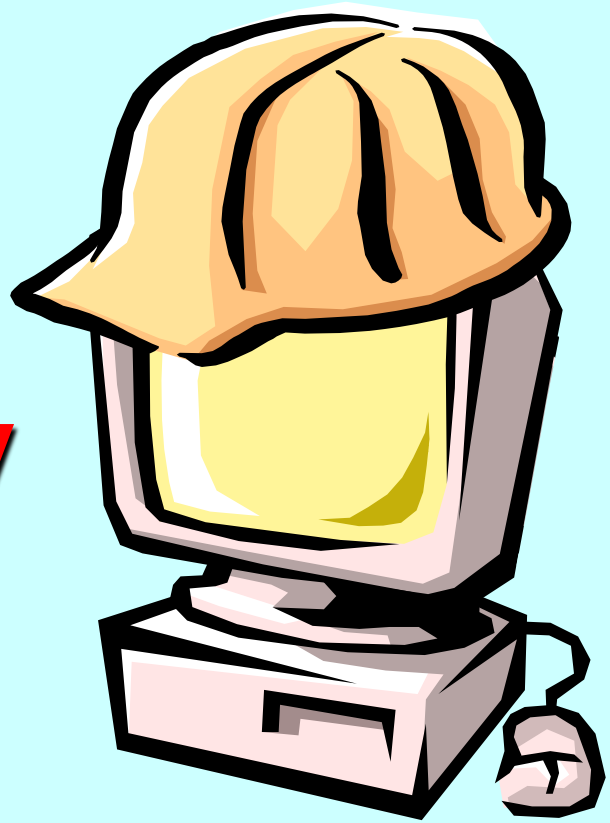
Fundamentals of Cybersecurity



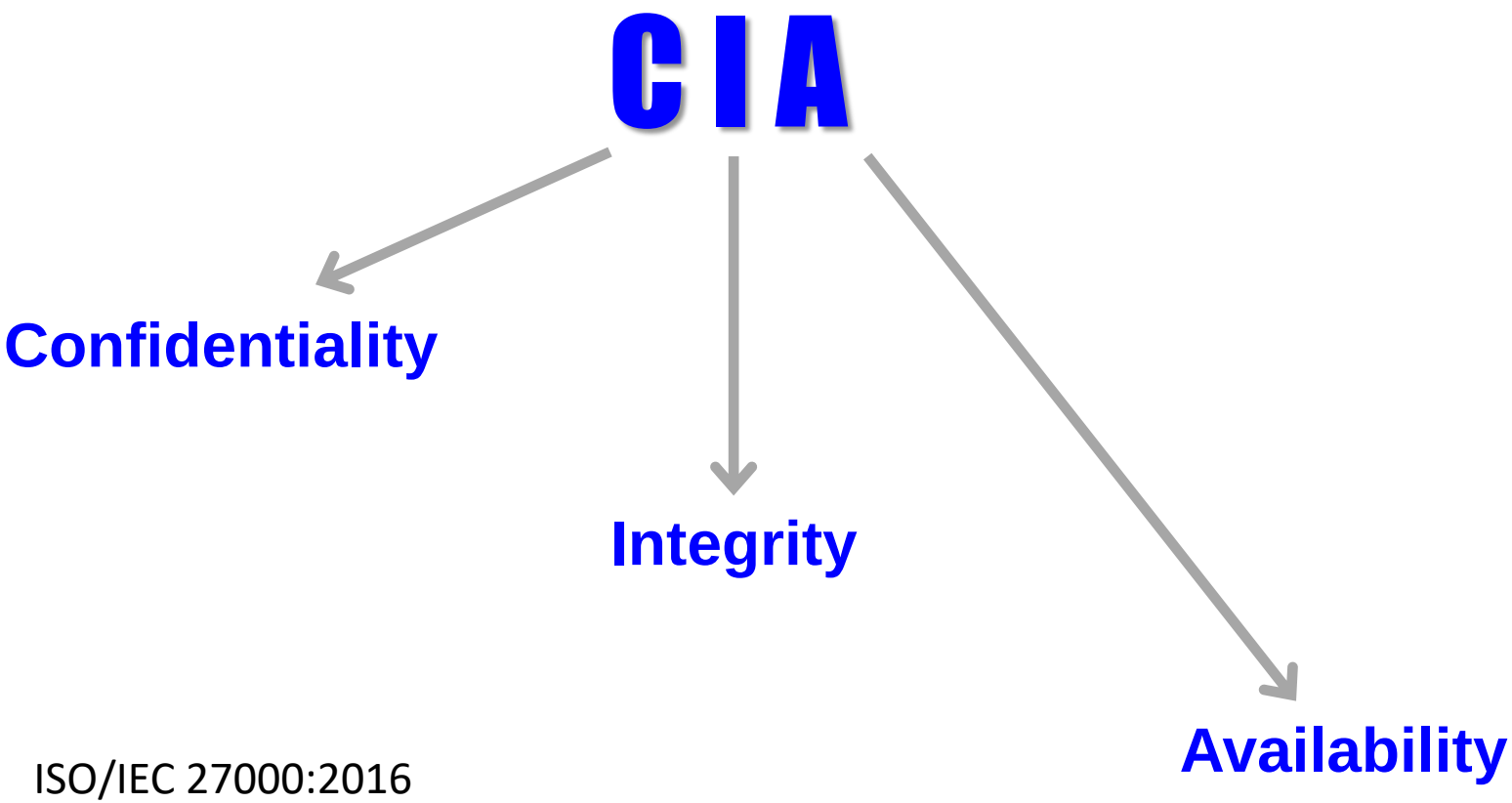
Michał Szychowiak

https://www.cs.put.poznan.pl/mszychowiak

Agenda

1. **Basic security attributes:**
    1. Confidentiality
    2. Integrity
    3. (Availability)
2. **Basic security attributes toolbox:**
    1. Authentication
    2. Authorization
    3. Access Control

The CIA Triade



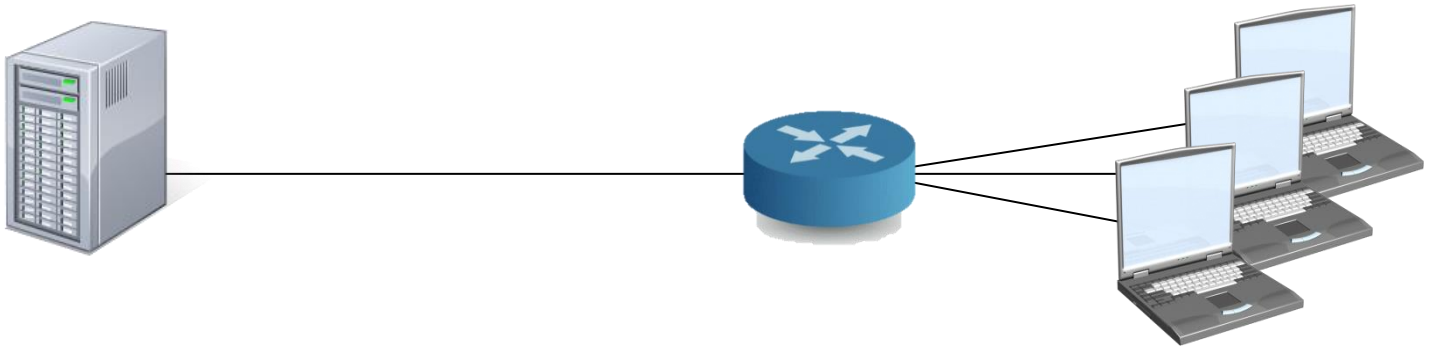
ISO/IEC 27000:2016

ISO/IEC 27001:2014-12

CONFIDENTIALITY

Confidentiality

Threat model



- data at rest (back-end) threats
- data processing (front-end) threats
- in-transit threats
- remote eavesdropping (electromagnetic emission, van Eck radiation)

Confidentiality

Confidentiality protection

- Authentication
- Authorization & Access Control
- Anti-sniffing

AUTHENTICATION

Fundamentals

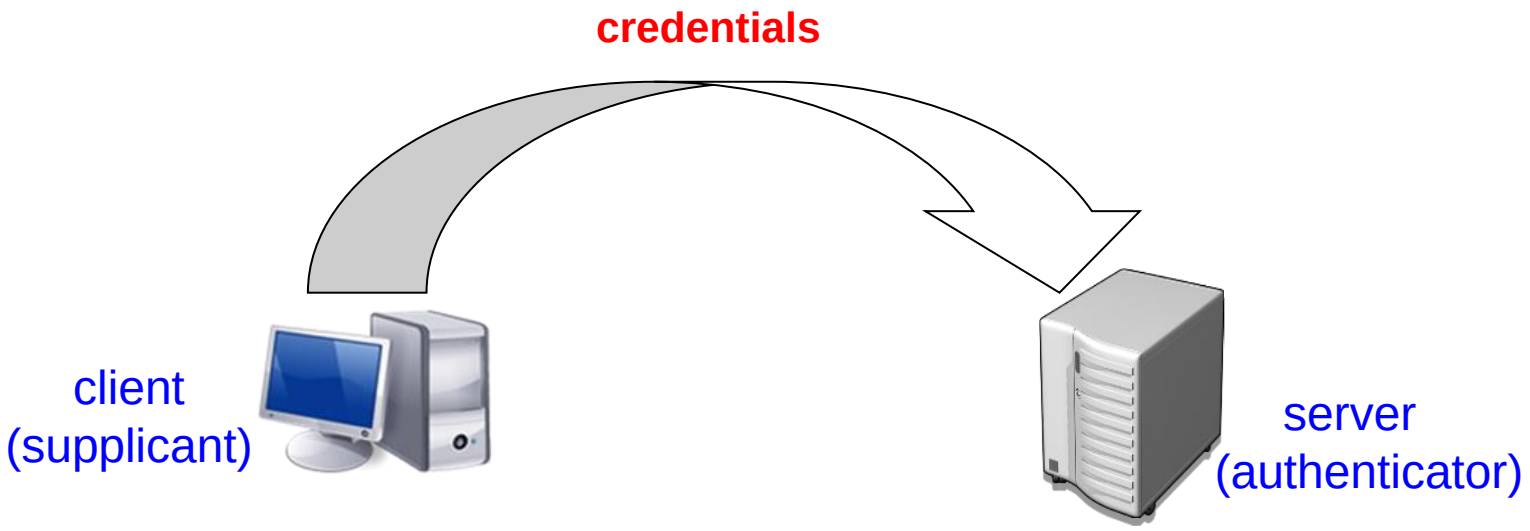
Basic terminology

1. Identification
   - system identifies users (→ *principals*) with UID (*user identifier*)

2. Authentication
   - verification of a user's identity, based on:
     - something you know (*proof by knowledge*), e.g. a password
     - something you have (*proof by possession*), e.g. smart card
     - something you are (*biometrics*)

