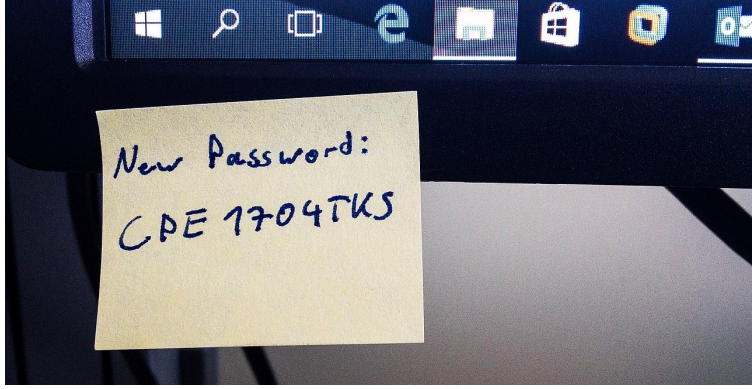
Risk assessment

- **There Is No Such Thing As Absolute Security and Safety**
- We always have to assess:
  - What do we want or need to protect?
  - What are possible threats?
  - What is the probability of them occuring?
  - What is the impact if it occurs?
  - What counter-measures can we take?
  - What is their cost (in terms of price, complexity, usability,…)?
- Periodically reassess threats, impacts, measures, costs, effectivity and user acceptance

Movie: Armageddon
Meteor hits Paris

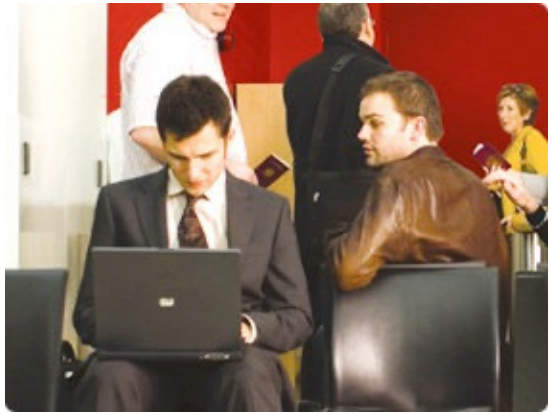
- We could now continue with a formal threat-impact-measures-cost presentation
- We won't: Instead present some measures *we* take, and measures *you* should take … a random selection, not meant for completeness

