NTNU

Norwegian University of Science and Technology

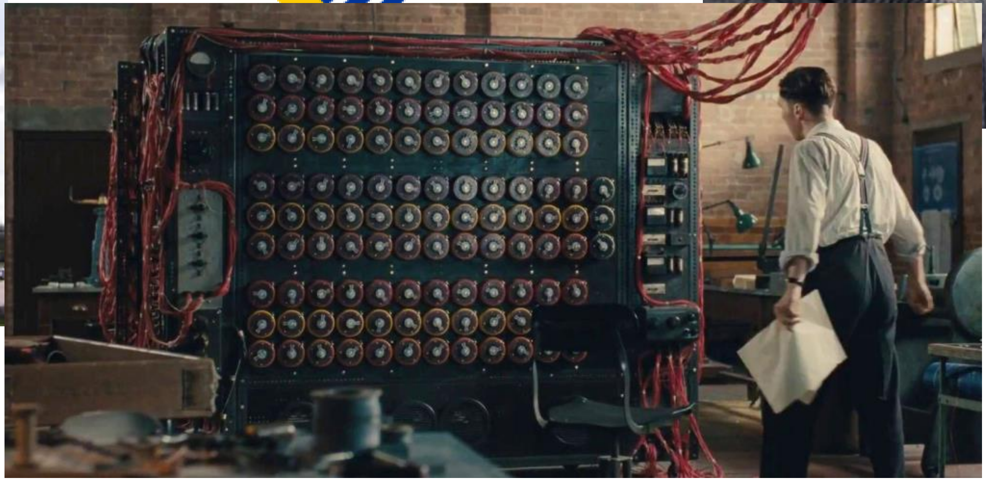
Technical tools to handle cybercrime

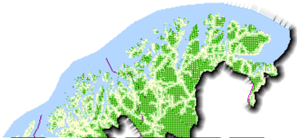
NTVA meeting in Datakriminalitet, 20/3/2018

Patrick Bours

NTNU/IIK

Who am I?

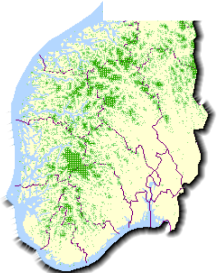




NTNU

Norwegian

Science and



Who are we?

Traditional look at IS

- Based on topics:
  - Biometrics
  - Forensics
  - Network security
  - Cryptology
  - Human/organizational aspects
  - Risk management
  - Software security
  - System security
  - Critical infrastructure security
  - …

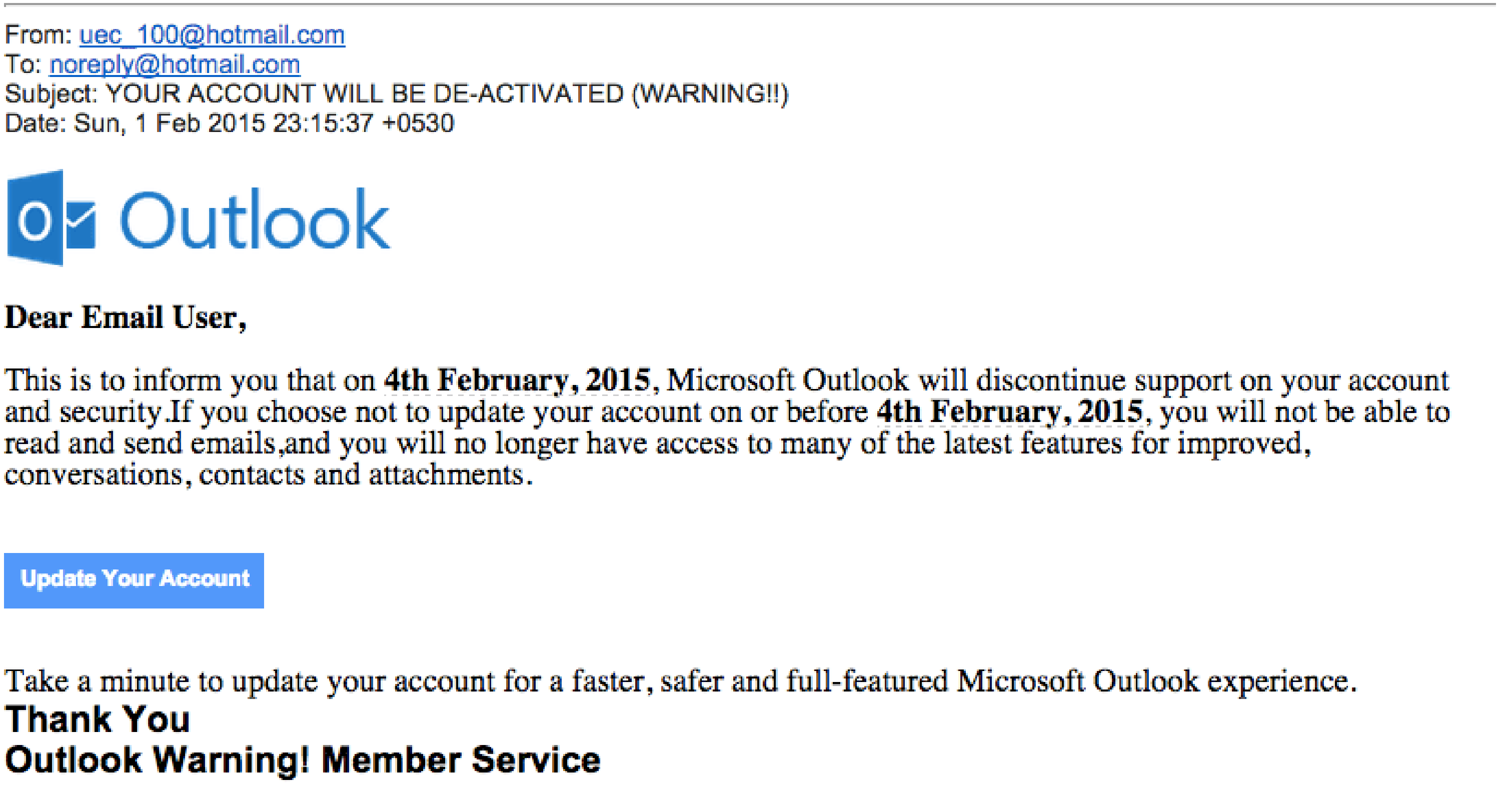
Layered look on IS

5	Societal Models	Digital economics; Risk; Socio-technical modelling; Simulation and modelling; Privacy, …
4	Digital Value Chain	Dependability and performance in complex digital ecosystems; Safe and secure systems; Robustness; Cyber range; Cyber defense; …
3	Application Domain	Cyber-physical systems; Internet of Things (IoT); Cloud; Smart grid; Networked services; Transport; Communication Systems; Healthcare; …
2	Network Technology	Telecommunication; Architectures and protocols; Software defined networks; …
1	Enabling Aspects	Cryptology; Authentication; Biometrics; Privacy Enhancing Technologies; Digital Forensics; Artificial Intelligence; Machine Learning; …

Today's presentation

- Threats
- Enabling aspects
  - Cryptology
  - Digital Forensics
  - Biometrics
- Example for a current project

Threats



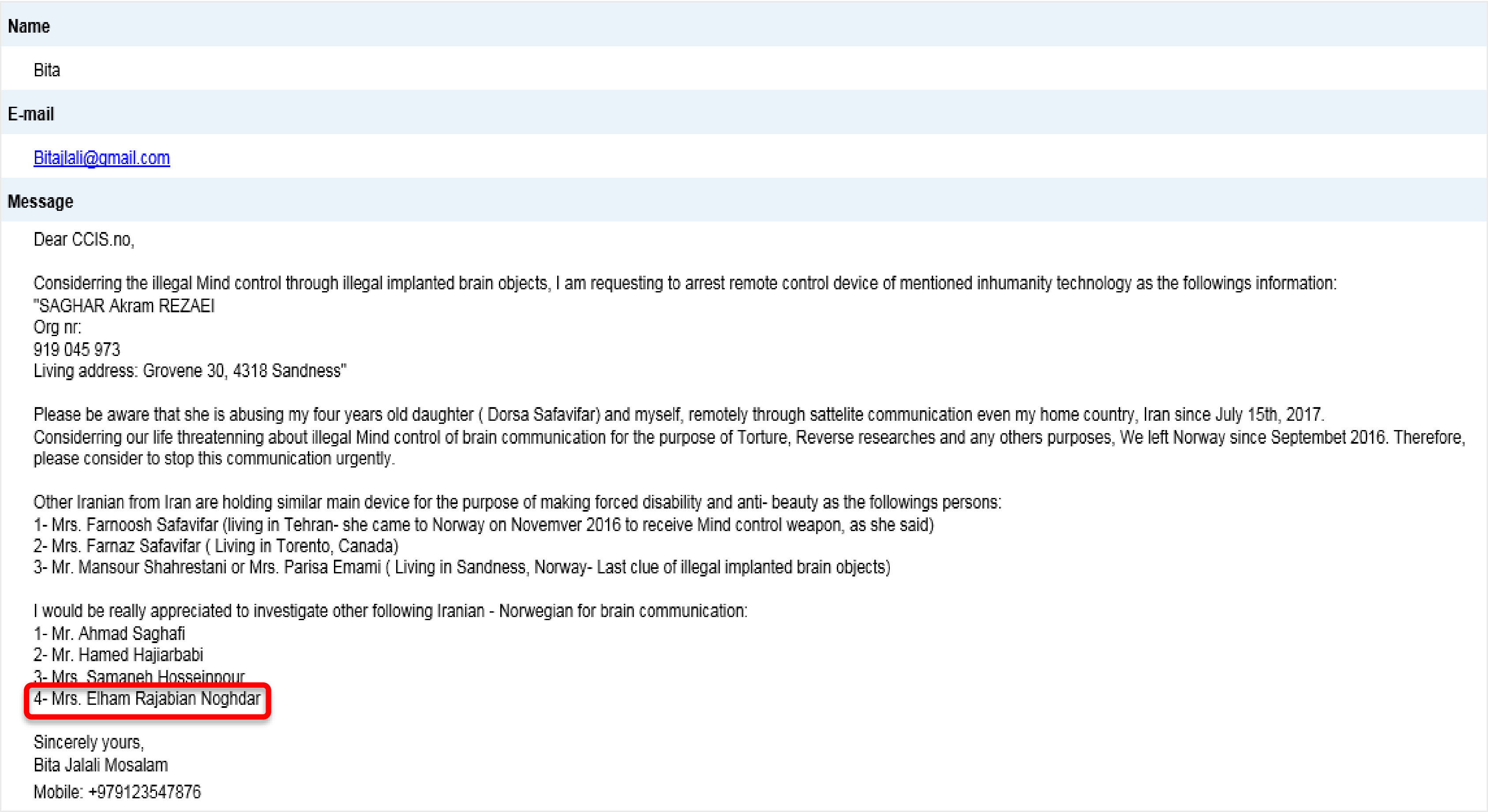
From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530

Dear Email User,

This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support on your account and security.If you choose not to update your account on or before **4th February, 2015**, you will not be able to read and send emails,and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

Take a minute to update your account for a faster, safer and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service

Threats



Name

Bita

E-mail

Bitajlali@gmail.com

Message

Dear CCIS.no,

Considerring the illegal Mind control through illegal implanted brain objects, I am requesting to arrest remote control device of mentioned inhumanity technology as the followings information:
"SAGHAR Akram REZAEI
Org nr:
919 045 973
Living address: Grovene 30, 4318 Sandness"

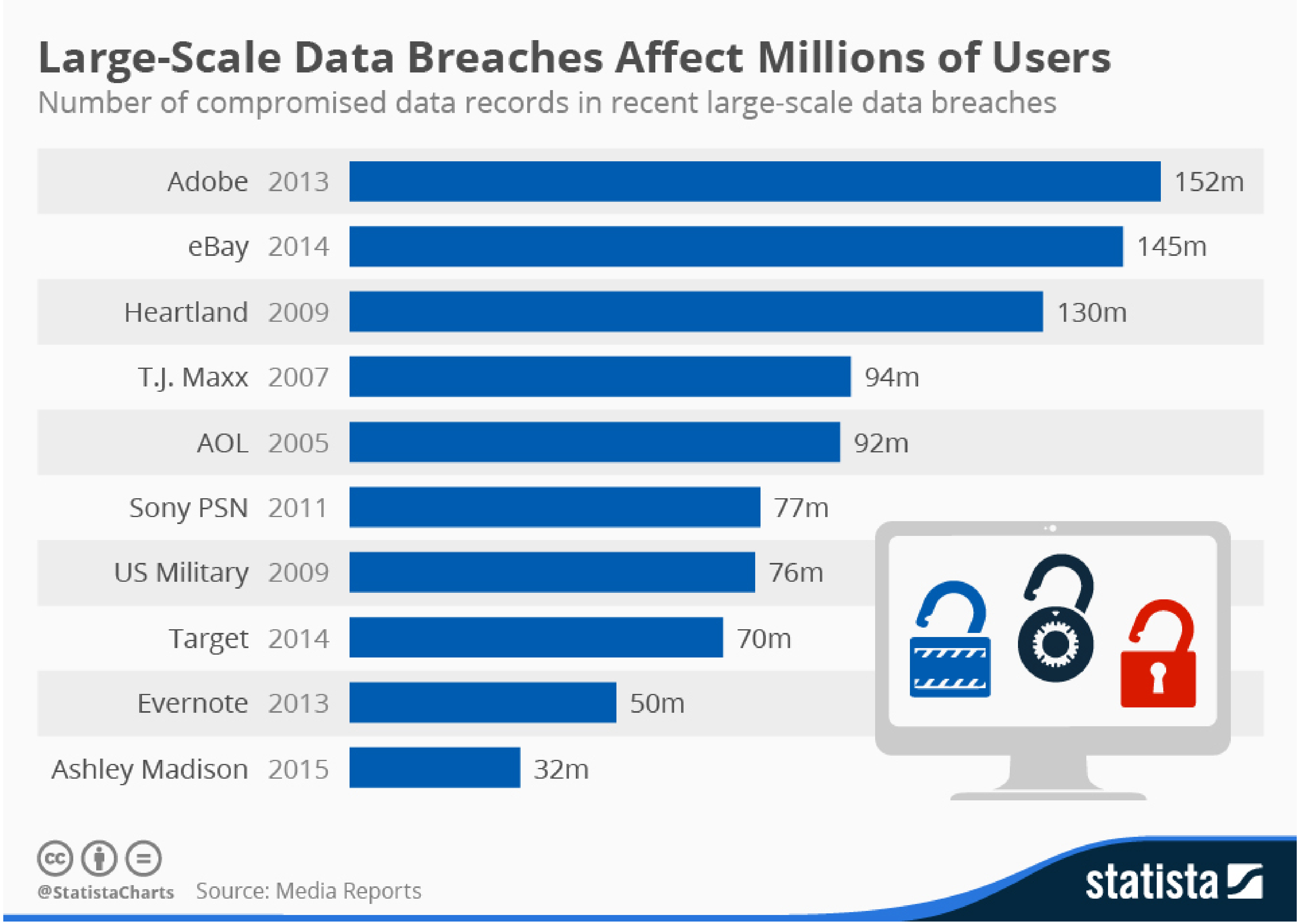
Please be aware that she is abusing my four years old daughter (Dorsa Safavifar) and myself, remotely through sattelite communication even my home country, Iran since July 15th, 2017.
Considerring our life threatenning about illegal Mind control of brain communication for the purpose of Torture, Reverse researches and any others purposes, We left Norway since Septembet 2016. Therefore, please consider to stop this communication urgently.

