



Fundamentals of Cybersecurity



Michał Szychowiak

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



Agenda

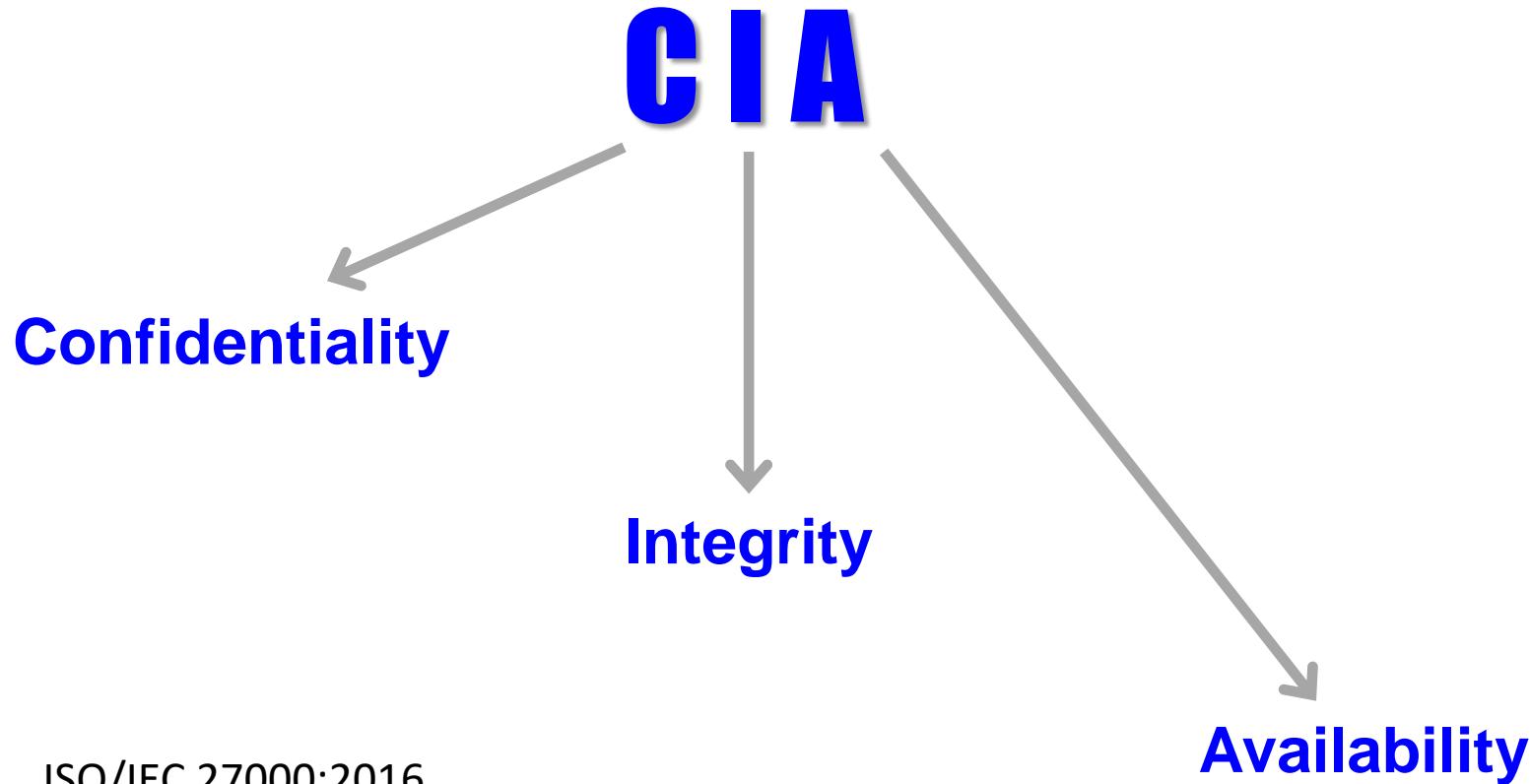
1. Basic security attributes:

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

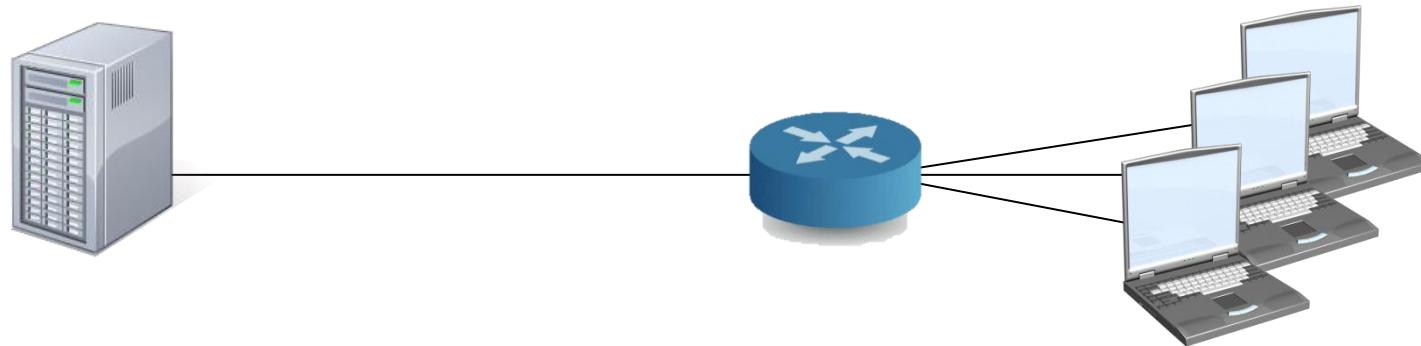
ISO/IEC 27001:2014-12

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*)

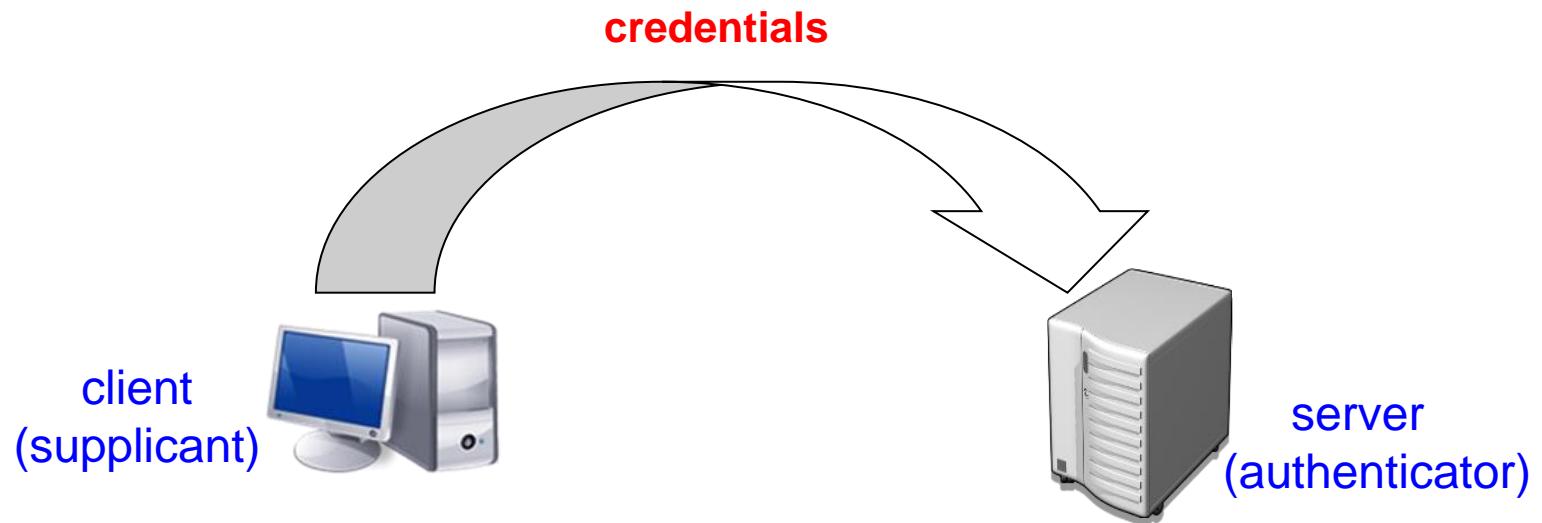
2. Authentication

- 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*)

