CYBER SECURITY

Lezione 02 – Autenticazione e controllo degli accessi

La DIFESA... AuteAuto

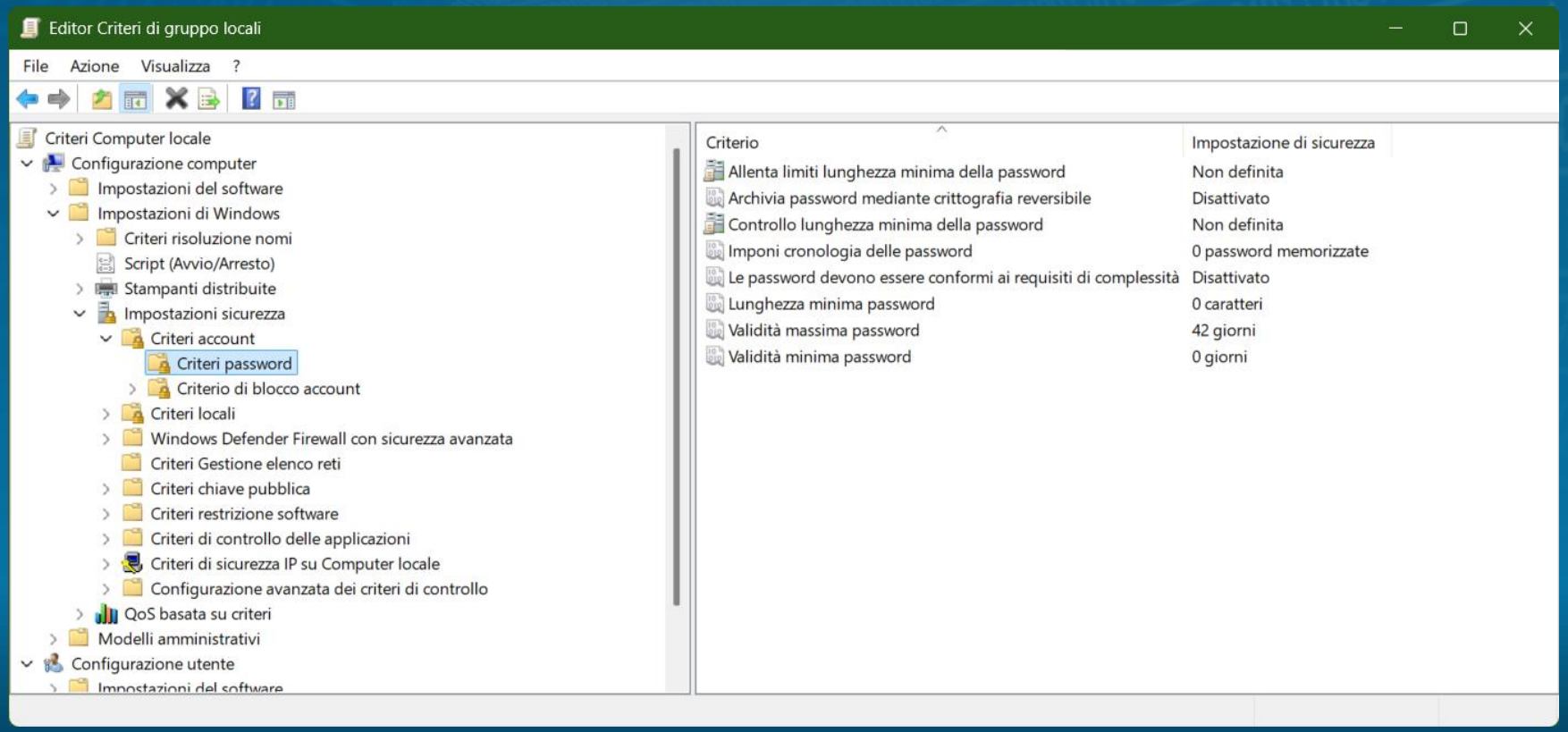
AUTENTICAZIONE
&
AUTORIZZAZIONE

Gestione Account

- Creare una account locale non admin
- Verifica installazione applicazioni con utente senza privilegi
- Verifica accesso cartelle con utente senza privilegi
- Verifica accesso a risorse di rete con utente senza privilegi

