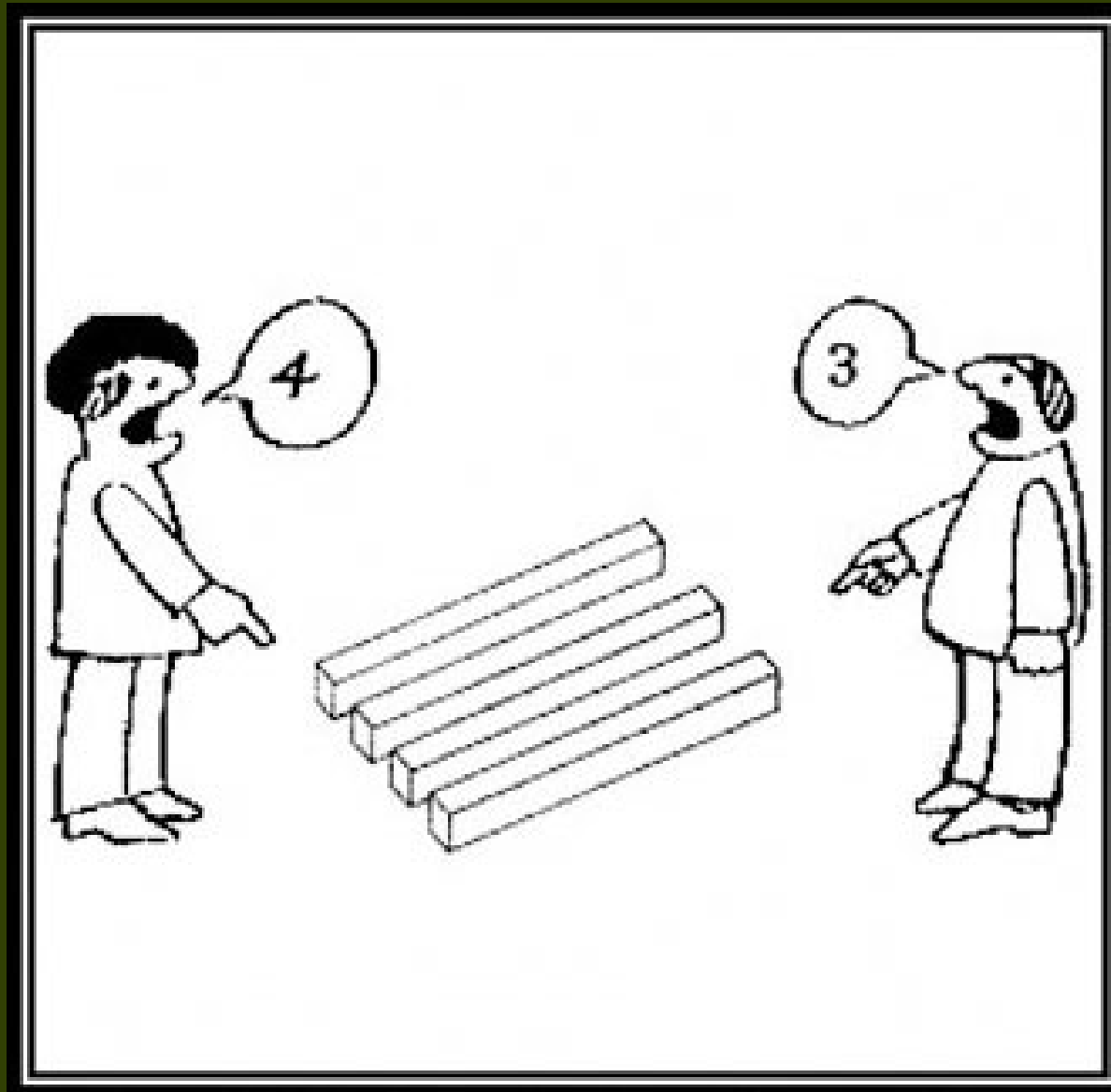


CONTENTS

- Professional part
 - Paradigm shift
 - Virtual world – real security
 - Old rules, howto-s: good for re-thinking – Passwords