R
I
P
L
A
Y

Authentication

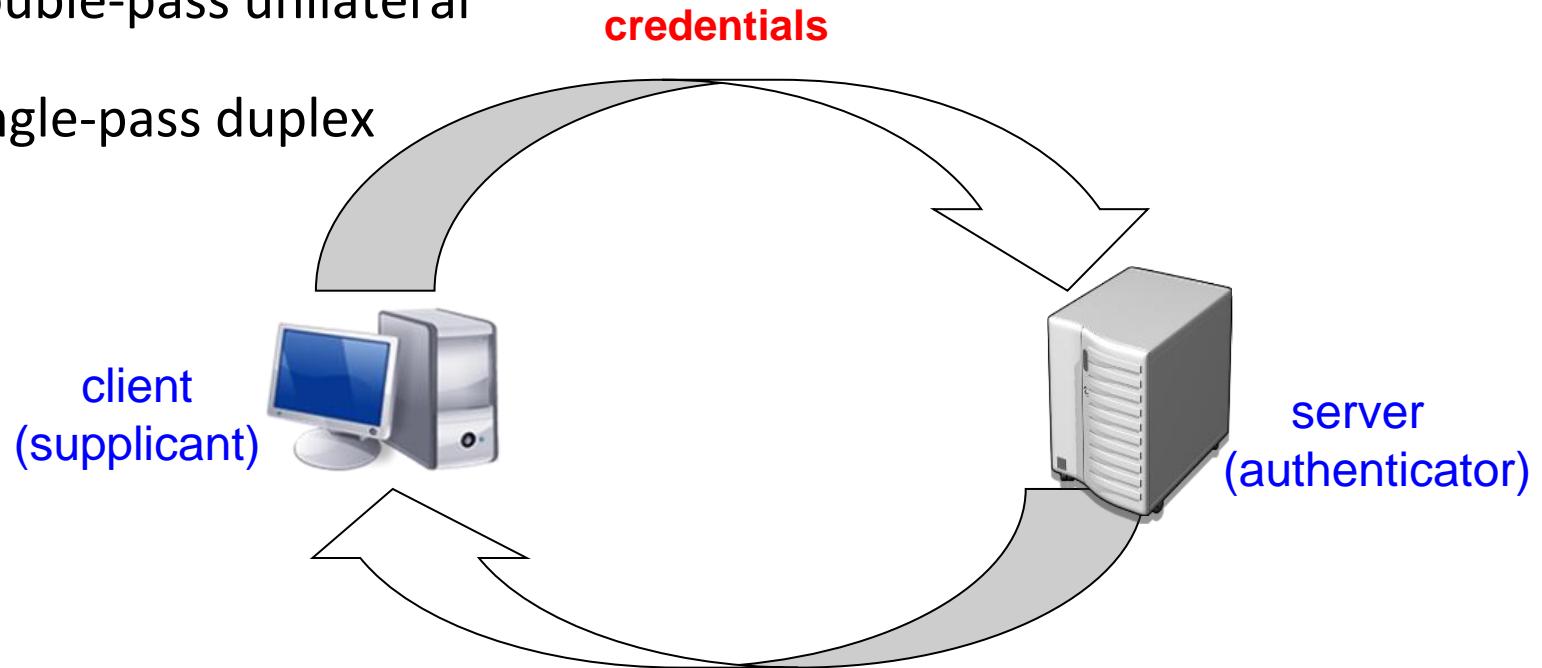
Unilateral authentication



Authentication

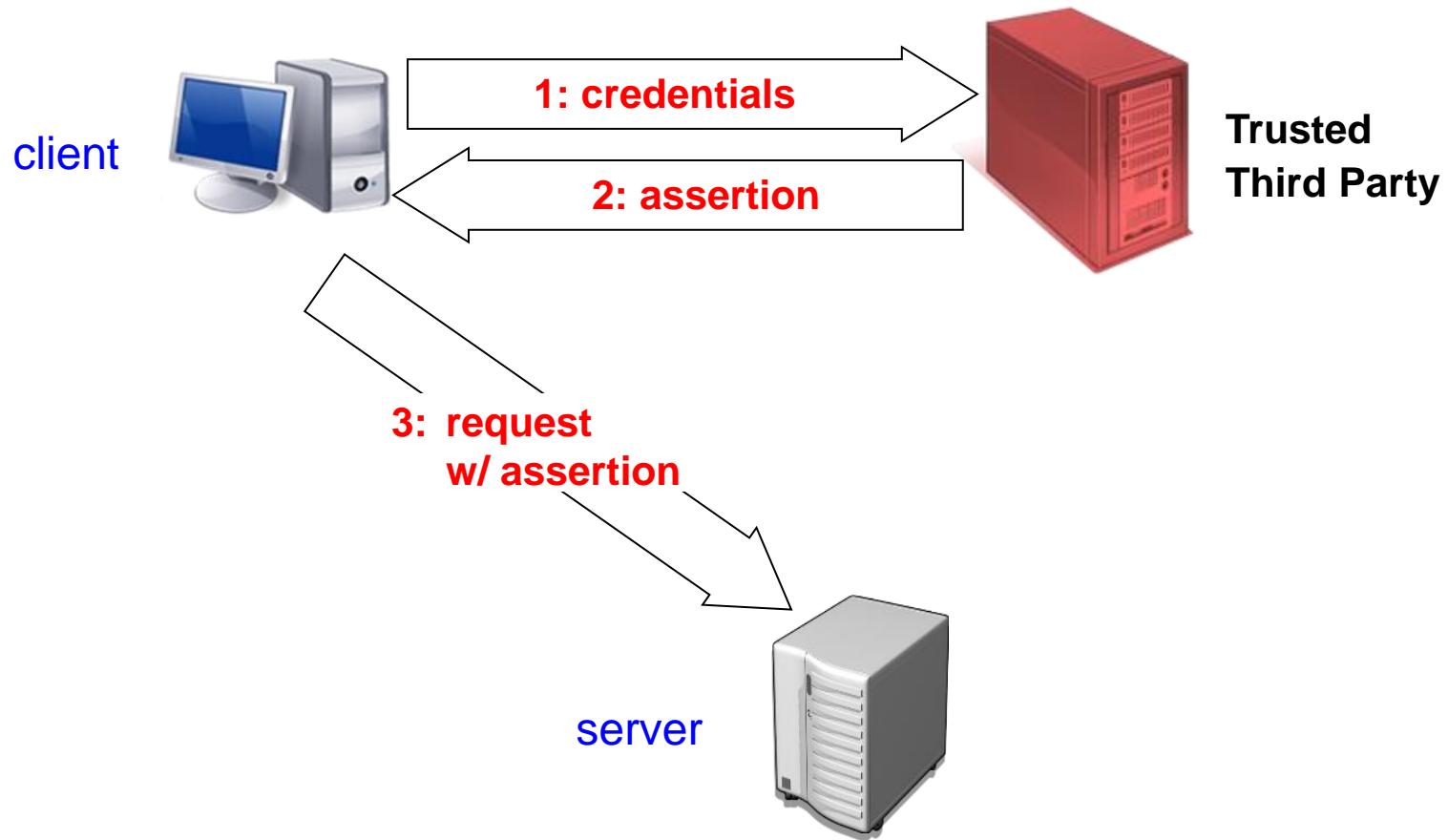
Mutual authentication

- double-pass unilateral
- single-pass duplex



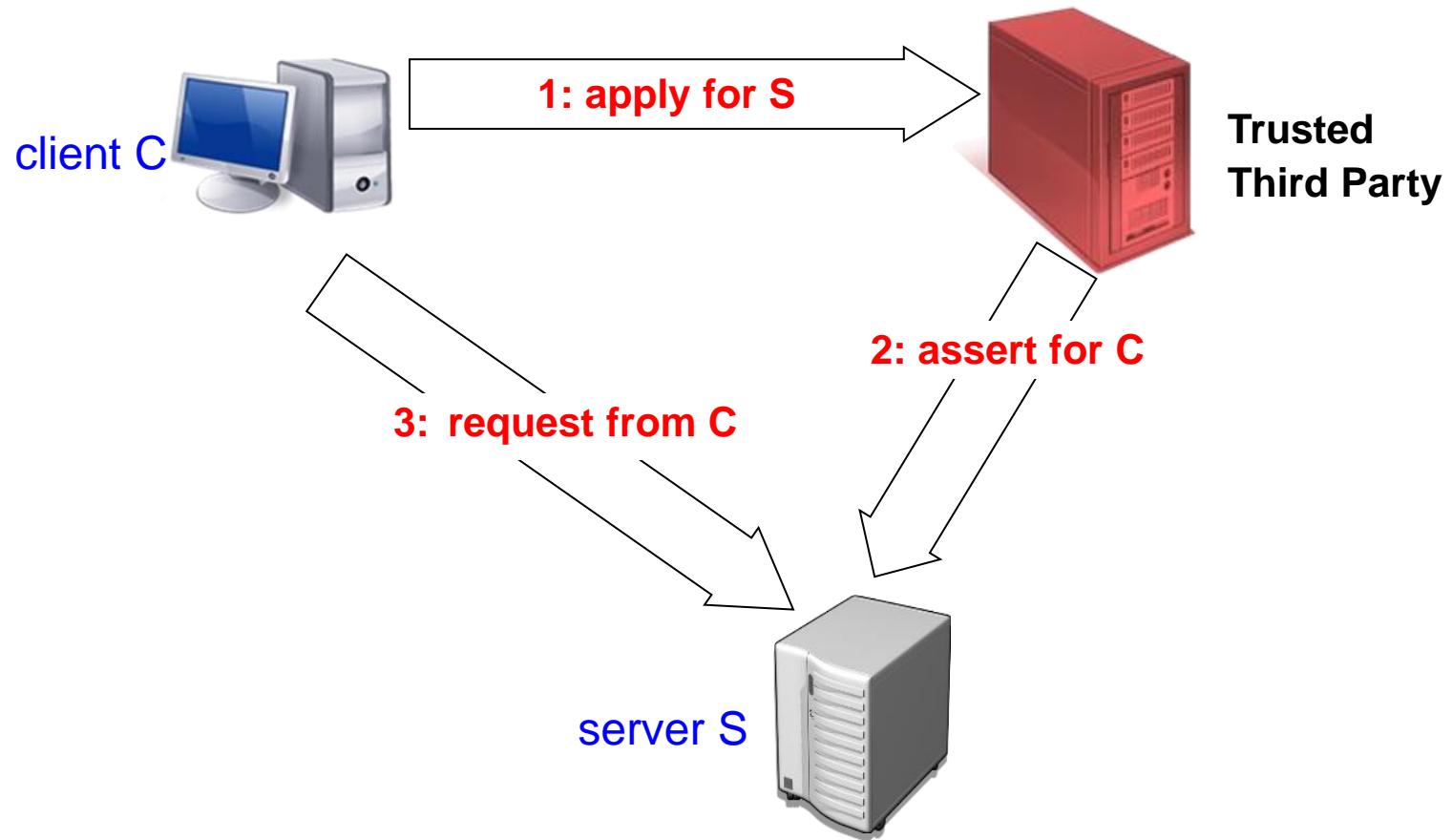
Authentication

Trusted Third Party



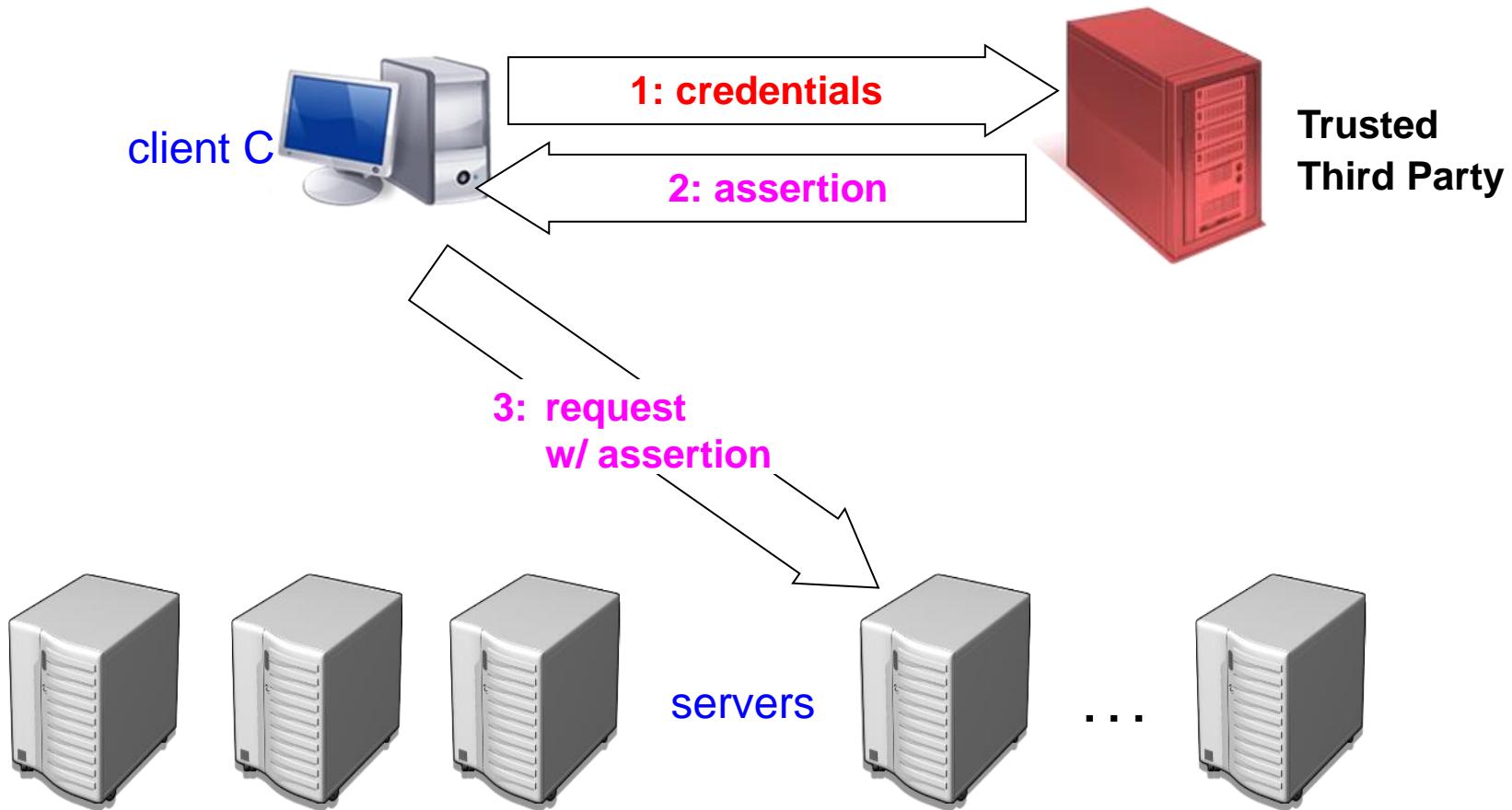
Authentication

Trusted Third Party – why not this way?



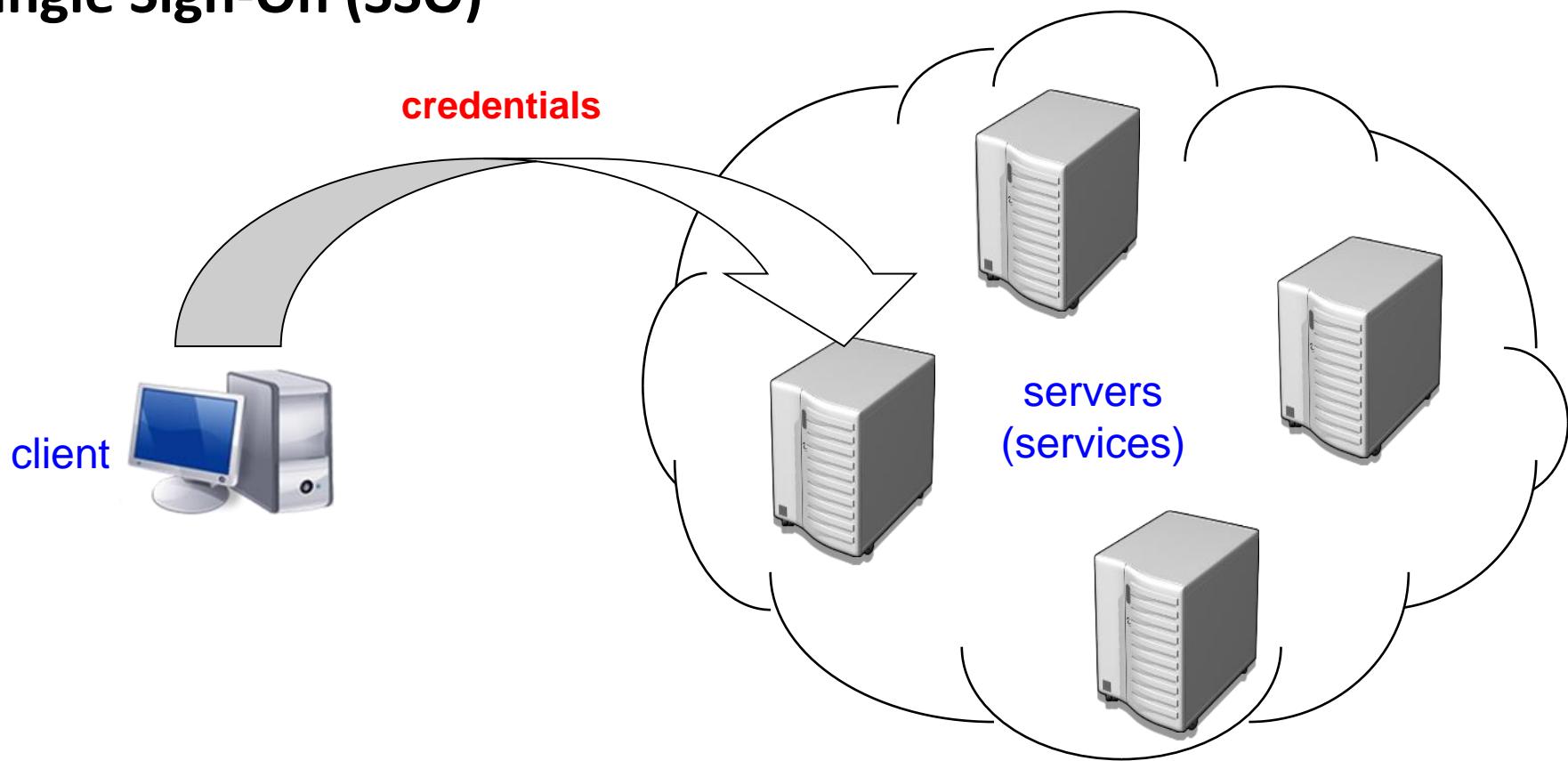
Authentication

Trusted Third Party



Authentication

Single Sign-On (SSO)



Authentication

Single Sign-On (SSO)

The screenshot shows the eLogin system interface. At the top, there is a header with the Politechnika Poznańska logo and the text "eLogin PUT central authentication system". On the left, a vertical menu lists "Main page", "Available systems", "Password", "Certificates", and "Settings". The main content area is titled "eLogin" and contains a welcome message: "Welcome to eLogin system. The main purpose of eLogin system is making it easier to log in to various systems through single sign-on authentication." The phrase "single sign-on authentication" is highlighted with a red rectangle. Below this, another message says: "To log in to specific system **display their list** and click on the system name."

Menu

- Main page
- Available systems
- Password
- Certificates
- Settings

eLogin

Welcome to eLogin system. The main purpose of eLogin system is making it easier to log in to various systems through single sign-on authentication.

To log in to specific system **display their list** and click on the system name.