Authentication

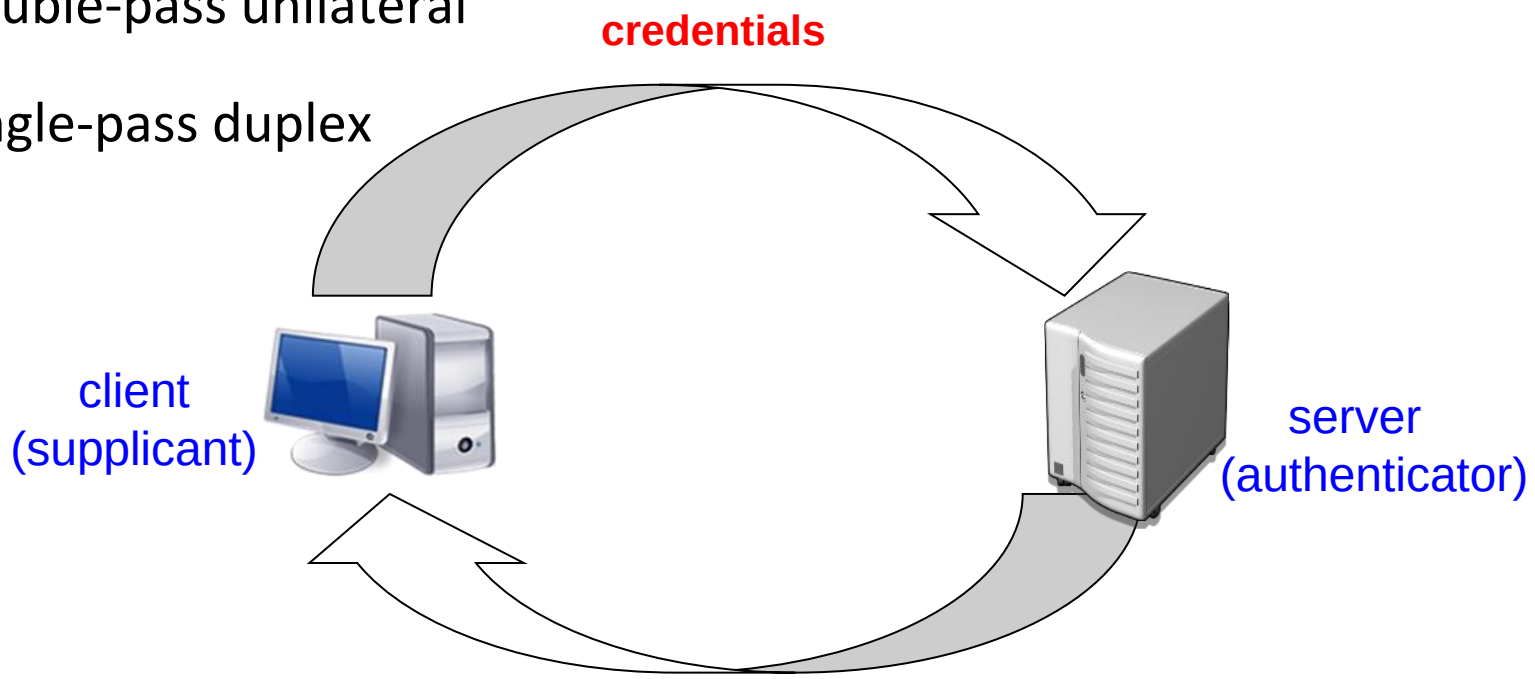
Unilateral authentication



Authentication

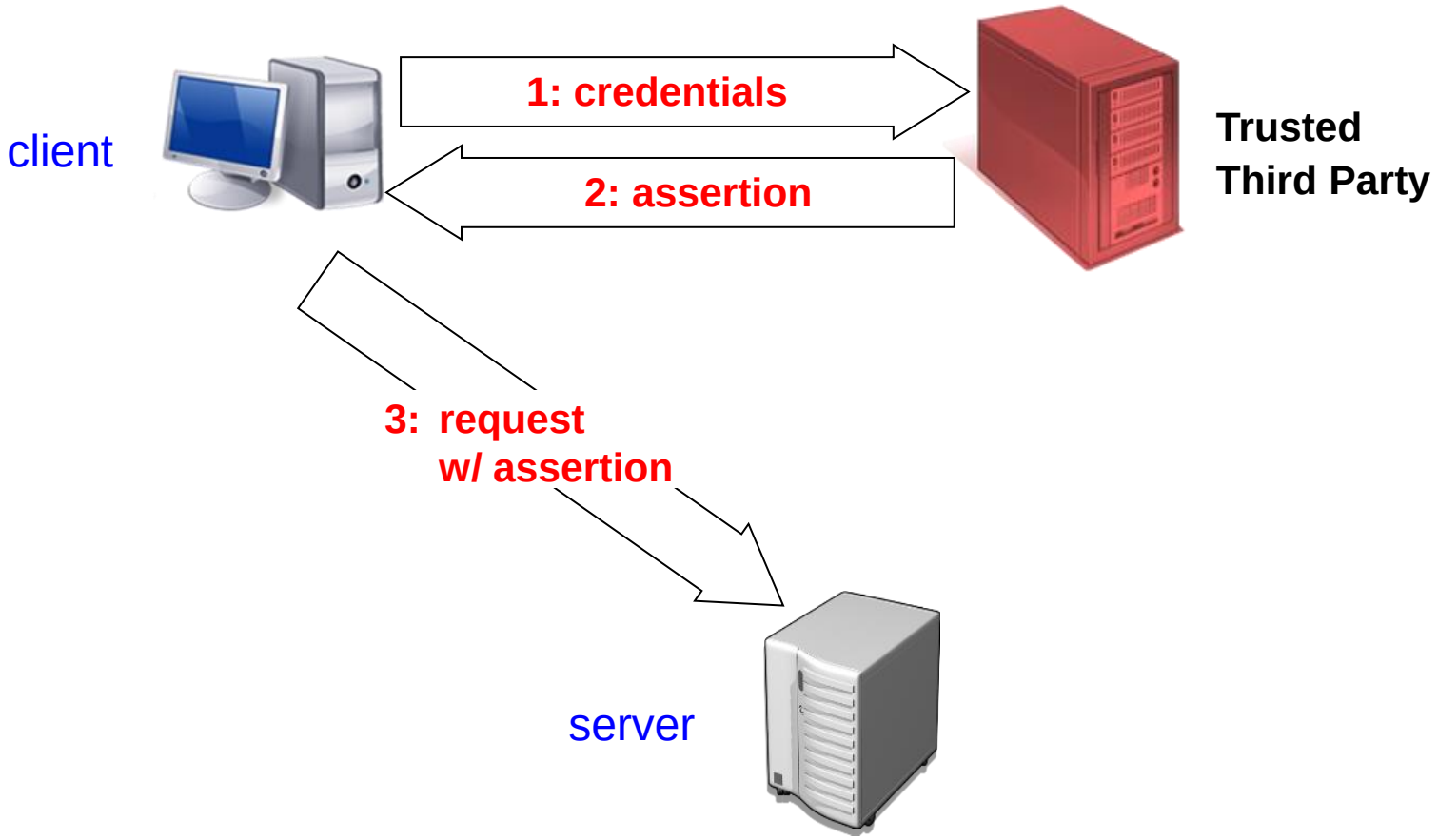
Mutual authentication

- double-pass unilateral
- single-pass duplex



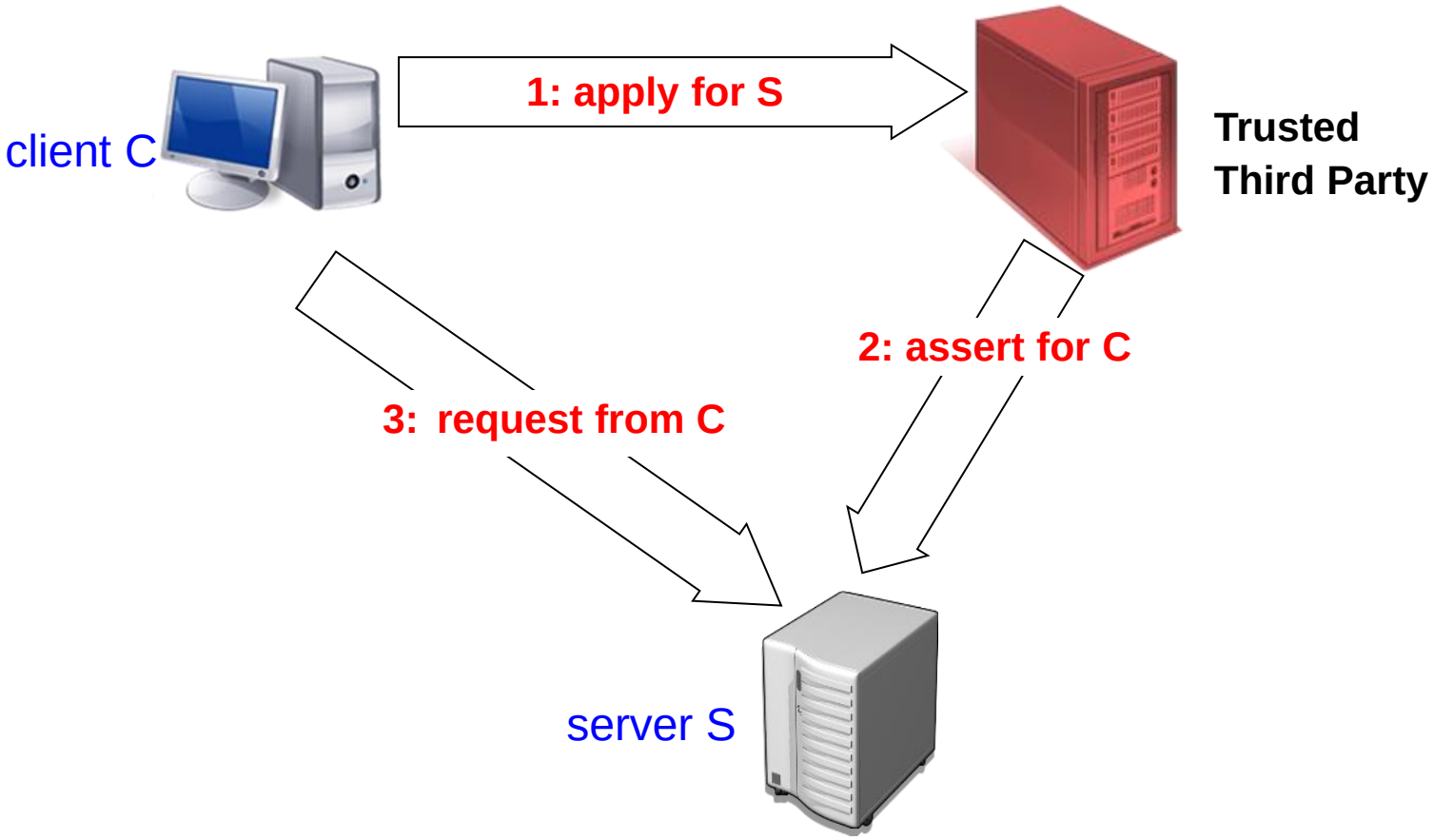
Authentication

Trusted Third Party



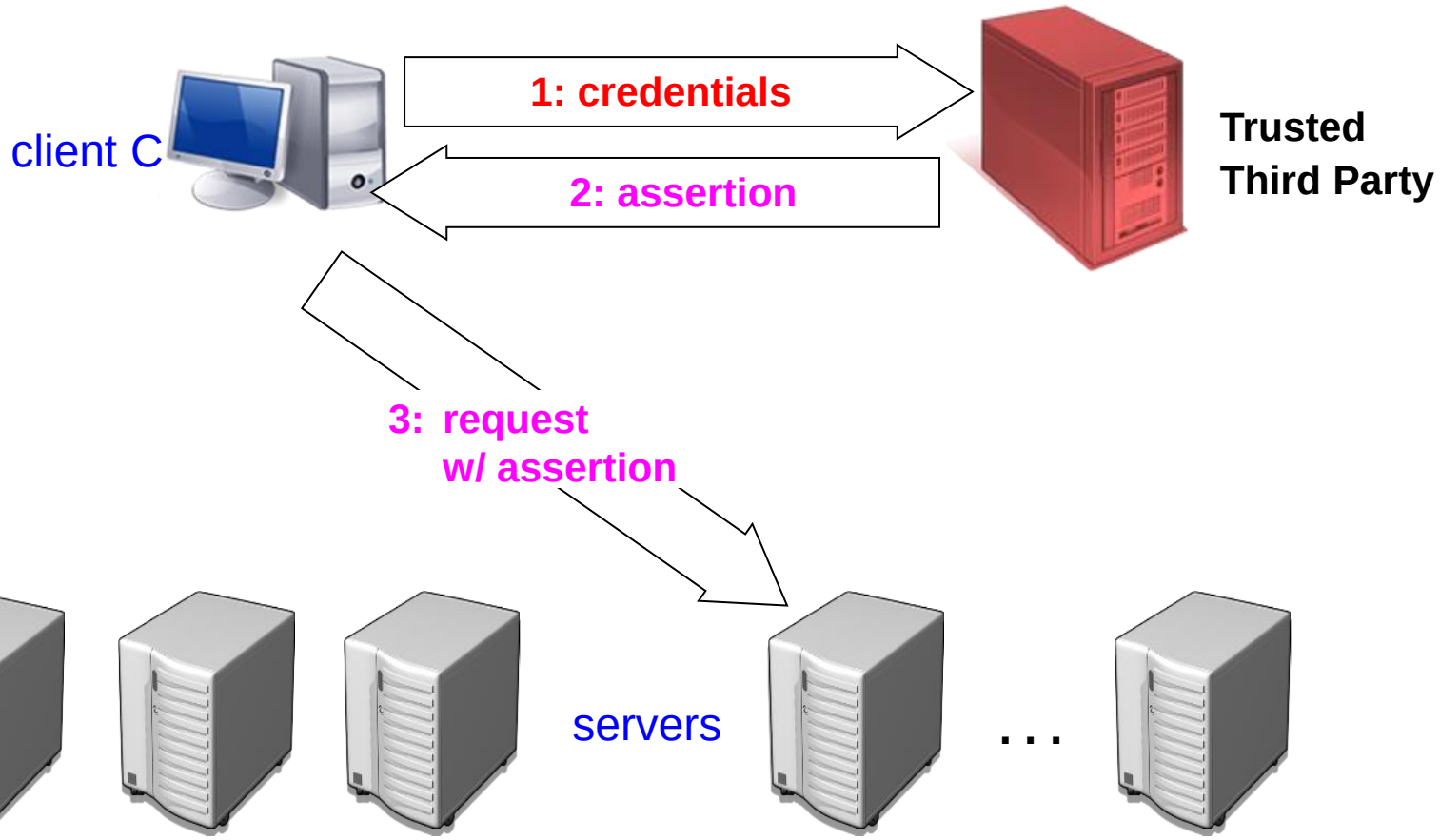
Authentication

Trusted Third Party – why not this way?



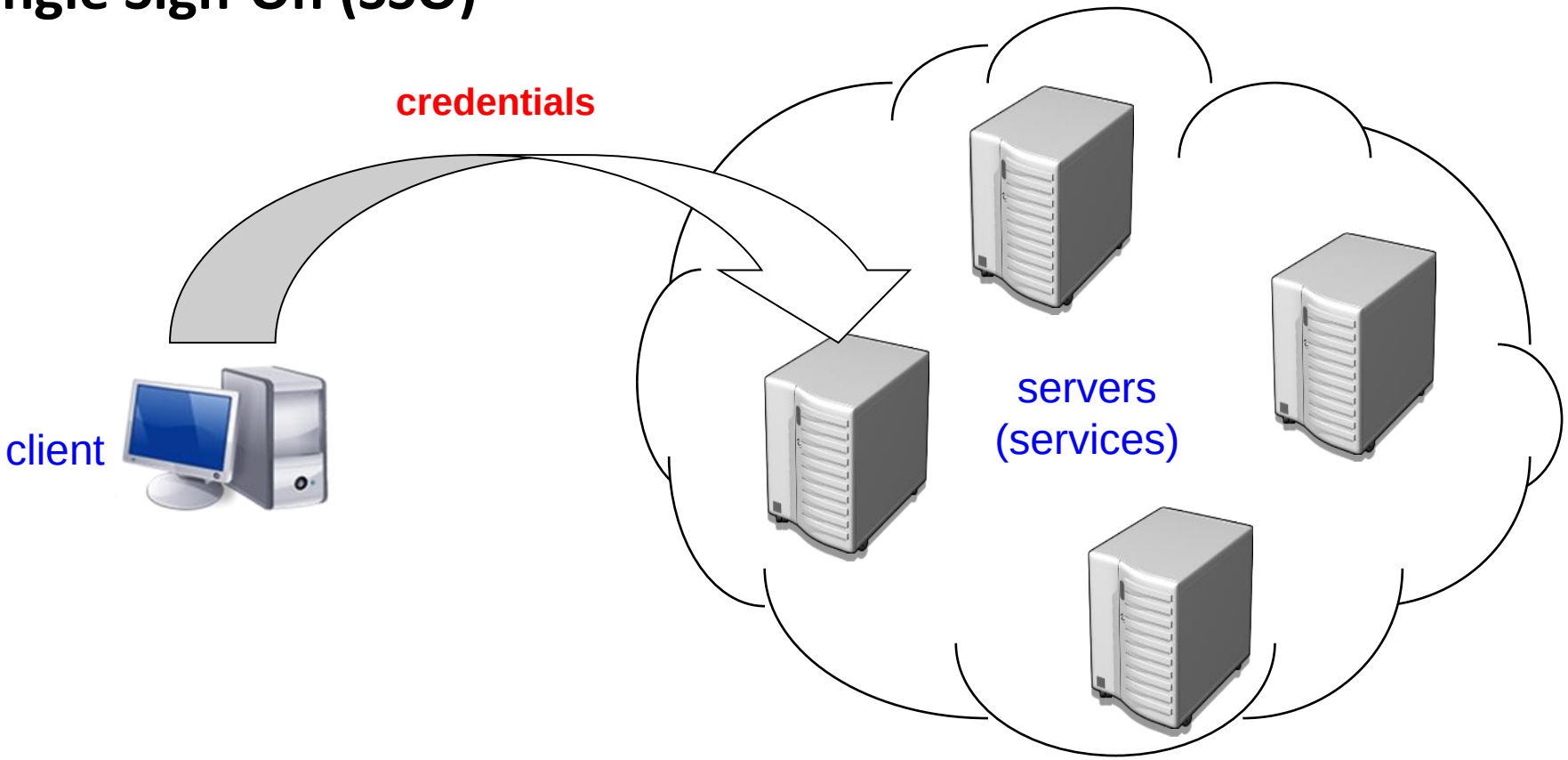
Authentication

Trusted Third Party



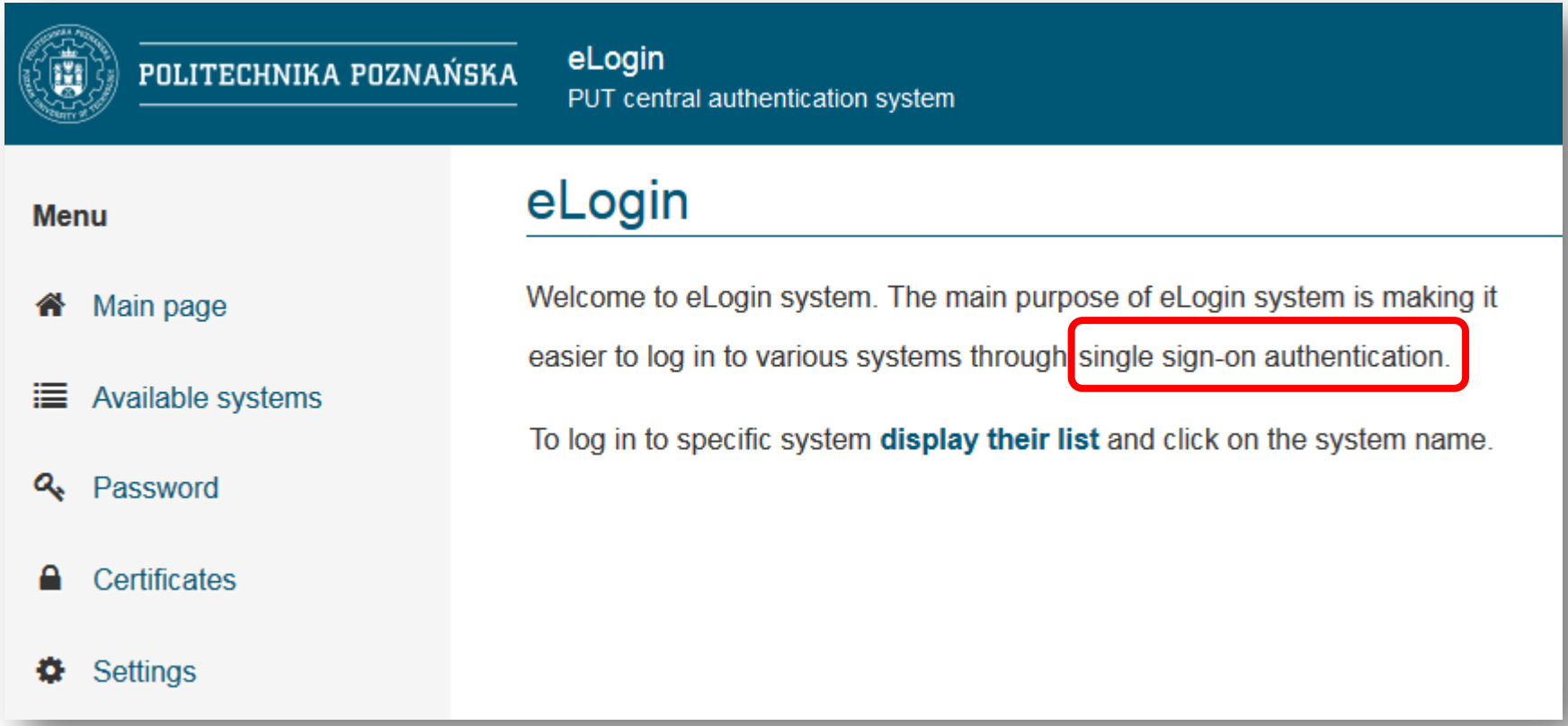
Authentication

Single Sign-On (SSO)



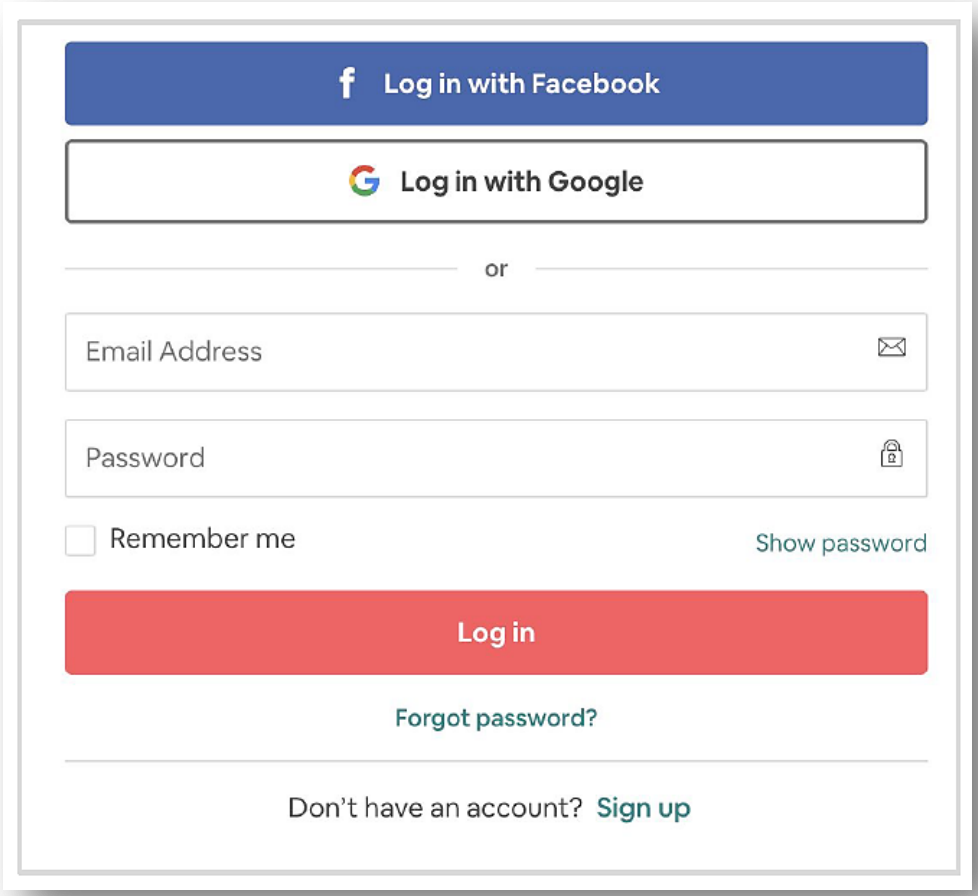
Authentication

Single Sign-On (SSO)