PARADIGM



PARADIGM

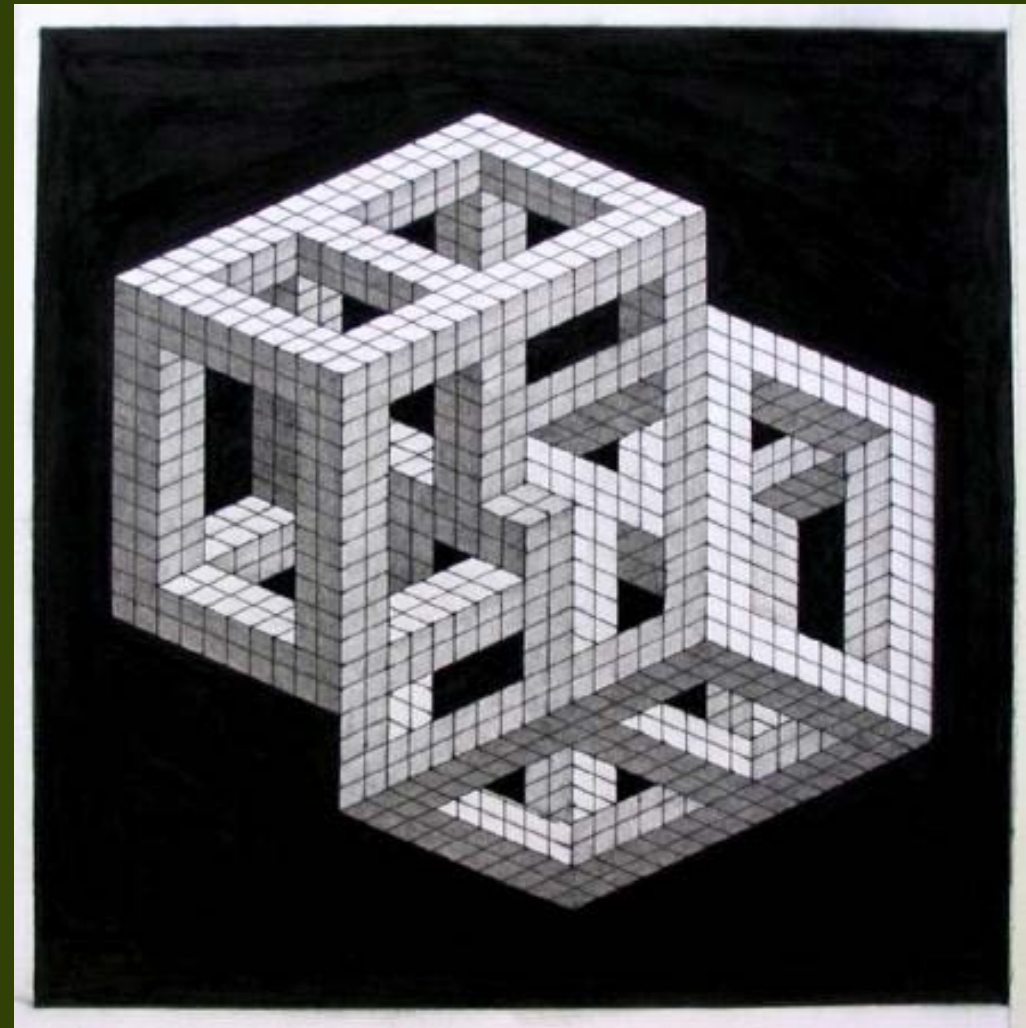
- What is that, how could you describe it?

PARADIGM

- Set of generally accepted views and rules
The way you think the world works
 - In a given field
 - In a given time period
- To deny them is dangerous
- For example:
 - The Earth is flat
 - De strigis, quae non sunt, nulla questio fiat
 - PC – Political Correctness