Authentication

Single Sign-On (SSO)

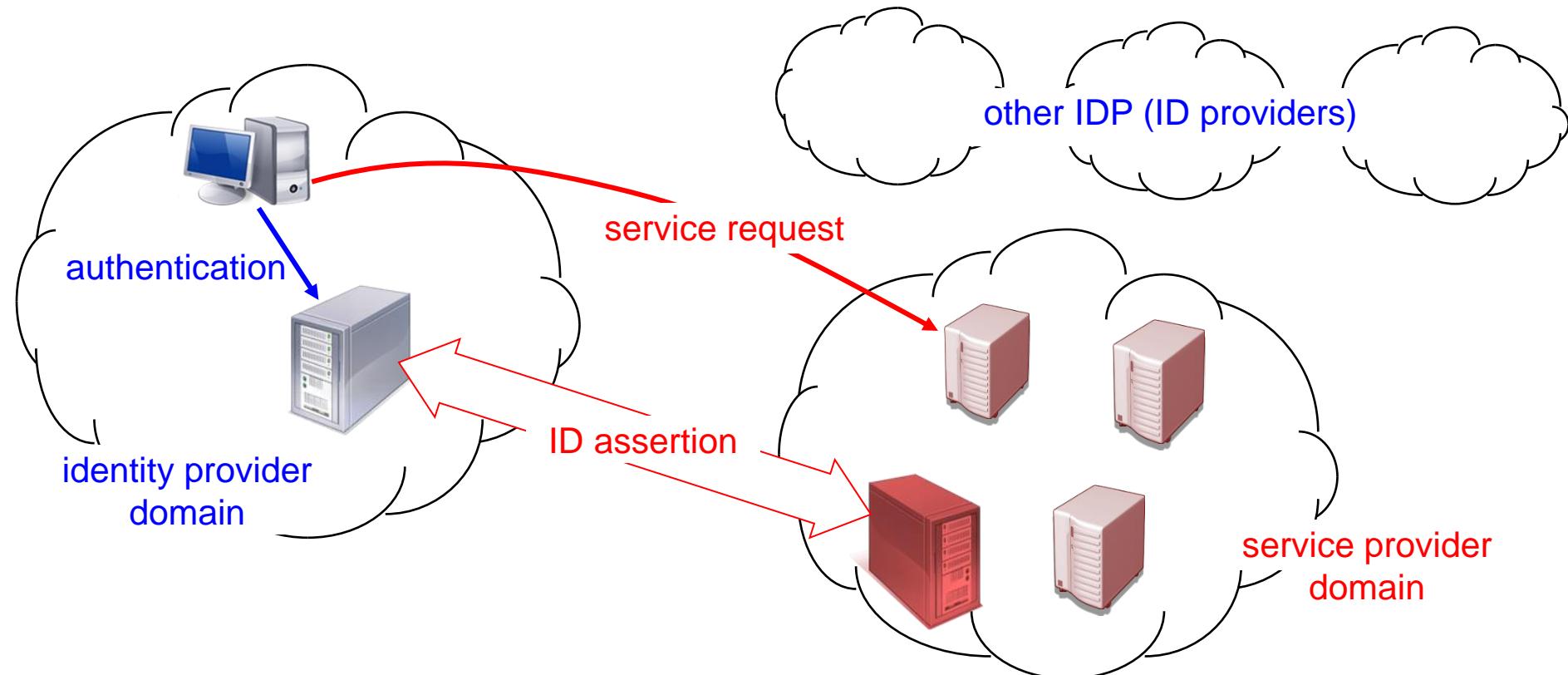
The image shows a user interface for Single Sign-On (SSO) authentication. At the top, there are two prominent social login buttons: 'Log in with Facebook' (with a blue background and white text) and 'Log in with Google' (with a white background and blue text). Below these, a horizontal line with the word 'or' in the center separates them from the standard log-in fields. The next section contains two input fields: 'Email Address' and 'Password'. To the right of the 'Email Address' field is an envelope icon, and to the right of the 'Password' field is a lock icon. Below the 'Email Address' field is a checkbox labeled 'Remember me' and a link 'Show password' to its right. At the bottom of the form is a large red button with the text 'Log in' in white. Below this button are two links: 'Forgot password?' and 'Don't have an account? [Sign up](#)'. The entire form is set against a light gray background.

Authentication



Federated ID

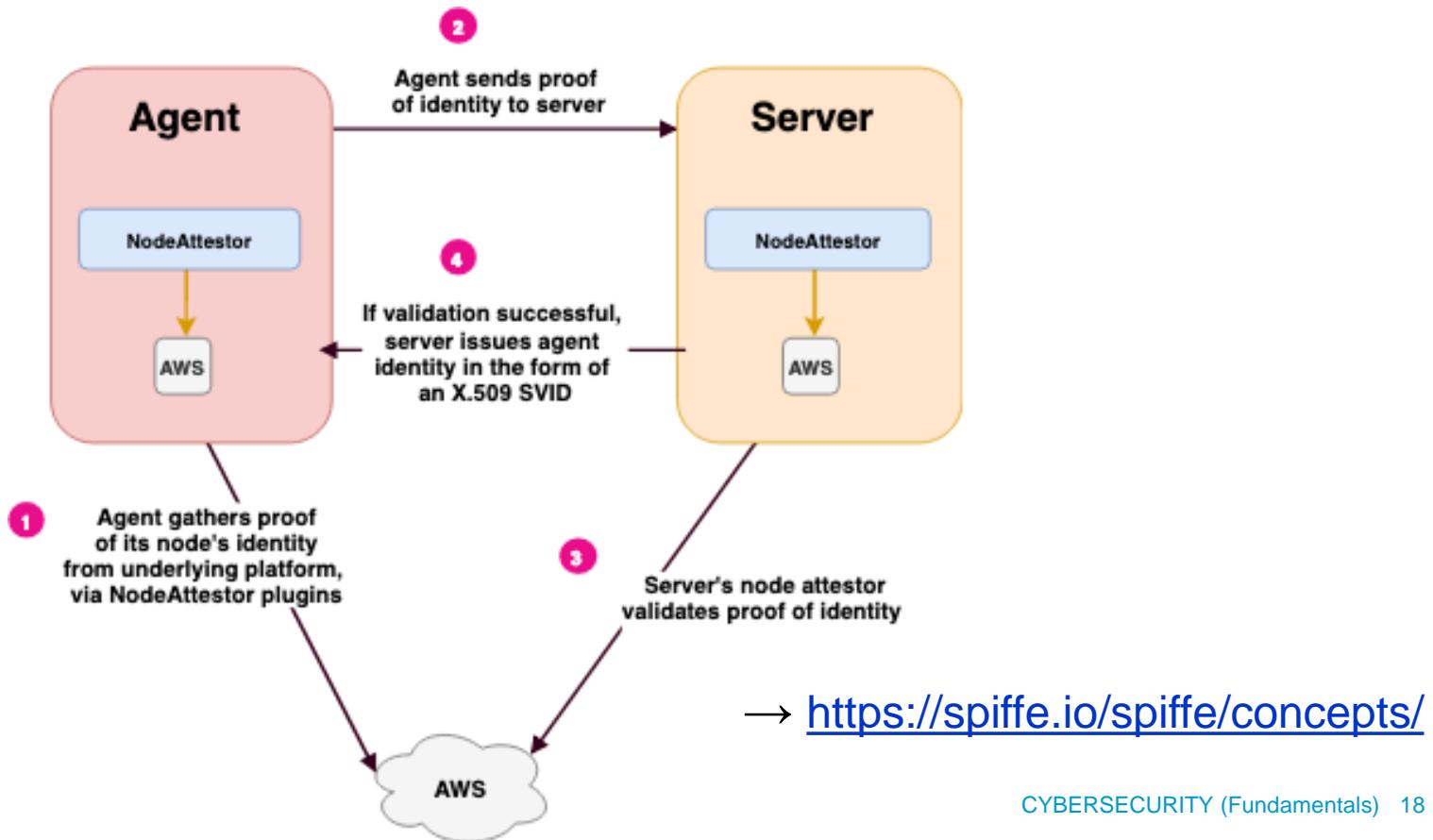
- SAML, WS-Federation, WS-Trust, OpenID, OIDC, Cloud IAM, ...



Authentication

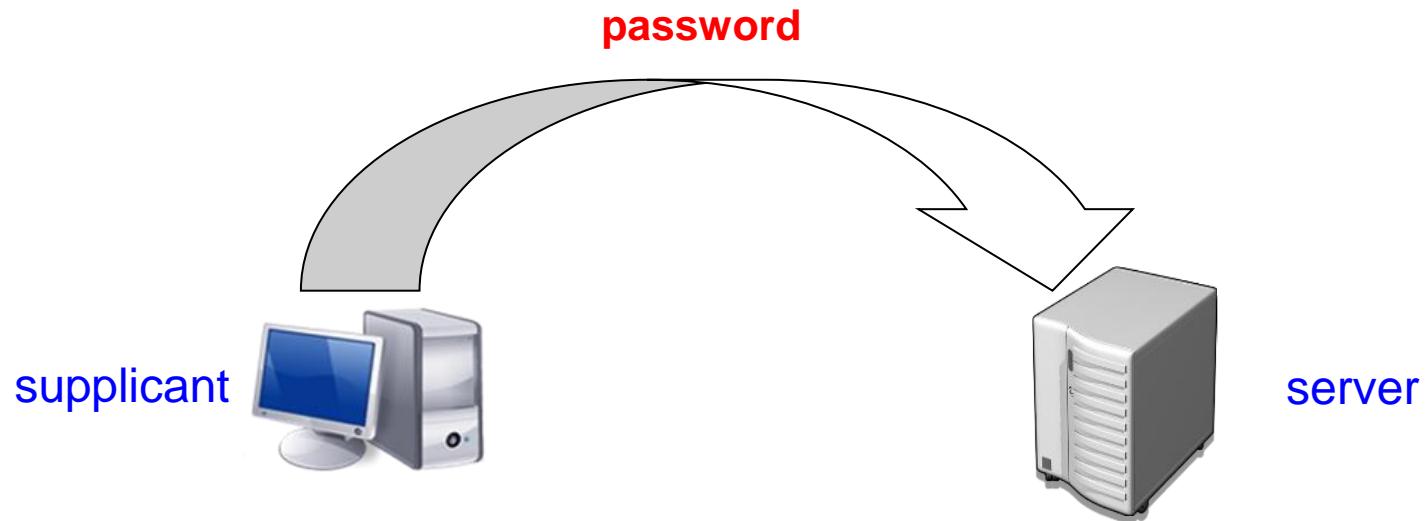
SPIFFE (Secure Production Identity Framework for Everyone)

- open-source standards for issuing identity to heterogeneous services



Authentication

Password authentication



TO: CUSTOMER SUPPORT
SUBJECT: MY SECURITY

IS MY PASSWORD
SAFE FROM
RUSSIAN HACKERS?

TO: CUSTOMER
SUBJECT: YOUR SECURITY

DA.