Authentication

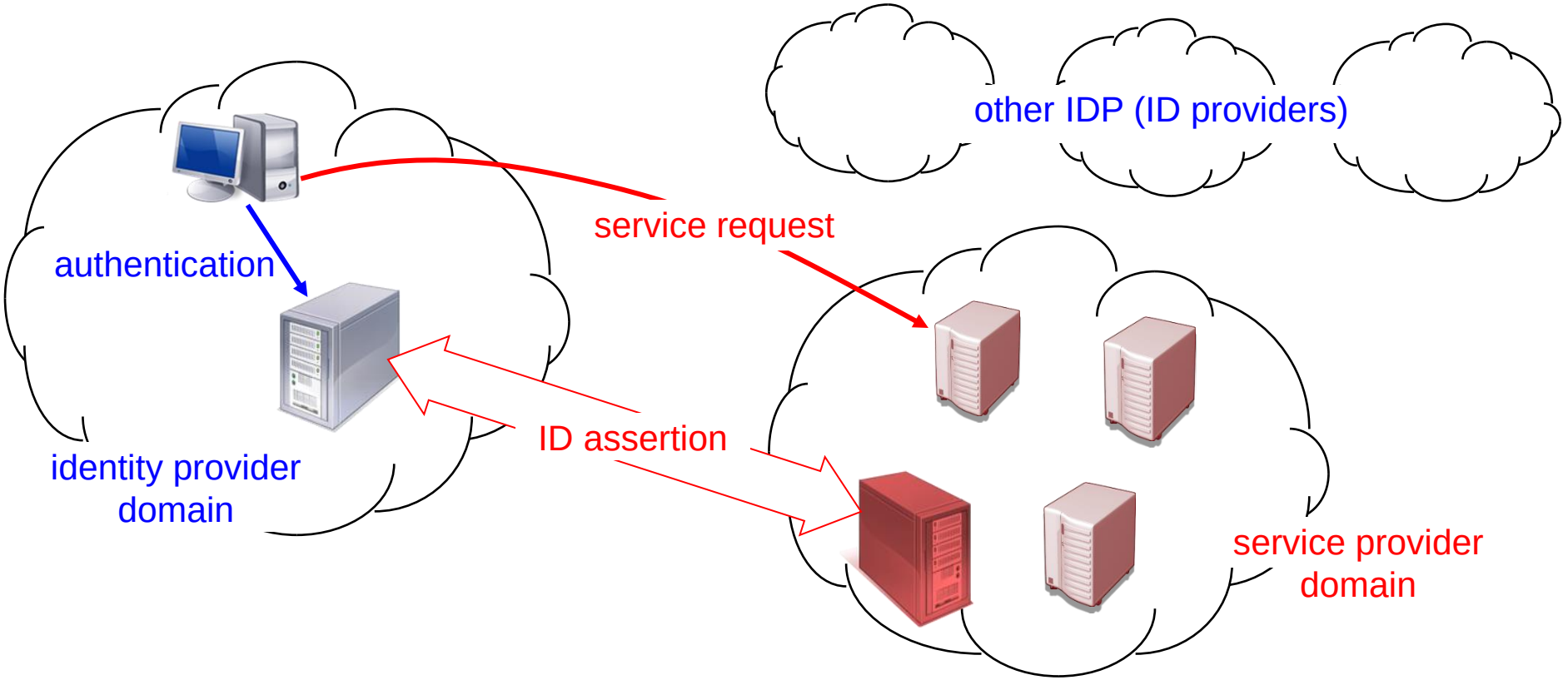
Single Sign-On (SSO)



Authentication

Federated ID

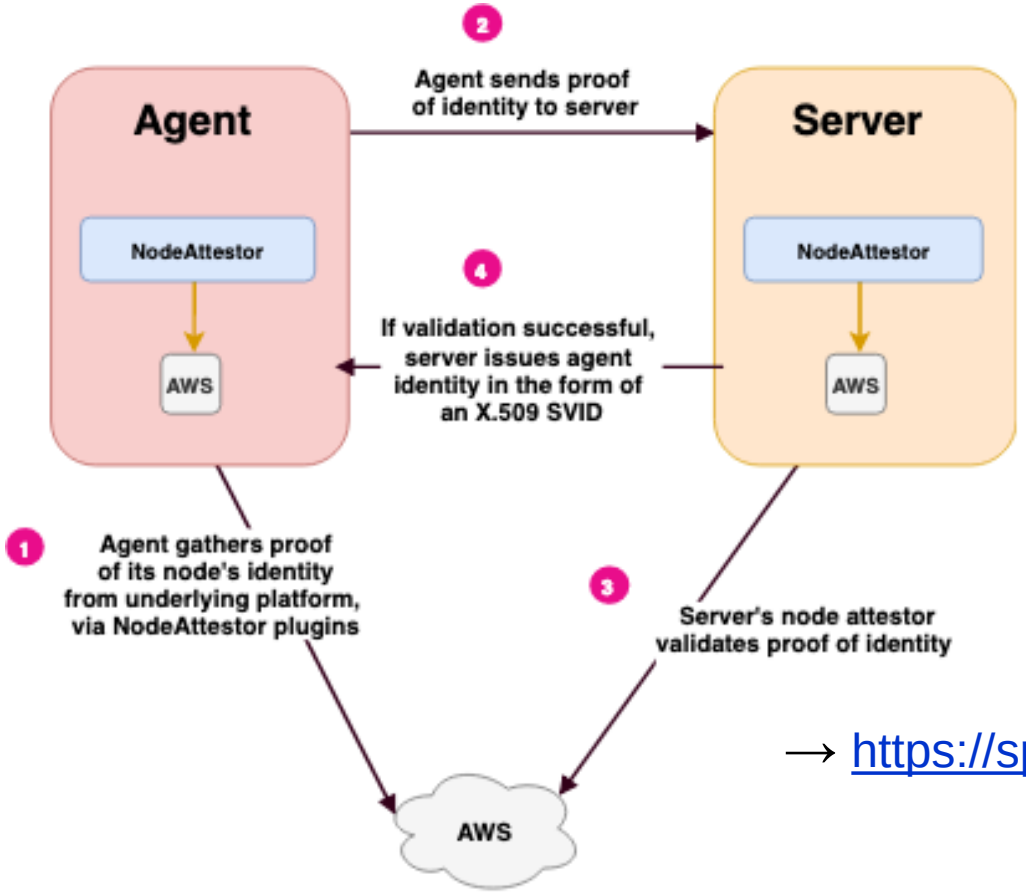
- SAML, WS-Federation, WS-Trust, OpenID, OIDC, Cloud IAM, ...



Authentication

SPIFFE (Secure Production Identity Framework for Everyone)

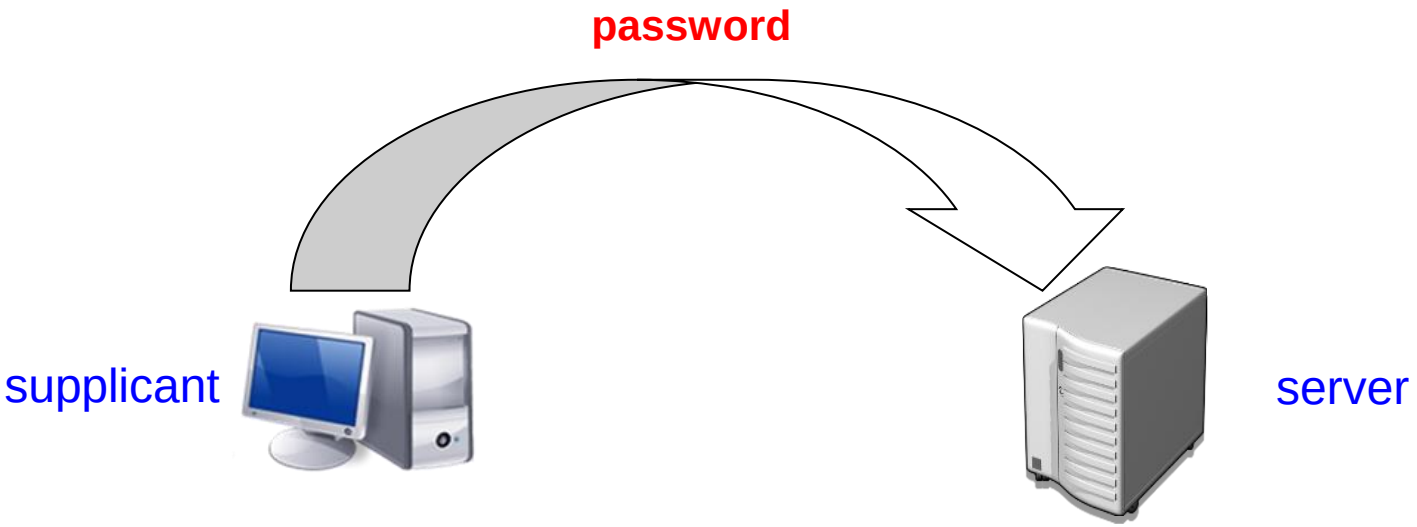
- open-source standards for issuing identity to heterogeneous services



→ https://spiffe.io/spiffe/concepts/

Authentication

Password authentication




STAR TRIBUNE
SACK
TO: CUSTOMER SUPPORT
SUBJECT: MY SECURITY
IS MY PASSWORD SAFE FROM RUSSIAN HACKERS?
TO: CUSTOMER
SUBJECT: YOUR SECURITY
DA.
TAP TAP TAP

Authentication

Passwords

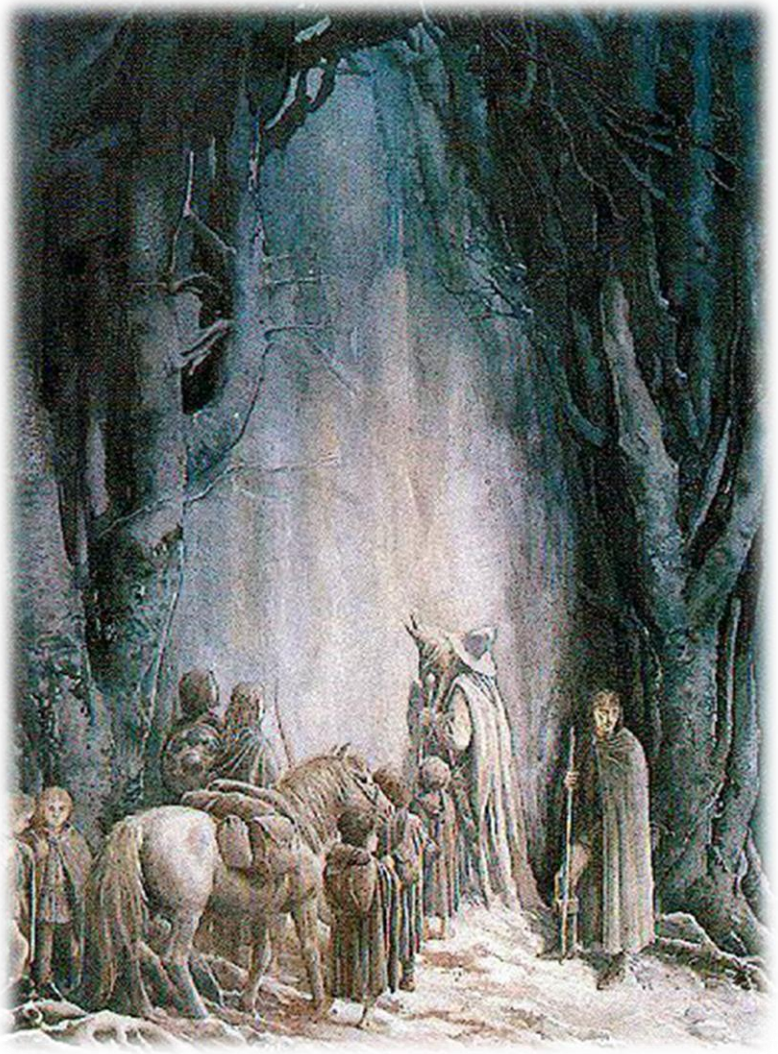
pâpmu mâttum c mjmu

"What does it mean by *speak, friend, and enter*?" asked Merry.

"That is plain enough." said Gimli. "If you are a friend, speak the password, and the doors will open, and you can enter." (…)

"But do not you know the word, Gandalf?" asked Boromir in surprise.

"I do not know the word yet. But we shall soon see …"



Authentication

Password attacks

- password guessing

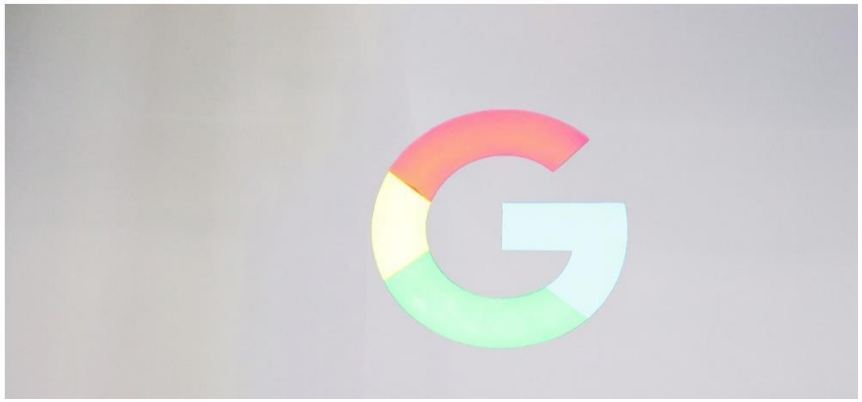
Authentication

Password attacks

- password guessing – brute-force attacks, dictionary attacks
- password stealing (at-rest attack)

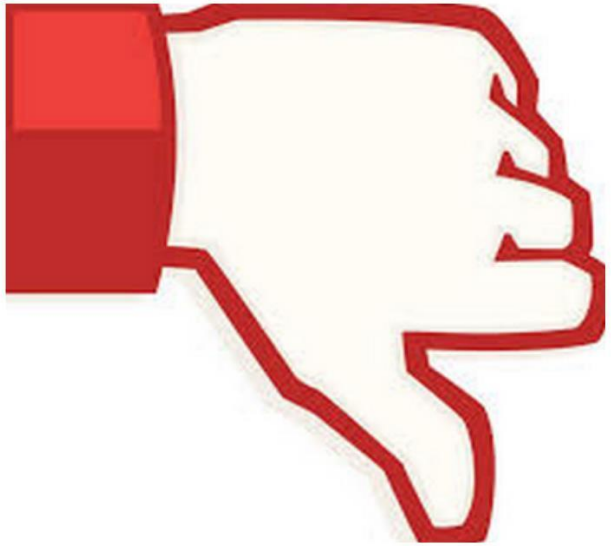
LILY HAY NEWMAN SECURITY 05.21.19 05:14 PM

GOOGLE HAS STORED SOME PASSWORDS IN PLAINTEXT SINCE 2005



21 MAR 19

Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years



APPS \ MOBILE \ TECH

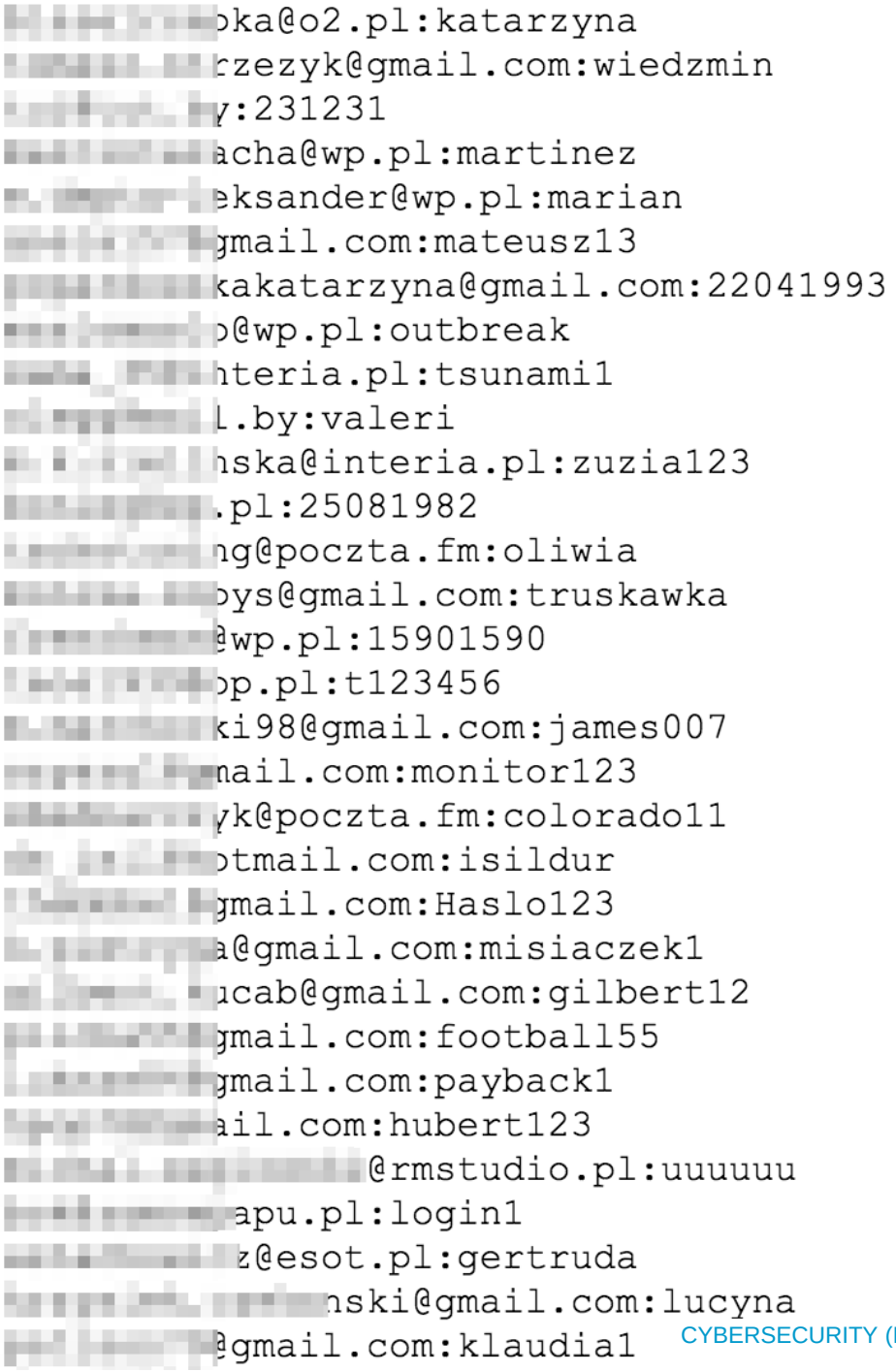
Twitter advising all 330 million users to change passwords after bug exposed them in plain text