Other Iranian from Iran are holding similar main device for the purpose of making forced disability and anti- beauty as the followings persons:
1- Mrs. Farnoosh Safavifar (living in Tehran- she came to Norway on Novemver 2016 to receive Mind control weapon, as she said)
2- Mrs. Farnaz Safavifar (Living in Torento, Canada)
3- Mr. Mansour Shahrestani or Mrs. Parisa Emami (Living in Sandness, Norway- Last clue of illegal implanted brain objects)

I would be really appreciated to investigate other following Iranian - Norwegian for brain communication:
1- Mr. Ahmad Saghafi
2- Mr. Hamed Hajiarbabi
3- Mrs. Samaneh Hosseinpour
4- Mrs. Elham Rajabian Noghdar

Sincerely yours,
Bita Jalali Mosalam
Mobile: +979123547876

Threats

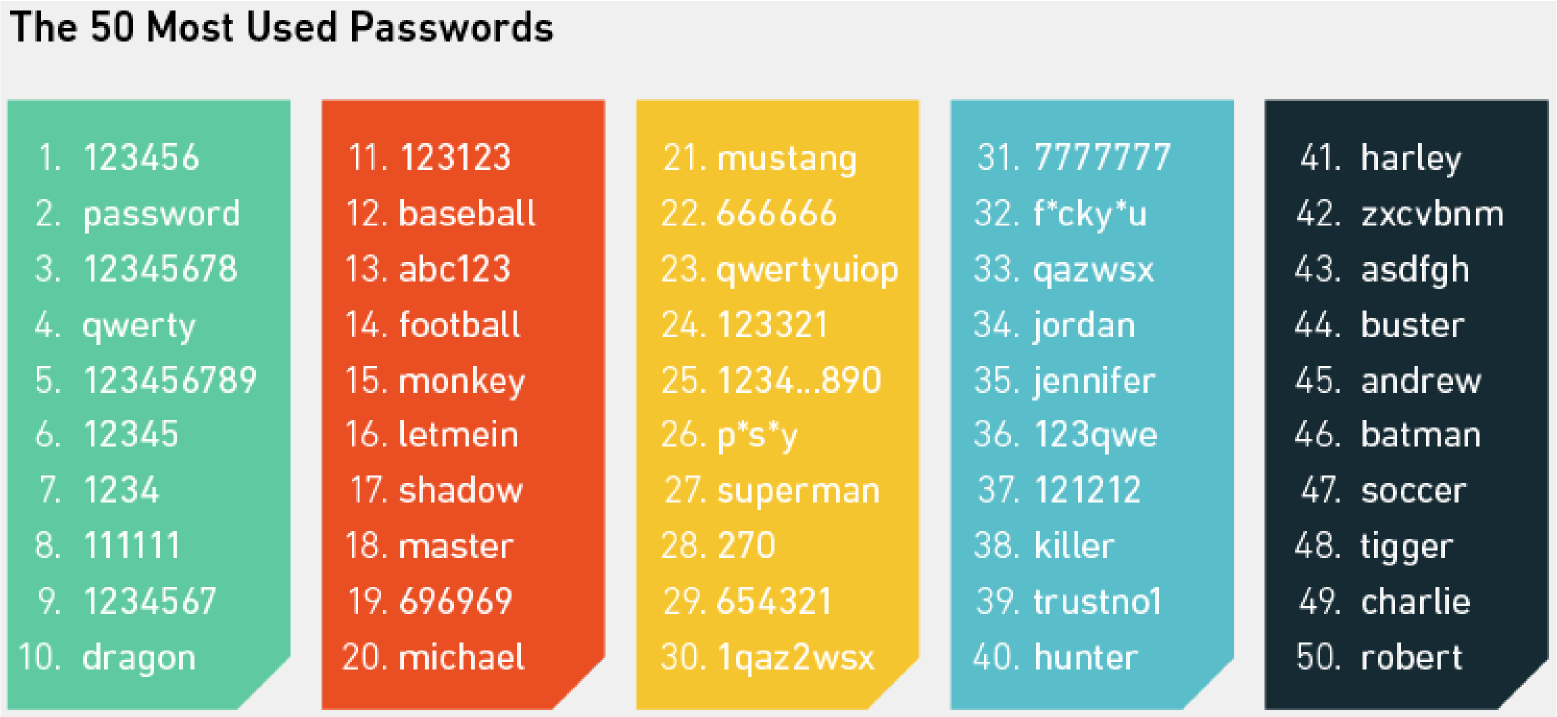


Large-Scale Data Breaches Affect Millions of Users

Number of compromised data records in recent large-scale data breaches

Source: Media Reports

Threats

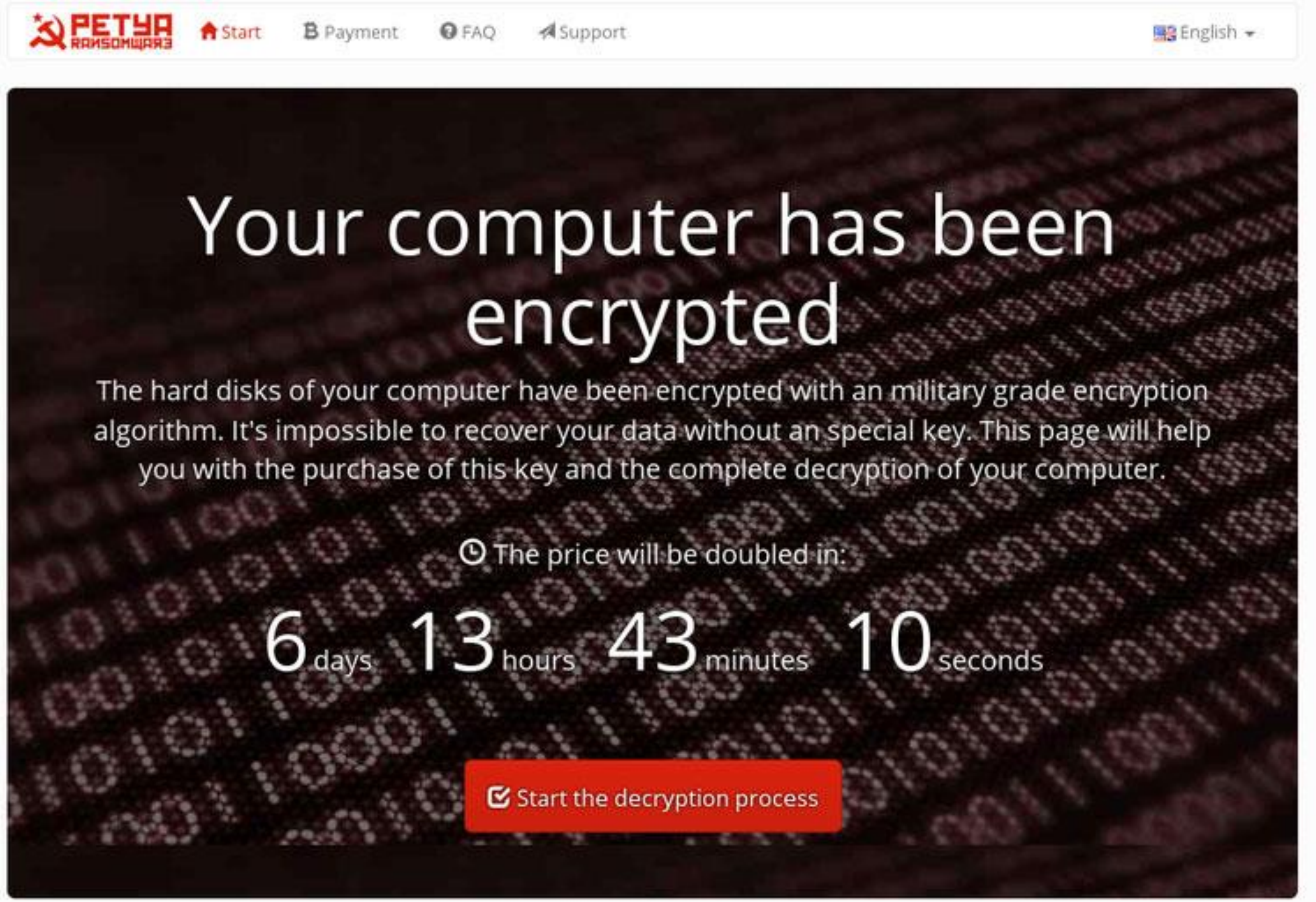


The 50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Threats

Threats



Your computer has been encrypted

The hard disks of your computer have been encrypted with an military grade encryption algorithm. It's impossible to recover your data without an special key. This page will help you with the purchase of this key and the complete decryption of your computer.

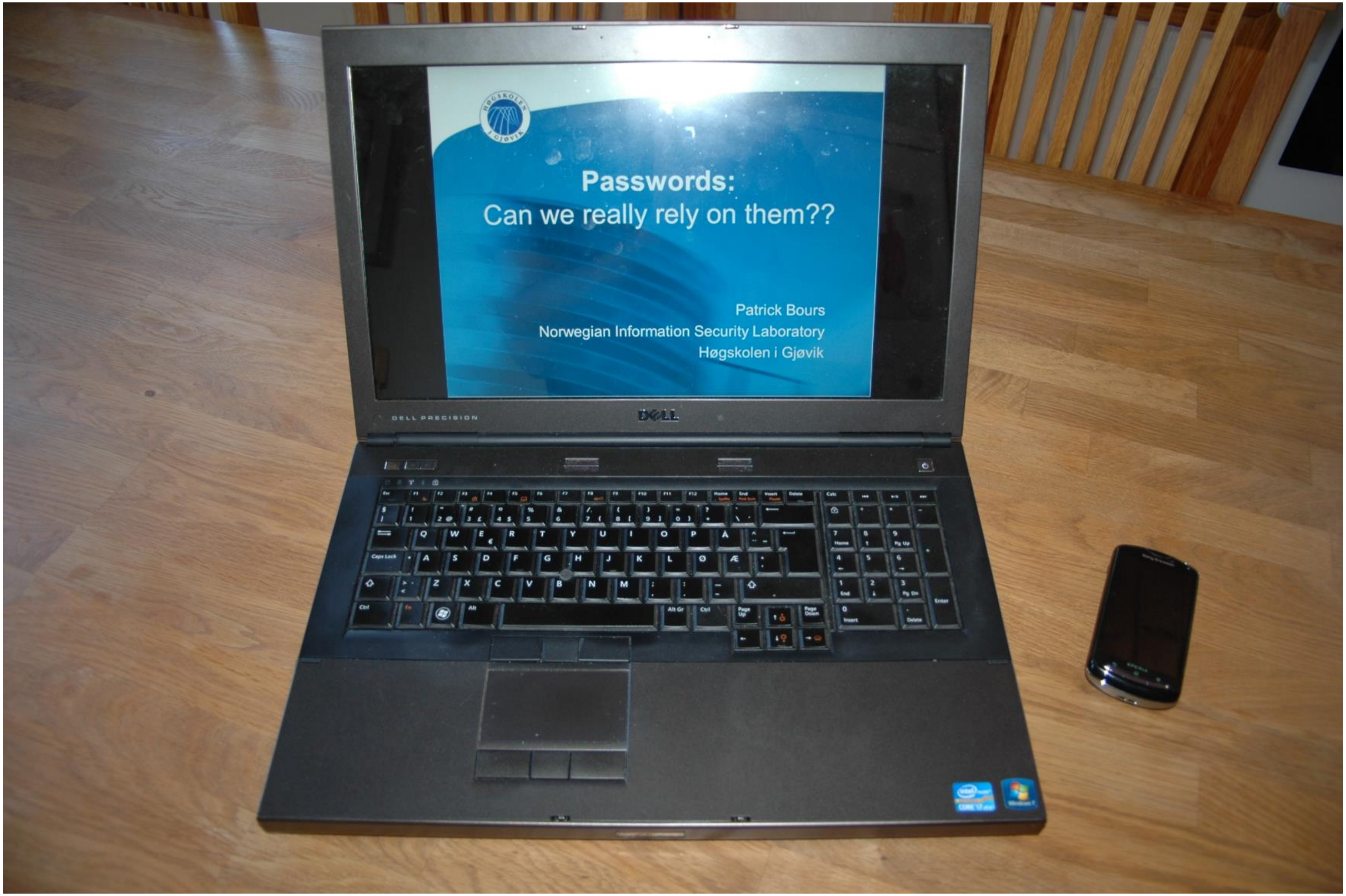
The price will be doubled in:

6 days 13 hours 43 minutes 10 seconds

Threats

“I R
SE
DON'T FALL I
Be wary of strangers
Do not remit or transf
“YOU HAVE BROKEN THE LAW.
PAY UP OR I WILL CHARGE YOU.”
I'M YOURS.”
EX SCAM
messaging apps
Do not purchase gift cards or online shopping credit for people you have not met

Threats



Passwords:
Can we really rely on them??