Authentication

Passwords

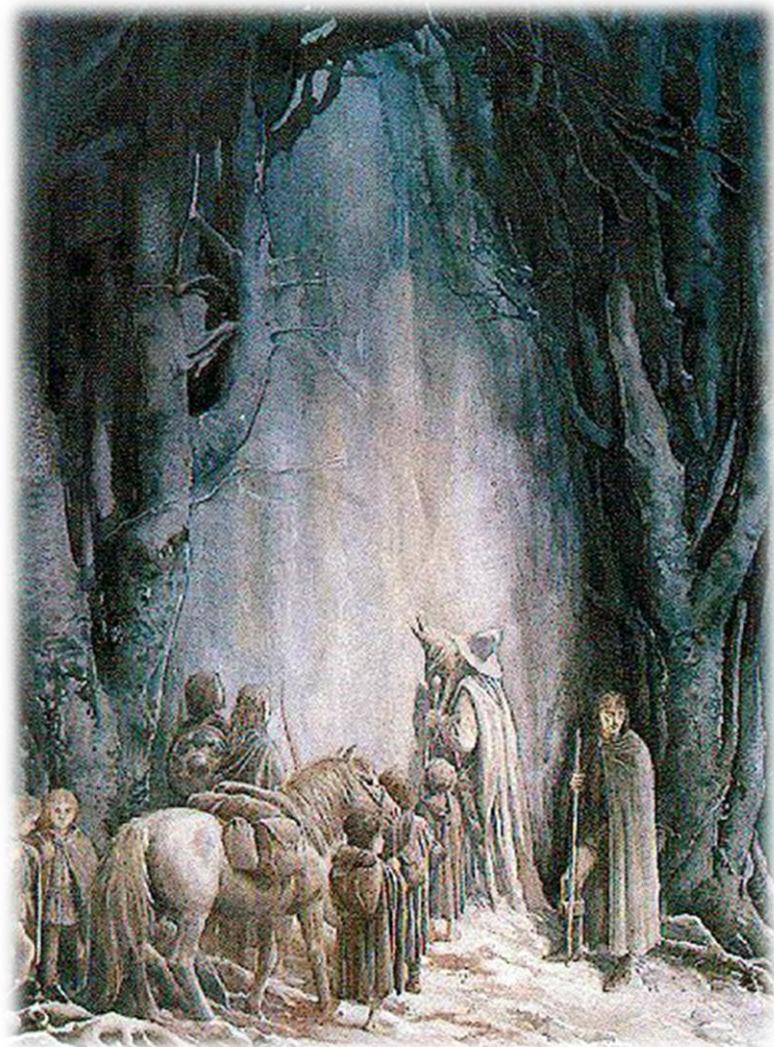
passwords are ciphers

“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

Login: admin

Password: i dont know

Password is incorrect

Login: admin

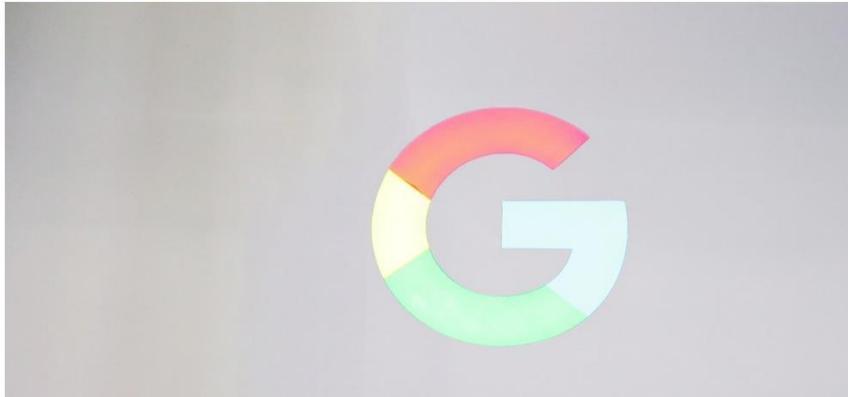
Password: incorrect

Authentication

Password attacks

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

GOOGLE HAS STORED SOME PASSWORDS IN PLAINTEXT SINCE 2005



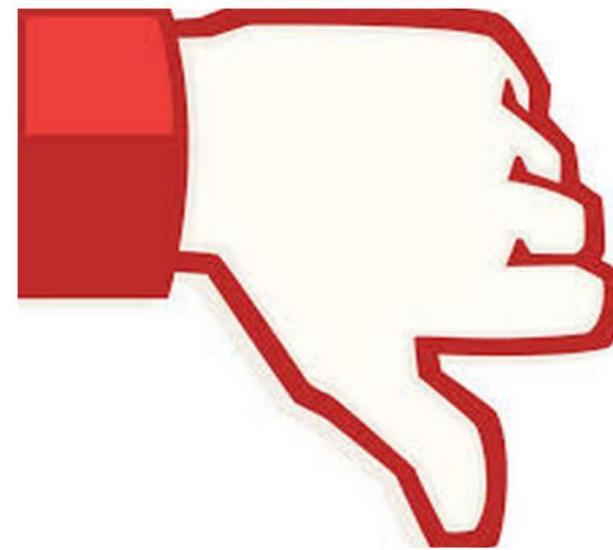
APPS \ MOBILE \ TECH

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

67

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

MAR 19

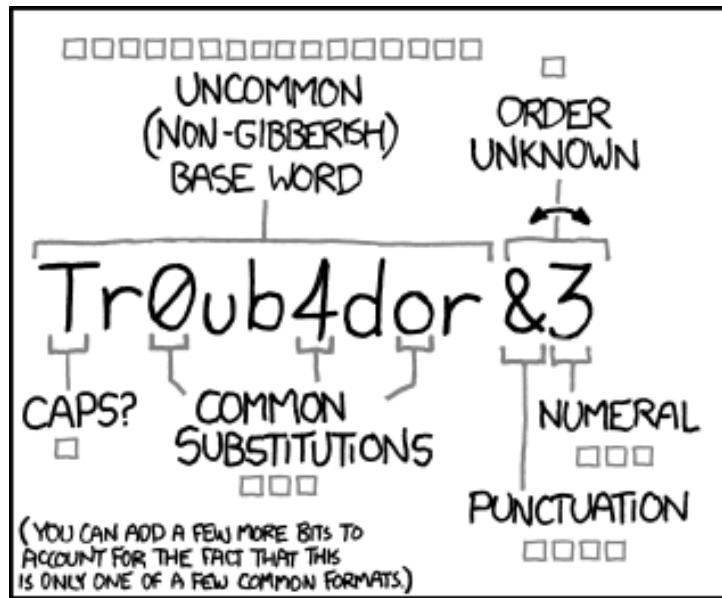


Authe

Password attacks

→ morele.net 2018

[REDACTED]@o2.pl:katarzyna
[REDACTED]@gmail.com:wiedzmin
[REDACTED]:231231
[REDACTED]acha@wp.pl:martinez
[REDACTED]eksander@wp.pl:marian
[REDACTED]@gmail.com:mateusz13
[REDACTED]kakatarzyna@gmail.com:22041993
[REDACTED]@wp.pl:outbreak
[REDACTED]interia.pl:tsunami1
[REDACTED]l.by:valeri
[REDACTED]nska@interia.pl:zuzia123
[REDACTED].pl:25081982
[REDACTED]ng@poczta.fm:oliwia
[REDACTED]bys@gmail.com:truskawka
[REDACTED]@wp.pl:15901590
[REDACTED]op.pl:t123456
[REDACTED]ki98@gmail.com:james007
[REDACTED]ail.com:monitor123
[REDACTED]yk@poczta.fm:colorado11
[REDACTED]otmail.com:isildur
[REDACTED]gmail.com:Haslo123
[REDACTED]a@gmail.com:misiaczek1
[REDACTED]ucab@gmail.com:gilbert12
[REDACTED]gmail.com:football155
[REDACTED]gmail.com:payback1
[REDACTED]ail.com:hubert123
[REDACTED]@rmstudio.pl:uuuuuu
[REDACTED]apu.pl:login1
[REDACTED]z@esot.pl:gertruda
[REDACTED]nski@gmail.com:lucyna
[REDACTED]@gmail.com:klaudial CYBERSECURITY (Fundamentals) 25



~28 BITS OF ENTROPY

□□□□□□
□□□□□□
□□□□□□
□□□□□□

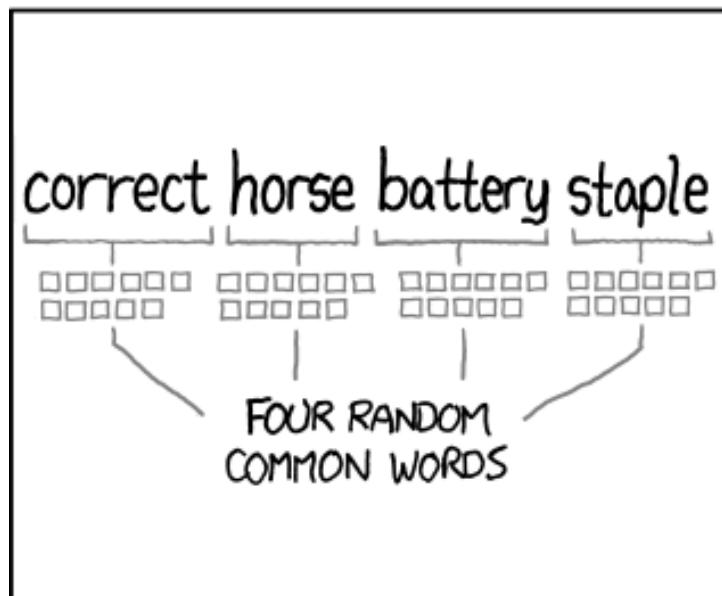
$2^{28} = 3$ DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?
AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

□□□□□□□□□□□□
□□□□□□□□□□□□
□□□□□□□□□□□□
□□□□□□□□□□□□

$2^{44} = 550$ YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS:
HARD

THAT'S A BATTERY STAPLE.
CORRECT!

DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

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.

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

$$P = \frac{L \cdot R}{S} \quad L = \text{time}$$

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/>

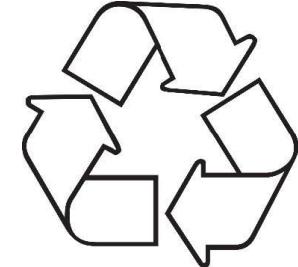
➔ <https://www.grc.com/haystack.htm>

Authentication

Other password problems

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

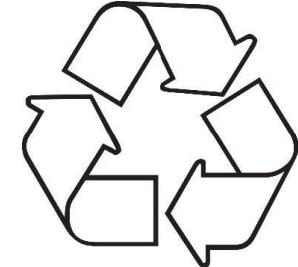
Authentication



Password reuse

One password to rule them all!

Authentication

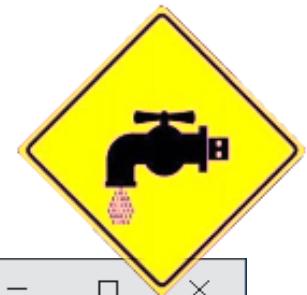


Password reuse

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



Authentication



A screenshot of a web browser displaying the <https://haveibeenpwned.com> website. The page has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the header is a large white button containing the text "';--have i been pwned?'. Underneath it, a sub-header reads "Check if you have an account that has been compromised in a data breach". A search bar contains the email address "michal.szychowiak@cs.put.poznan.pl". To the right of the search bar is a dark button labeled "pwned?". The main content area is green and displays the message "Good news — no pwnage found! No breached accounts and no pastes (subscribe to search sensitive breaches)". At the bottom, there are links for "Notify me when I get pwned" and "Donate", along with social media icons for Facebook and Twitter.

Authentication



258

pwned websites

4,846,841,219

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 ⓘ
- myspace 359,420,698 MySpace accounts
- 网易 NetEase 234,842,089 NetEase accounts ⓘ
- in 164,611,595 LinkedIn accounts
- A 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
16682	qwerty
13093	123456789
10138	12345
10113	zaq12wsx
6220	111111
5182	misiek
4776	monika
4418	marcin
4369	12345678
4240	mateusz

4073	1234567
3933	123123
3850	qwerty1
3620	karolina
3563	agnieszka
3450	bartek
3351	password
3348	qwe123
3343	damian
3266	1qaz2wsx
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](#)



Sincerely,

Dark Sources Security

[FreeBreachReport](#)

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

Authentication



Good-password policy

A password is like underwear – keep it hidden!

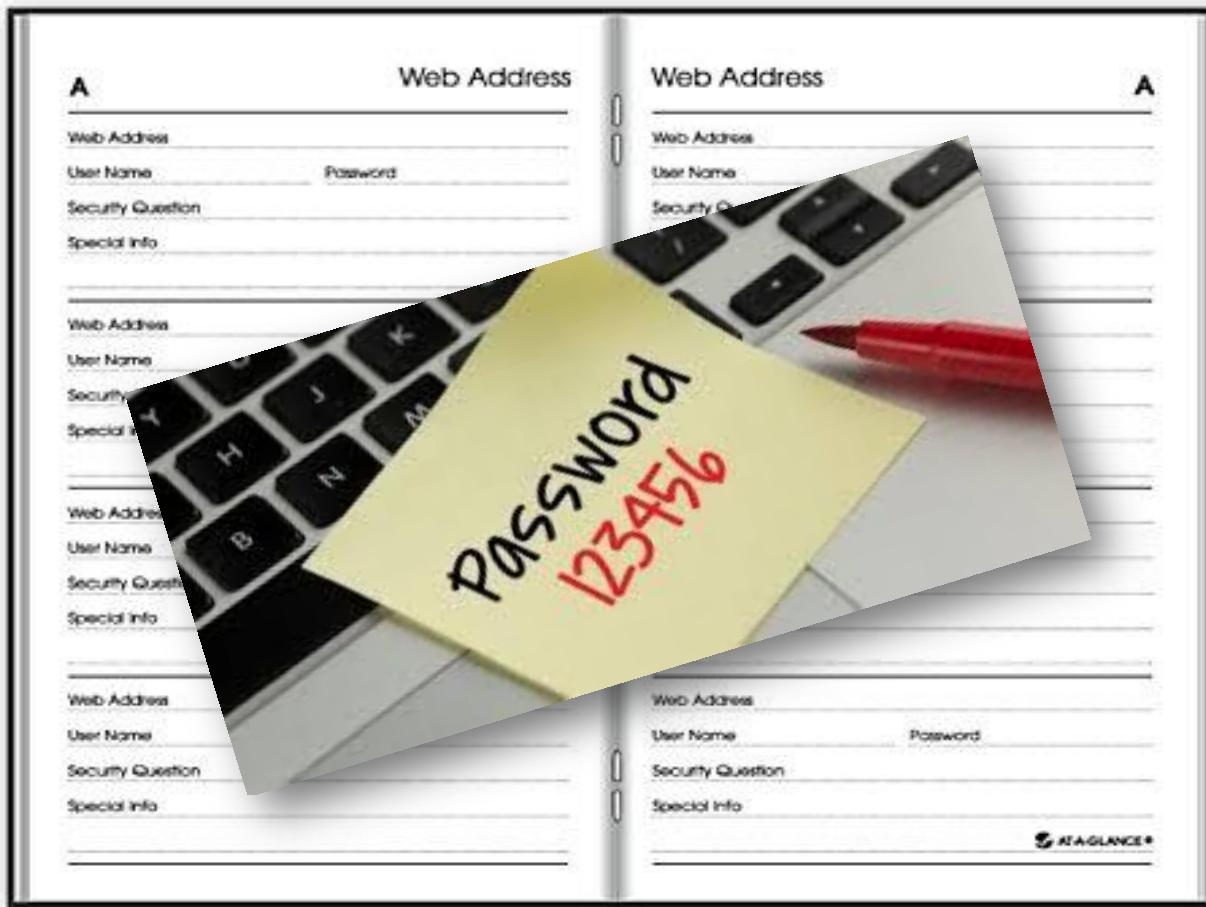
A password is like underwear – change it often!

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

→ [https://www.owasp.org/index.php>Password Storage Cheat Sheet](https://www.owasp.org/index.php>Password_Storage_Cheat_Sheet)

Authentication

Password management



Authentication

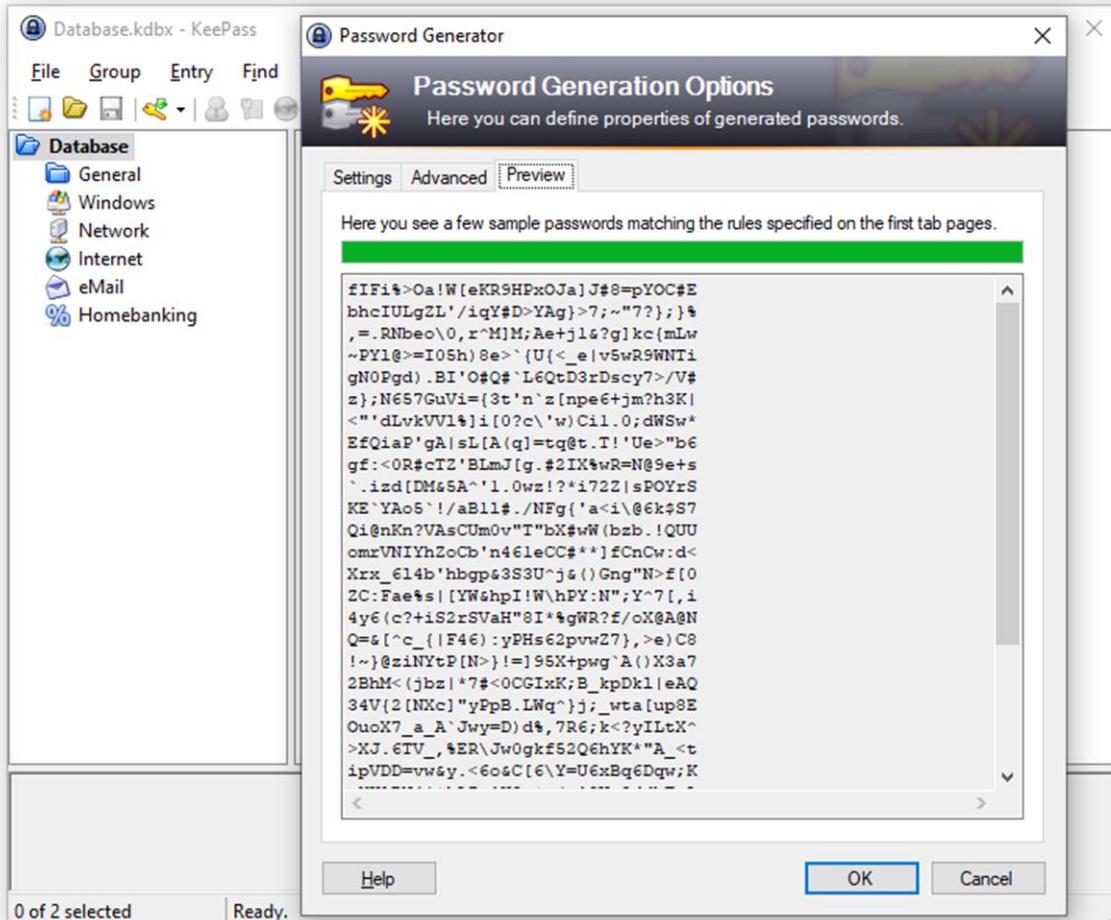
Password management

The screenshot shows the Firefox Protections Dashboard with the URL `about:protections` in the address bar. The page highlights several security features:

- Block ad trackers across more devices**: Describes mobile browser protection against ad tracking, available for [Android](#) and [iOS](#).
- Look out for data breaches**: Encourages checking Firefox Monitor for known breaches and signing up for breach alerts.
- Never forget a password again**: Promotes Firefox Lockwise for securely storing passwords, with a "Save Passwords" button.