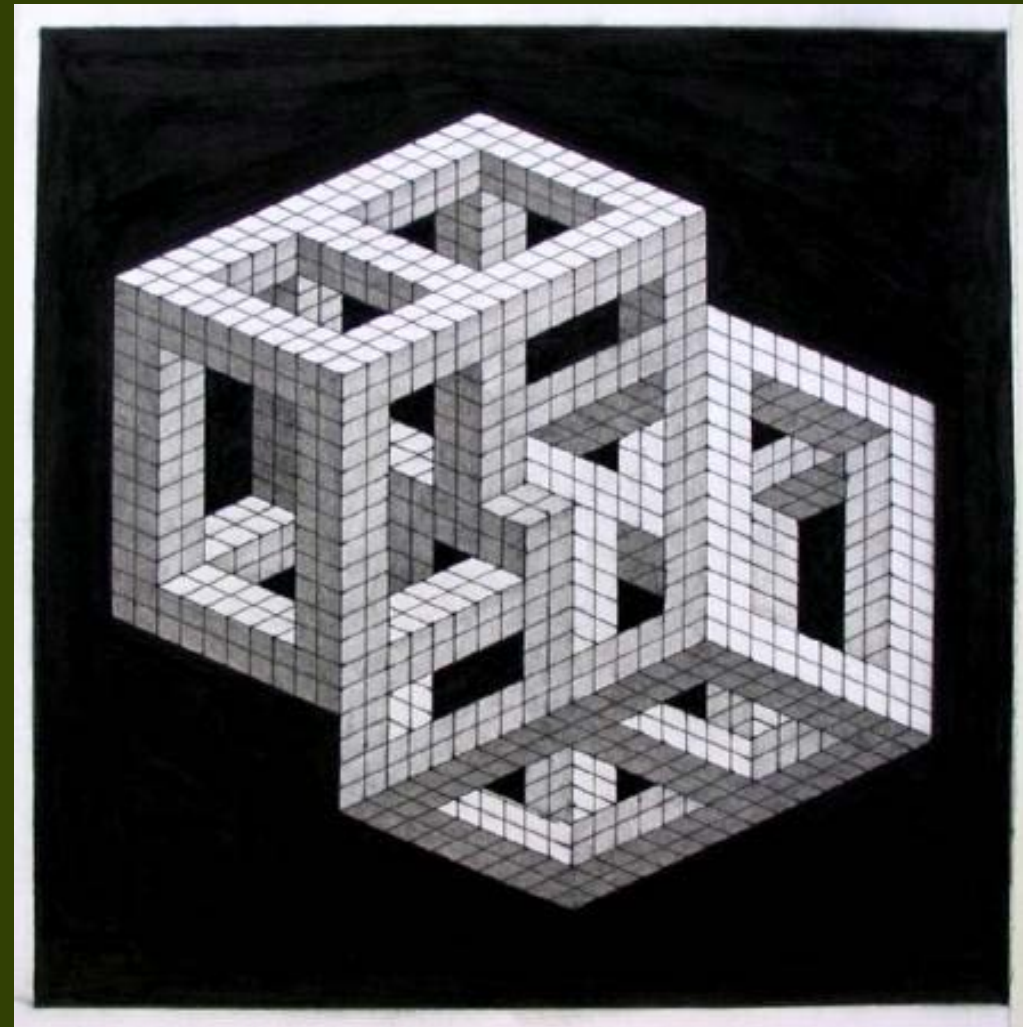
PARADIGM SHIFT

- Paradigm shift – when the paradigm changes
- Why?



PARADIGM SHIFT

- Paradigm shift – when the paradigm changes
 - Knowledge exceeds its former limits
 - Revolutionary new technology
 - Book printing
 - Steam engine
 - Internet = digital network