Patrick Bours
Norwegian Information Security Laboratory
Høgskolen i Gjøvik

Cryptology

- Cryptology = Cryptography + Cryptanalysis

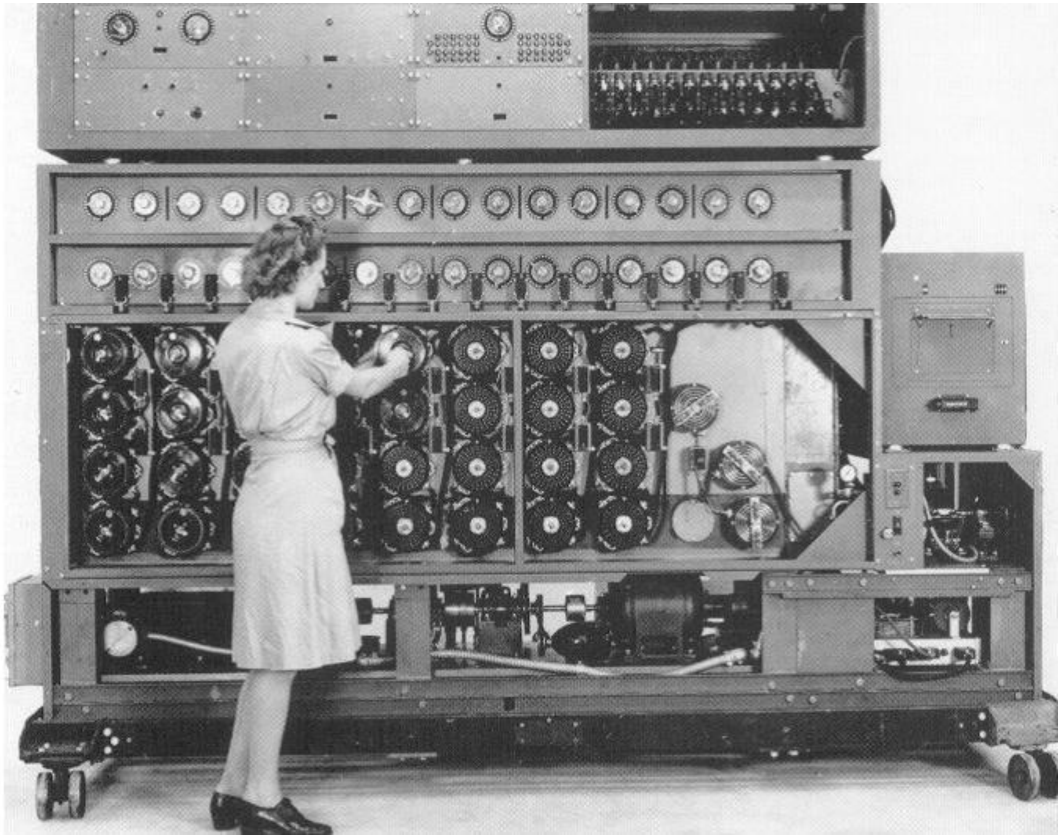
- **Cryptography:**
  Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it[1]

- **Cryptanalysis:**
  Cryptanalysis refers to the study of ciphers, ciphertext, or crypto-systems with a view to finding weaknesses in them that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm[2]

[1] http://searchsoftwarequality.techtarget.com/definition/cryptography

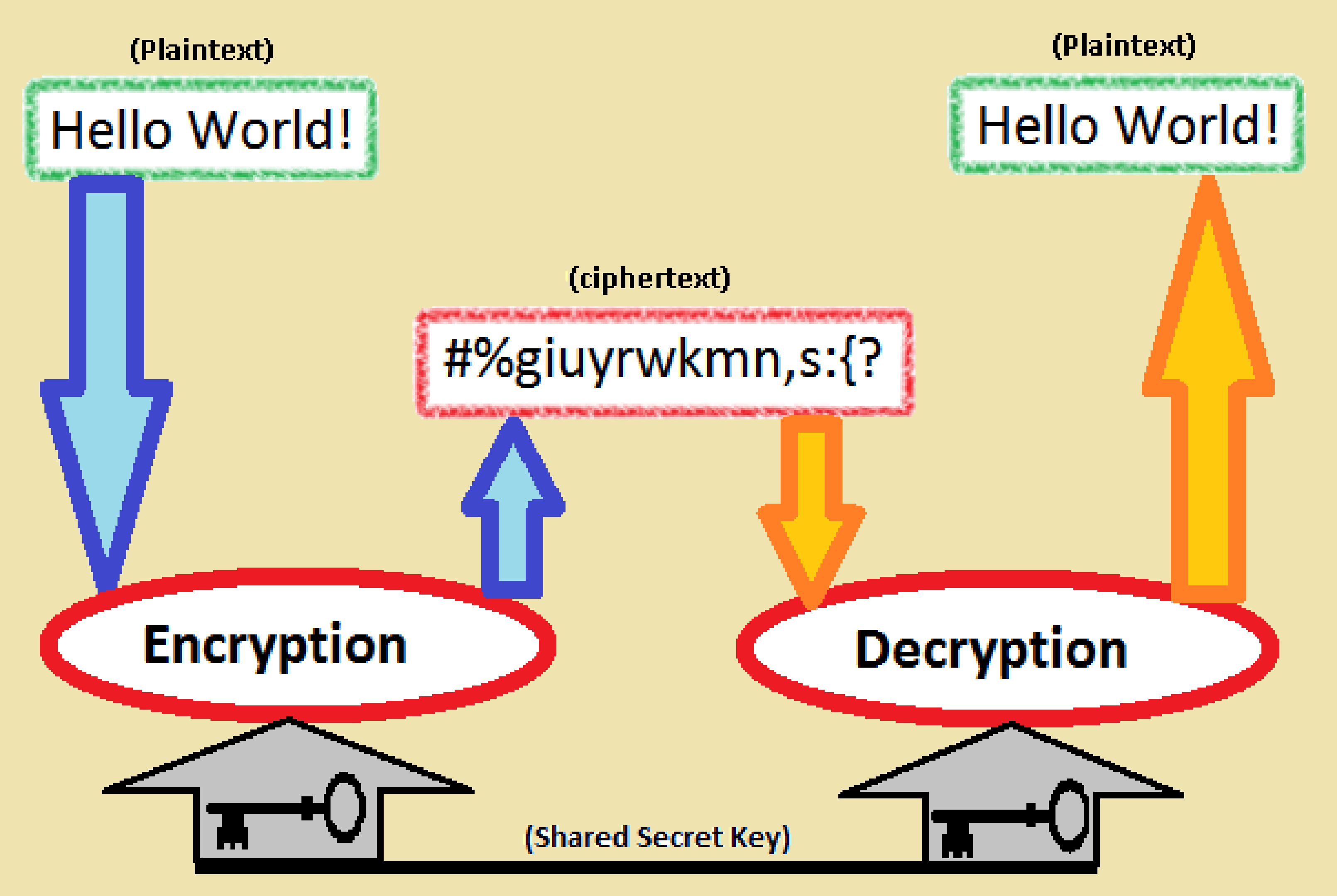
[2] http://searchsecurity.techtarget.com/definition/cryptanalysis

Cryptography vs Cryptanalysis: Enigma vs The Bombe



https://pocketbookuk.com/2015/02/22/the-imitation-game-alan-turing/

Terminology

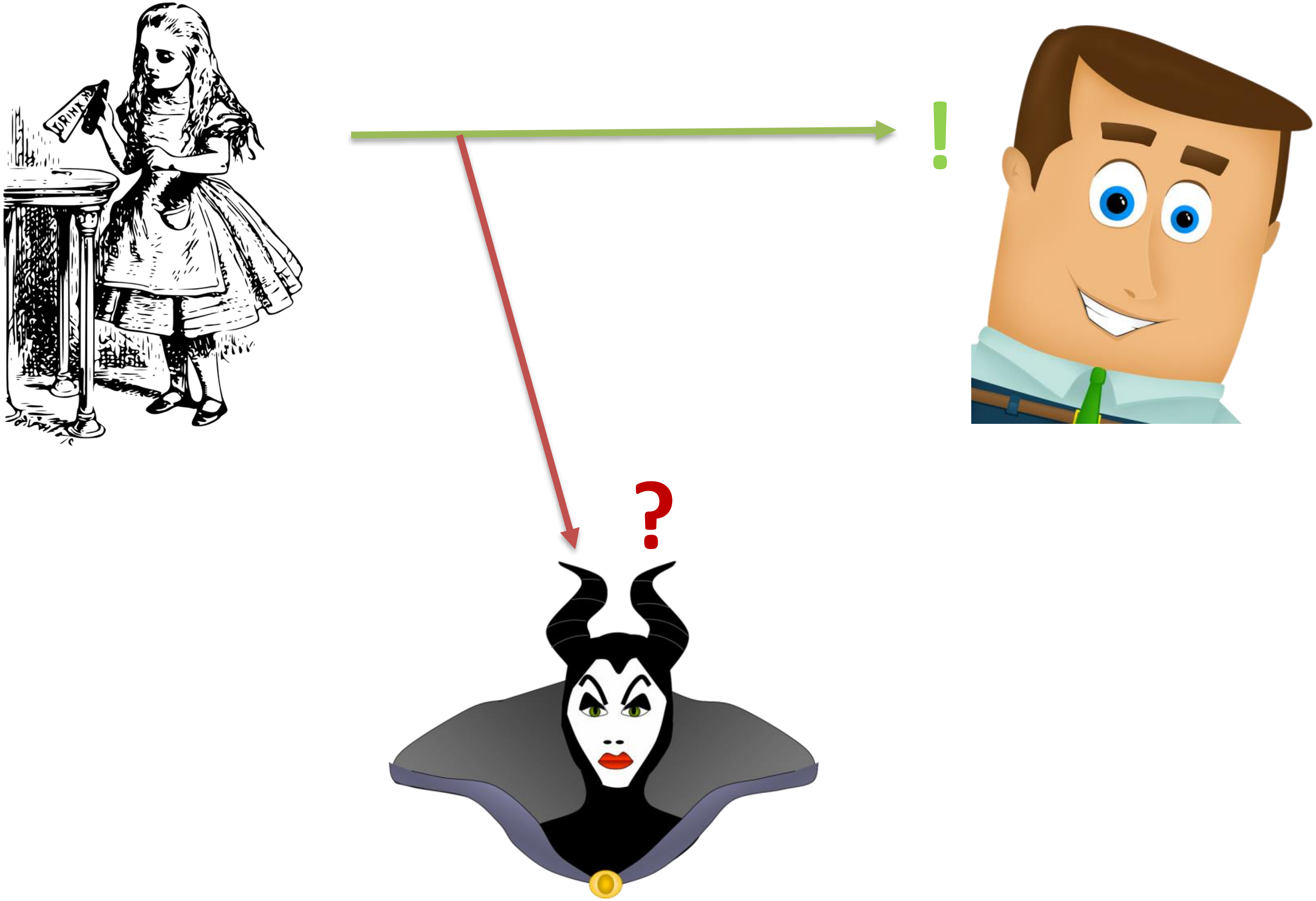


Terminology

- Alice
- Bob
- Eve

- Carol
- Dave

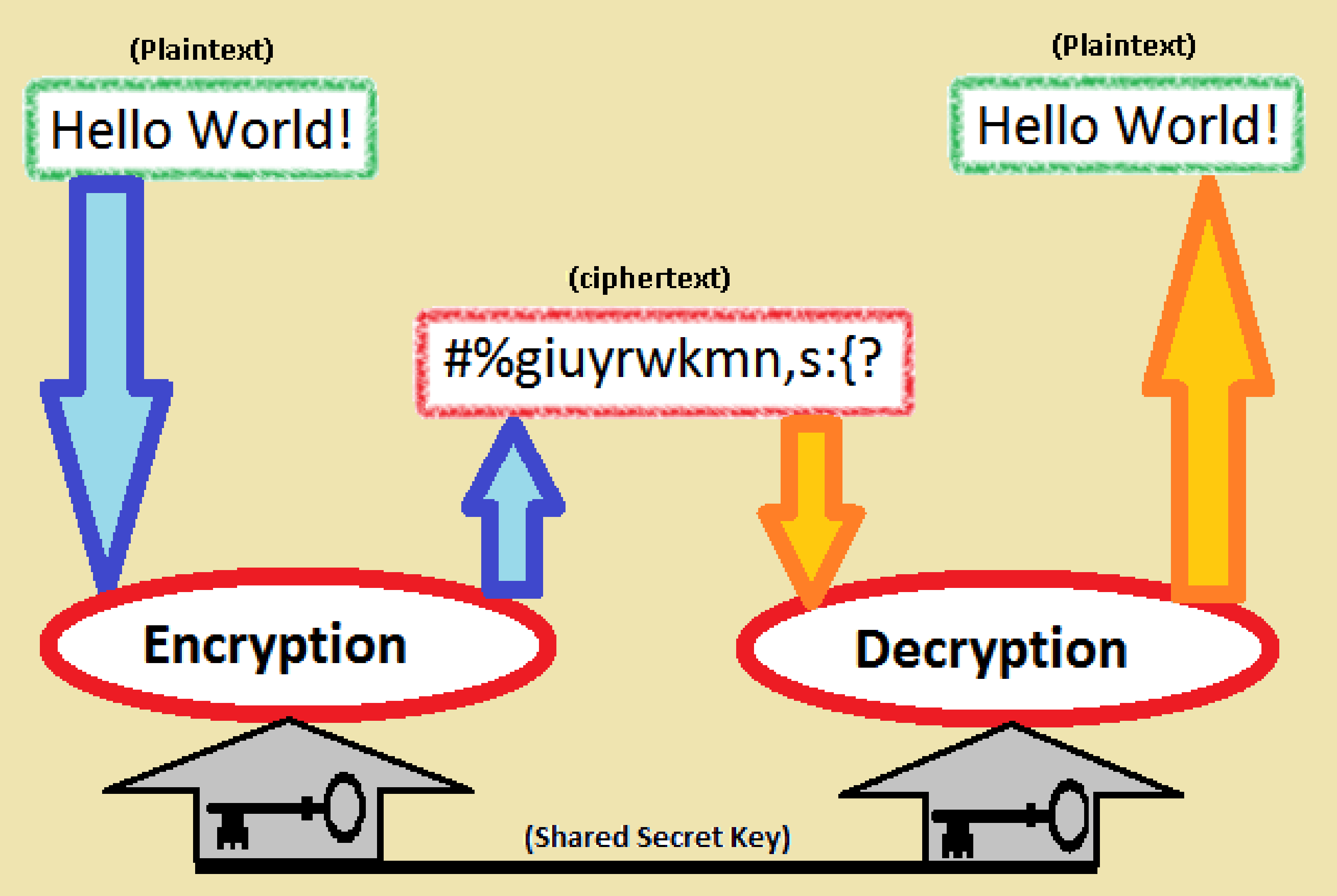
Terminology



Symmetric vs Asymmetric

- Symmetric:
  - Encryption key = Decryption key
  - In general: Encryption algorithm ≠ Decryption algorithm
  - Both sender and receiver must have the same key K
    - Also called Secret Key Crypto
  - Key distribution is a problem!
    - Must happen before secure communication is possible
    - Different keys for different pairs of persons
- Asymmetric
  - Encryption Key ≠ Decyption key
  - In general: Encryption algorithm = Decryption algorithm
  - Each user has a pair of keys: 1 public and 1 private (secret)
    - Also called Public Key Crypto
  - Key distribution is less of a problem
    - Public key can be published online
    - Must only ensure correctness of published public keys