Authentication

Password management



Authentication

Password management

Welcome to MyBank. Your new password for this site is [REDACTED]. Write this down and keep it secure, as you would your credit card or passport.

If you'd like a different password, click "New password", otherwise please log in with your email address and new password

Login _____

Email address _____

Password _____

Show typing

Authentication

- Windows Data Protection API (DPAPI)
- Credential Manager API

Password management

New Account

Your password for the user name
'example@example.com' is 'MqASqalY'.
How do you want to protect this password?

This is a low-security password used for news sites

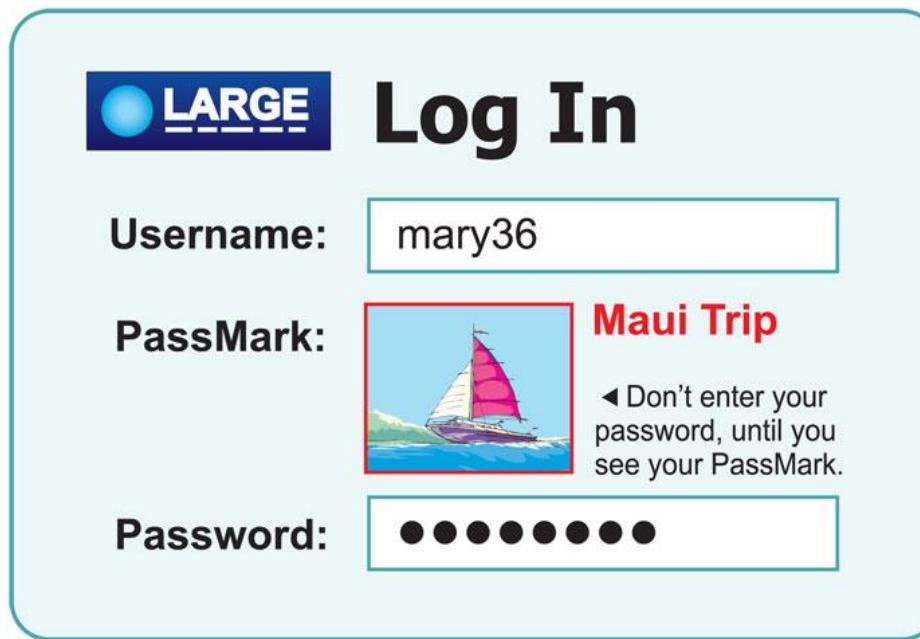
and web forums. Provide it to the site without asking for confirmation

This is a medium-security password used at online stores and for email. Ask for the master password the first time that it's used

This is a high-security password used for online banking and finance. Ask for the master password every time that it's used