PARADIGM SHIFT

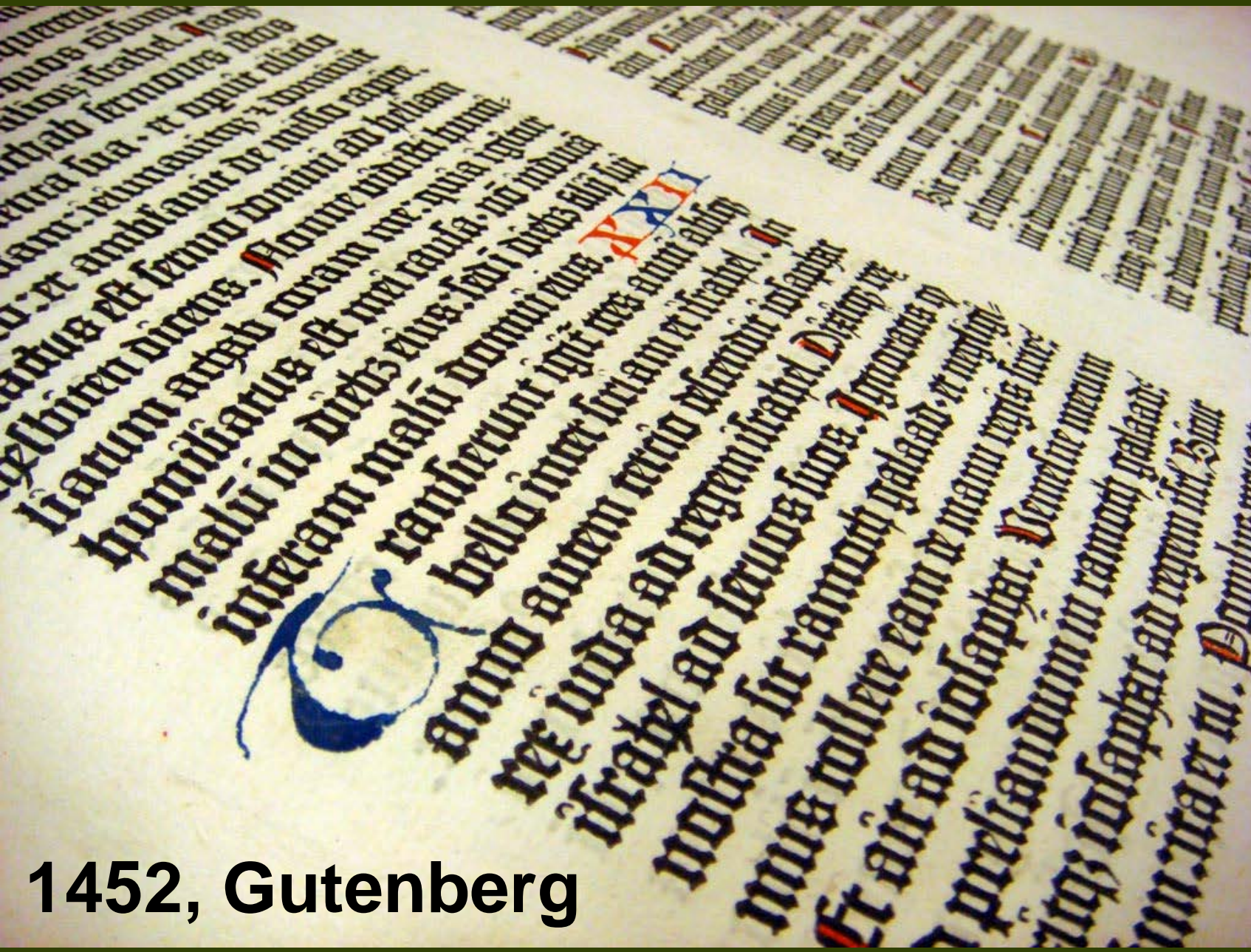
- Paradigm shift – when the paradigm changes
 - Gutenberg
 - Digital networks – Internet
 - Books, music, movies
 - Cyber crime, cyber war
 -

PARADIGM SHIFT

Corvina codex
from the library of
King Matthias



PARADIGM SHIFT I.



1452, Gutenberg

PARADIGM SHIFT I.

- One copy – cca. one year, one monk
- 10 thousand copies – few days
- **Art → Industrial process**
- What are the consequences?

PARADIGM SHIFT I.

- Codex copying ended
- Books became primary tool for
 - storing and
 - transferring the knowledge



PARADIGM SHIFT II.

Today the print is considered:

- Expensive
- Slow
- Hard to carry
- Copying: quality decreases (slow, expensive)

PARADIGM SHIFT II.



PARADIGM SHIFT II.

- Cost of copying and carrying to somewhere?

PARADIGM SHIFT II.

- Copying needs:
 - Zero cost
 - Zero time
 - Quality is the same
- Carrying to anywhere:
 - Zero cost
 - Zero time

PARADIGM SHIFT II.