Group Policy

- Prevedi la gestione delle policy per autenticazione



Autenticazione

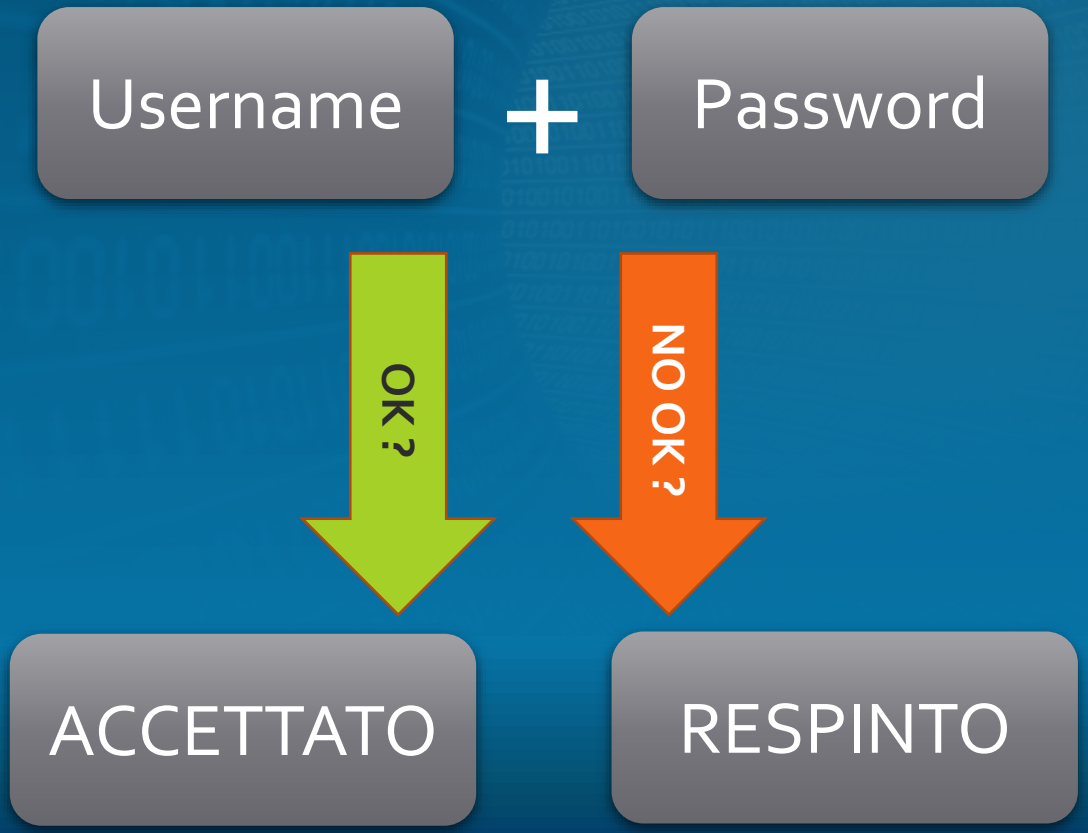
- Autenticazione (authentication) = *processo mediante il quale si verifica l'identità di un'entità (utente, processo, computer, messaggio).*