Passwords _ 1

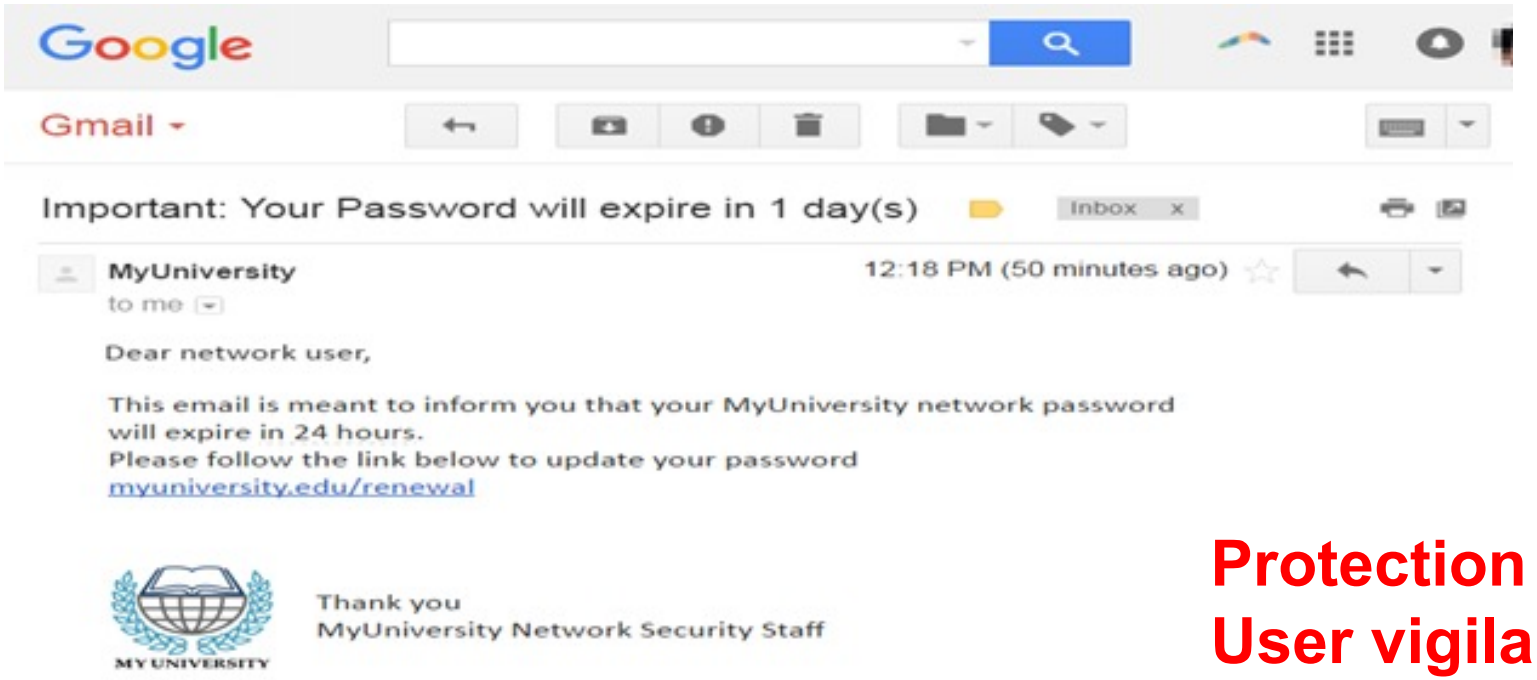


- Passwords are the (one) authentication method for computer systems
- Organizations usually have password management systems, and passwort policies
  - Password management: Have one password for multiple/all systems of the organization
  - Password policies: E.g >=8 characters of >=3 categories, no word contained in dictionary, change every 6 month
- Organizations: Do not store passwords in cleartext , use strong hashing functions, secure the password DB
- YOU: Chose complex passwords, to prevent guessing, and to protect against stealing of password DB
- Why change every 6 month? Prevent breach via third-party service in case password is reused
- You should have passwords for each different service
  - Password Managers are (usually) OK … beware of cloud based systems
  - You can write down your password, but protect this paper as you would protect your wallet e.g.
- Never share your password with anyone else! Even not your service provider!

Passwords _ 2: New threats



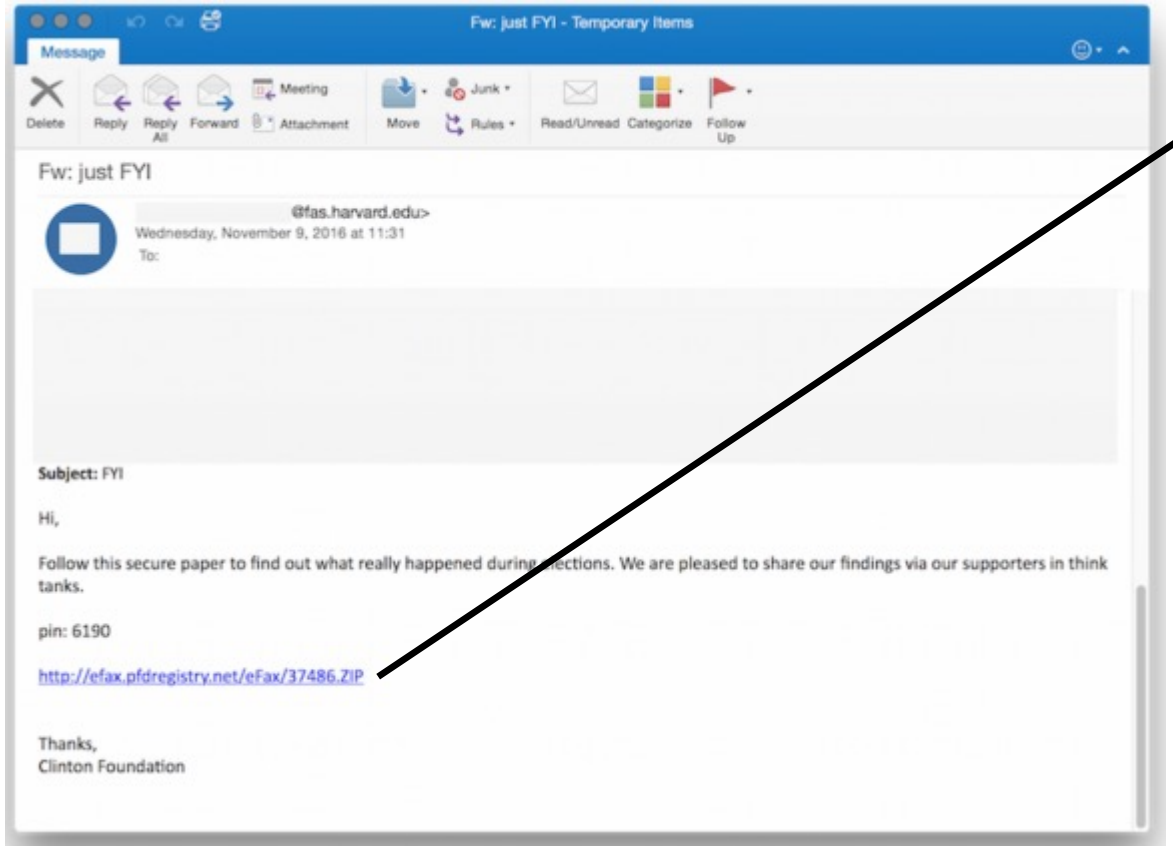
- The best password does not help, if it gets stolen in cleartext:
  - If someone watches you while typing (bus situation, keylogger, …)
  - If you enter the password via insecure connections (e.g. plain http)
  - If you fall for phishing attacks