- Google, Ctrl-F



PARADIGM SHIFT II.

Knowledge transfer
has never been
so easy!

BUT!

VIRTUAL WORLD REAL SECURITY

- Internet has become part of everydays
- Amount of data increases
- Our dependency on data increases day by day

OLD RULES ARE GOOD TO RE-THINK



Tivadar Földi

OLD
RULES & HOWTO-S
ARE
GOOD TO RE-THINK

*

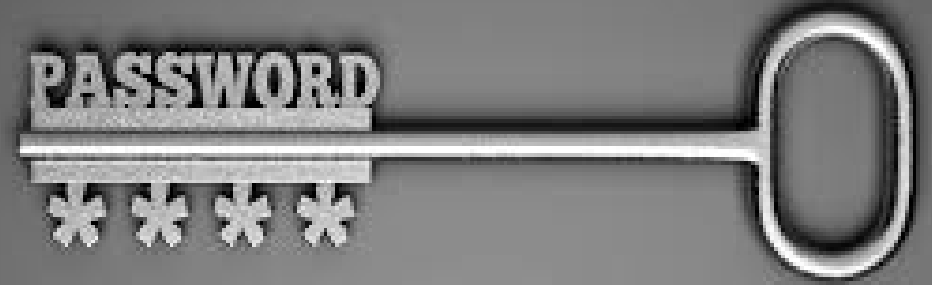
PASSWORDS

USER AUTHENTICATION METHODS

USER
KNOWS
SG.
IN HIS MIND



USER HAS SG.



BIOMETRIC



USER AUTH METHODS

- Price
- Complexity
- False +/-
- Known incidents

PASSWORD RULES

- What makes a good password?
- Example?
- The most important rules?

PASSWORD RULES

- From the point of view of the management?

GOOD PASSWORD USER - GENERAL POINT

- Must be memorable!
- Must NOT be guessable by others!

MUST BE MEMORABLE

- You should know 😊

MUST NOT BE GUESSABLE

- How can you guess someone else's password?
- ?
- ??
- ?? ??

„DEFAULT” PASSWORDS

- Factory default pwds in wifi devices
- asdfgh, 123456 – default pwds of lazy sysadmins
- (French bank)



RELATIONSHIP between person and pwd

- Date of birth
- Name of girl-/boyfriend, wife/husband
- Name of pet, favourite star, beer, etc.
- (example - celebs, Obama)

RELATIONSHIP between username and pwd (strings)

- admin - admin
- admin - admin!admin, admin01



RELATIONSHIP between username and pwd (logical)

- James Bond -- ???

RELATIONSHIP between username and pwd (logical)