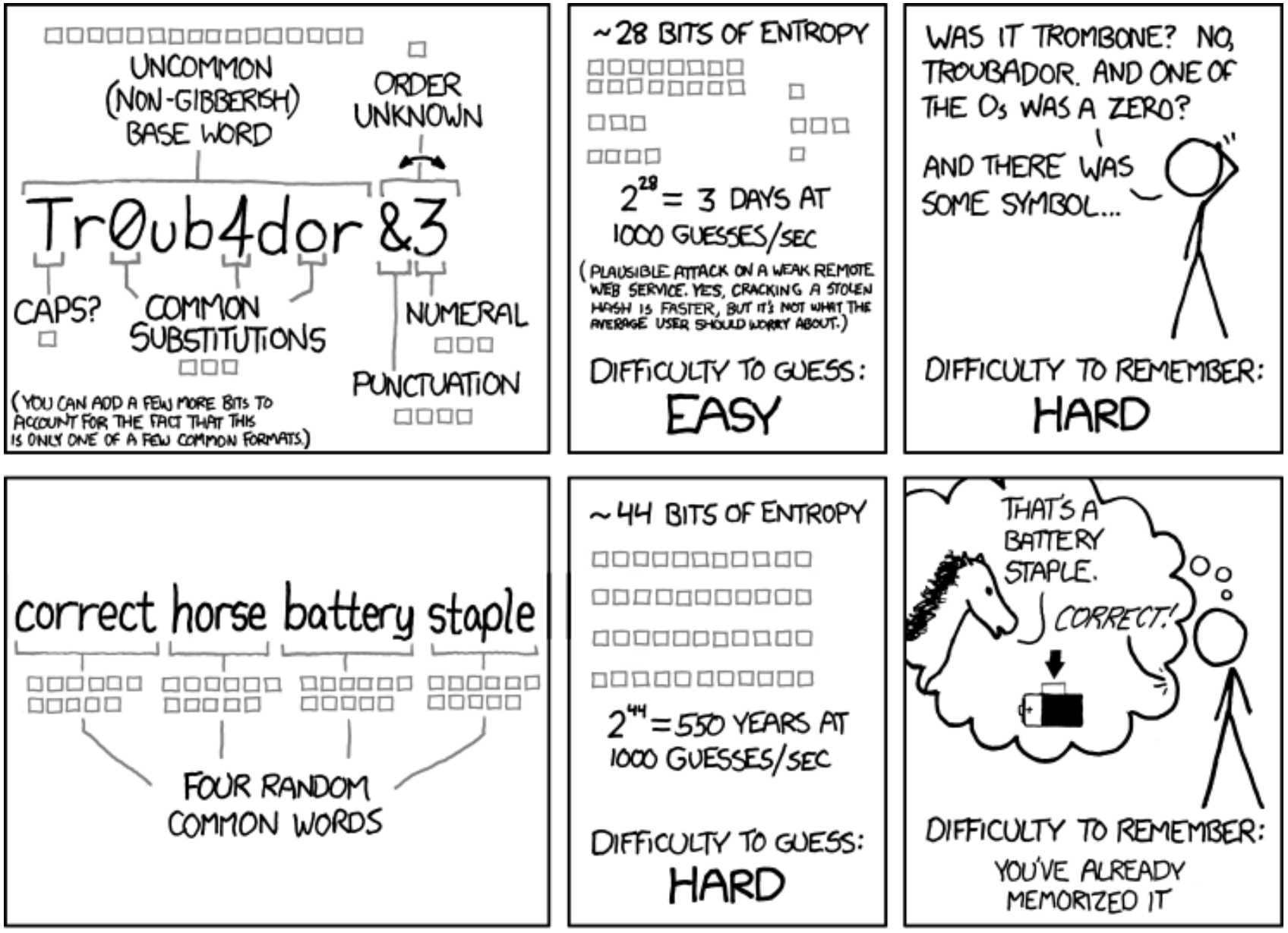
67

Authe

Password attacks

- morele.net 2018





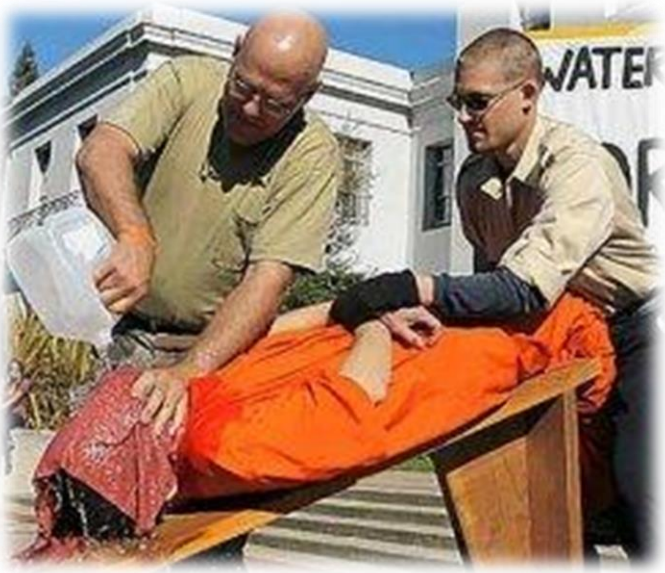
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

https://xkcd.com

Authentication

Password attacks

- password guessing – brute-force attacks, dictionary attacks
- password stealing (at-rest attack)
- password eavesdropping (in-transit attack)
- non-technical methods to obtain passwords (e.g. buying, …)



Authentication

Other password problems

- long-lasting and outdated passwords

$$P = \frac{L \cdot R}{S}$$

L = time

R = password-cracking power

S = search space (for k-length passwords from N-char alphabet: $S = N^k$)

➔ https://random-ize.com/how-long-to-hack-pass/

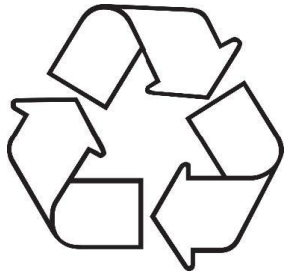
➔ https://www.grc.com/haystack.htm

Authentication

Other password problems

- long-lasting and outdated passwords
- default passwords
- backdoor passwords
- password reuse (⟶ *credential stuffing attack*)

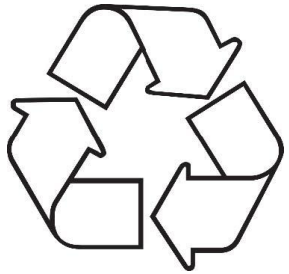
Authentication



Password reuse

One password to rule them all!

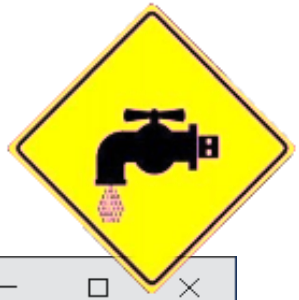
Authentication

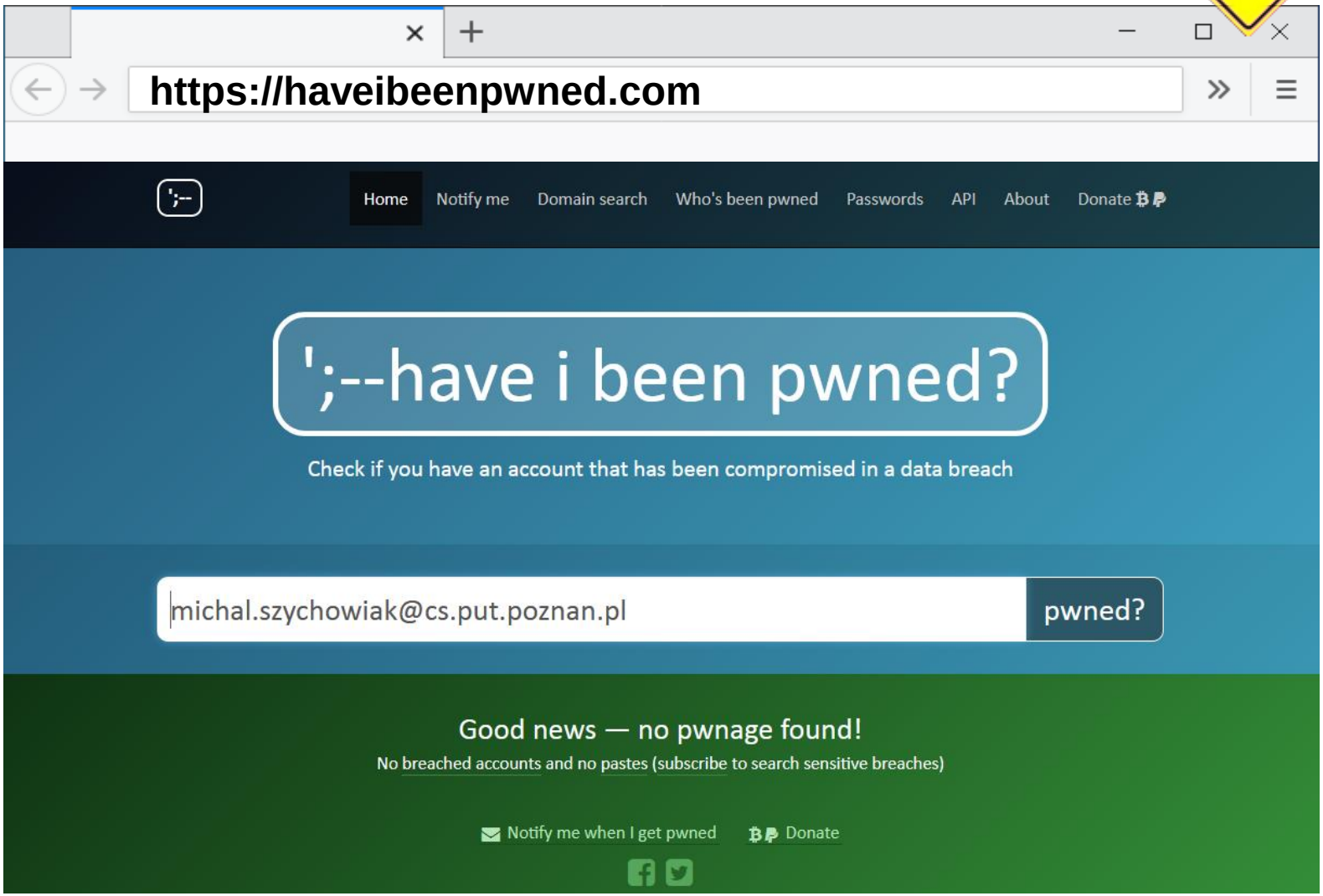


Password reuse

- LinkedIn data breach in 2016 – 164 mln passwords leaked!

Authentication





Authentication

258	4,846,841,219
pwned websites	pwned accounts

Top 10 breaches

711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts

Authentication

Password strength

Some insight on morele.net leak:

3034561	wp.pl	3347	gov.pl
2917637	interia.pl	130	policja.gov.pl
1482686	o2.pl	37	mon.gov.pl
688295	op.pl	39	sejm.pl
336581	tlen.pl	7	prezydent.pl
311673	vp.pl		

- only lowercase: 6 002 860 (45.43%)
- only digits: 878 898 (6.65%)
- single terminal digit: 1 359 345 (10.29%) – almost always ‘1’

Authentication

Passwords – dictionary attacks

46818	123456	4073	1234567
16682	qwerty	3933	123123
13093	123456789	3850	qwerty1
10138	12345	3620	karolina
10113	zaq12wsx	3563	agnieszka
6220	111111	3450	bartek
5182	misiek	3351	password
4776	monika	3348	qwe123
4418	marcin	3343	damian
4369	12345678	3266	1qaz2wsx
4240	mateusz	3024	qwerty123

Authentication

Beware of social engineering scam!

Od Free Hack Report <noreply@getyourhackreport.com>
Temat **Your password[redacted].... is available on the Dark Web**
Do [redacted]
Program Thunderbird uznał tę wiadomość za niechcianą.

Billions of Passwords Have Been Breached. YOU ARE ON THE LIST!

WHAT WE DO?

- We monitor the Dark Web to find stolen data
- We intercept the data that people trade and sell
- We clean the data and associate it with an email address
- We notify you when your info has been part of a breach

https://www.gethackedreport.com/?affiliate=39323_1&watch=video

Watch our 2 Minute Video That Explains How These People Get Your Information and What You Can Do - Watch Video Now!

GET YOUR FREE BREACH REPORT TODAY AND SEE WHAT INFO THESE PEOPLE ALREADY HAVE ABOUT YOU - Go To FreeBreachReport

You are receiving this e-mail because your info was found on the dark web from a security breach that happened with one or more website you have registered for over the last several years.

To be removed from any future notices from Dark Sources Security unsubscribe

http://secure.fatjacket.com/unsub/

Sincerely,
Dark Sources Security
FreeBreachReport

Authentication

Good-password policy

A password is like underwear – keep it hidden!

A password is like underwear – change it often!

A password is like underwear – don't share it with friends!

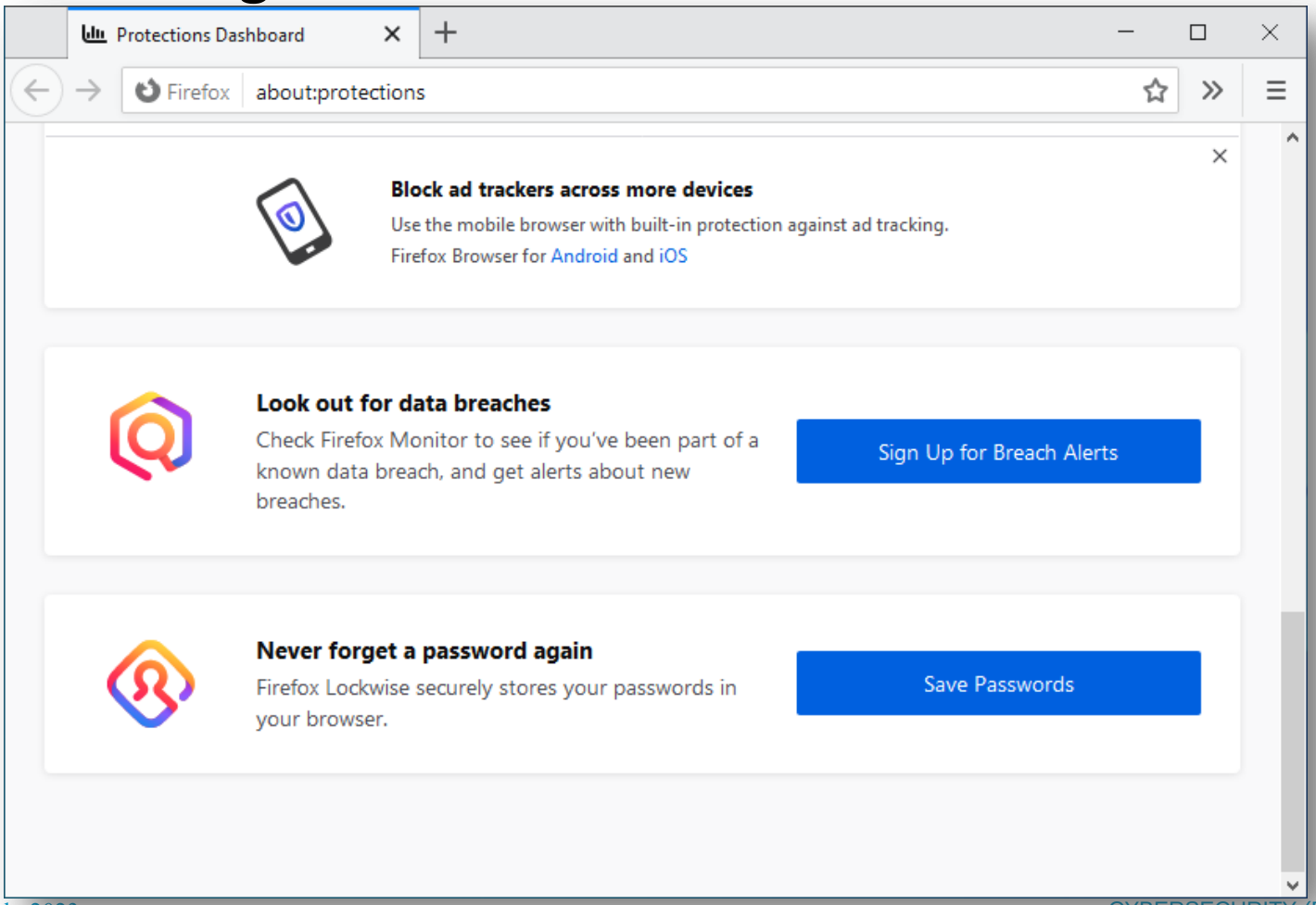
➔ https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