Protection very hard for the organization
User vigilance is important here!

Email Security

- Besides password phishing attacks, emails are an entry point for malware (probably nowadays #1 entry point)



Example: Download an Office document
- Scanning emails for viruses will report nothing

↓

Office document contains Macros
- Is the automatic execution of macros disabled?

↓

Often, macro code is obfuscated, anti-virus-scanners do not (yet) know signature

↓

Macro installs malware on the system, in the contex of the user. User rights are enough for many malicious actions:
- Sending spam
- Encrypting data and asking for ransom
- Installing keylogger

Computer management

What is the most secure operating system? Linux? Windows? macOS? Android? iOS? …

- Use an operating system under support
  - No Windows 7 … No Ubuntu 16.04 after 04/2021
- Use anti-virus-software
- Use regular updates, in a timely manner
  - Usually, automatic updates are OK
- Organizations usually have centrally administered systems
  - Some management and updates are done for you
  - With additional configurations
  - With (sometimes) restricted user rights

→ Do you really need your own administered system?

- Install from trusted sources only
  - Linux: Normal repositories are OK
  - Windows: chip.de etc are not OK. Go to vendor site
  - … and also update the applications regularly
- BTW: Careful with licenses:
  - Teamviewer, VirtualBox ExtensionPack, … might not be allowed for enterprise use, hence at DESY
  - … and certainly no cracked software
- Principle of least privilege
  - When working, do you need admin rights?
  - Does your private laptop need access to internal network?

Data integrity: Backup

“No one needs backup, only restore”

- Backup prevents the loss of data because of
  - Disaster (fire, breakdown of server,…)
  - User mishap (accidental deletion, overwriting, …)
  - Malicious actions (Sabotage, virus, …)
- DESY does some central backup
  - Home-Directory on Linux (AFS) and Windows
  - Some other systems
  - Policies differ, and are rather complicated (retention period, versions, media, …)
  - Not all DESY-IT managed data is backuped!

- Evaluate the protection level you need
  - And adapt backup strategies
- Storage systems ususally have some operational safety features (e.g. RAID)
  - But this is NOT backup
- Q: What is the safest hard-drive?
- A: EVERY hard-drive can and will fail. With backup, you minimize impact
- Personally, I use TimeMachine with my Mac. I recommend similar tools for everyone on their personal devices!