Authentication

Password (account) image



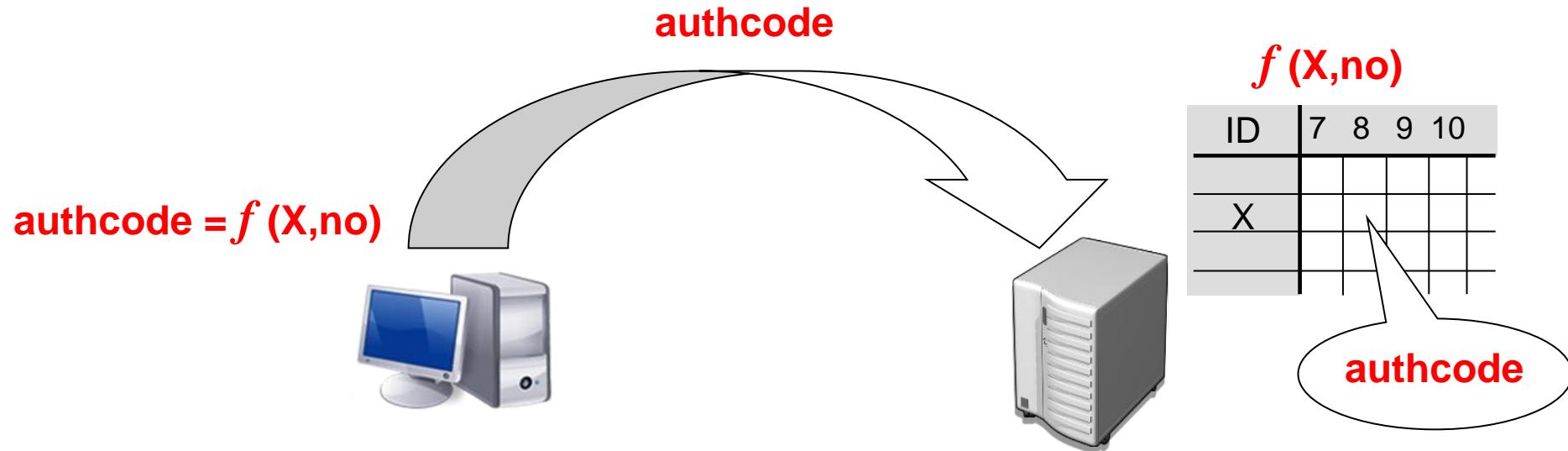
Authentication

OTP – *One-Time Passwords*

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

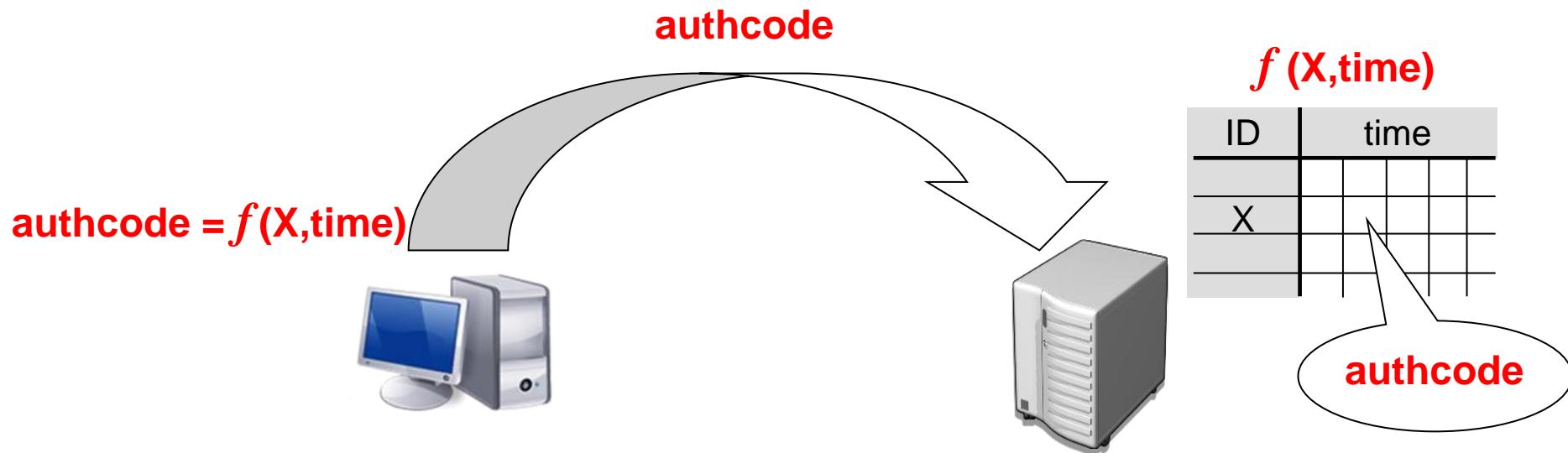
Authentication

TAN/ITAN – [Indexed] Transaction Authentication Numbers



Authentication

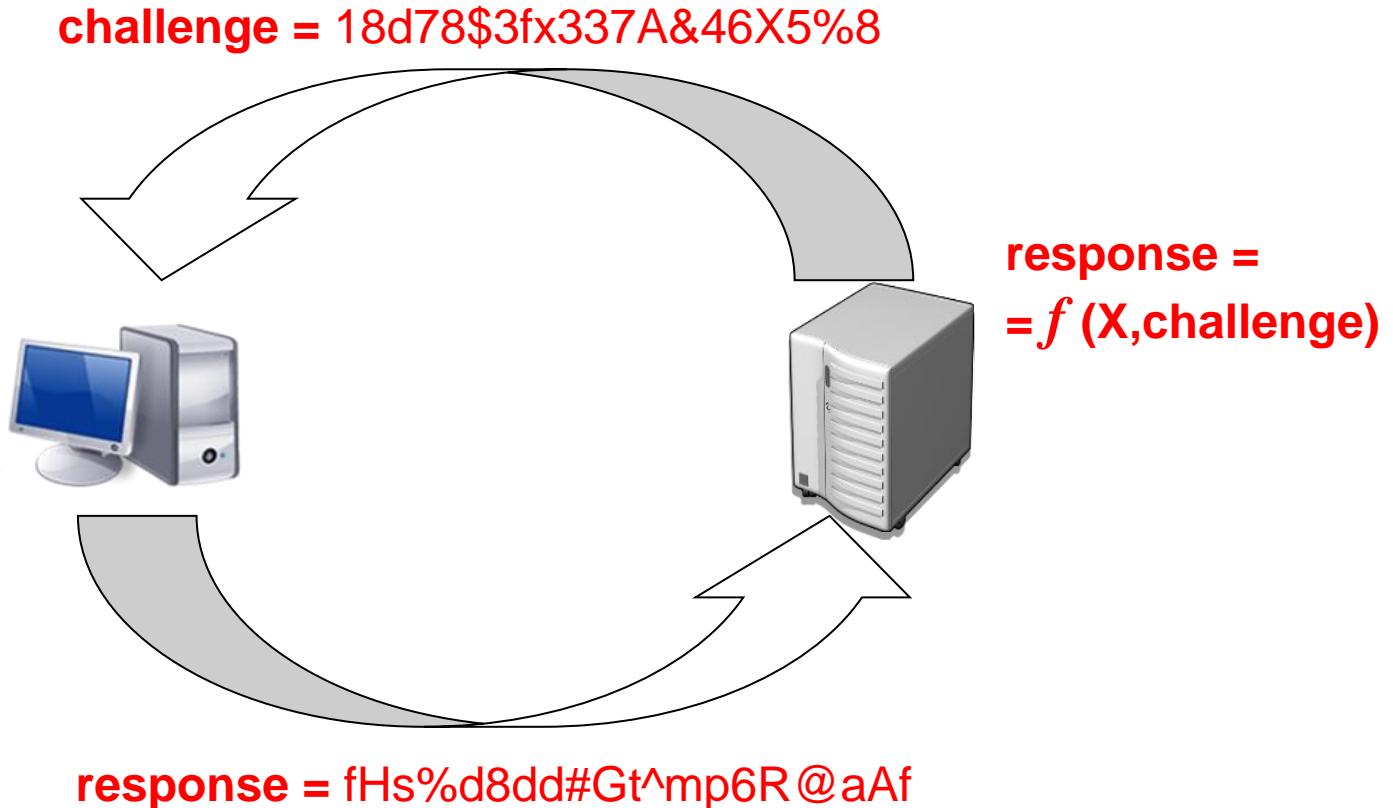
Time synchronization



Authentication

Challenge-Response

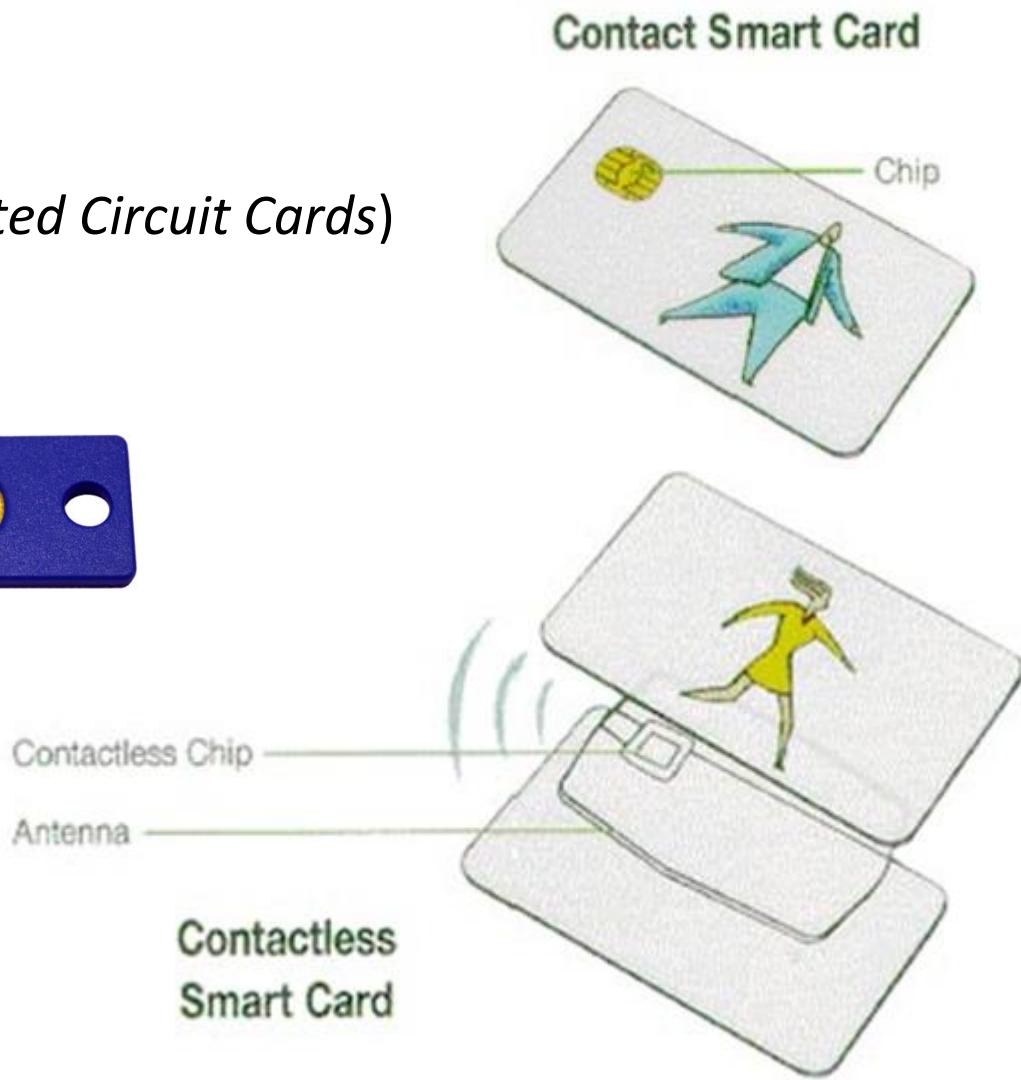
response =
 $=f(X, challenge)$



Authentication

Security tokens

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



Authentication

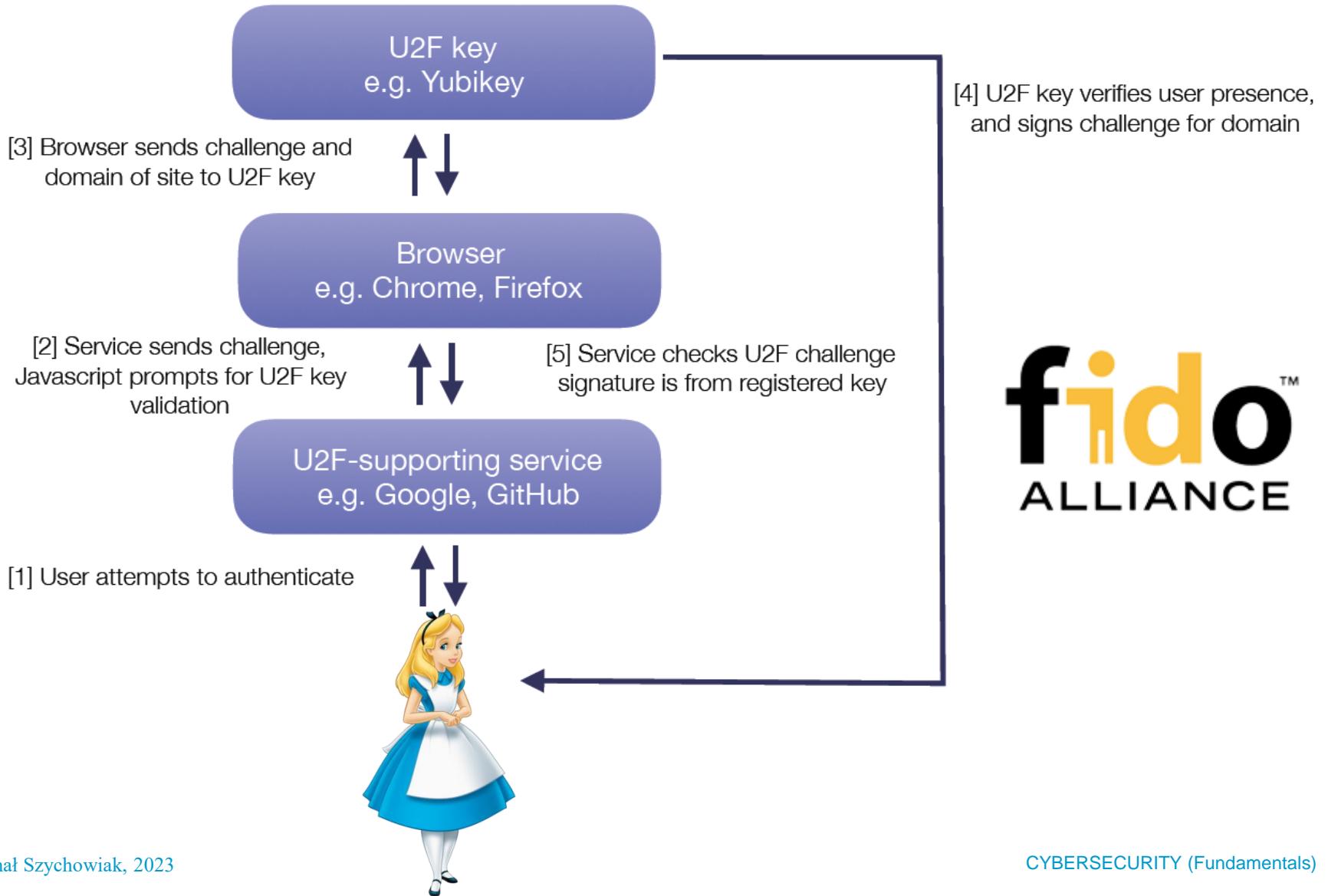
Two-Factor Authentication (2FA)



```
$ 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)

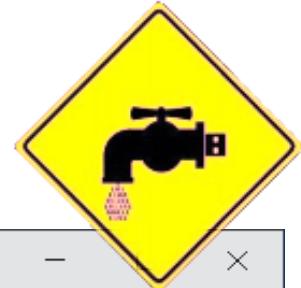


The screenshot shows a news article from KrebsOnSecurity. At the top left is the site's logo 'KrebsOnSecurity' with the subtitle 'In-depth security news and investigation'. Below the logo is a portrait of Matt Krebs. To the right of the portrait is a sidebar with 'ADVERTISING/SPEAKING' at the top, followed by a 'Mailing List' button and a 'Subscribe here' link. A small image of a smartphone screen displays some code. The main headline reads '18 T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account'. The text below the headline discusses a T-Mobile employee who made unauthorized changes to a subscriber's account to steal their Instagram account. It includes a quote from Paul Rosenzweig, a T-Mobile customer from Boston who had his account hijacked. The text also mentions that Rosenzweig had previously adopted T-Mobile's advice to block mobile number port-out scams.



The screenshot shows a news article from Motherboard. At the top left is the site's logo 'MOTHERBOARD'. The main headline reads 'TELL YOUR DAD TO GIVE US BITCOIN: How a Hacker Allegedly Stole Millions by Hijacking Phone Numbers'. The text below the headline discusses a 20-year-old college student who hijacked over 40 phone numbers and stole \$5 million, including from cryptocurrency investors at a blockchain conference Consensus. The author is listed as 'By Lawrence Prasenjit@LawrenceP'. There are links for 'Share' and 'Tweet'.

Authentication



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)

FYEKO 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 ~~computationally secure with a high~~.

“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
fraudsters.
It solves one problem,
not the others.”

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

Serious 2FA Bypass Vulnerability Affected Facebook And Instagram