Symmetric Crypto

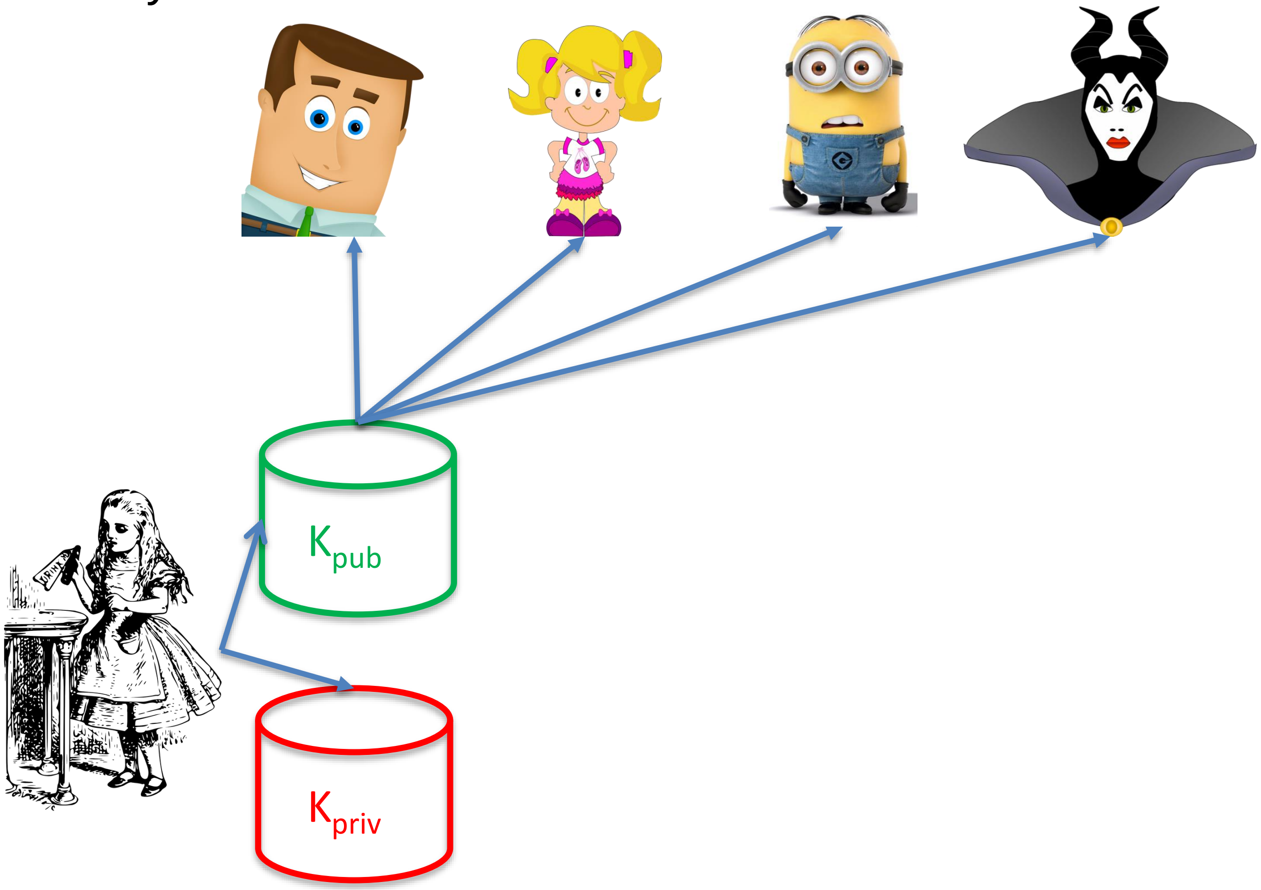


Symmetric Crypto

- Example:
  - I share different keys with different persons
  - If I want to share message Confidential with Alice, I will use my key to encrypt the message:
    - Cipher text: turvallisuus
  - Everybody can try to decrypt this text:
    - Bob: ?
    - Carol: ?
    - Dave: ?
    - Eve: ?
    - Alice: sikkerhet
  - Same message encrypted for
    - Bob: güvenlik
    - Carol: sicherheit
    - Dave: безопасность
    - Eve: seguridad

Asymmetric Crypto

- Alice makes her public key available to all, but keeps the private key to herself

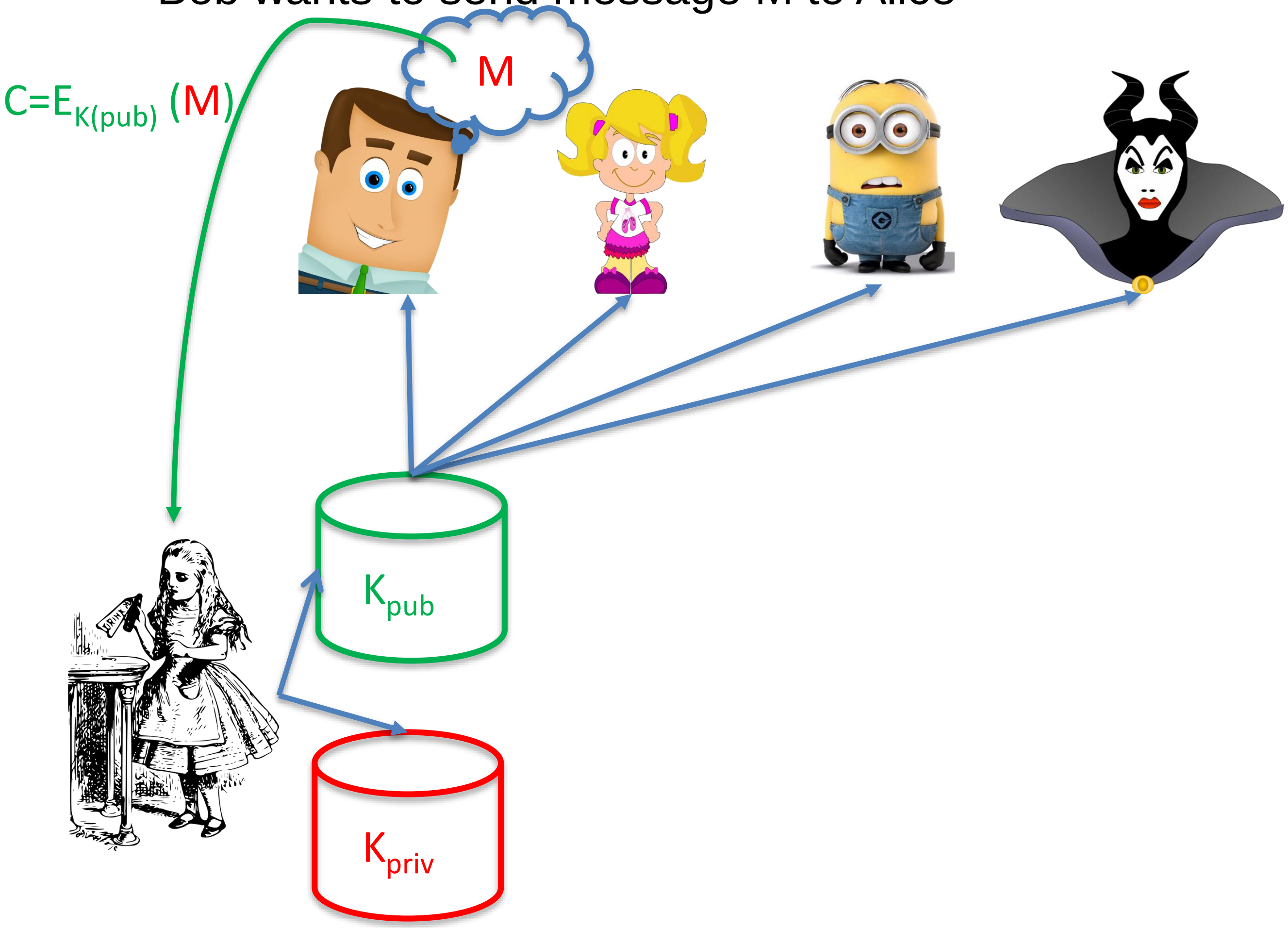


Asymmetric Crypto

- Analogy:
  - Public key:
  - Private key:
  - Encryption method:
  - Key distribution:

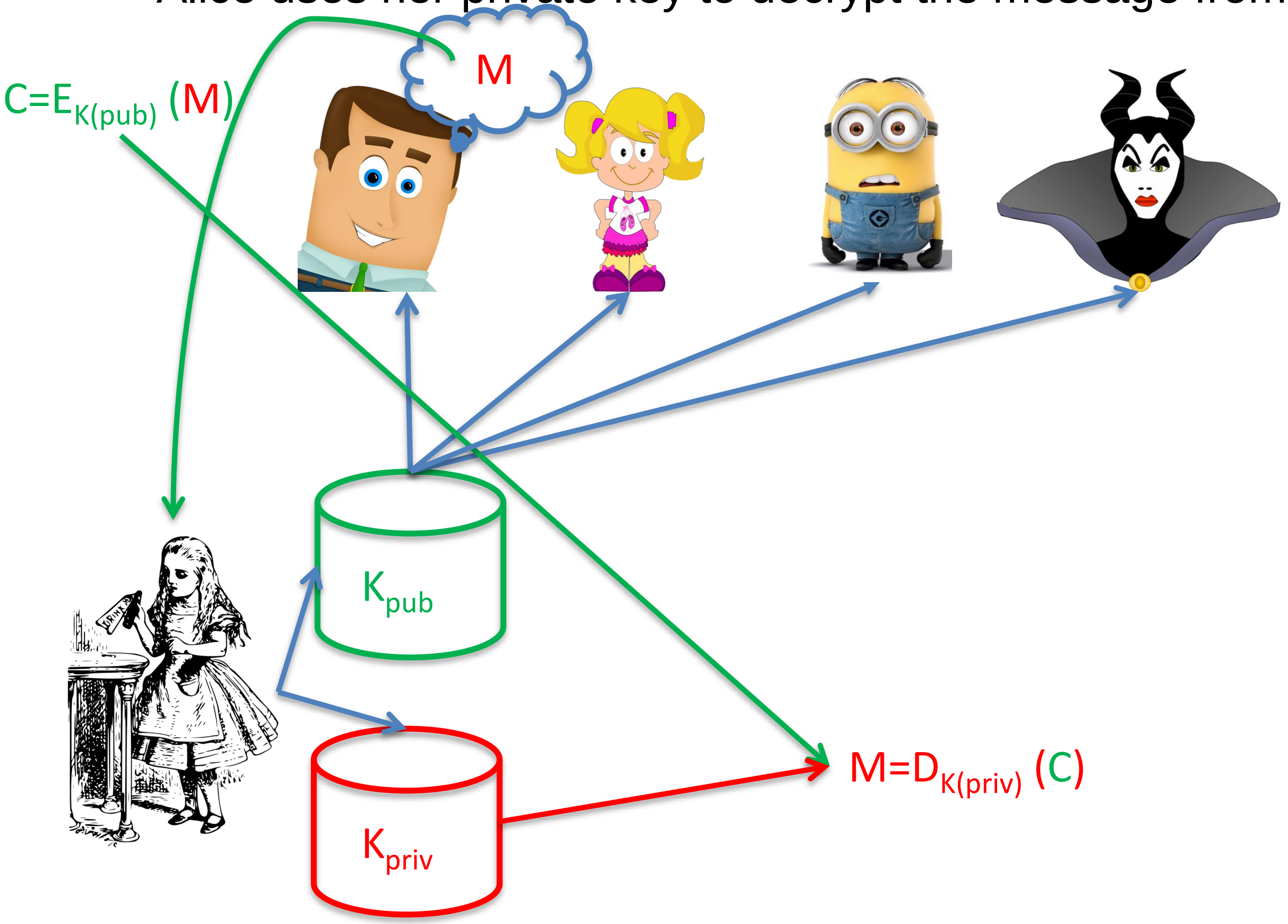
Asymmetric Crypto

- Bob wants to send message M to Alice



Asymmetric Crypto

- Alice uses her private key to decrypt the message from Bob



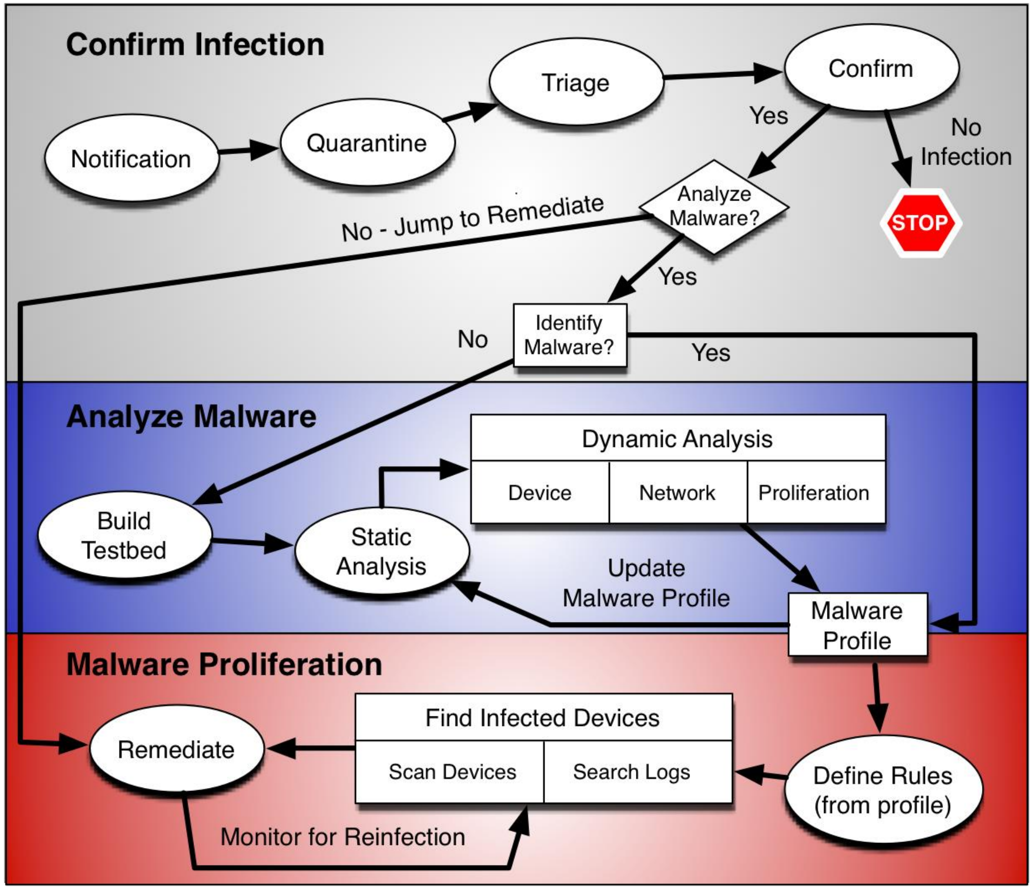
Digital Forensics

- What not!

Digital Forensics

Malware analysis

- Classification of malware
  - Reverse engineering
  - “Classical” virus scanners don’t always work
  - Anomaly behaviour detection



Digital Forensics

Seagate 60TB SAS SSD

The Highest Capacity SSD in the World

60

- Reach 1PB of storage with only 17 drives
- Ideal for large storage arrays, active archives and read-intensive environments
- New level of power efficiency: 4TB/watt
- 3.5" form factor offers higher density than two 16TB 2.5" SSDs
- Features ultra-dense NAND technology from Micron
- Leverages unique Seagate IP and decades of experience in enterprise storage

SEAGATE

$3398 10MB

THE HARD DISK YOU'VE BEEN WAITING FOR

plete micro-size disk

STORAGE
SPEED
VALUE
SUPPORT

COMP subsystem is now bytes of storage: 5 megabytes Compare the price and 8-inch

MORE SOFTWARE
Included with the system is software for testing, formatting, I/O drivers for CP/M®, plus an automatic CP/M driver attach program. Support software and drivers for MP/M® and Oasis® are also available. The sophisticated formatting program assigns alternate sectors for any weak sectors detected during formatting, assuring the lowest possible error rate — at least ten times better than floppies.

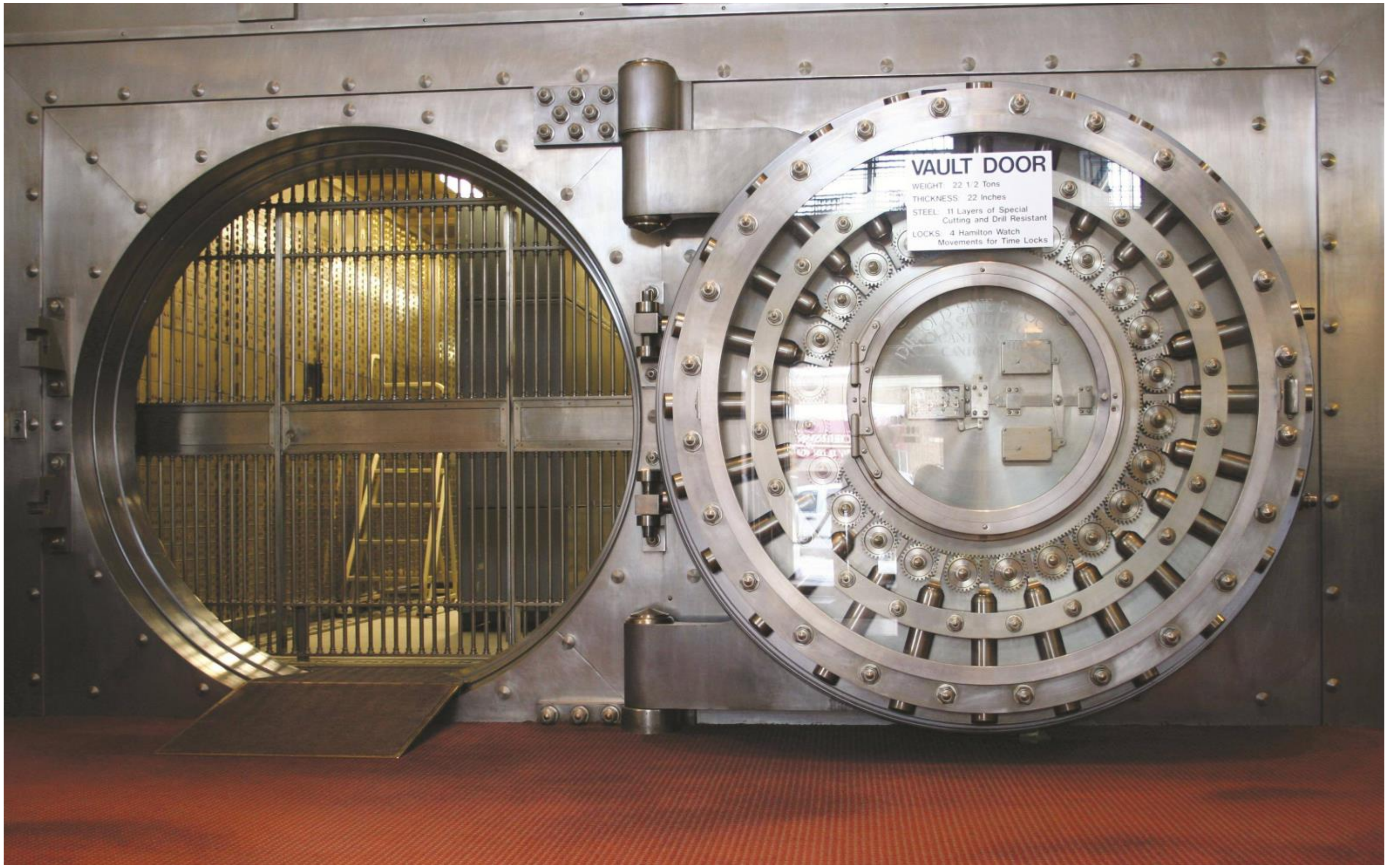
WARRANTY
The system has a full one-year warranty on parts and

XCOMP

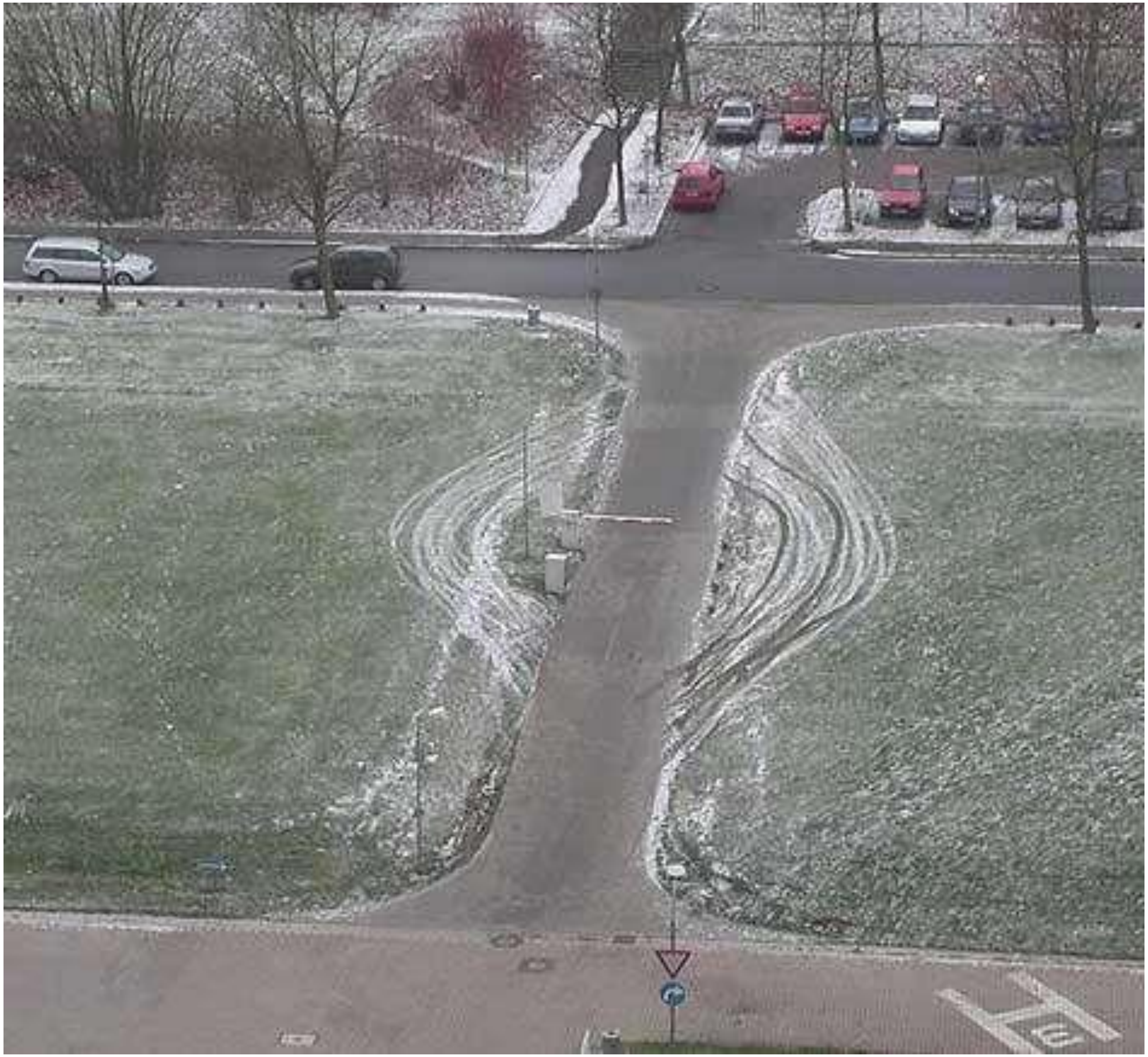
memecenter.com/miniriedy

Digital Forensics

Access control

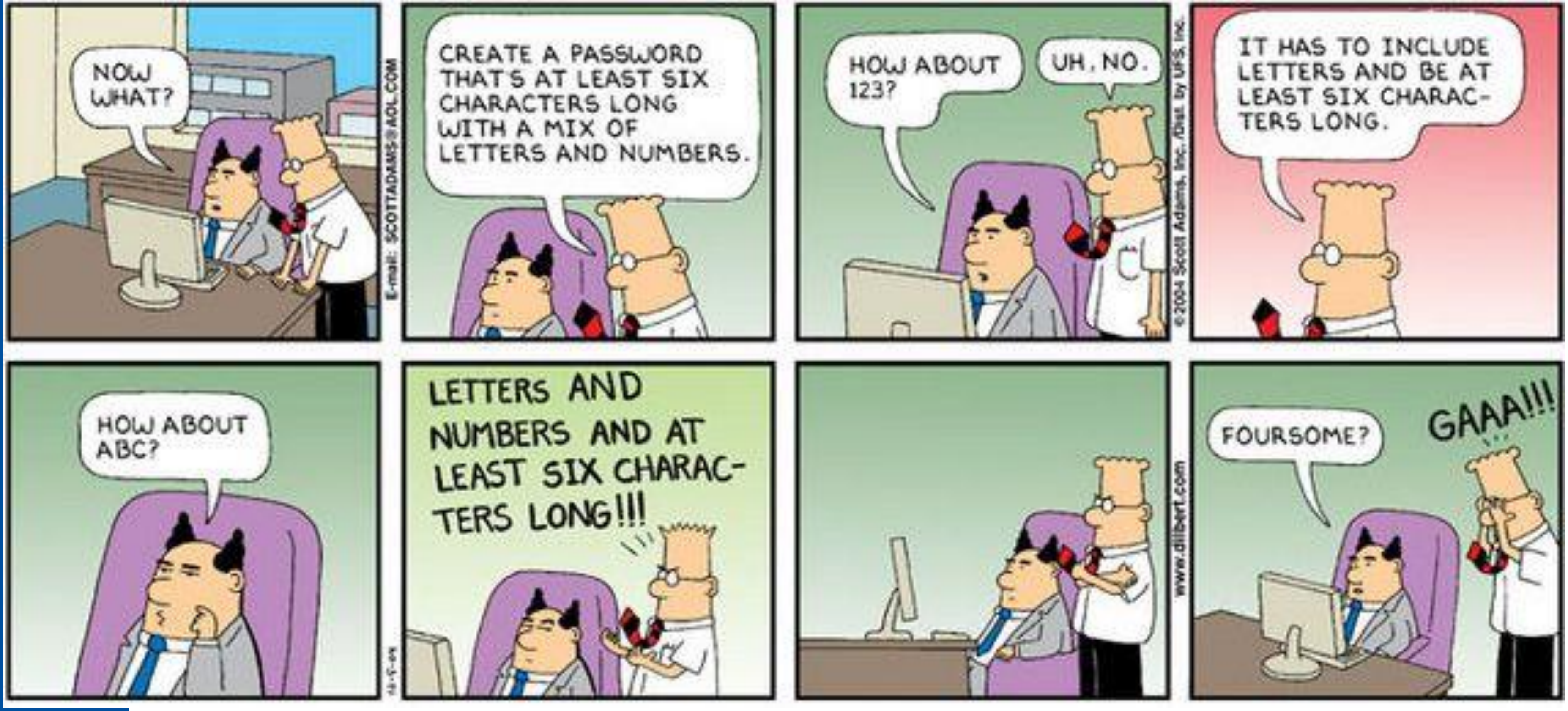

VAULT DOOR
WEIGHT: 22 1/2 Tons
THICKNESS: 22 Inches
STEEL: 11 Layers of Special Cutting and Drill Resistant
LOCKS: 4 Hamilton Watch Movements for Time Locks