Network security

- Use encrypted protocols only
  - https, ssh, …
- Limit number of services listening on the network
  - Applies when you are the administrator of a machine
  - E.g. do you need an ssh server running on your laptop?
- Understand that not all systems from an organization are open to the whole internet
  - E.g. login to most DESY systems is only possible by hopping through bastion.desy.de
- Understand that even within an organization, several security levels are implemented
  - Other systems are restricted even from within DESY machines: Only accessible through special nodes

Data security and Data privacy

- Organization: GDPR forces DESY to:
  - Provide a reason for handling and storing personal information
  - Tell users what we will do with the personal information
  - Who has access to the data
  - For how long we will store the data
  - Personal data for service providers: IP adress, account name, …
- YOU also are involved:
  - Best not store sensitive data on personal computers, instead leave on central server (DESY, not Google!)
  - Is the hard-drive of your laptop encrypted?
  - Transferring data: Via USB disks? Via unencrypted emails? Via Dropbox etc?

… just in case something happens, or you observe something

- Communicate as early as possible:
  - With your group administrator
  - With it-security@desy.de (or similar contacts at your organization)
  - Observation: contact system administrators. At DESY-IT, uco@desy.de is central entry point
- Limit damage: e.g.:
  - System infection: Do NOT SHUTDOWN a system
  - System infection: Take the system off the network (cable, disable WLAN, …)
  - Compromised password: Change your password from a clean/unaffected system
- Wait for instructions, and describe with as much details as possible what you did and observed

- **Usually, no-one will blame you!**

We *are* under attack

```
[root@bastion07 ~]# grep "Failed password for" /var/log/secure-20200908  | wc -l
1042
```

Mülhaupt, Tobias (via RT)	[rt #990678] Angebot
Mülhaupt, Tobias	[grid] Angebot
Mülhaupt, Tobias (via RT)	[rt #990667] Angebot
Mülhaupt, Tobias	[atlas-germany-computing] Angebot
Mülhaupt, Tobias	Angebot
Mülhaupt, Tobias (via RT)	[rt #990661] Angebot
Mülhaupt, Tobias	[naf-ilc-support] Angebot
Mülhaupt, Tobias (via RT)	[rt #990648] Angebot
Mülhaupt, Tobias	[poise-users] Angebot
Mülhaupt, Tobias (via RT)	[rt #990591] Angebot
Mülhaupt, Tobias	[naf-ilc-support] Angebot
Mülhaupt, Tobias (via RT)	[rt #990580] Angebot
Mülhaupt, Tobias (via RT)	[rt #990574] Angebot

ResearchProfessional News

GERMANY 07 JAN 2020 |

Cyberattack hits Giessen university

By Hristio Boytchev in Berlin Share

ZDNet SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: Your digital privacy is under attack. Can anything be done to protect it?