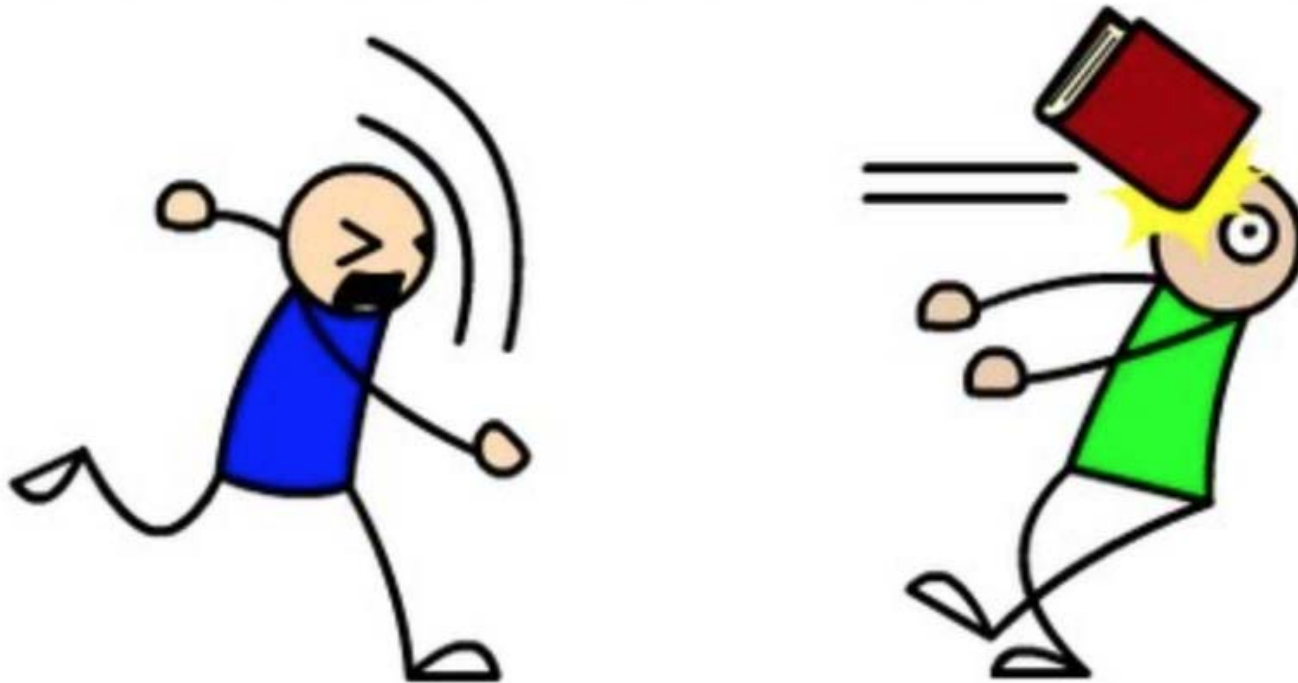
- James Bond -- 007



DICTIONARY ATTACK

- Software tries all the words from a list

DICTIONARY ATTACK!



ADVANCED DICTIONARY ATTACK

- Software tries all the words from a list and simple modifications
- Based on the known pwd structures
- E.g.:
password – password01..password99
etc.

BRUTE FORCE



BRUTE FORCE

- Software tries out all the possible char combinations
- What is the result?
- What is the question?

BRUTE FORCE

- Software tries out all the possible char combinations
- What is the result? – Will find it!
- What is the question? – How much time?

BRUTE FORCE

- Number of possible combinations?

BRUTE FORCE

- Number of possible combinations?
- Char set: 80, length: 8...

BRUTE FORCE

- Number of possible combinations?
- Char set: 80, length: 8...

$$80^8 \sim 10^{15}$$

- It means: ??? ???

BRUTE FORCE

- Number of possible combinations?
- Char set: 80, length: 8...

$$80^8 \sim 10^{15}$$

- It means: length makes a good pwd, not the mixed type of chars in it.
- Charset: limited
- Length: unlimited

BRUTE FORCE calculations in Excel/Calc

- Cracking speed: Jeremy Gosney
- 25 AMD Radeon GPUs
- How many tries/sec??



BRUTE FORCE calculations in Excel/Calc

- Cracking speed: Jeremy Gosney
- 25 AMD Radeon GPUs
- ~350 billion tries/sec $\sim 10^{12}$
(on NTLM hashes)
- Do some calculations!?

BRUTE FORCE calculations in Excel/Calc

<i>Charset</i>	<i>Length</i>	<i>Cracking time</i>
80	8	?
100	8	?
80	10	?
80	21	?

BRUTE FORCE calculations in Excel/Calc

<i>Charset</i>	<i>Length</i>	<i>Cracking time</i>
80	8	half hour
100	8	3 hours
80	10	4 months
80	21	10^{20} years

BRUTE FORCE

- 3 hrs - 4 months: no difference 😞
- 3 hrs - 4 billion years: THIS is a difference 😊



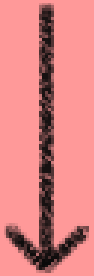
GUESSING METHODS SUMMARY

- „Default” passwords
- Relationship between
 - Person and pwd
 - Username and pwd (as strings)
 - Username and pwd (logical)
- Dictionary
- Advanced dictionary
- Brute force

EXPERIENCE

- Length is more important than the complexity of char set!

SHADOW PASSWORD & HASH FUNCTION



```
jay:$1$V5C7ior3$Q5dgwwZqG9MldIINAhytZ0:13790:0:99999:7:::
```

Here's an entry from the `/etc/shadow` file. You can tell that this hash was created by the MD5 algorithm, by the "\$1\$" prefix.