written by Abeerah Hashim | January 30, 2023

CYBER SECURITY

NEWS

2 MIN READ

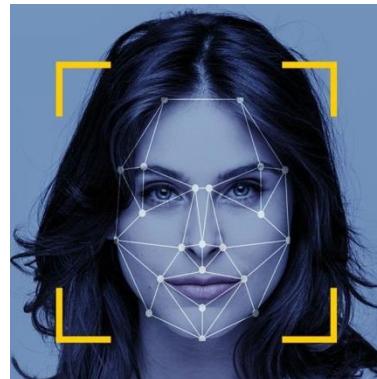
Crypto.com Hack Originating From 2FA Bypass Exceeds \$30 Million Forcing Refunds and New Security Measures



ALICIA HOPE · JANUARY 27, 2022

Authentication

Biometrics



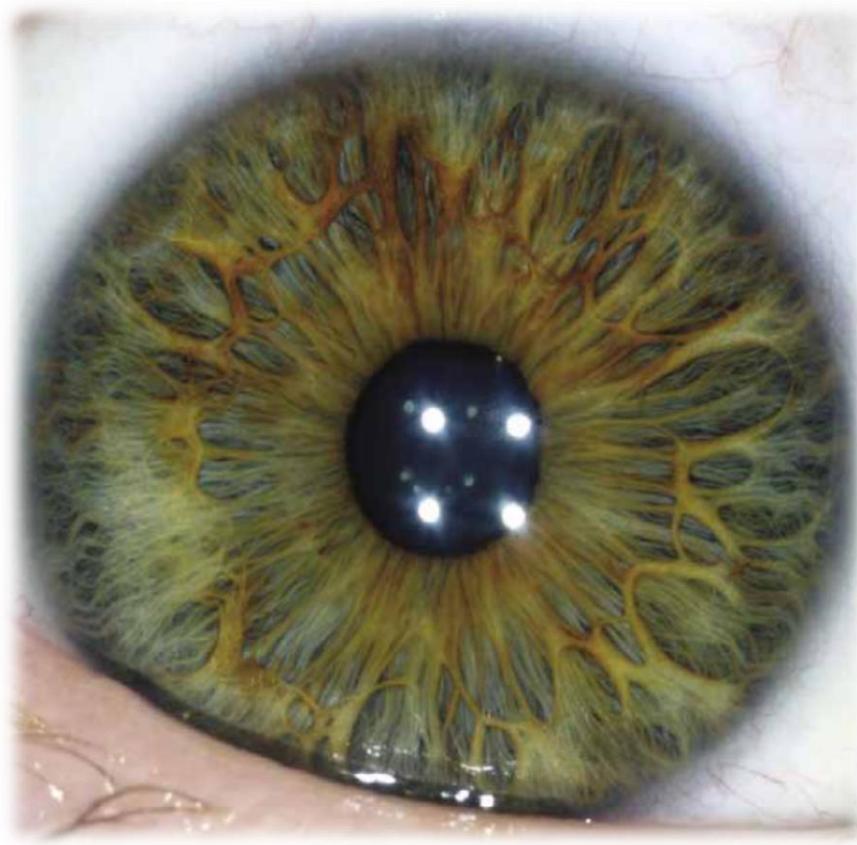
Authentication

Biometrics



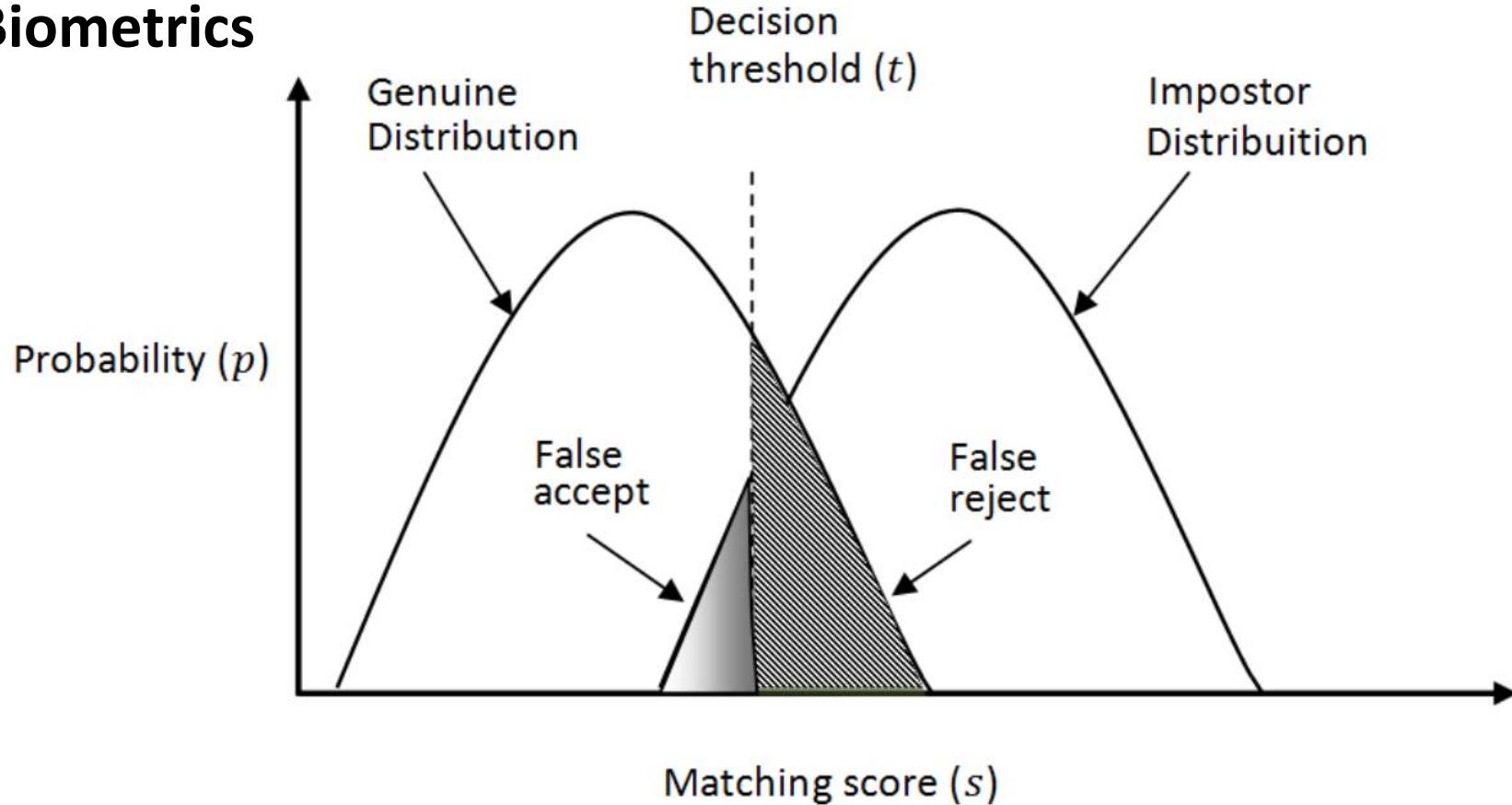
Authentication

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

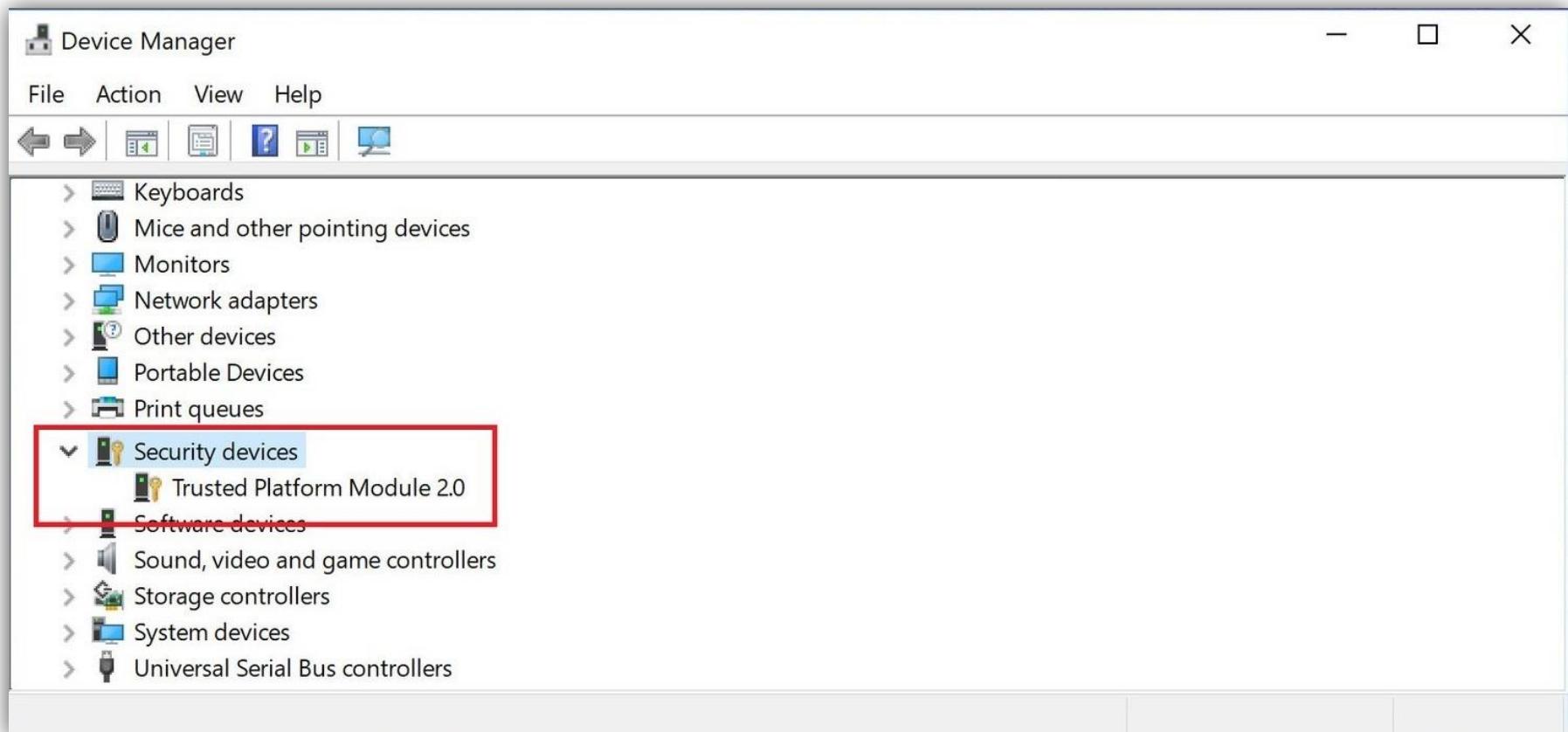
Biometric authentication standards

- ➔ 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



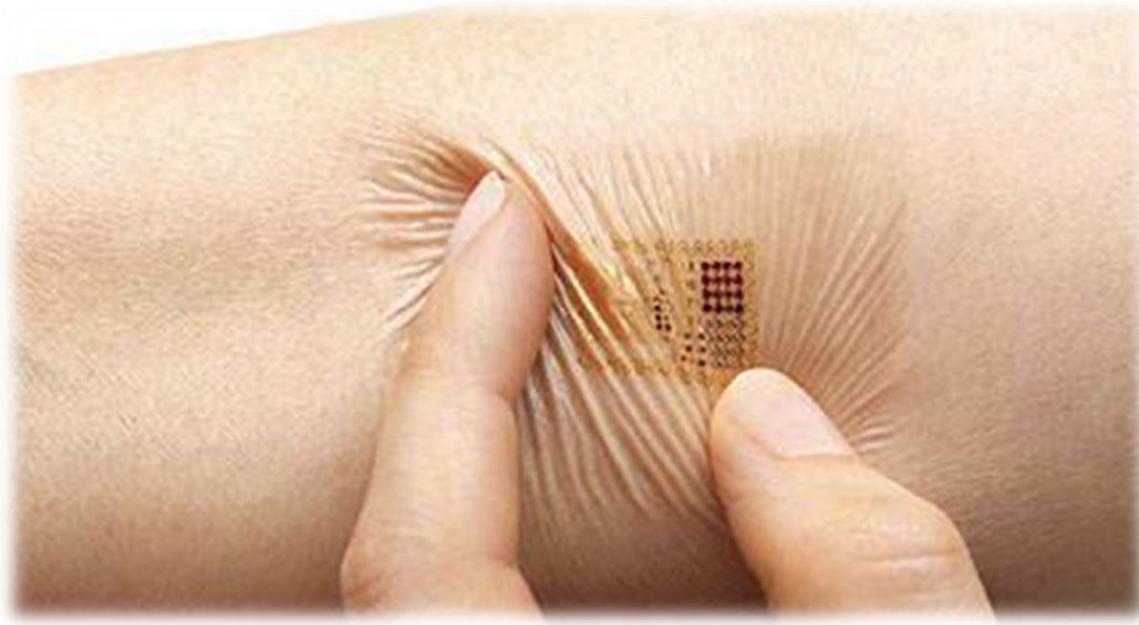
Trusted Platform Module (TPM)



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

CHECKPOINT

MULTIFACTOR AUTHENTICATION



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

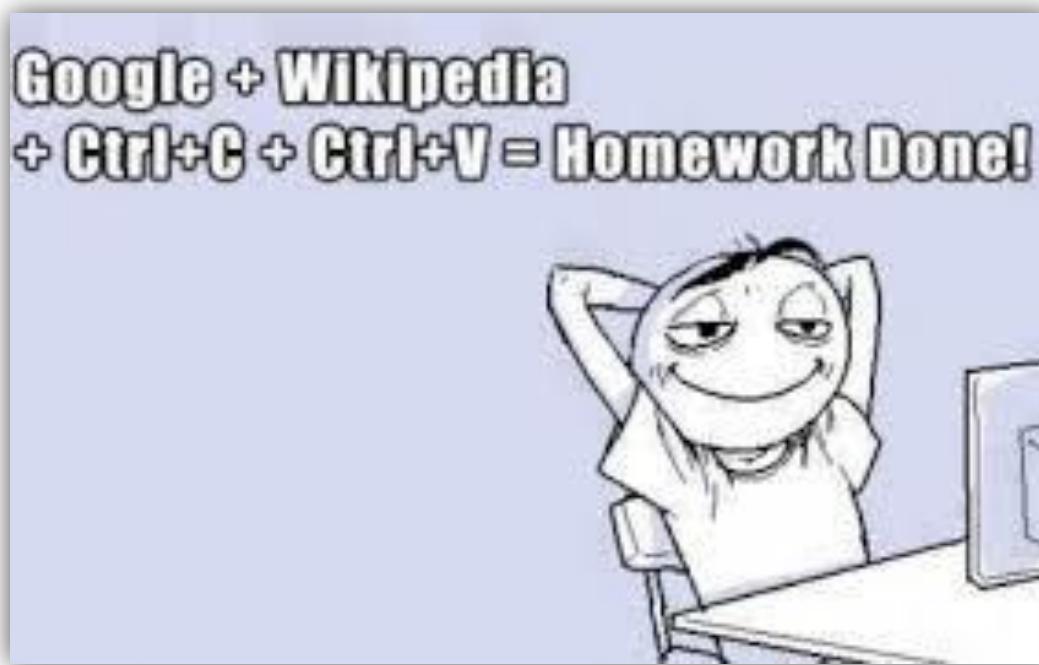
A slide from "Modern Two-Factor Authentication: Defending Against User-Targeted Attacks" by Dug Song and Jon Oberheide, Duo Security, 2012

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



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

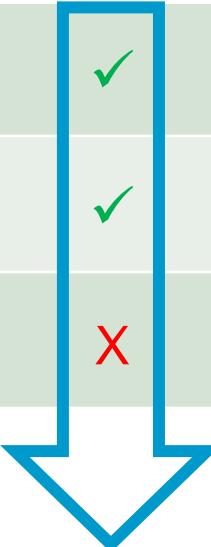
Access Control Lists (ACL)

Access control matrix:

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

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 $L = \langle S, \mathbb{D}=\{D_1, D_2, \dots\} \rangle$

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

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

Sensitivity relation

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

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

but:

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

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

$$\Leftrightarrow L_P \geq L_O$$

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

$$\Leftrightarrow L_P \leq L_O$$

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

$$\Leftrightarrow L_P = L_O$$

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

$$\Leftrightarrow L_{P_1} \leq L_{P_2}$$

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

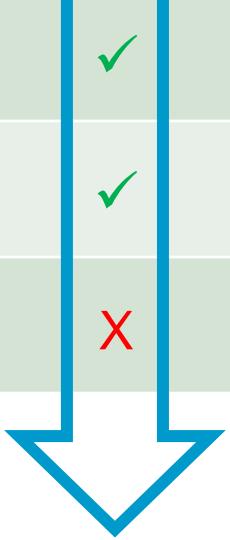
Authorization + Access Control

Access Control Lists (ACL)

Access control matrix:

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

ACL

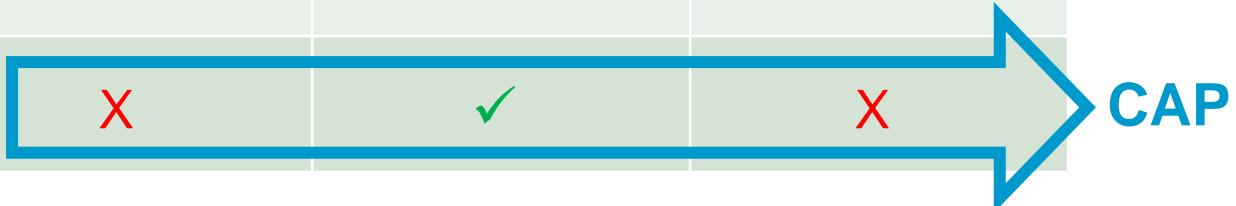


Authorization + Access Control

CAP (access control CAPability)

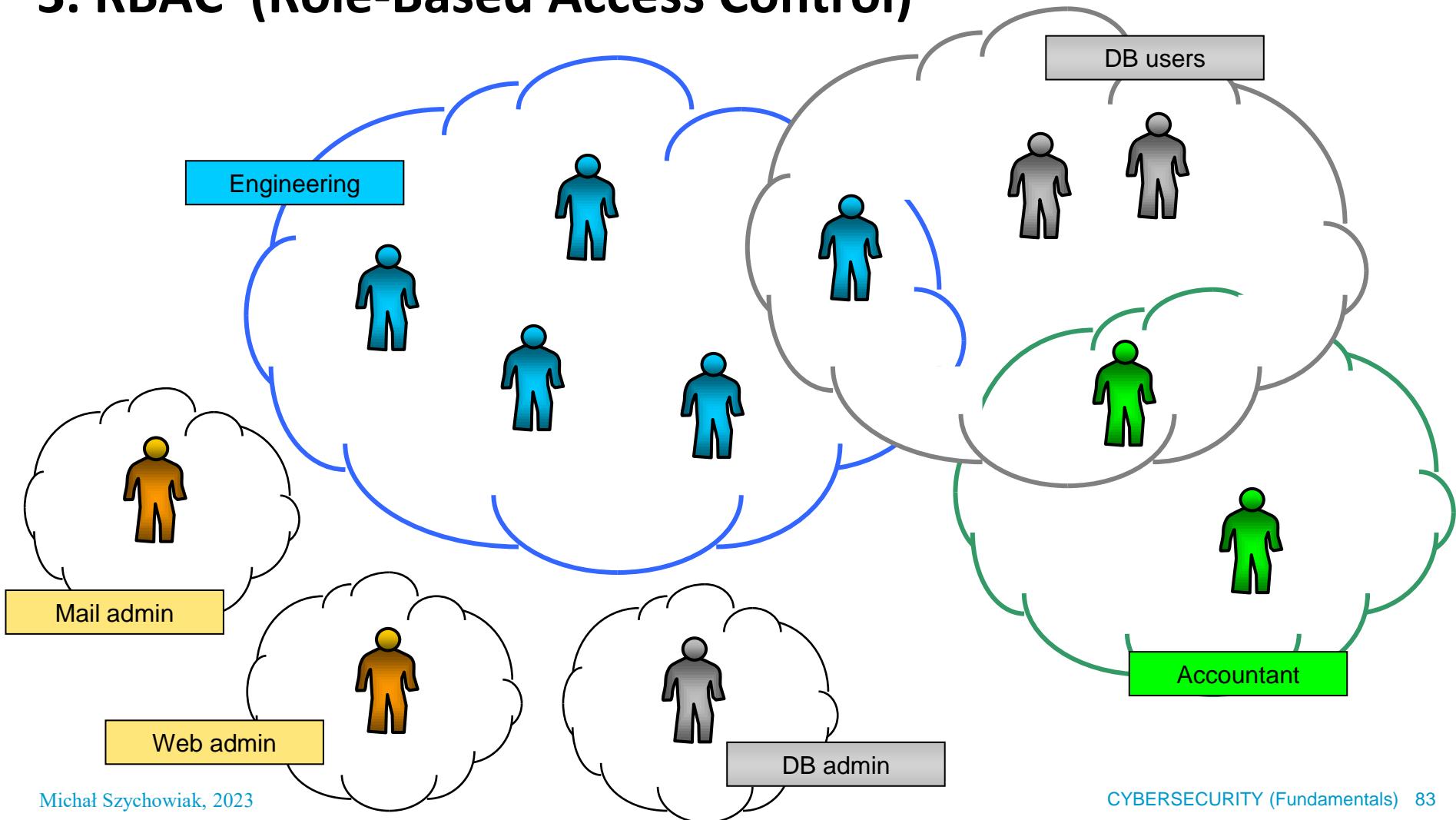
Access control matrix:

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



Authorization + Access Control