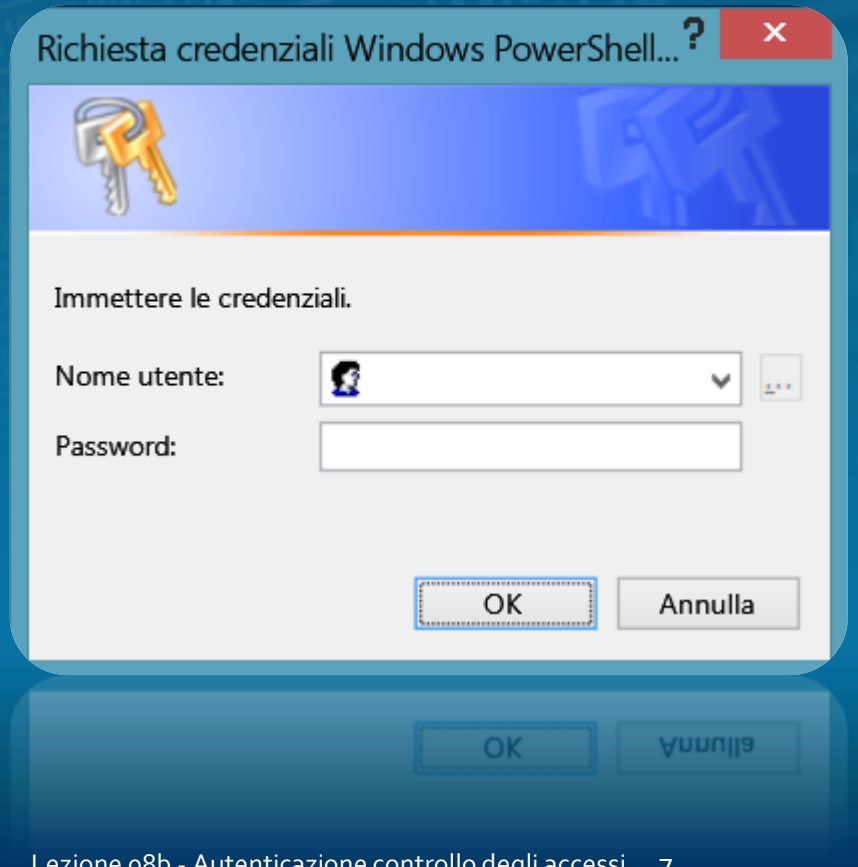
AUTENTICAZIONE

- ➔ NON ESISTE l'identità CERTA di un utente:
- ➔ test che, se superati, forniscono una garanzia sufficiente sull' identità dell'interlocutore.