SHADOW PASSWORD & HASH FUNCTION

- MD5: crackable
- NTLM: ~350 billion tries per sec
- Bcrypt: ~ 72 thousand tries per sec

MISBELIEVES

- Pwd should contain different type of chars:
 - Gmail
 - Federal Trade Commission
 - Twitter
 - OTP (biggest bank in Hungary)
 - (nearly everywhere)

MISBELIEVES

- Pwd generation sw by HP




The screenshot shows a Windows-style application window titled "Site-Specific Passwords Versio...". On the left side of the window is the HP logo with the word "invent" underneath it. The main area of the window contains three input fields:

- Your password:** A text box containing "qwerty". The first six characters are obscured by "xxxxxxx".
- Site name:** A text box containing "amazon".
- Site password:** A text box containing "SHX9AGgvKlls".

At the bottom of the window, there are two buttons: "Generate" and "Help".

MISBELIEVES

- Stanford University



orange eagle key shoe

21 CHARACTERS!
*including the spaces

The image shows the Stanford University logo, which consists of four elements: an orange, an eagle, a key, and a shoe. Below each element is its name in a typewriter-style font, underlined. A large blue bracket spans all four words, with an arrow pointing down to the text '21 CHARACTERS!' and '*including the spaces'.

MISBELIEVES

- Stanford University - Could you calculate?

MISBELIEVES

- Stanford University - Could you calculate?

$$2000^4 \sim 1,6 * 10^{13}$$



16 sec

MISBELIEVES

- 1 Use a "passphrase": a sentence you can remember. Then replace each word of the phrase with its initial, a similar digit or symbol, or, at random, use a whole word. For example:

MY DOG NATE WOOFES AND RUNS IN HIS SLEEP



→ The new password is mdN8w@r!hs. (Don't use this one, though.)

- 2 That may still be tough to remember. If you need to, write a reminder and hide the paper somewhere safe. But write the phrase or a hint, not the password.
- 3 Generally, if you have a strong password, you don't need to change it unless you suspect you've been hacked. But don't use the same one for different services.

MISBELIEVES

- When do you change your password?
- Do you use the same pwd for different sites?
- Can you write your pwds down?
- Would you use a pwd management program?
- Is it possible to write down your passwords?