Authentication

Password management

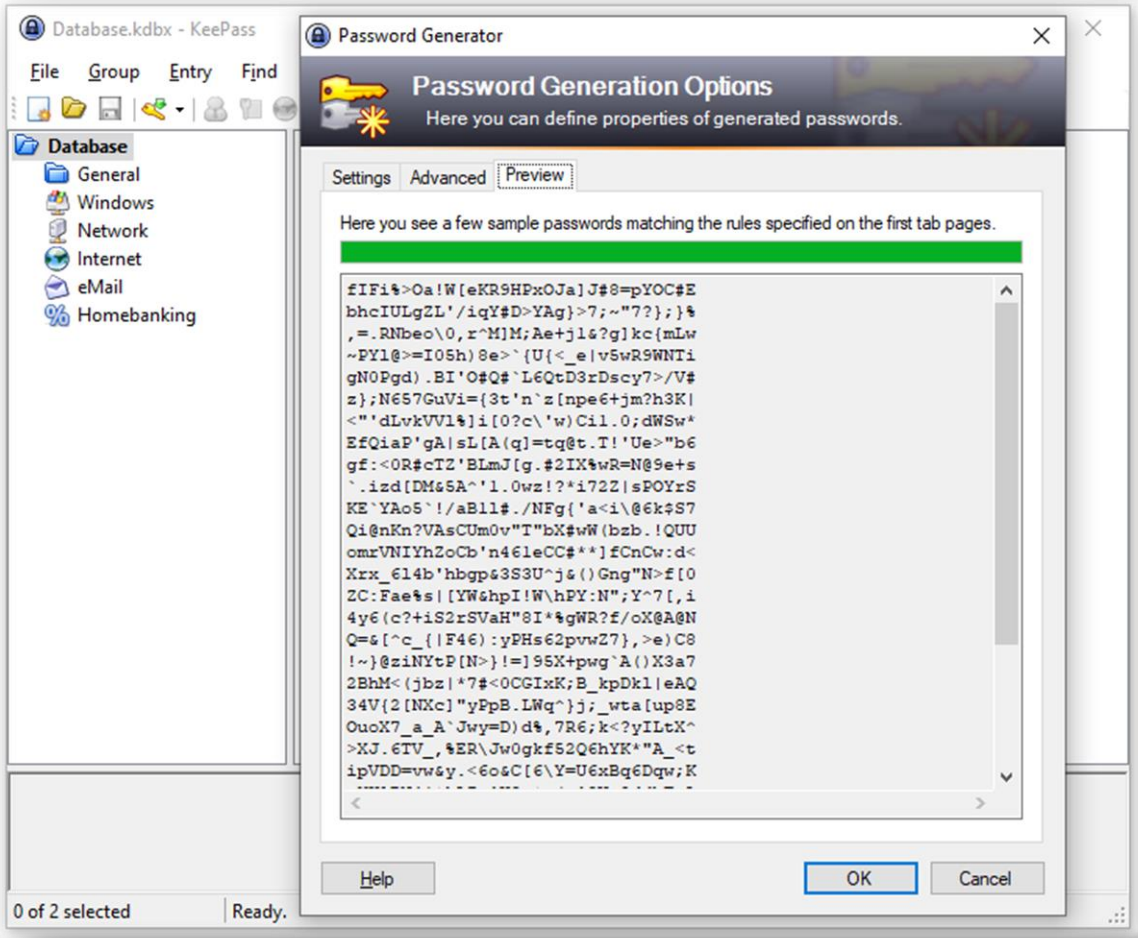
Authentication

Password management



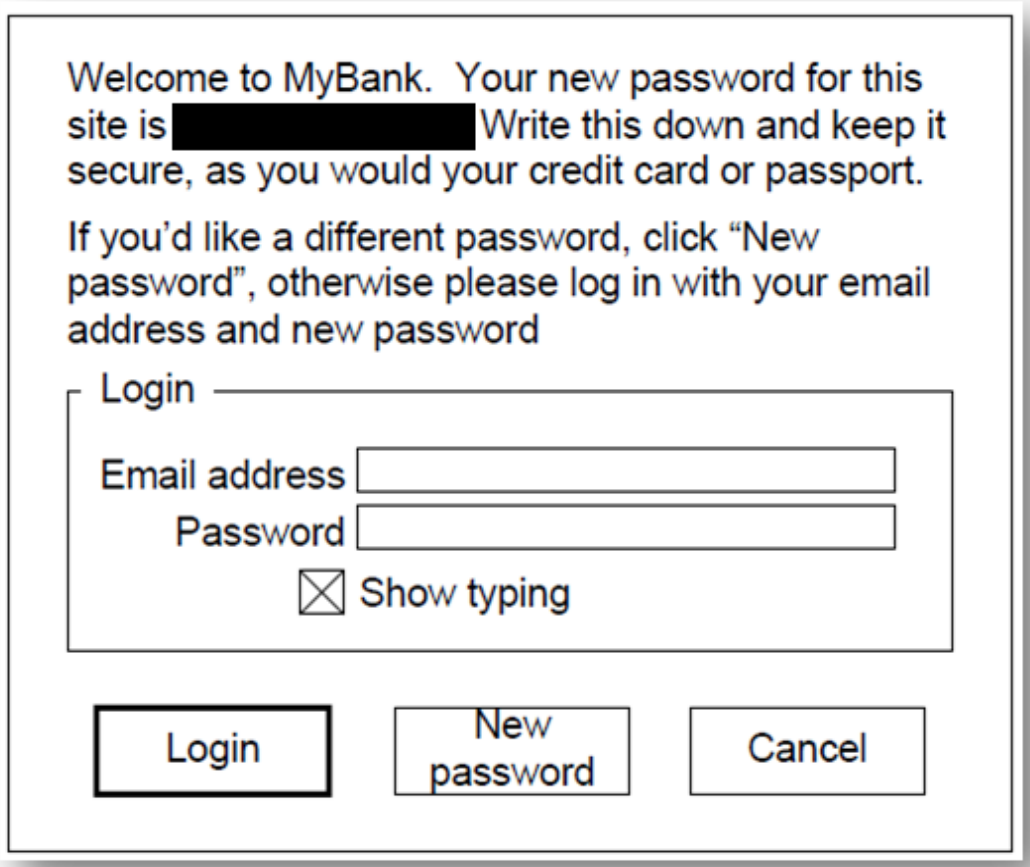
Authentication

Password management



Authentication

Password management

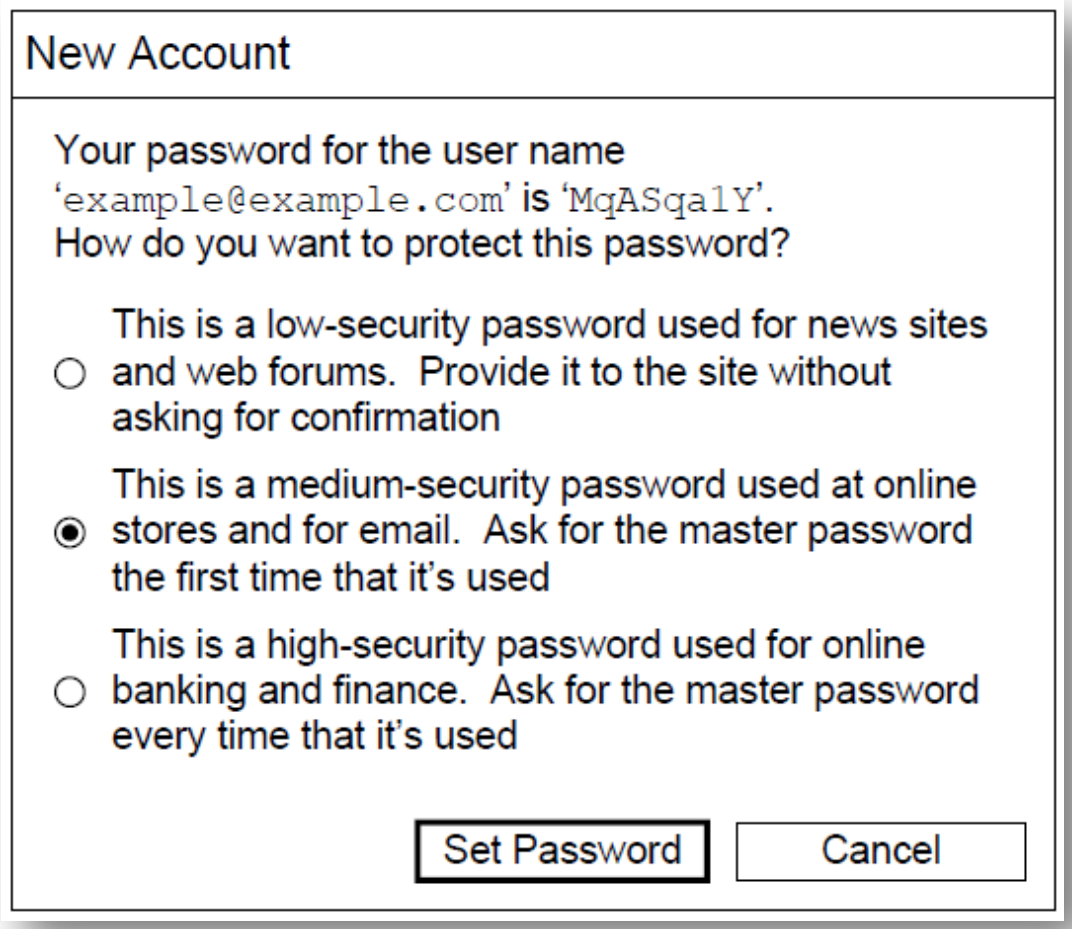


Authentication

Password management

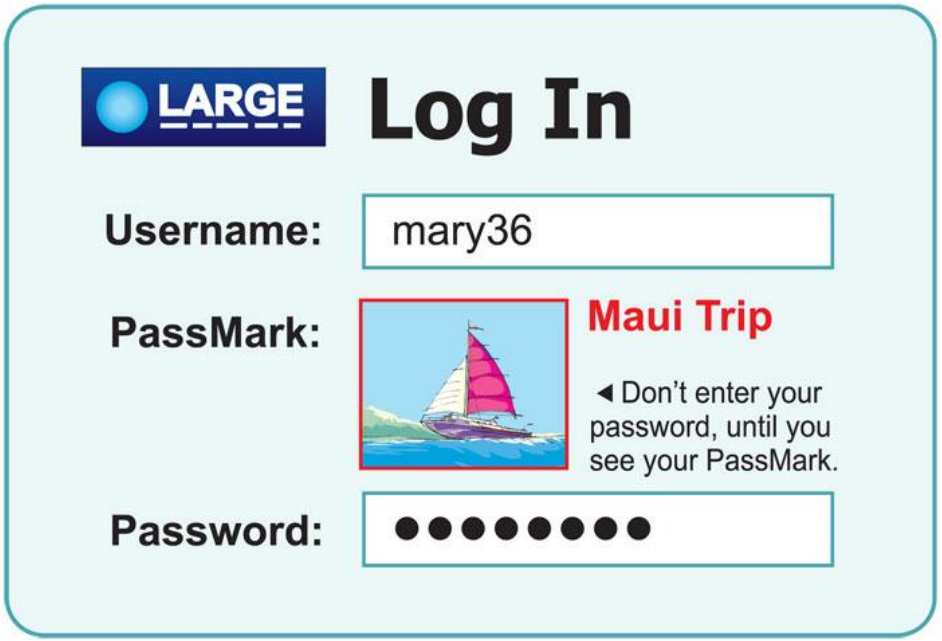
→ Windows Data Protection API (DPAPI)

→ Credential Manager API



Authentication

Password (account) image



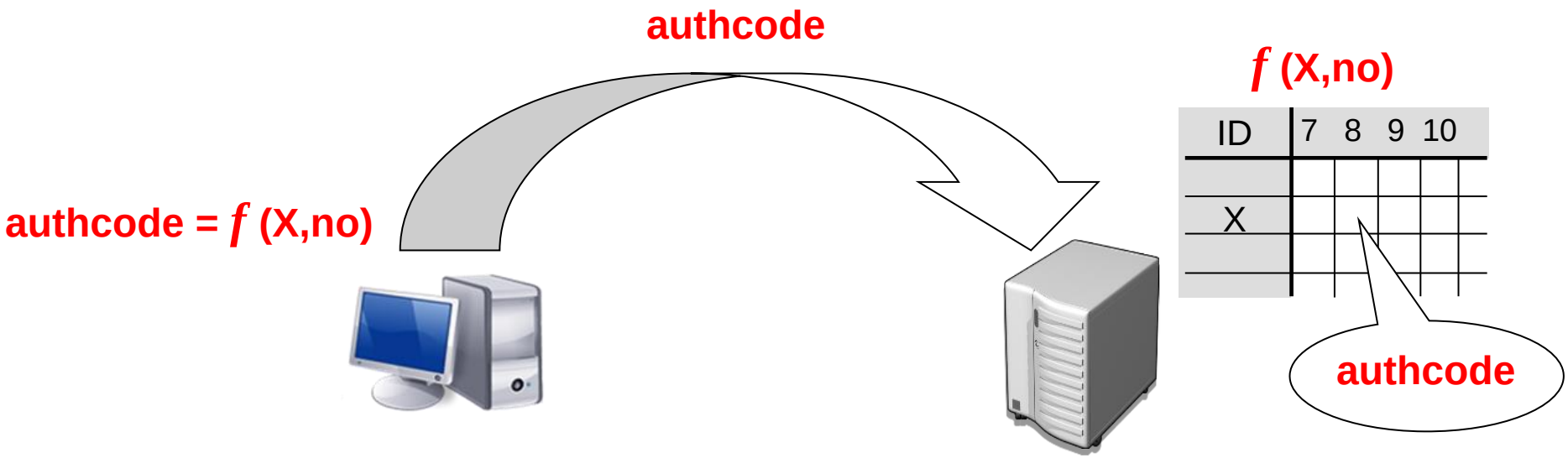
Authentication

OTP – *One-Time Passwords*

- TAN/ITAN – [*Indexed*] *Transaction Authentication Numbers*
- Time synchronization
- Challenge-Response