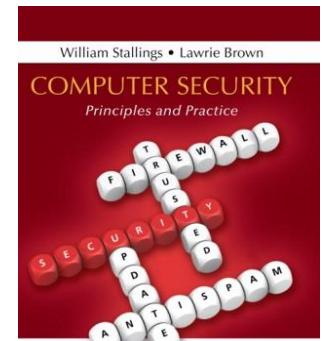
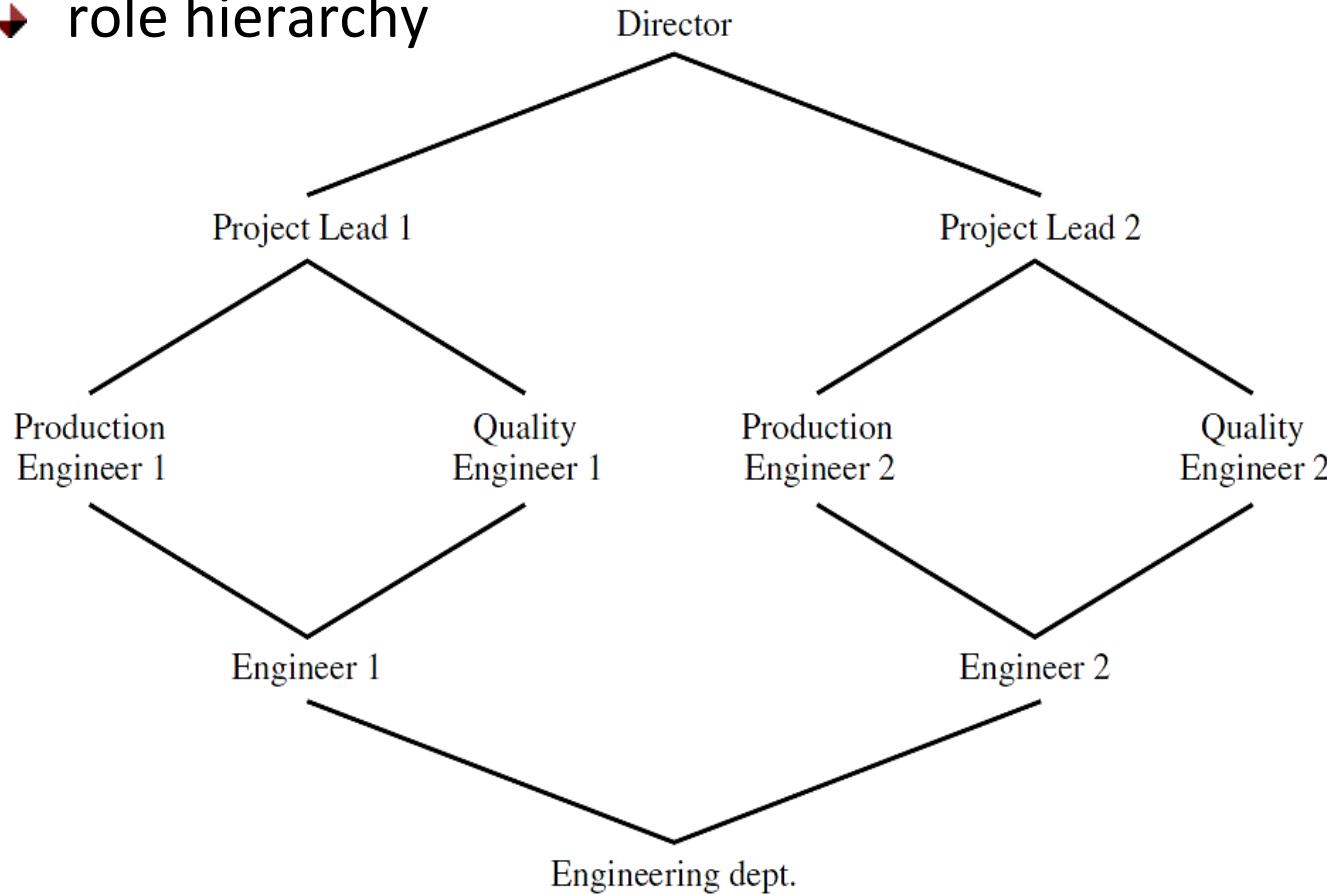
3. RBAC (Rôle-Based Access Control)



Authorization + Access Control

3. RBAC (Rôle-Based Access Control)

→ role hierarchy

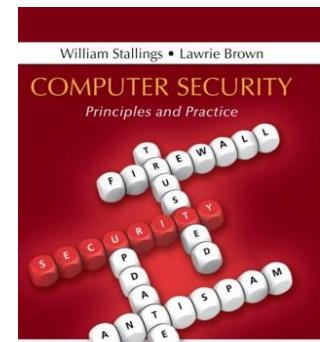
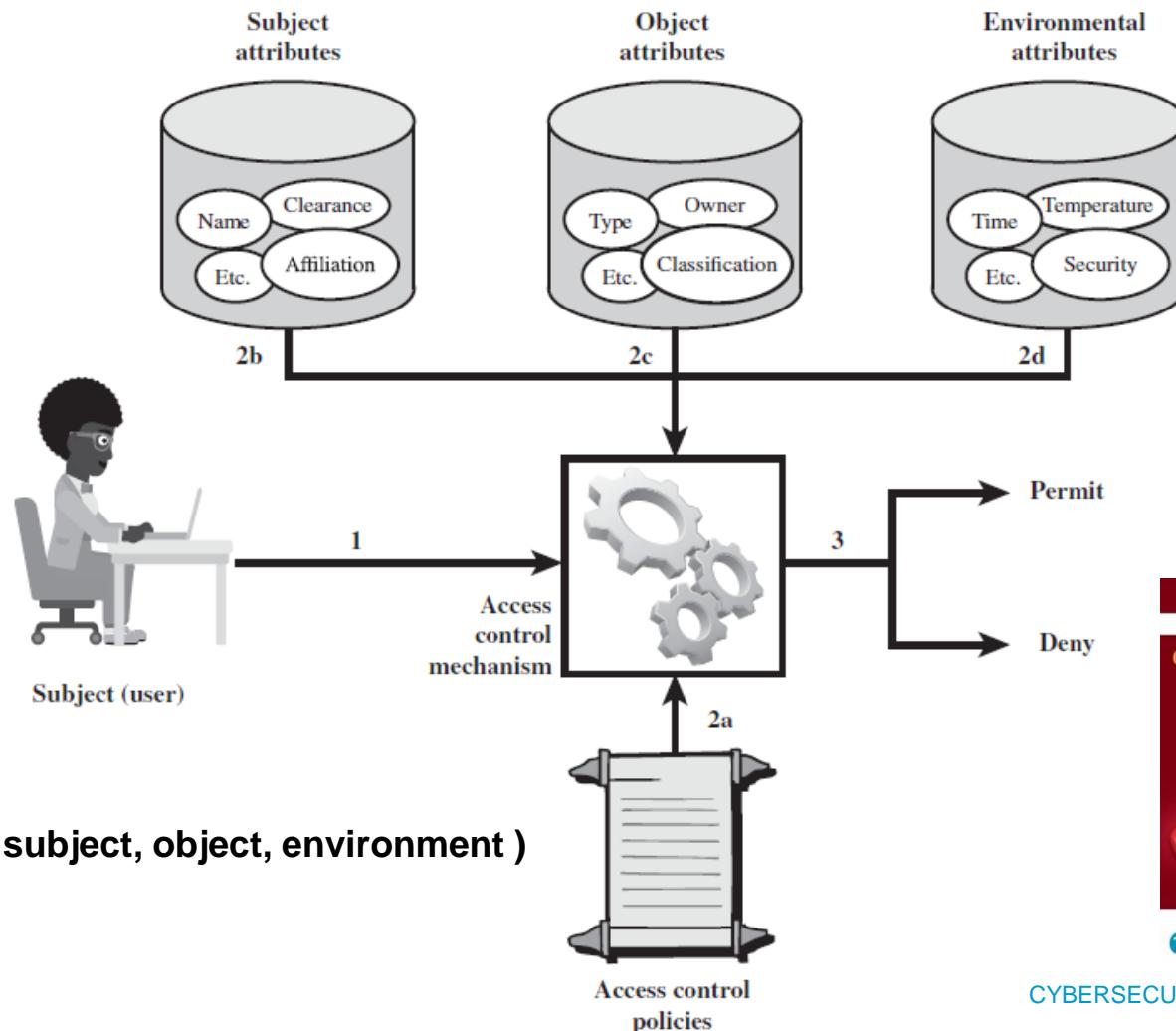


P Pearson

Fourth Edition

Authorization + Access Control

4. Attribute-Based Access Control (ABAC)



INTEGRITY

Integrity

Threat model:

- unauthorized (or unintended) modification (or destruction)

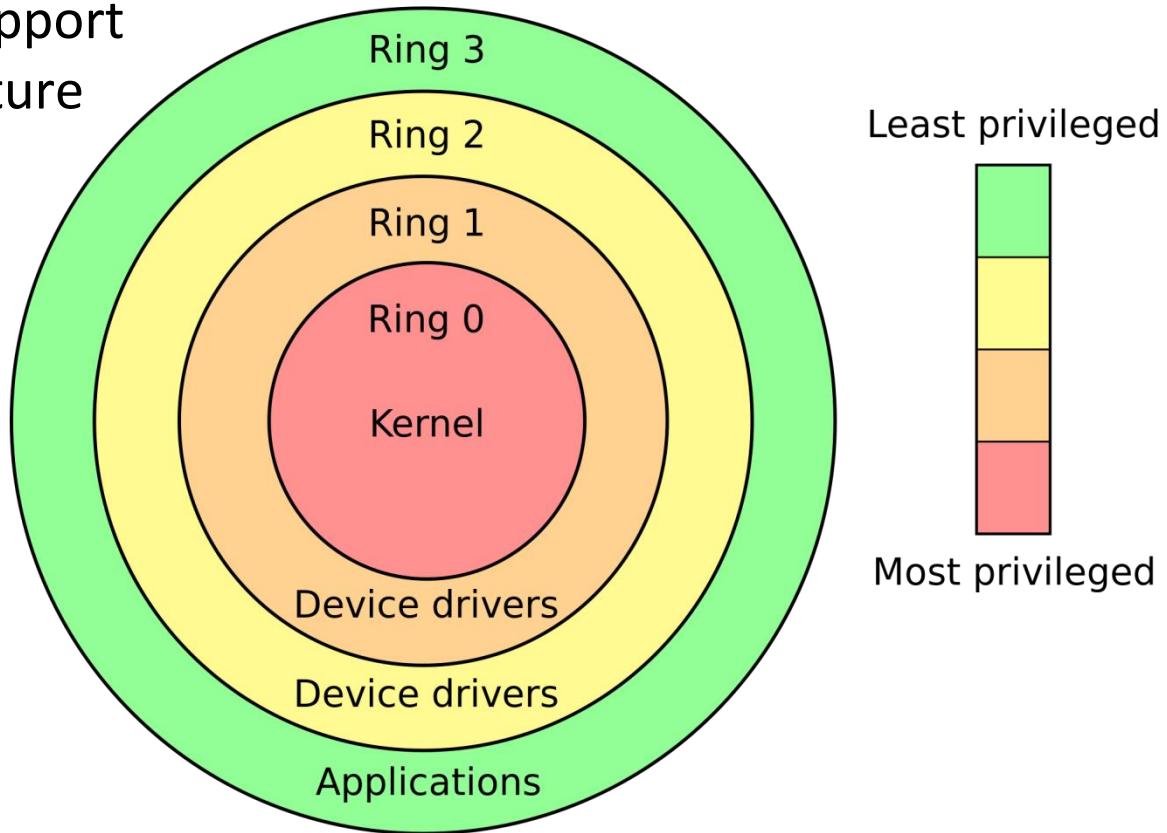
Protection:

- 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

no write-up

(no read-up)

no execute-up

Mandatory Integrity Control (MIC)

Windows Integrity Levels

0 = untrusted

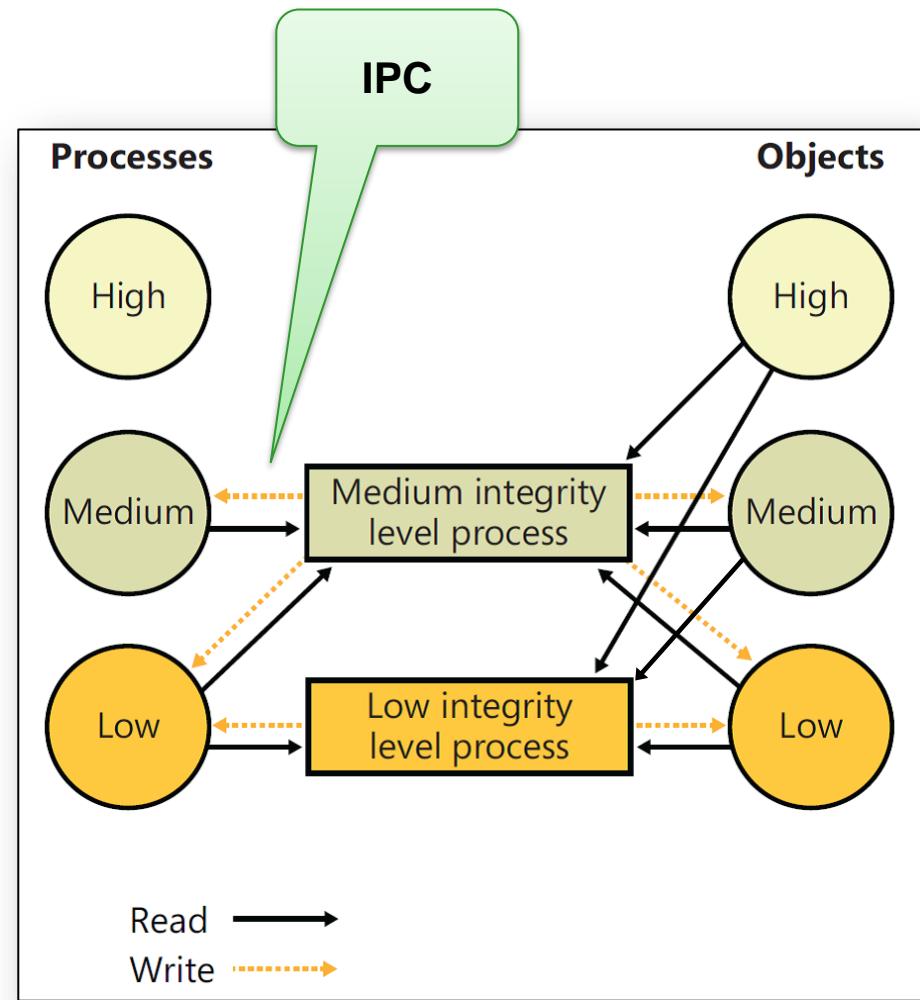
1 = low

2= medium

3 = high

4 = system

5 = protected (kernel-mode)



Event Logging

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded Events), Applications and Services Logs (Hardware Events, Internet Explorer, Key Management Service), Microsoft (AppV, User Experience Virtualization, Windows (AAD, All-User-Install-Agent, AllJoyn, AppHost, AppID, ApplicabilityEngine, Application Server-App, Application-Experience, AppLocker, AppModel-Runtime)), and System. The System log is selected, showing 897 events. The right pane shows a table of events with columns: Level, Date and Time, Source, and Event ID. An event from Windows Remote Management (Event ID 10121) is selected. A detailed view of this event is shown in the bottom-right window, with tabs for General and Details. The General tab shows the message: "The WinRM service has been configured to accept basic authentication for unsecure HTTP connections." The Details tab lists event properties: Log Name: System, Source: Windows Remote Management, Logged: 2/7/2021 5:22:25 PM, Event ID: 10121, Task Category: None, Level: Information, Keywords: Classic. The Actions pane on the right provides options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To this L..., View, Refresh, Help, Event Properties, Attach Task To This Ev..., Copy, Save Selected Events..., and Refresh.

Level	Date and Time	Source	Event ID
Information	2/7/2021 5:22:01 PM	FilterManager	6
Error	2/7/2021 5:22:01 PM	Service Control Manager	7000
Information	2/7/2021 5:22:25 PM	Windows Remote Management	10121
Information	2/7/2021 5:22:25 PM	Windows Remote Management	10148
Warning	2/7/2021 5:21:55 PM	NDIS	10400
Information	2/7/2021 5:21:53 PM	Directory-Services-SAM	16977
Information	2/7/2021 5:21:53 PM	Directory-Services-SAM	16962
Warning	2/7/2021 5:21:52 PM	NDIS	10400

“That's all folks!”