BEST PRACTICE FOR USERS

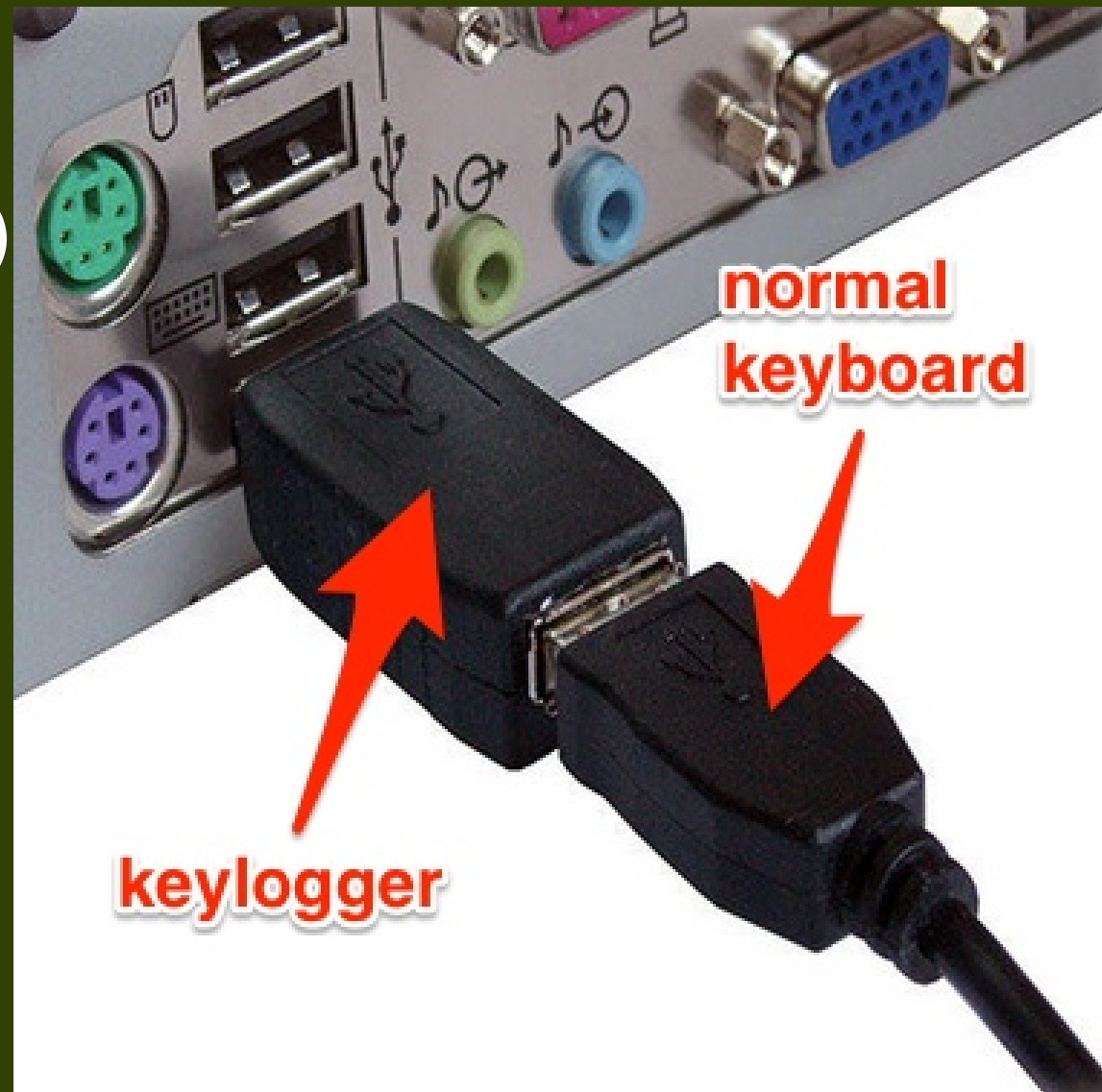
- Long password
- Don't use a common method to generate
- Should be memorable, e.g.:
three words at least,
add some extras at three positions at least.

BEST PRACTICE FOR USERS

- E.g.:
Petrovic Karadjordje
- was born on 3 Nov 1768
- **3Petrovic11Karadjordje1768**
- Dictionary attacks are language-dependent!

YOU MAY HAVE THE BEST PWD...

- Shoulder surfing
- Hidden camera
- Keylogger (hw/sw)
- Phishing emails
- Bad sysadmin
- ...etc...



SYSADMINS' BEST PRACTICE

- Blacklist of most common passwords



SYSADMINS' BEST PRACTICE

- Passwords must NOT be stored not even encrypted
- Shadow password: strong hash function



```
jay:$1$V5C7ior3$Q5dgwwZqG9MldIINAhytZ0:13790:0:99999:7:::
```

Here's an entry from the `/etc/shadow` file. You can tell that this hash was created by the MD5 algorithm, by the "\$1\$" prefix.

SYSADMINS' BEST PRACTICE

- „salting“: concatenate with a unique string before hashing (username e.g.)

```
kea:$1$c680fI2D$0D56JmqHLzVDbjK2IoDNM/:1480
tbmi:$1$c680fI2D$0D56JmqHLzVDbjK2IoDNM/:1480
bnk:$1$c680fI2D$0D56JmqHLzVDbjK2IoDNM/:1480
syxtus:$1$c680fI2D$0D56JmqHLzVDbjK2IoDNM/:1480
paller:$1$c680fI2D$0D56JmqHLzVDbjK2IoDNM/:1480
ricsi:$1$c680fI2D$0D56JmqHLzVDbjK2IoDNM/:1480
```

SYSADMINS' BEST PRACTICE

- Change only if a security incident happened (or might happen), don't make users change them every month.

CONCLUSION

- Passwords are free of charge
- Will be used in the future, too
- **If used carefully, they are very secure**
- You must be careful not only for yourself.



GOOD DOG!

Invalid password.

You have one more try.