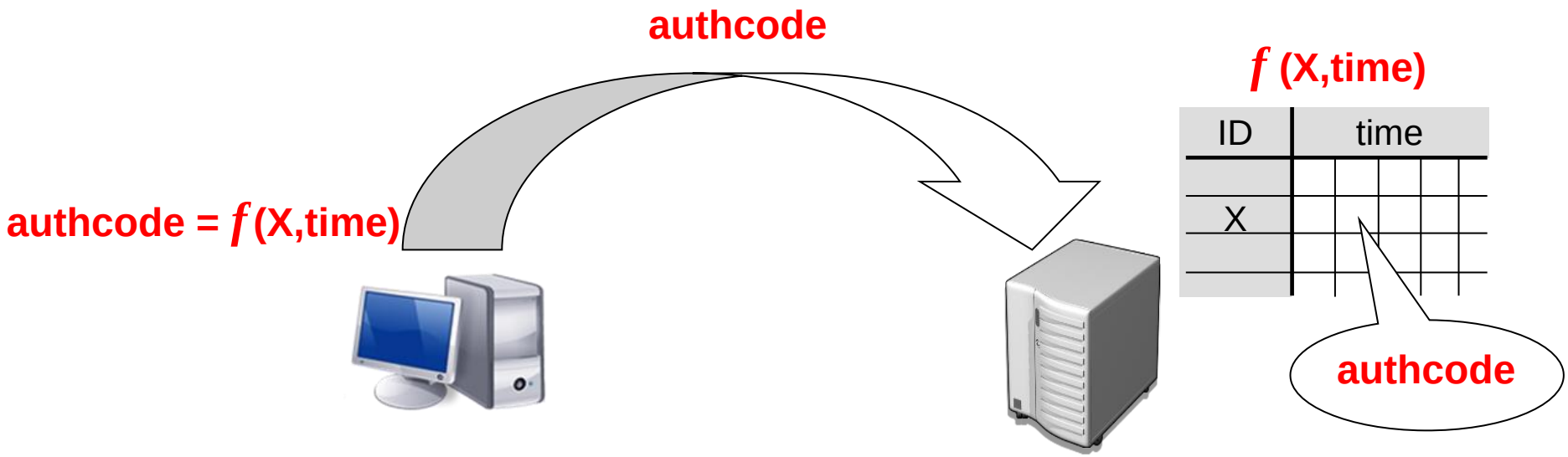
Authentication

TAN/ITAN – [*Indexed*] *Transaction Authentication Numbers*



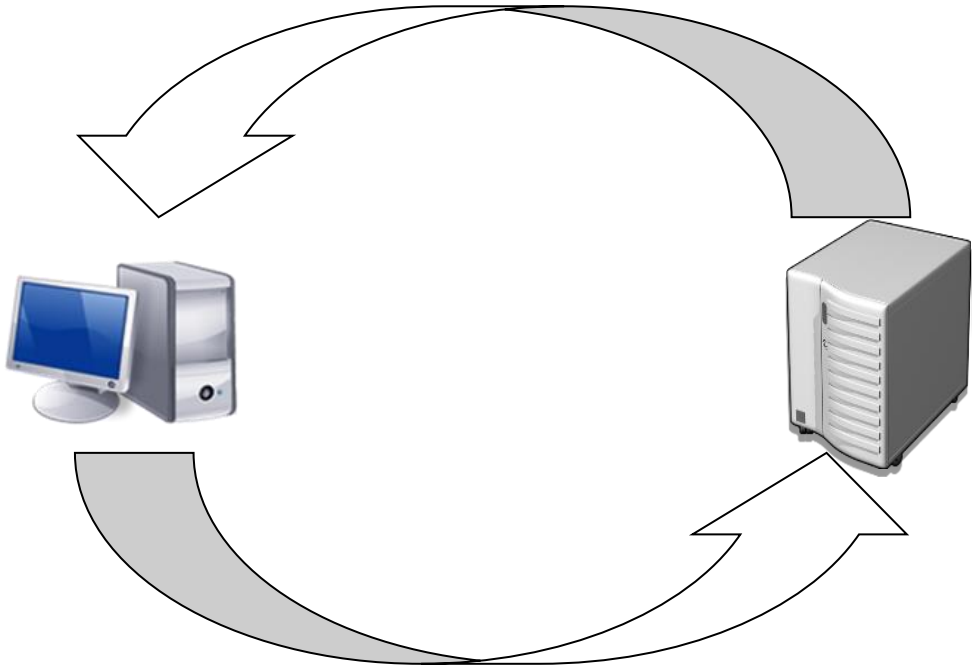
Authentication

Time synchronization



Authentication

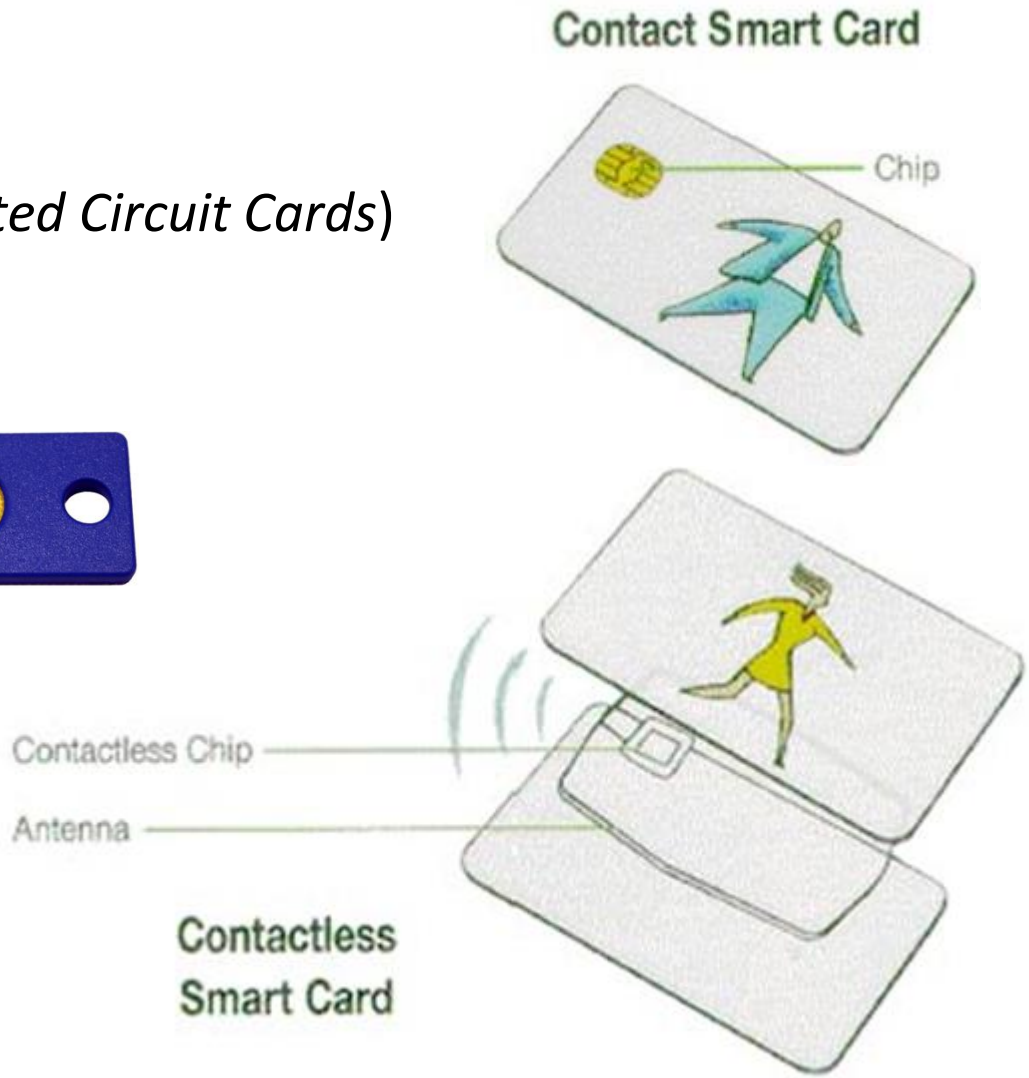
Challenge-Response



Authentication

Security tokens

- smart cards (ICC – *Integrated Circuit Cards*)
- smart keys
- i-buttons
- USB tokens



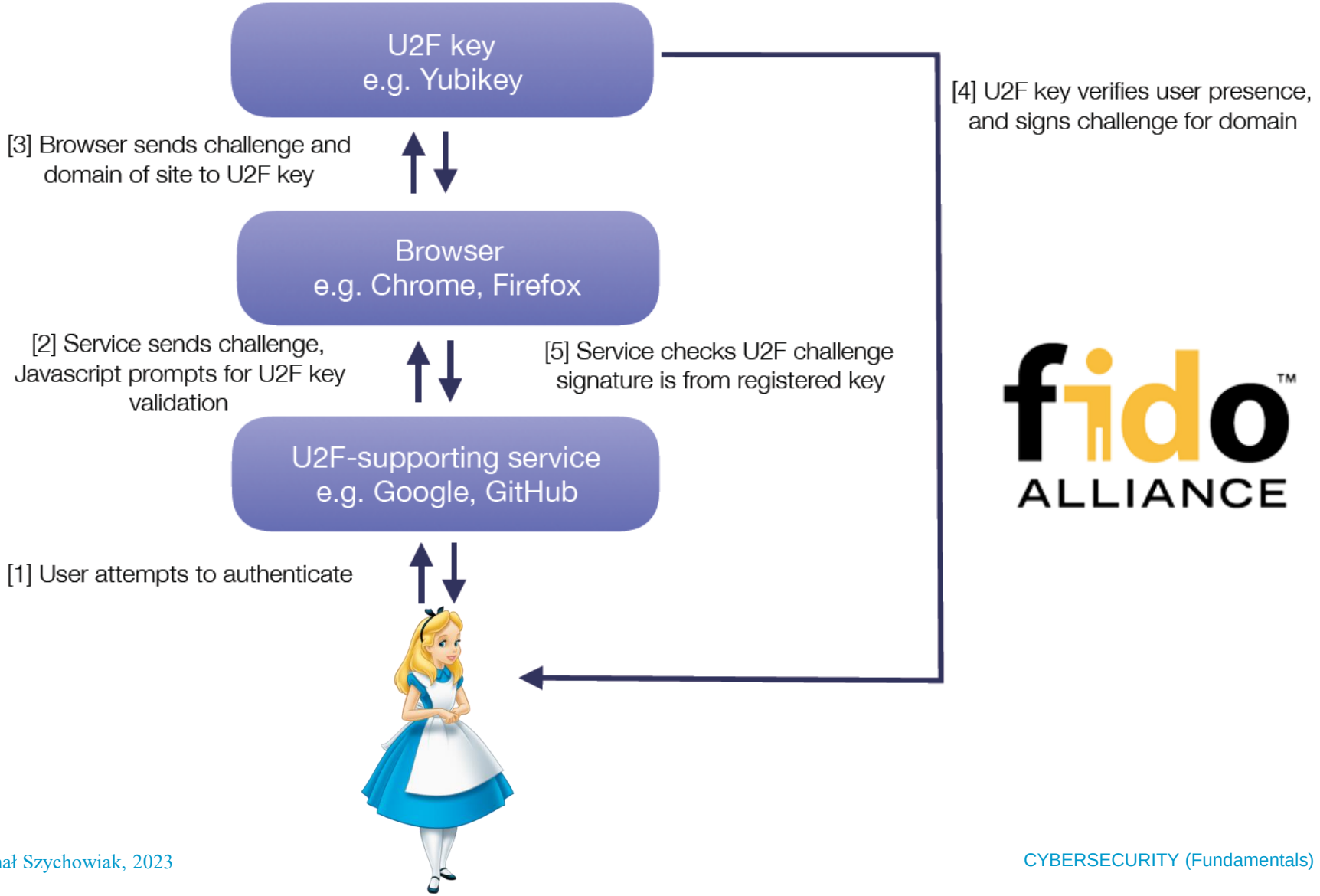
Authentication

Two-Factor Authentication (2FA)


```
$ ssh 134.212.121.12
Confirm user presence for key ECDSA-SK SHA256:esvq6KPZ5FGtt...
[Tab your YubiKey U2F Security Key now]
```

- e.g. Universal 2nd Factor (U2F) standard →

Authentication



Authentication

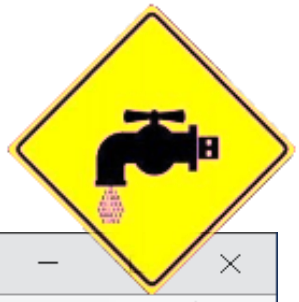
Two-Factor Authentication (2FA)

Authentication

Two-Factor Authentication (2FA)

- smartphone (e.g. 3D Secure)

Authentication



https://phonesearch.gofyeo.com

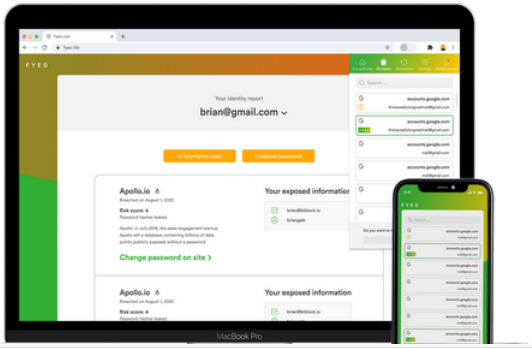
Has your phone number or email been leaked?

Prevent identity fraud. Your email + phone number is the perfect match for cybercriminals to initiate takeovers of your online accounts.

Enter your email or phone number | Search

For phone search: format must be country code + phone number with no spaces. (example +19705551234)

Download the raw hashed research data here. (File size 22.8GB)

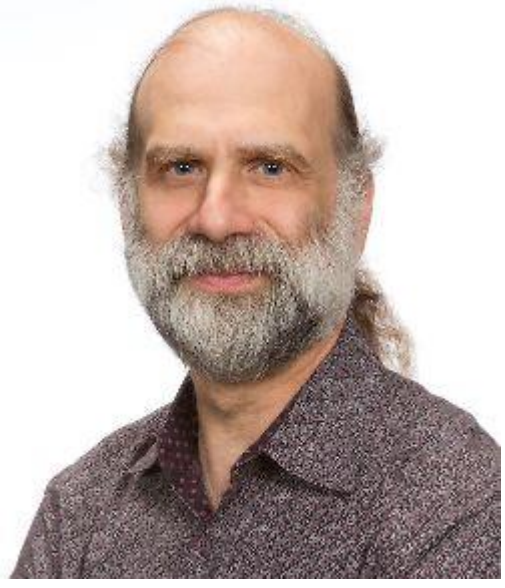


FYEO Identity: decentralized password management and identity monitoring made simple

The FYEO Identity (“FYEO ID”) password manager is based on private key technology that generates passwords from strong key material that is

“Two-factor authentication isn't our savior.
It won't defend against phishing.
It's not going to prevent identity theft.
It's not going to secure online accounts from fraudulent transactions.
It solves the security problems we had 10 years ago, not the security problems we have today.”

Bruce Schneier



“Two-factor authentication isn't our savior.
It won't defend against phishing.
It's not going to prevent identity theft.
It's not going to secure online accounts from
fraudu
It solv
not th

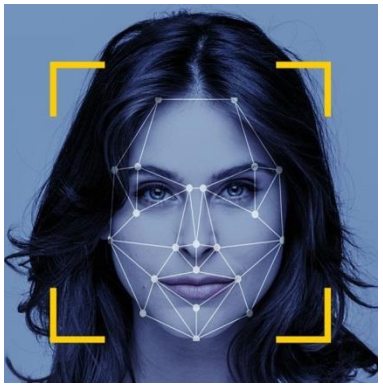
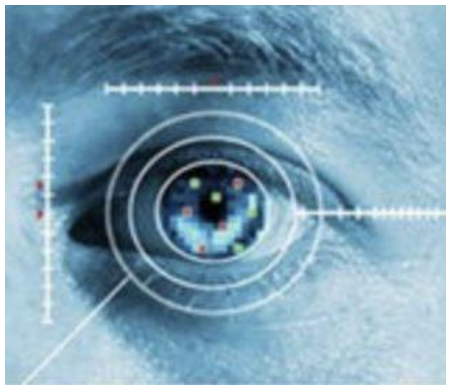
Latest Cyber Security News | Network Security Hacking ◇ News ◇ Vulnerabilities

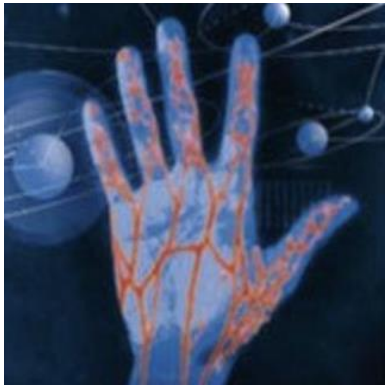
Serious 2FA Bypass Vulnerability Affected Facebook And Instagram

written by Abeerah Hashim | January 30, 2023

Authentication

Biometrics





Authentication

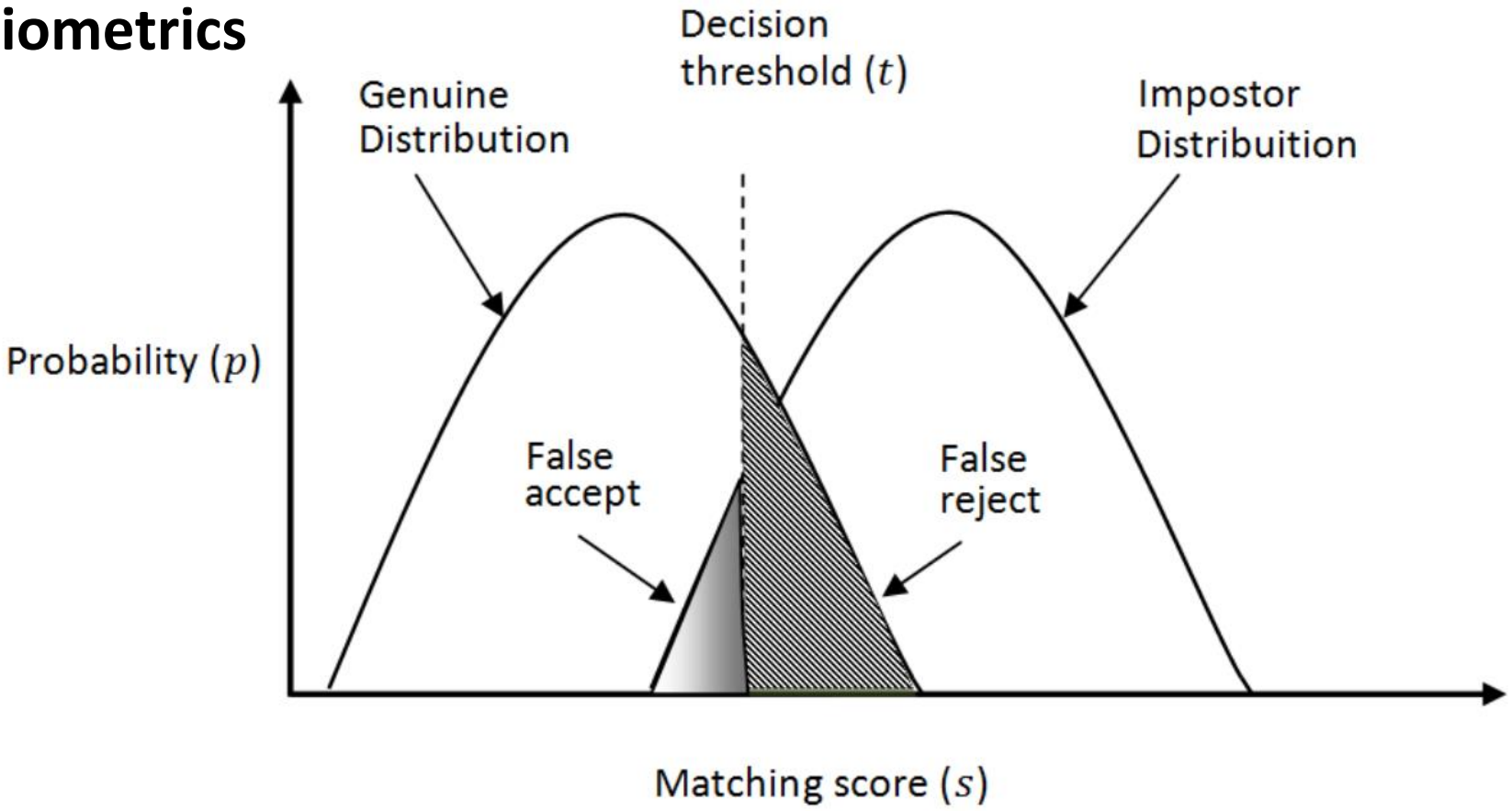
Biometrics

Authentication

Biometrics

Authentication

Biometrics



☺ https://www.youtube.com/watch?v=vI3OvT4b-sA

Authentication

Biometrics

Authentication

Biometric problems

- attribute state permanency:
  - once compromised = compromised forever
  - once lost = lost forever

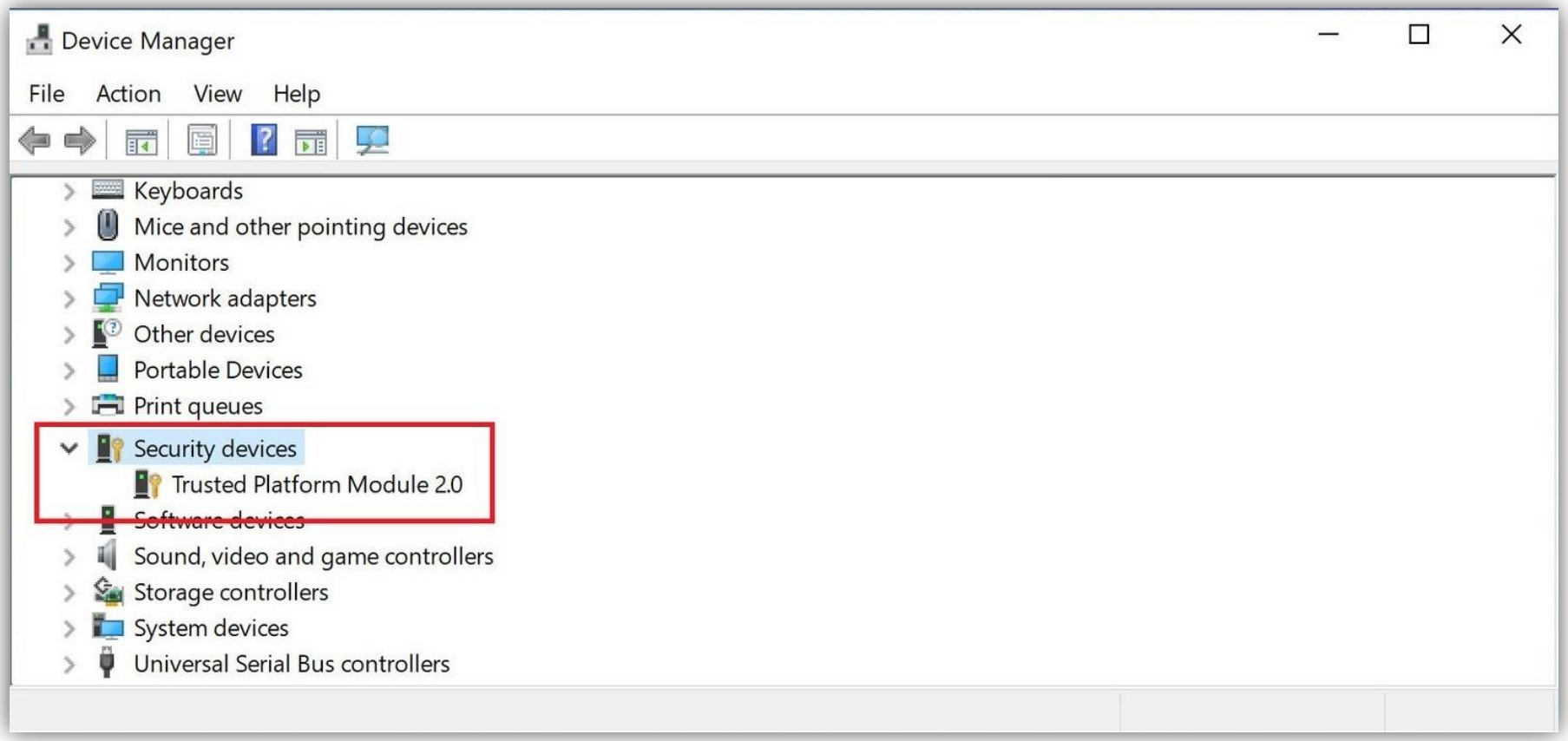
Authentication

Biometric authentication standards

- OATH = Initiative for Open Authentication
  www.openauthentication.org
- TCG = Trusted Computing Group
  www.trustedcomputinggroup.org
  - e.g. Trusted Platform Module – TPM (CC EAL 3+, 4+, ...)