Access control



Access control

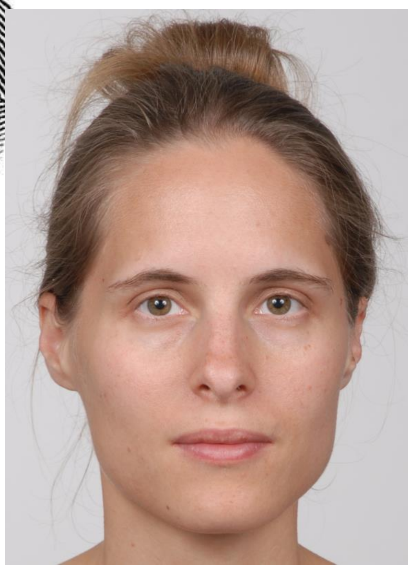
- How can we get access?
  1. Password (something we **know**)


NOW WHAT?
E-mail: SCOTTADAMS@AOL.COM
CREATE A PASSWORD THAT'S AT LEAST SIX CHARACTERS LONG WITH A MIX OF LETTERS AND NUMBERS.
HOW ABOUT 123?
UH, NO.
© 2004 Scott Adams, Inc./Dist. by UFS, Inc.
IT HAS TO INCLUDE LETTERS AND BE AT LEAST SIX CHARACTERS LONG.
HOW ABOUT ABC?
LETTERS AND NUMBERS AND AT LEAST SIX CHARACTERS LONG!!!
www.dilbert.com
FOURSOME?
GAAA!!!

Access Control

- How can we get access?
  1. Password (something we **know**)
  2. Token (something we **have**)

Access Control



- How can we get access?
  1. Password (something we **know**)
  2. Token (something we **have**)
  3. Biometrics (something we **are** / **do**)

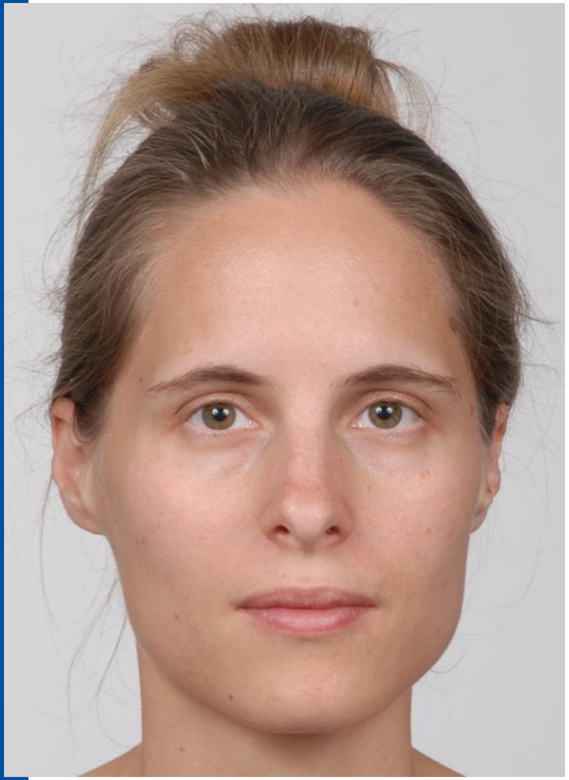
I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES, AND I BRING YOU MY NEWEST BIOMETRIC SCANNER.
scottadams@aol.com
www.dilbert.com
INSTEAD OF A PASSWORD, I PUT THIS ON YOUR HEAD AND SQUEEZE UNTIL YOU SCREAM IN A WAY THAT ONLY YOU CAN SCREAM.
11-17-07 ©2007 Scott Adams, Inc./Dist. by UFS, Inc.
NO, THAT'S NOT YOU.
GAAA! GAAA! GAAA!

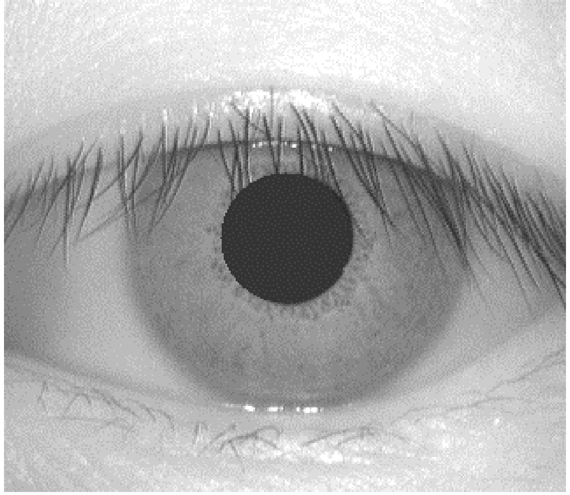
Biometrics

- ISO definition:
  - Automated recognition of individuals based on their behavioural and biological characteristics

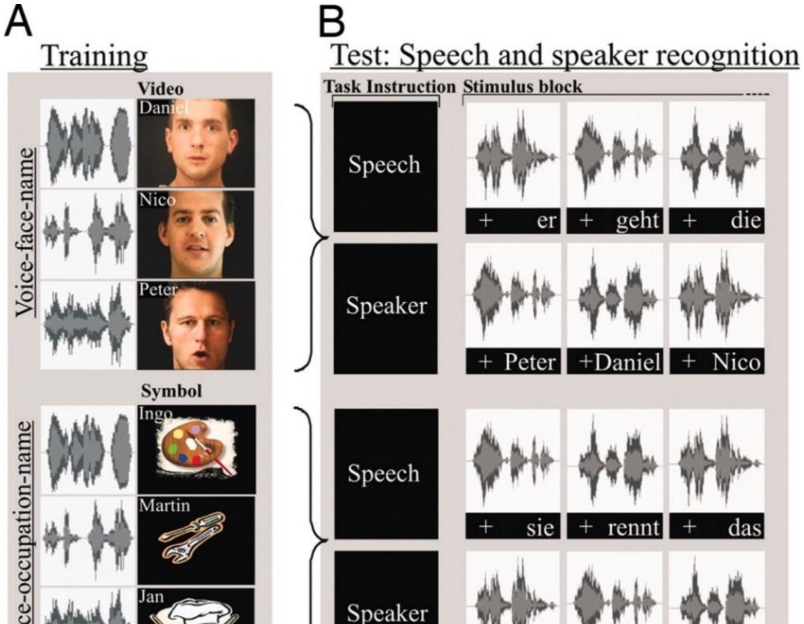
  - **Behavioural** has to do with the function of the body
  - **Biological** has to do with the structure of the body

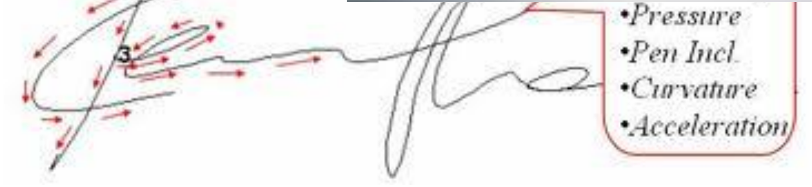
Biological biometrics

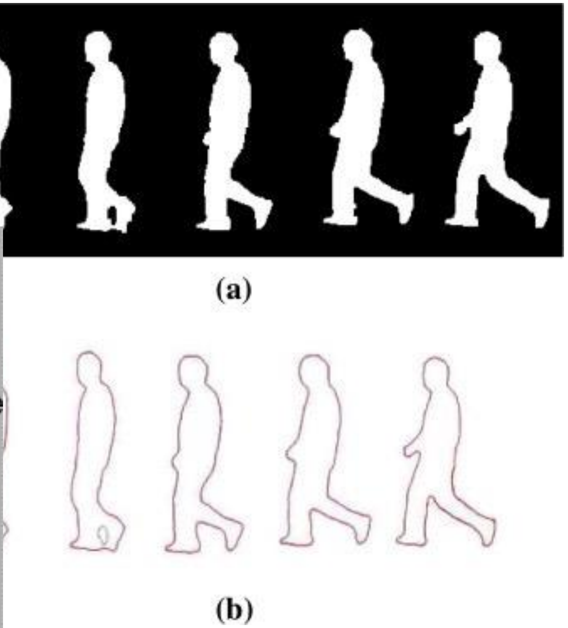




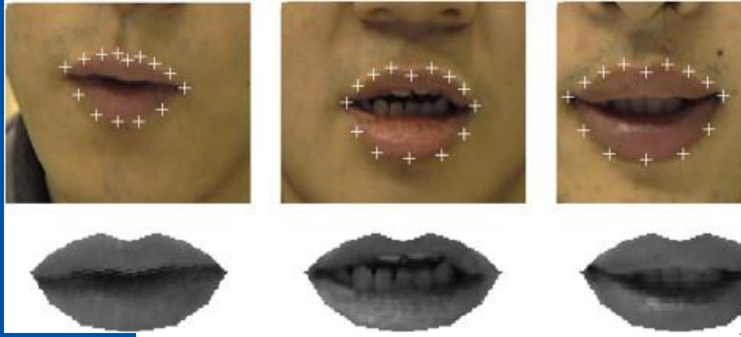
Behavioural biometrics

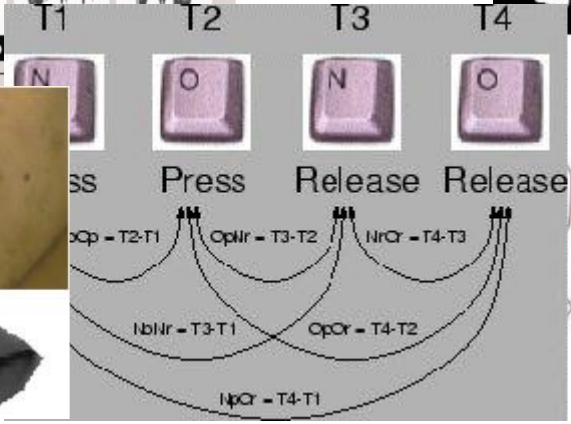




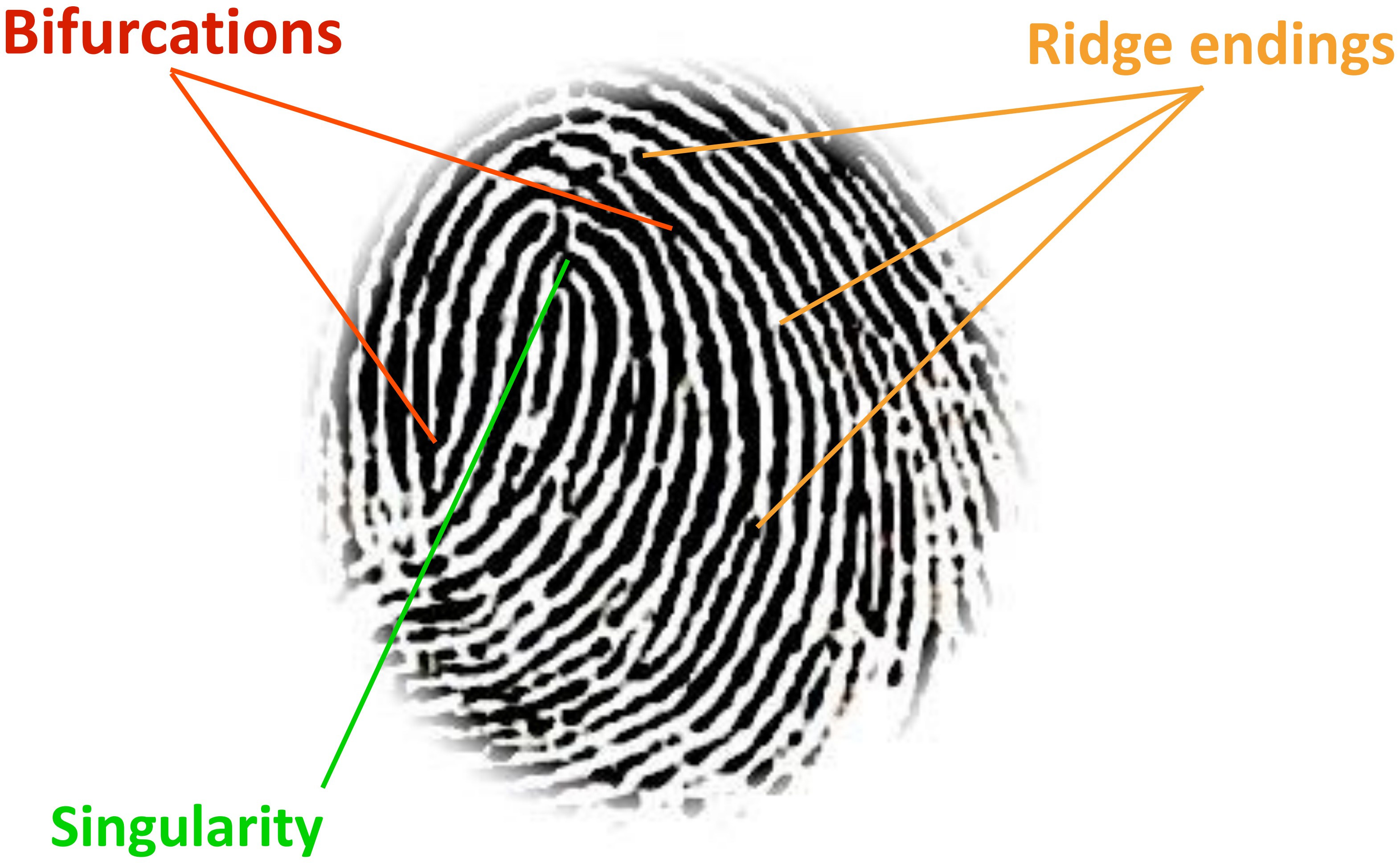

(a)