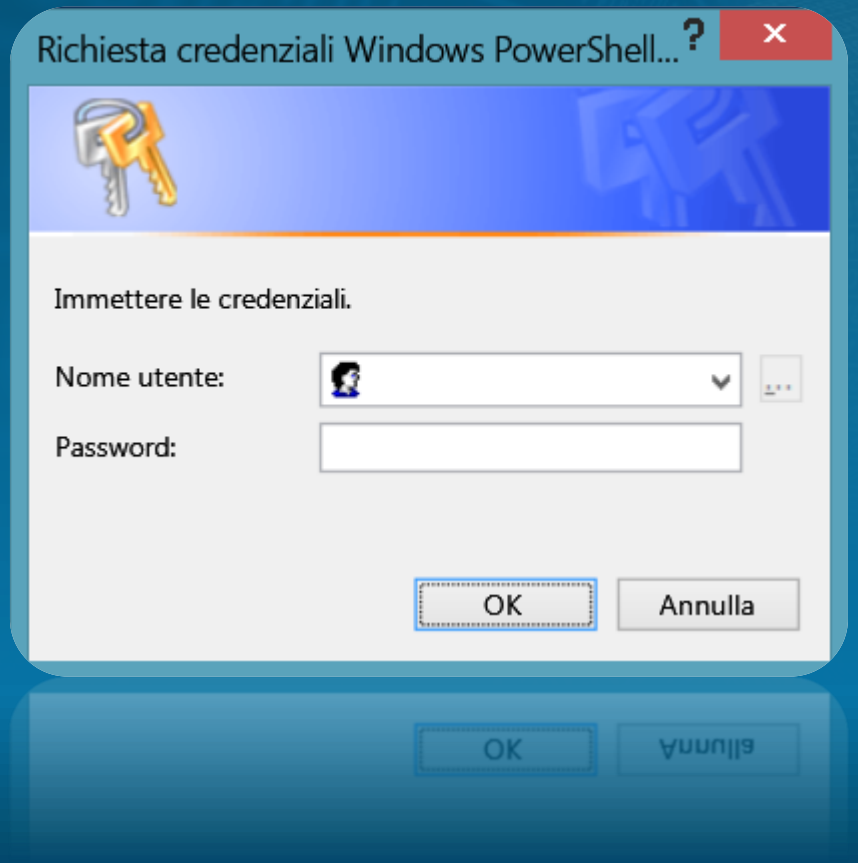
AUTENTICAZIONE ED AUTORIZZAZIONE

- CREDENZIALI





AUTENTICAZIONE ED AUTORIZZAZIONE

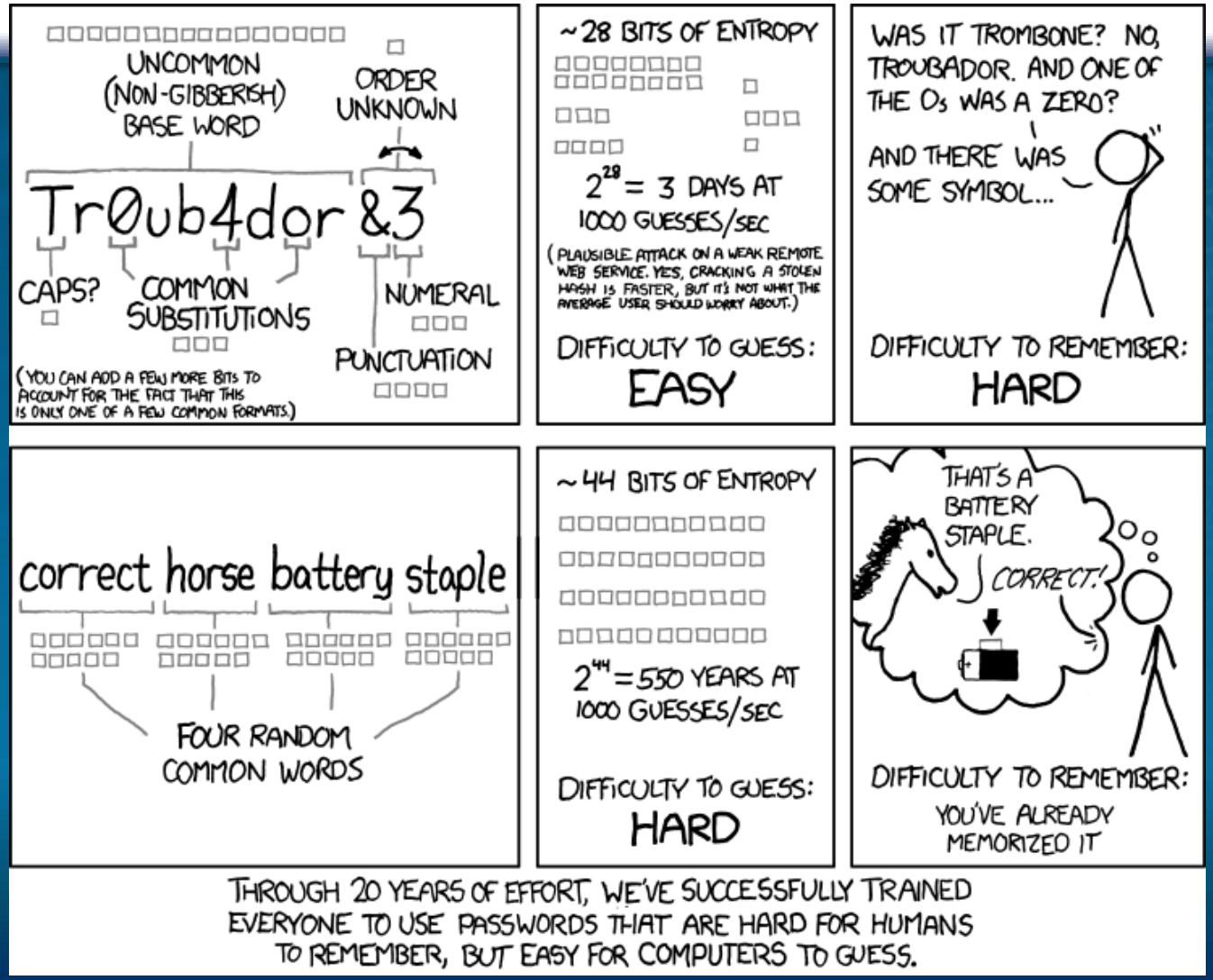


- *L'autenticazione verifica solo che un'entità sia quella che dichiara di essere, senza entrare nel merito dell'accesso al sistema.*

OK ?

Accesso **SOLO**
alle risorse Autorizzate

LA DIFESA... PASSWORD



https://xkcd.com/936/

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

Most-Common-Passwords-of-2016-Keeper-Security-Study

Password

- Regole pratiche whats-the-password
- PassPhrase
- MFA

- Mix maiuscole minuscole numeri e simboli per almeno 12 caratteri
- No ripetizioni, nomi di animali, familiari, etc. specie **se pubblicati sui social**
- Cambio frequente e diversa per diversi servizi

La DIFESA... Password

- Usare Password ROBUSTE
  - https://www.digitaltrends.com/computing/top-100-worst-passwords-2018/
- Mantenerle SEGRETE
- MAI usare le stesse credenziali per servizi diversi
- Cambiate SEMPRE le password di default dei dispositivi/programmi