Authentication

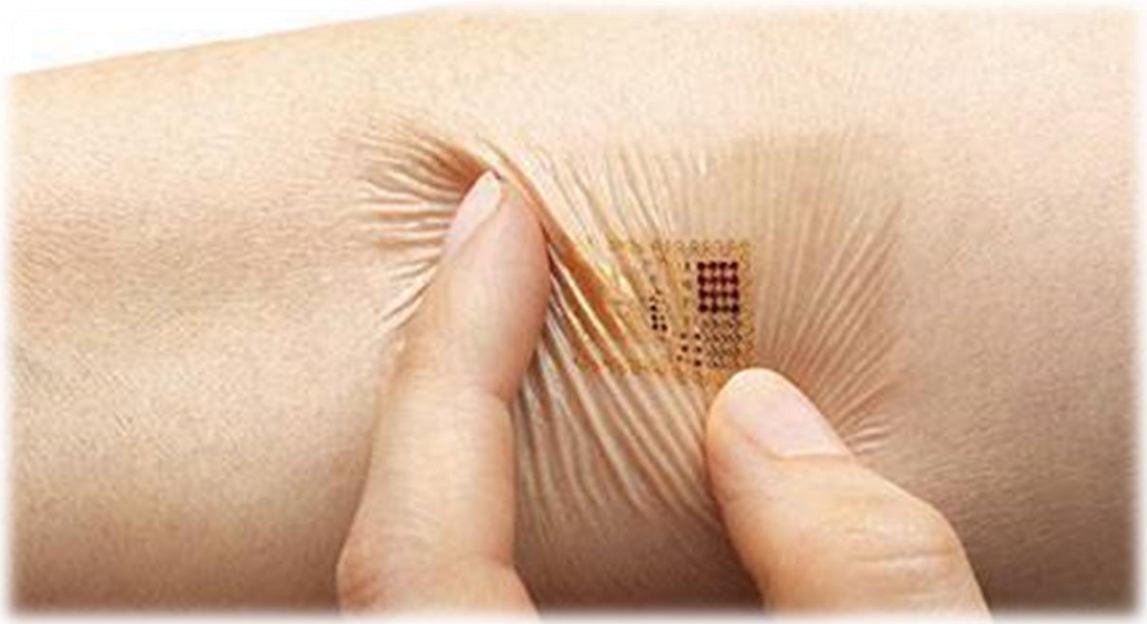
Trusted Platform Module (TPM)



Authentication

Bioelectronics

- electro-tattoo (RFID)



- “vitamin authentication”

https://techland.time.com/2013/05/31/motorola-is-working-on-a-password-pill-for-once-daily-authentication-oh-and-a-tattoo-too/

Authentication

Recap

- 3 basic ways to authenticate you:
  - something you know
  - something you have
  - something you are
- none is perfect
- 2FA / MFA

Authentication

MULTIFACTOR AUTHENTICATION

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

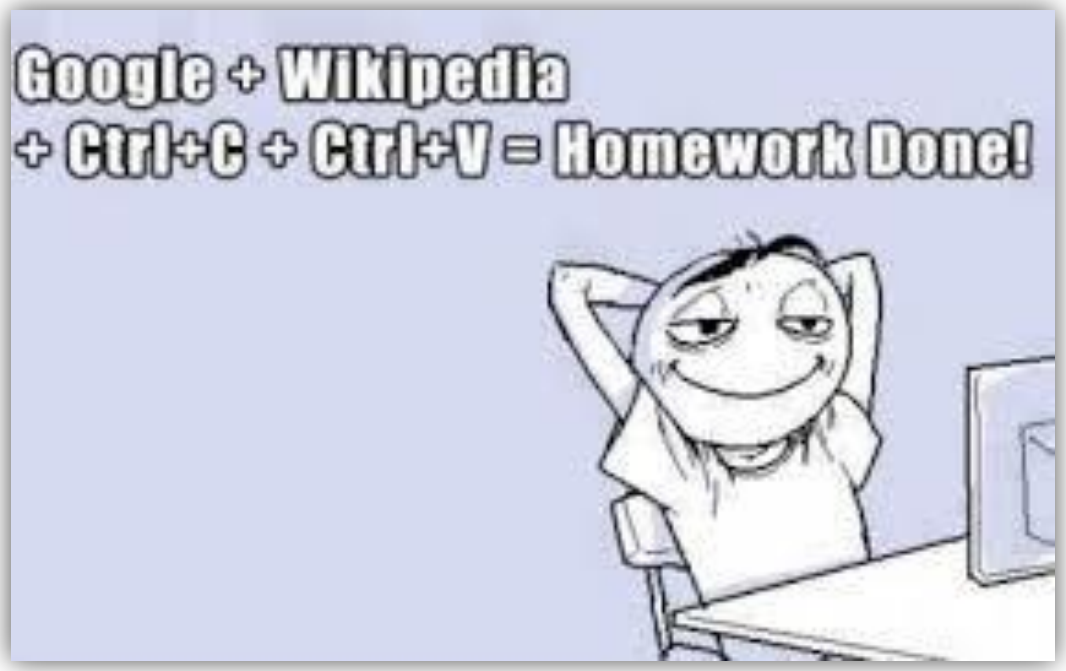
A slide from "Modern Two-Factor Authentication: Defending Against User-Targeted Attacks" by Dug Song and Jon Oberheide, Duo Security, 2012

HOMEWORK

=

Half Of My Energy Wasted On Random Knowledge

Windows Data Protection API (DPAPI) → Credential Manager API



AUTHORIZATION & ACCESS CONTROL

Fundamentals

Basic terminology

4. Authorization

- granting access rights for a principal

5. Access Control

- verification of compliance with (former) authorization

REPLAY

Authorization

Model

Object (Resource)

- unit of the access
- e.g.: program, file, service, database, database relation (a table)
- high granularity: distinct tuples of a database table

Subject (Principal)

- performs the access
- e.g.: user, host, process, service

Access rights (Permissions)

- operations on a given object permitted for a given subject

Authorization

Rudimentary approaches

1. ~~Everything is allowed.~~
2. Anything not (explicitly) forbidden is allowed.
3. Anything not (explicitly) allowed is forbidden.
4. ~~Everything is forbidden.~~

Authorization + Access Control

1. Discretionary Access Control (DAC)

- resource owner — makes the rules
- easy sharing of resources
- efficient, flexible, user-friendly
- unreliable — based on human's decisions (unconsciousness, laziness, carelessness, …)
- difficult to manage globally

Authorization + Access Control

Access Control Lists (ACL)

Access control matrix:

	object 1	object 2	object 3
James Bond	✓	✓	X
Hercule Poirot	✓	X	✓
Sherlock Holmes	X	✓	X

ACE
↑
Access Control Entry

ACL

Authorization + Access Control

2. Mandatory Access Control (MAC)

- precise access rules automatically deployed (authorized) by the system itself, and automatically executed (at the same time)
- the resource owner has nothing to say about it
- but the system (i.e. system administrator) has a lot of work to do configuring the policy

Mandatory Access Control (MAC)

Multi-Level Security (MLS)

Sensitivity level (S):

- identified by a *sensitivity label*, such as:

  public < company confidential < executives only < CEO secret

  unclassified < restricted < secret < top secret

Data domain (D):

- non hierarchical, e.g.:

  personal, production, research, financial, …

Mandatory Access Control (MAC)

Multi-Level Security (MLS)

Security label $L = \langle S, \mathbb{D}=\{D_1, D_2, \ldots\} \rangle$

$\langle$ secret, {personal}$\rangle$

$\langle$ top secret, {personal, financial}$\rangle$

Sensitivity relation

$$L_1 < L_2 \Leftrightarrow S_1 < S_2 \wedge \mathbb{D}_1 \subseteq \mathbb{D}_2$$

$\langle$ secret, {personal}$\rangle$ $<$ $\langle$top secret, {personal, financial}$\rangle$

but:

$\langle$ secret, {personal, financial}$\rangle$? $\langle$top secret, {research, financial}$\rangle$

Mandatory Access Control (MAC)

Bell-LaPadula's confidentiality model:

no read-up	A subject cannot read resources labeled higher than the subject's own security label.
no write-down	A subject cannot write into resources labeled lower than the subject's own security label.

Mandatory Access Control (MAC)

MAC 1: Subject P can read R or execute X object O

$\Leftrightarrow \mathrm{L}_P \geqslant \mathrm{L}_O$

MAC 2: Subject P can append A to or create C object O

$\Leftrightarrow \mathrm{L}_P \leqslant \mathrm{L}_O$

MAC 3: Subject P can (fully) modify M object O

$\Leftrightarrow \mathrm{L}_P = \mathrm{L}_O$

MAC 4: Transition T from one identity to another $P_1 \rightarrow P_2$

$\Leftrightarrow \mathrm{L}_{P_1} \leqslant \mathrm{L}_{P_2}$

Mandatory Access Control (MAC)

Implementations

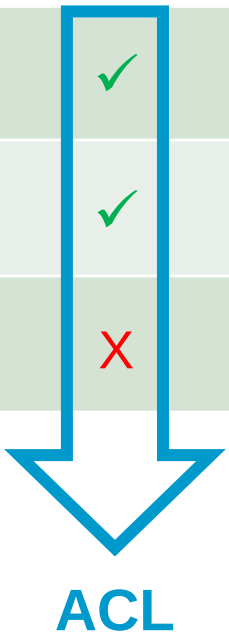
- RSBAC: MAC & MAC-Light modules
- SELinux: Multi-Level Security (MLS)
- Android: SEAndroid
- Tizen: Simplified Mandatory Access Control in Kernel (SMACK)
- AppArmor

Authorization + Access Control

Access Control Lists (ACL)

Access control matrix:

	object 1	object 2	object 3
James Bond	✓	✓	X
Hercule Poirot	✓	X	✓
Sherlock Holmes	X	✓	X



REPLAY

Authorization + Access Control

CAP (access control CAPability)

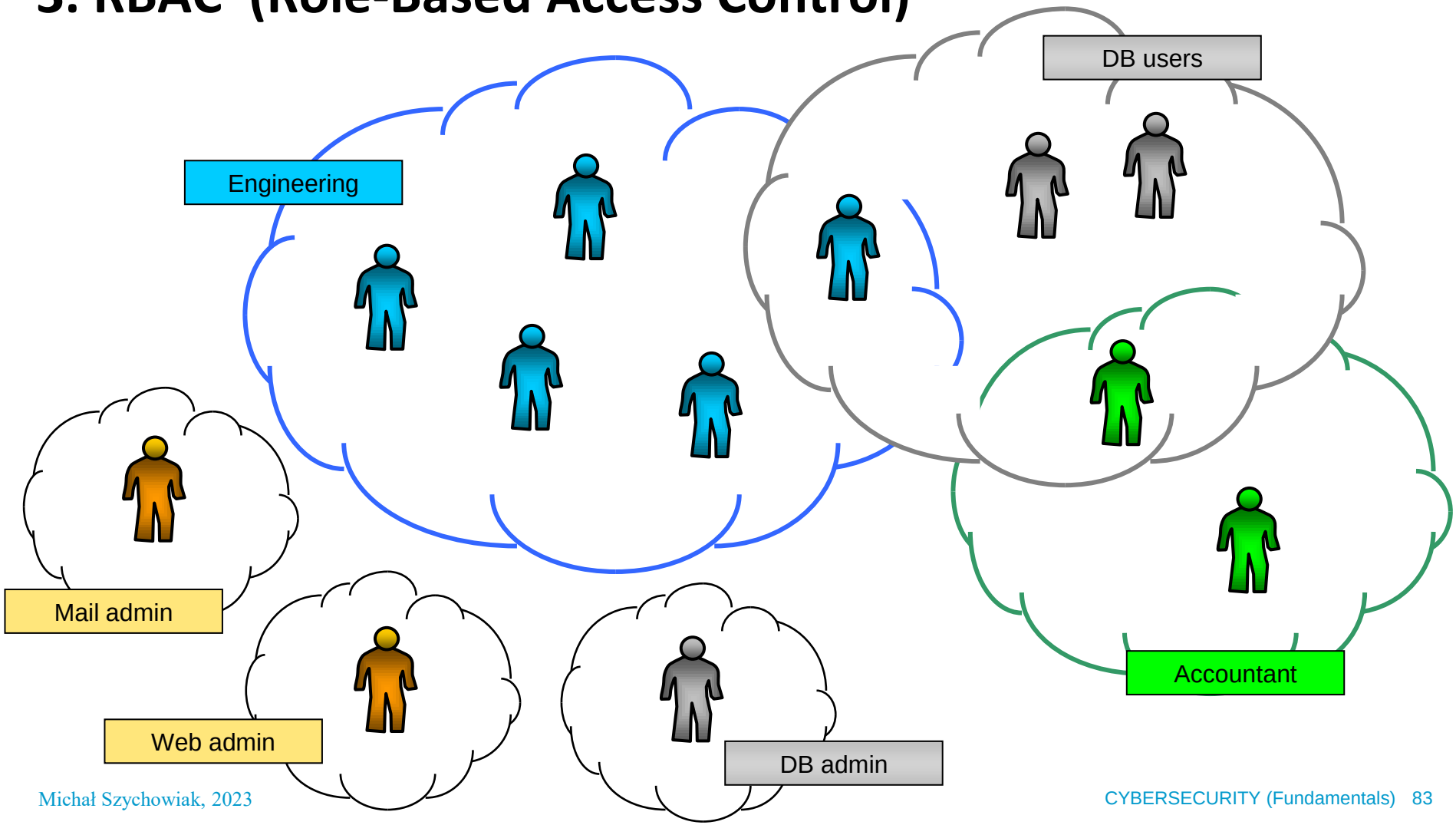
Access control matrix:

	object 1	object 2	object 3
James Bond	✓	✓	X
Hercule Poirot	✓	X	✓
Sherlock Holmes	X	✓	X

CAP

Authorization + Access Control

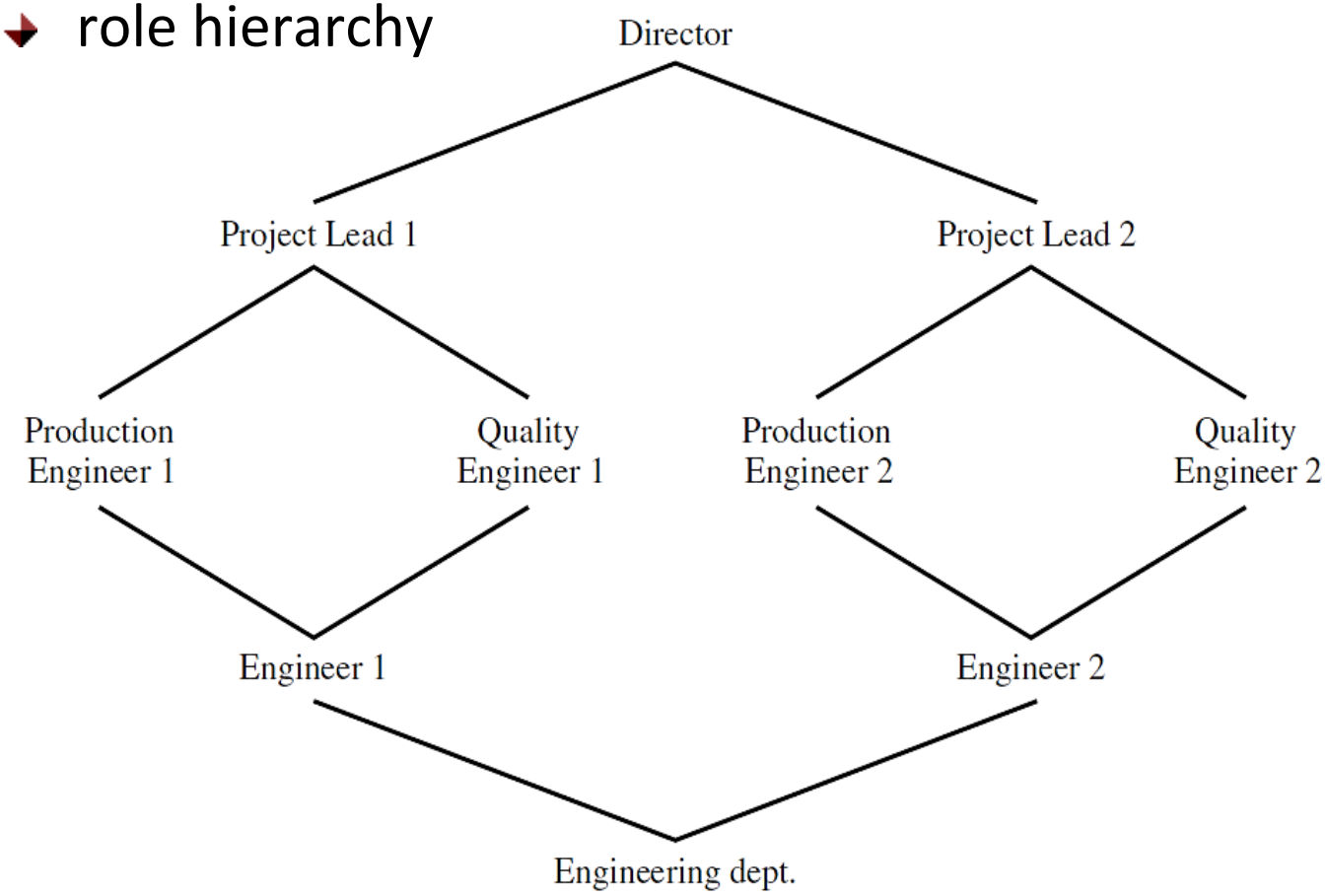
3. RBAC (Rôle-Based Access Control)