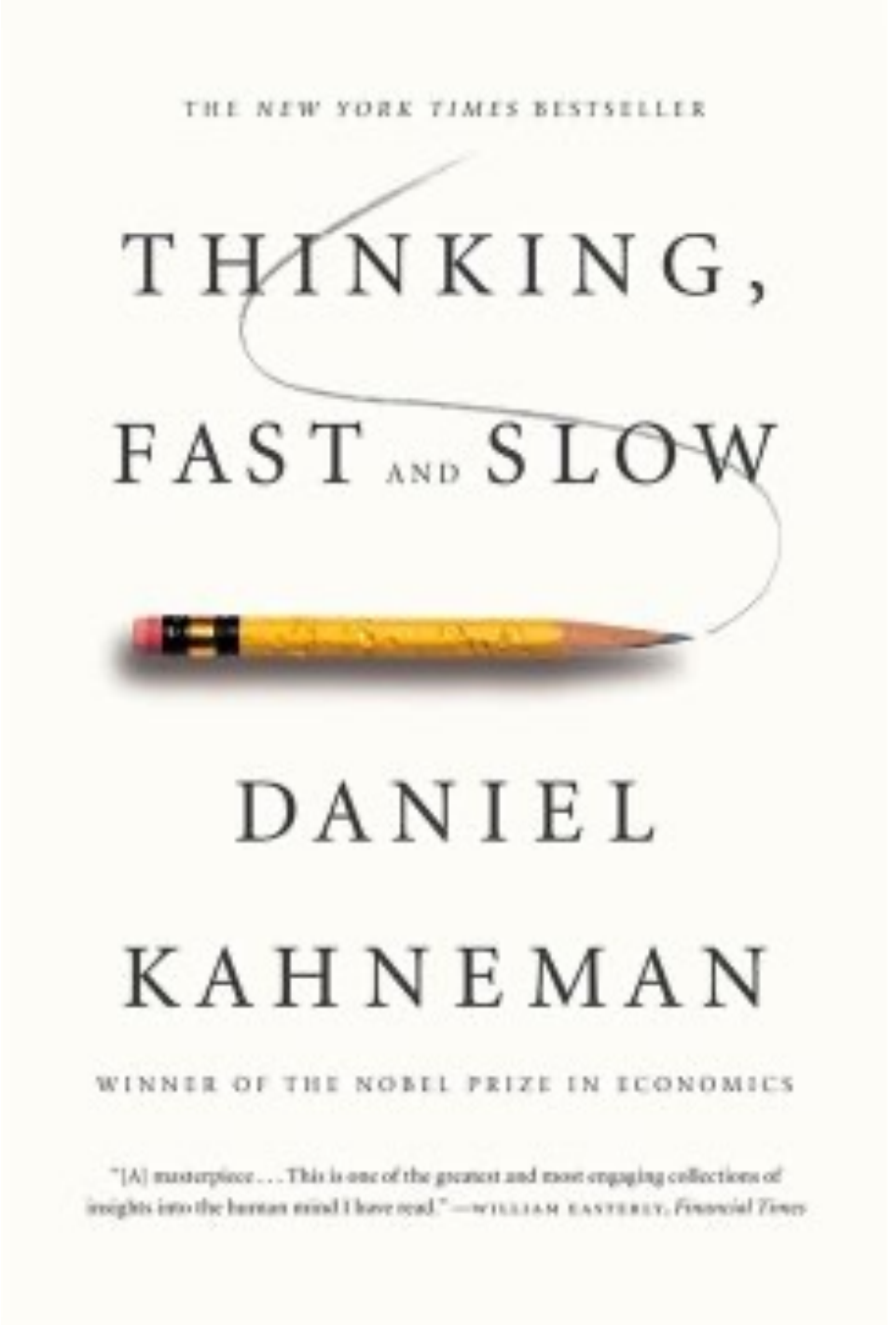
Supercomputers hacked across Europe to mine cryptocurrency

Confirmed infections have been reported in the UK, Germany, and Switzerland. Another suspected infection was reported in Spain.

Some psychology behind attacks

Very over-simplified summary for our context:

- Humans understand using the ”slow” system
- Humans act using the “fast” system
- Attackers try to trigger the “fast” and bypass the “slow” system
- We must train users to act correctly using the “fast” system
- We must help the “slow” system with correcting decisions of the “fast” system



Security is not complete without YOU

https://cds.cern.ch/record/1269310

Backup Slides

What’s this? Would you plug that into your computer?

https://shop.hak5.org/products/usb-rubber-ducky-deluxe

Passwords _ 1

- Why complicated password?
  - Prevent easy guessing (admin:admin , kemp:123456 , …)
  - Prevent brute force attacks on stored credentials.
    - e.g. password 123456 is saved as 1foobar$NvAPE3IOplw6rL8BLHuHl/
    - 1foobar$ indicates (deprecated) MD5 hash function, with foobar being the salt (in cleartext) and NvAPE3IOplw6rL8BLHuHl/ being 123456+salt hash value
    - Should attackers steal the organization password database, and crack with brute-force methods
    - Time for cracking increases exponentially with password complexity

Passwords _ 2

- Why change every 6 month? Organization:
  - Assumption: Our password DB is safe. Should we suspect it to be hacked, we will fix the system, and ask you to IMMEDIATELY change passwords
  - We know that users reuse passwords at other services. We do not trust other services. Should e.g. Dropbox kemp:v3ri$tr0nG be hacked, make sure that after some time the DESY password is changed, and attackers cannot compromise the DESY kemp account
- You should have passwords for each different service
  - One for DESY, another one for CERN, another one for Amazon, another one for Google, …
  - It is OK to use passwords managers. They usually come with very strong passwords, make suggestions for each individual service and help with regular changes.
    - Cloud based password managers are not recommended … but helpful.
    - Personal judgment is needed … sometimes, organization policies must be followed however.