(b)





Biometrics

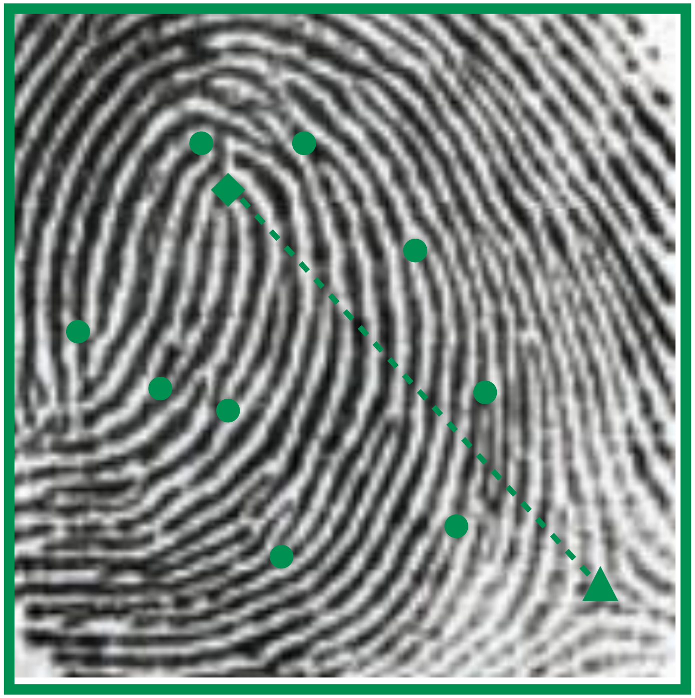


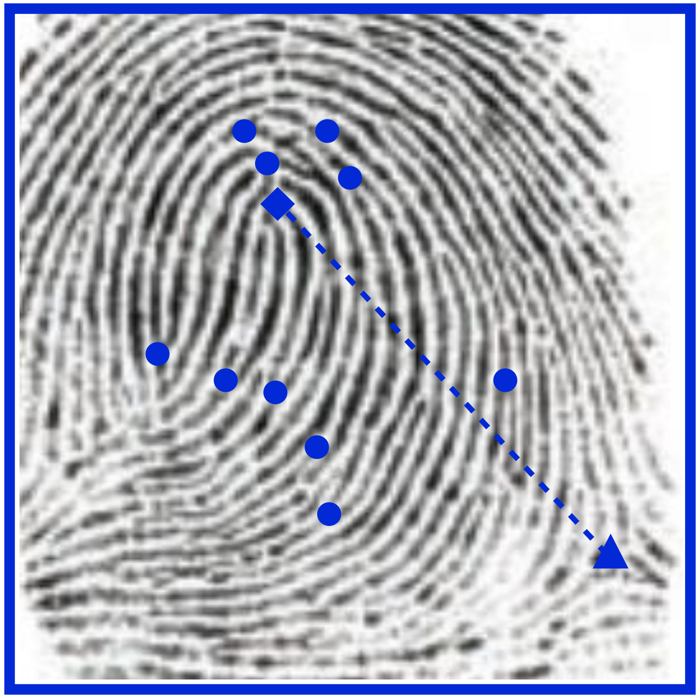
Biometrics

- Comparison of a reference image against a probe image

Biometrics

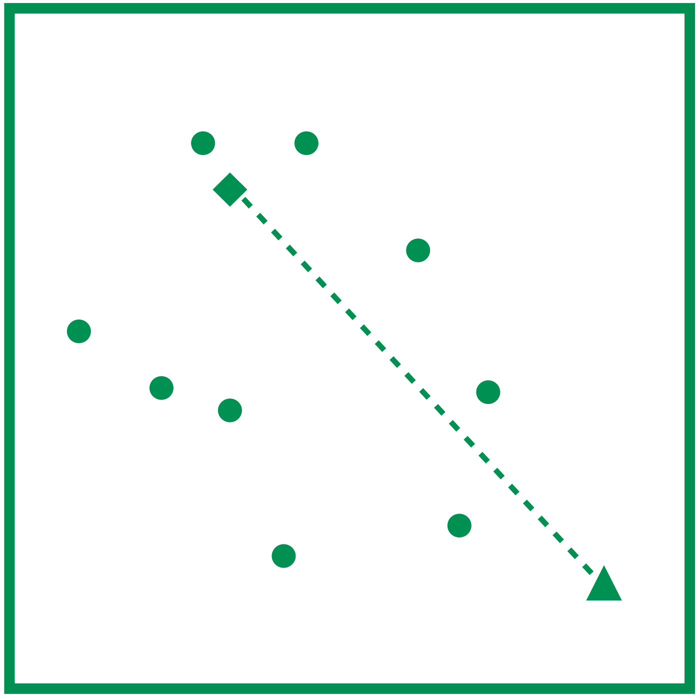
- Comparison of a reference image against a probe image

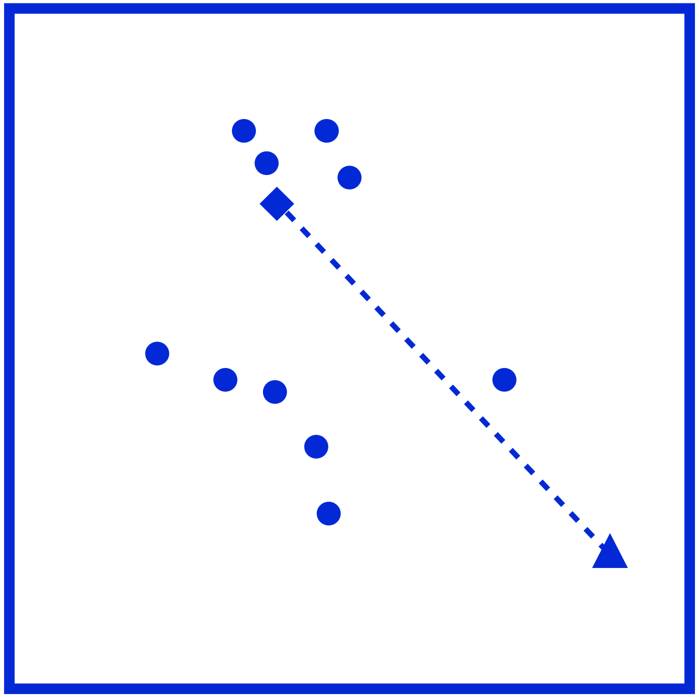




Biometrics

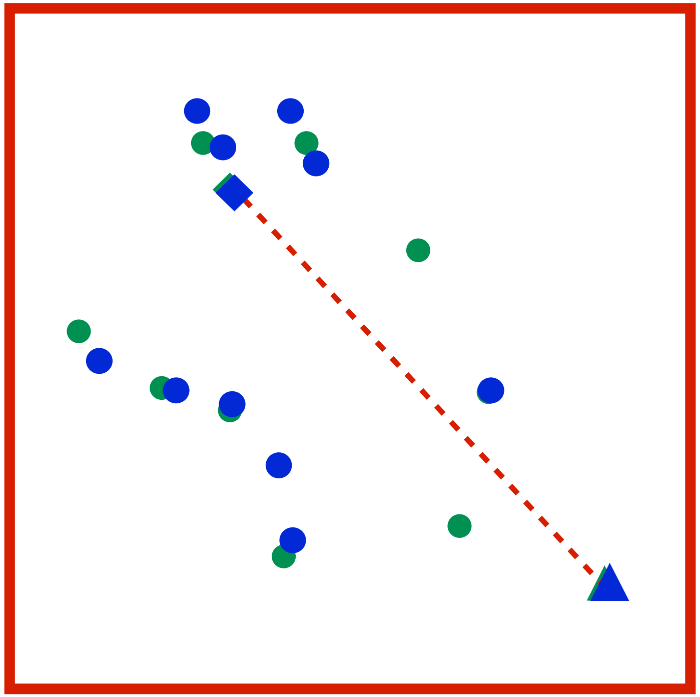
- Comparison of a reference image against a probe image

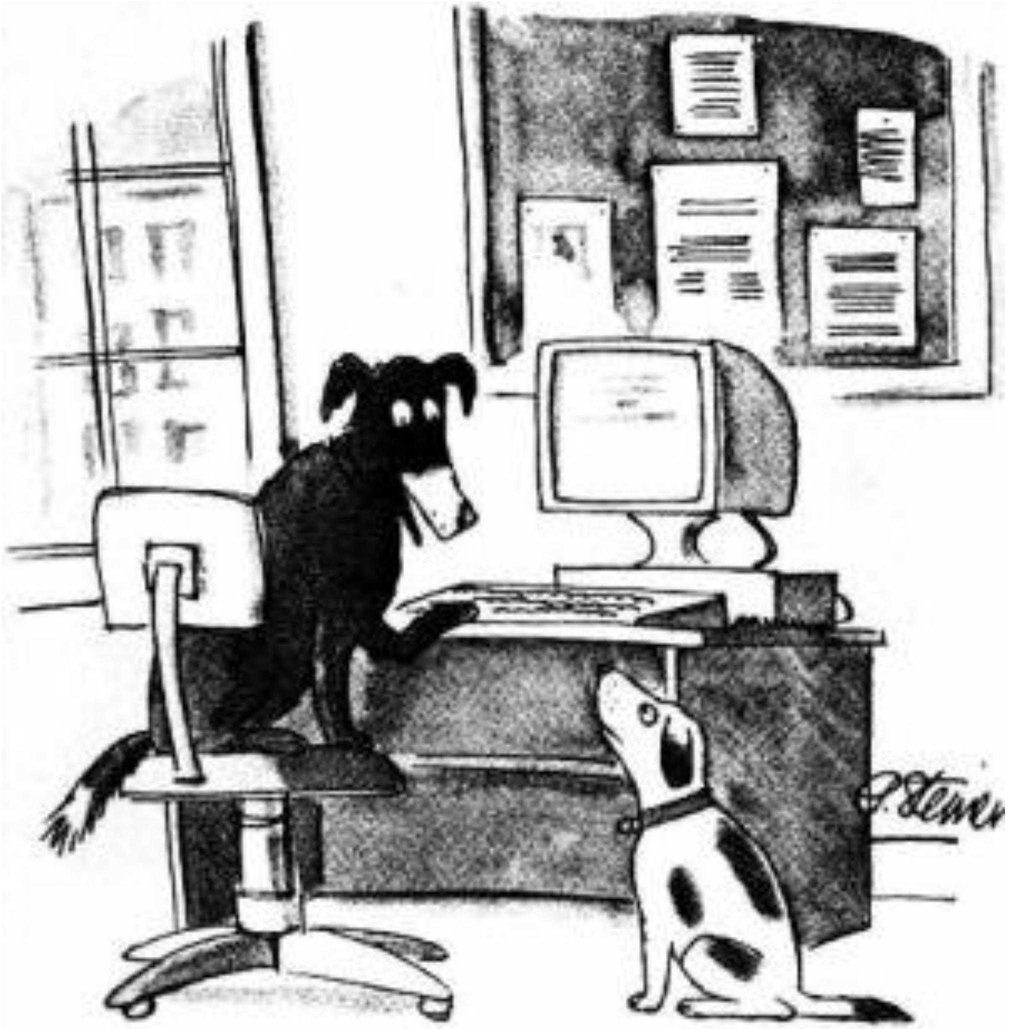




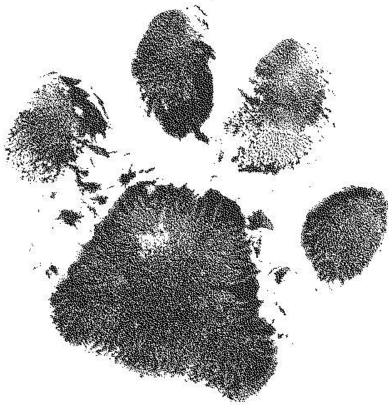
Biometrics

- Comparison of a reference image against a probe image





"On the Internet, nobody knows you're a dog."