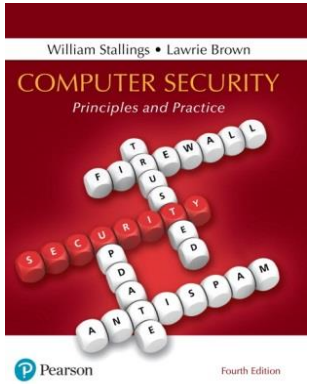


Authorization + Access Control

3. RBAC (Rôle-Based Access Control)

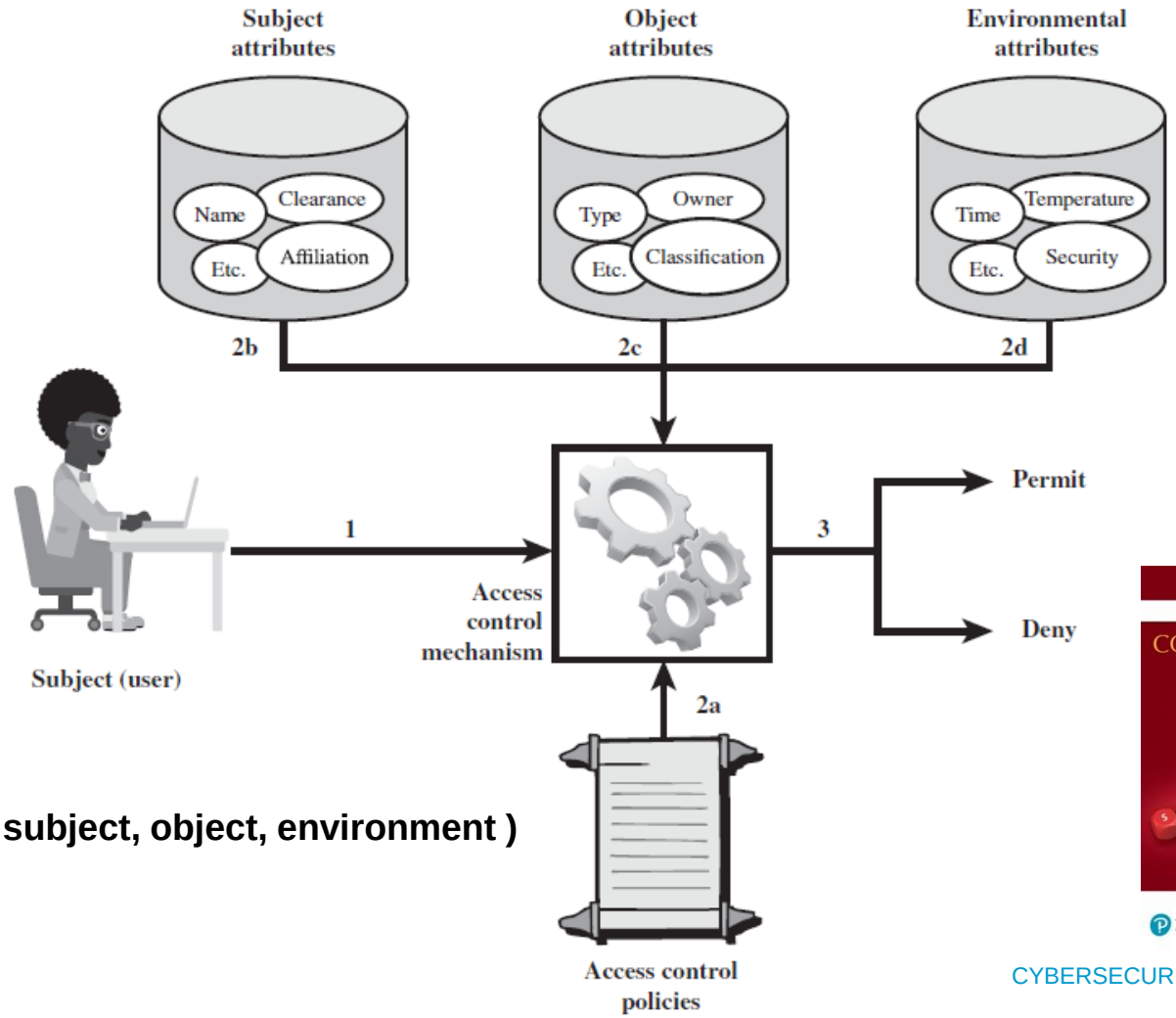
- role hierarchy



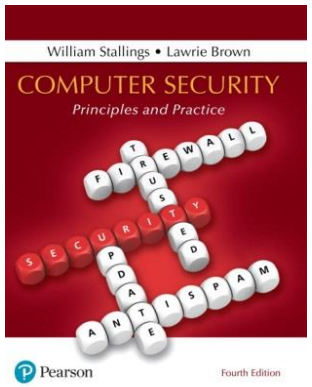


Authorization + Access Control

4. Attribute-Based Access Control (ABAC)



access_decision (subject, object, environment)



INTEGRITY

Integrity

Threat model:

- unauthorized (or unintended) modification (or destruction)

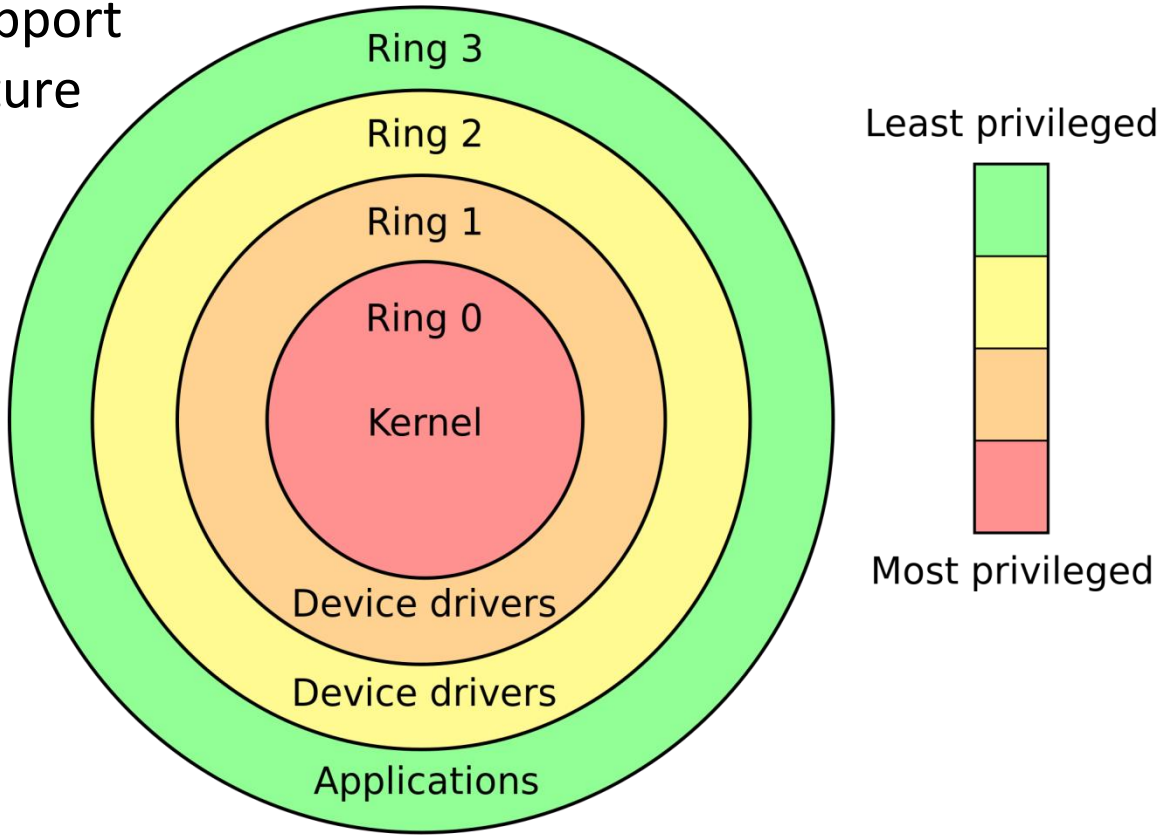
Protection:

- authorization and access control
- integrity checksums, cryptographic signature
- auditing (logging)
- anti-virus protection

Integrity

Process isolation

- hardware support
  x86 architecture



HOMEWORK

=

Half Of My Energy Wasted On Random Knowledge

- Supervisor Mode Execution Prevention (SMEP)
- Supervisor Mode Access Prevention (SMAP)

Mandatory Integrity Control (MIC)

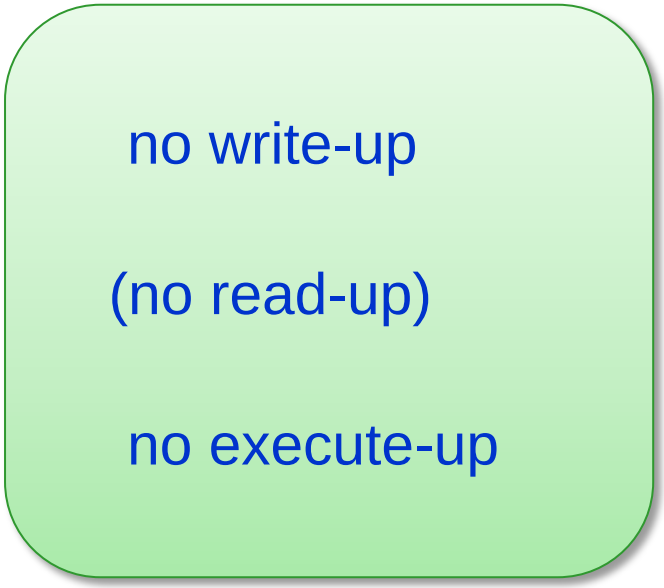
Biba's integrity model:

no read-down	A subject cannot read resources labeled lower than the subject's own security label.
no write-up	A subject cannot write into resources labeled higher than the subject's own security label.

Mandatory Integrity Control (MIC)

Implementations

- Linux, FreeBSB: Low Water-Mark Mandatory Access Control (LO MAC)
- Windows: Windows Integrity Levels



Mandatory Integrity Control (MIC)

Windows Integrity Levels

0 = untrusted

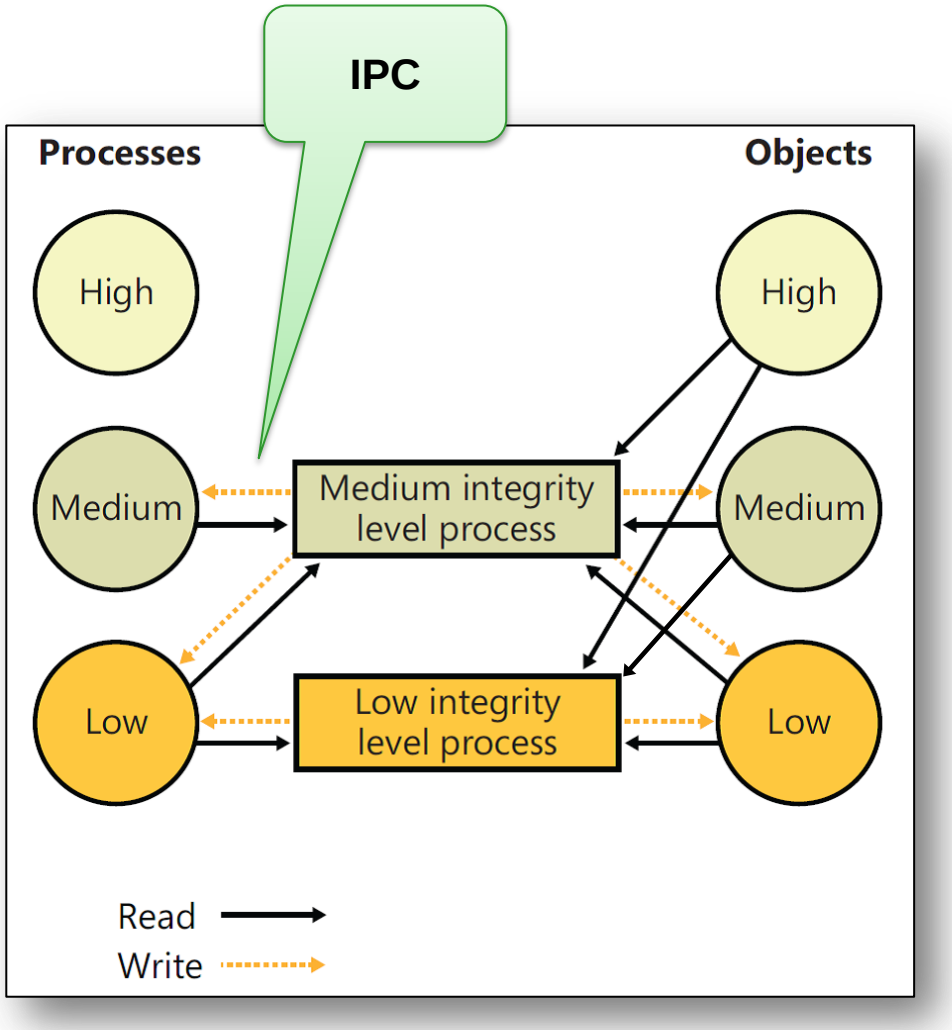
1 = low

2= medium

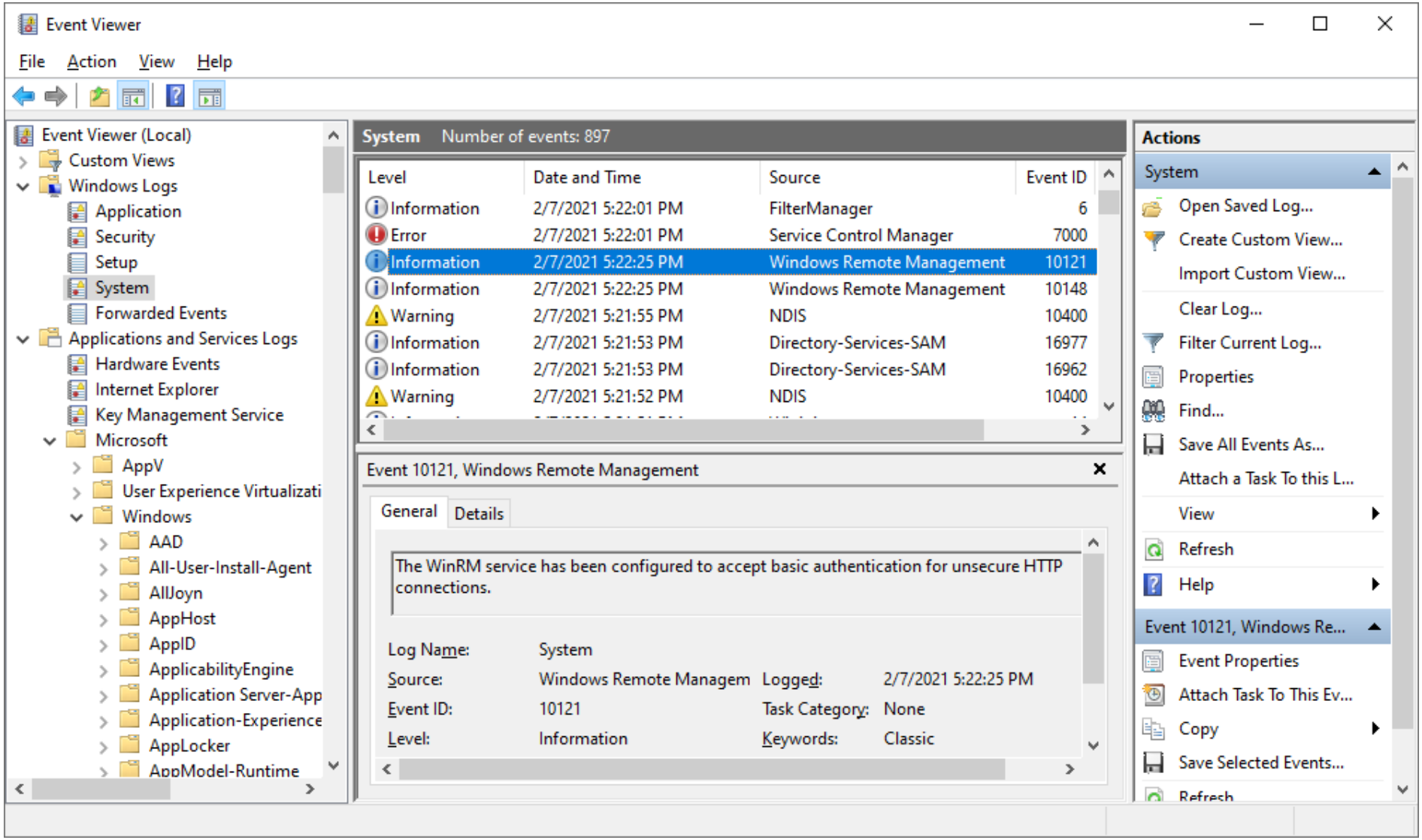
3 = high

4 = system

5 = protected (kernel-mode)



Event Logging




"That's all Folks!"