Chatroom Security project

Overall goal:

Protect children in a chatroom from sexual preditors

Chatroom Security project

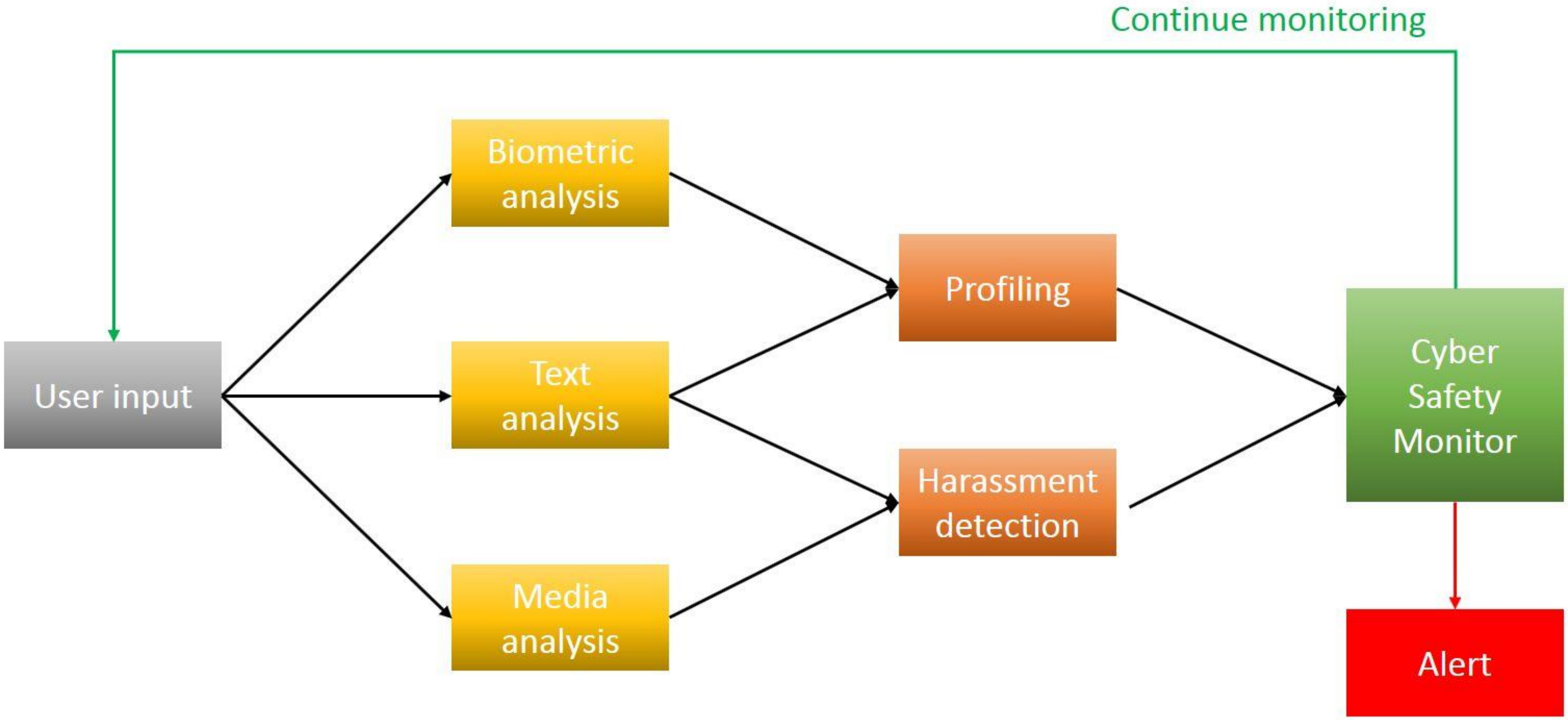
Overall goal:

Protect children in a chatroom from sexual preditors

Cyber safety project

Overall goal:

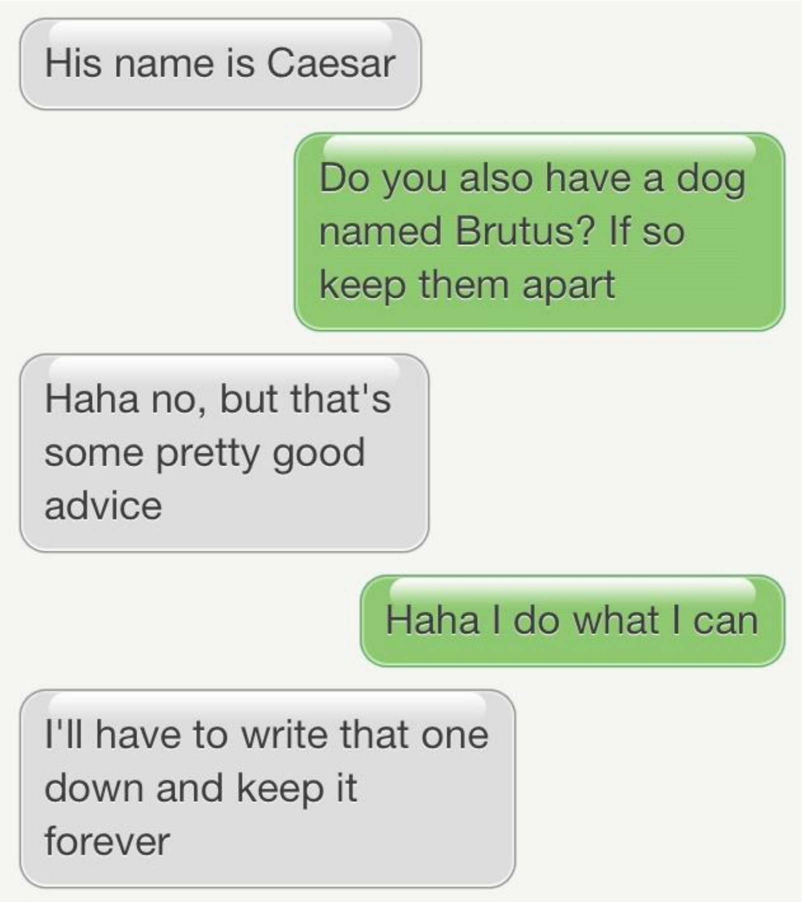
Protect children in online from sexual predators or cyber bullying



Profiling

PARA ACERCARSE
A TUS HIJOS
LOS ACOSADORES
USAN LAS FORMAS
MÁS DESCARADAS.
Hablá con ellos antes
que otros lo hagan.
EL PELIGRO ESTÁ AHÍ
AUNQUE NO LO VEAS.
#CONECTATESEGURO

Harassment detection



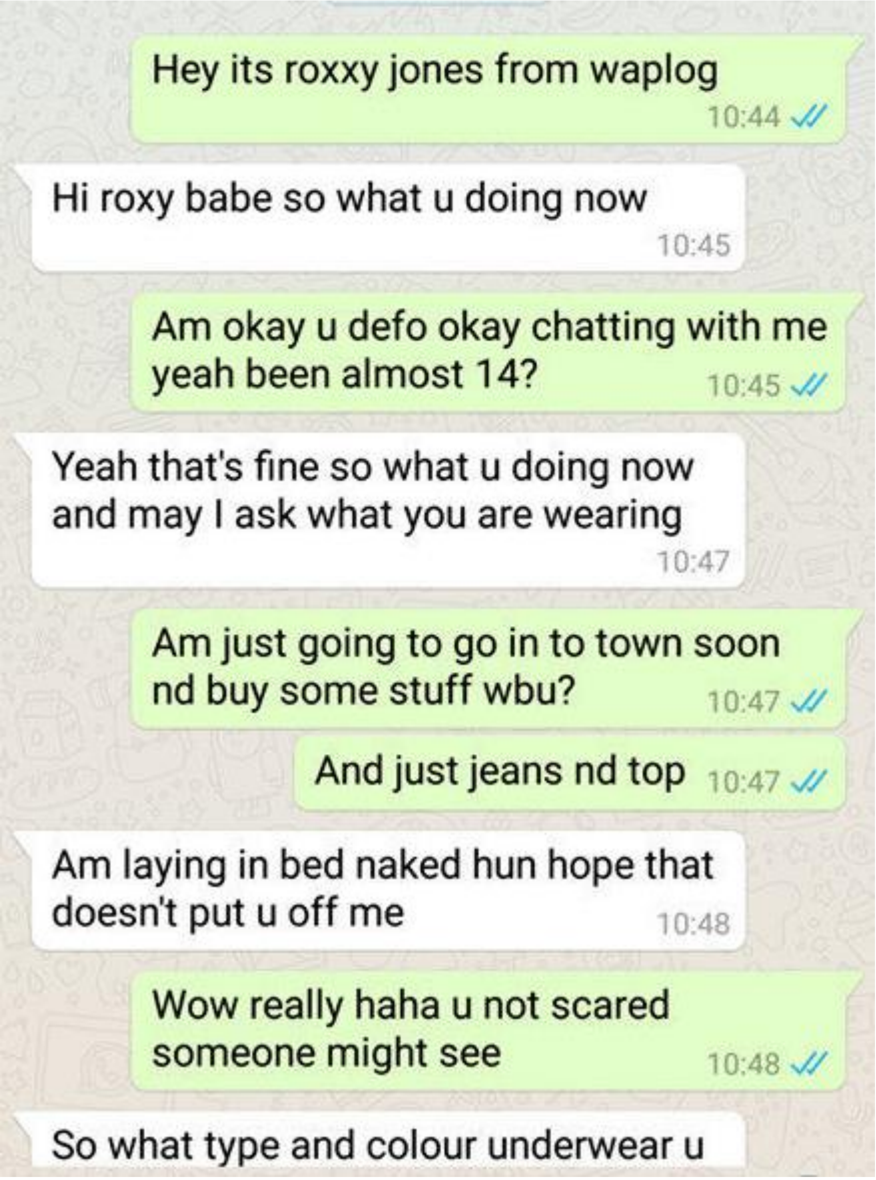
His name is Caesar

Do you also have a dog named Brutus? If so keep them apart

Haha no, but that's some pretty good advice

Haha I do what I can

I'll have to write that one down and keep it forever



Hey its roxxy jones from waplog 10:44

Hi roxy babe so what u doing now 10:45

Am okay u defo okay chatting with me yeah been almost 14? 10:45

Yeah that's fine so what u doing now and may I ask what you are wearing 10:47

Am just going to go in to town soon nd buy some stuff wbu? 10:47

And just jeans nd top 10:47

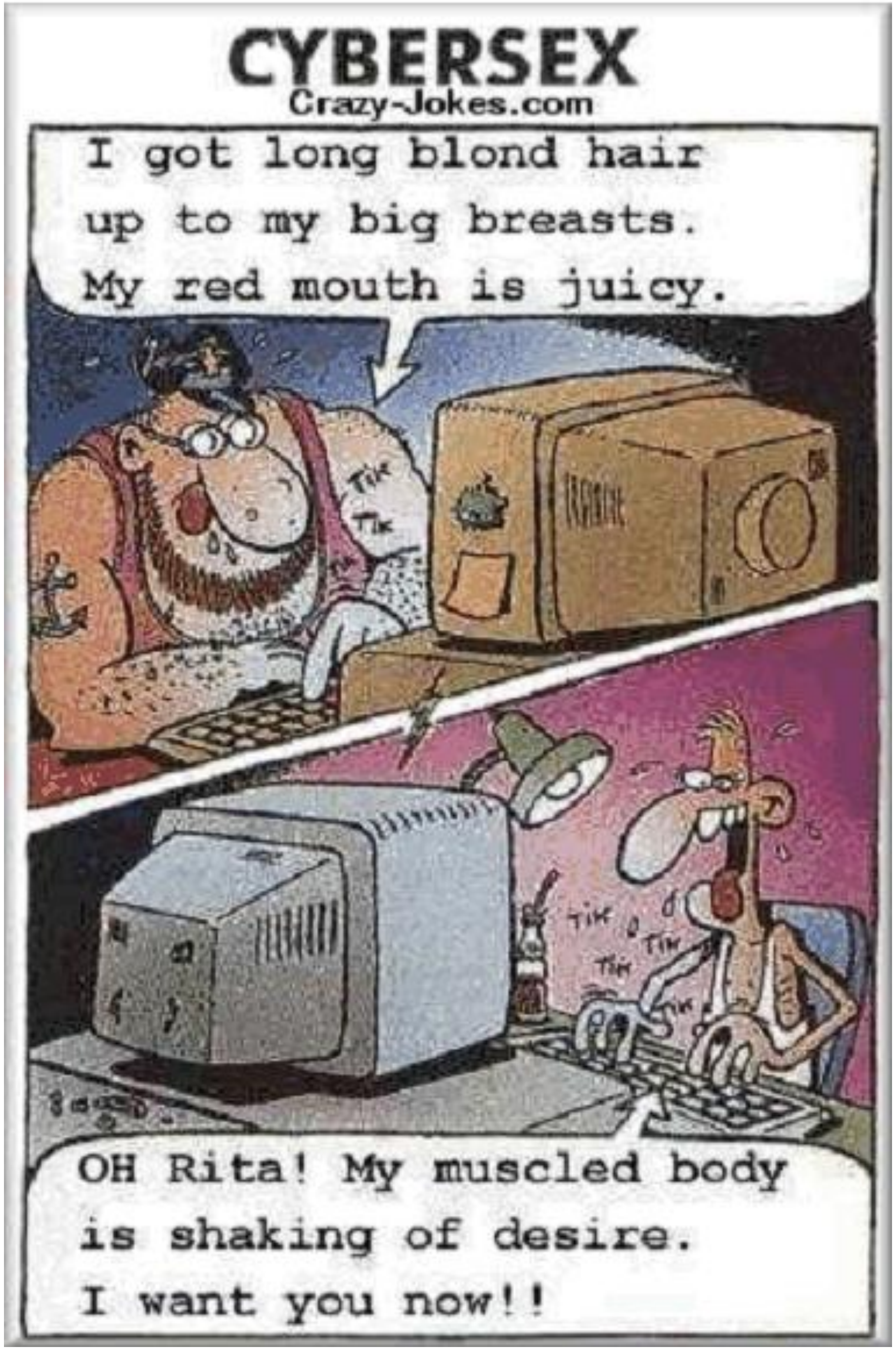
Am laying in bed naked hun hope that doesn't put u off me 10:48

Wow really haha u not scared someone might see 10:48

So what type and colour underwear u

Grooming

1. Targeting the victim
2. Gaining the victim’s trust
3. Filling a need
4. Isolating the child
5. Sexualizing the relationship
6. Maintaining control


CYBERSEX
Crazy-Jokes.com
I got long blond hair up to my big breasts. My red mouth is juicy.
TIK TIK
TIK TIK TIK TIK
OH Rita! My muscled body is shaking of desire. I want you now!!

NTNU

Questions?

- Contact details
  - – Email: patrick.bours@ntnu.no
  - – Skype: patrick.bours.norge
  - – Phone: 611 35 250

NTNU