PASSWORD: CRITERI DI SCELTA

- LUNGHEZZA
- CARATTERI
- CONTENUTO
- ASSEGNAZIONE VS VALORE DI DEFAULT
- PERIODO DI VALIDITA'
- CAMBIAMENTO
- CONSERVAZIONE
- MEMORIZZAZIONE

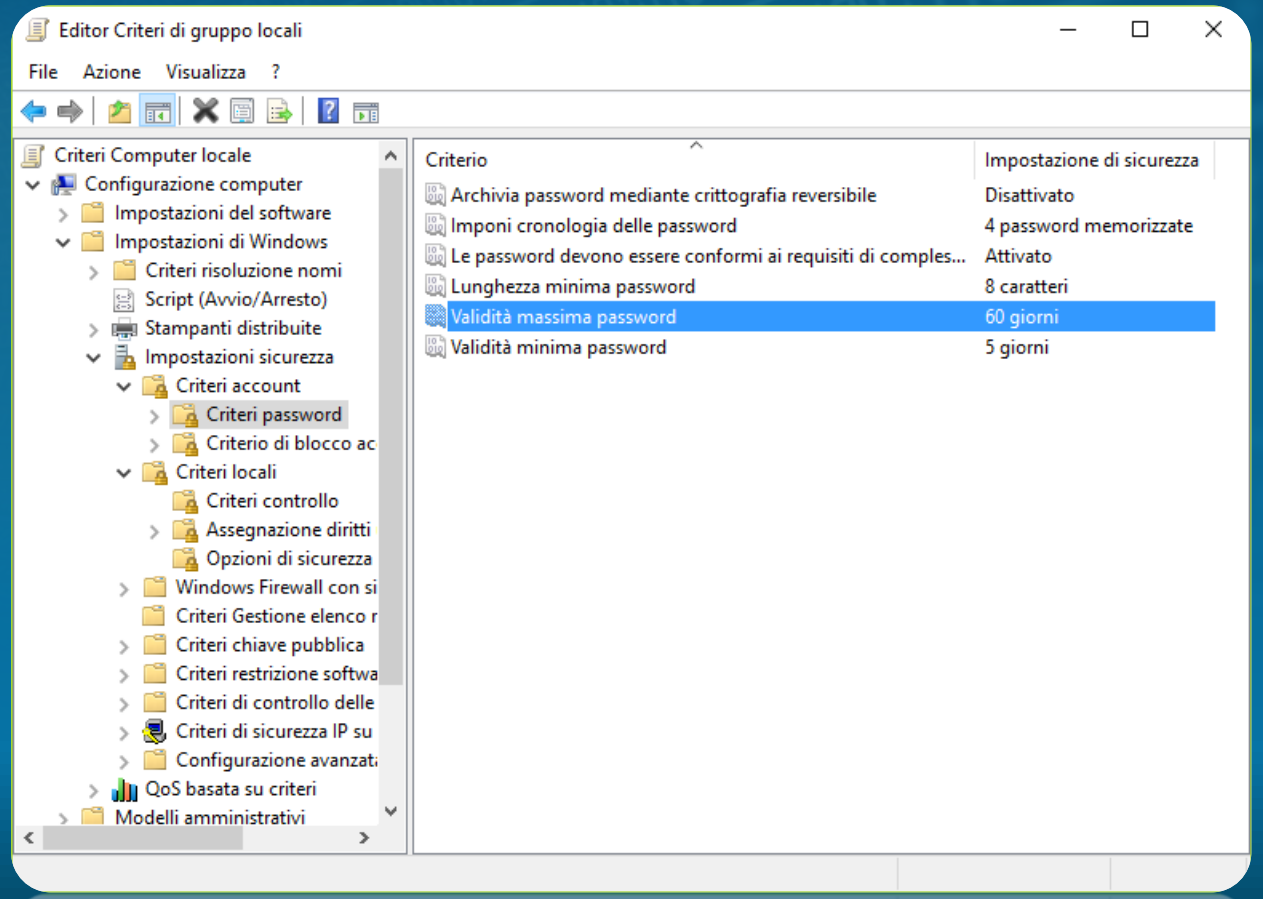
La DIFESA... Password

- Lunghezza 8-16 caratteri
- Usare minuscole MAIUSCOLE numeri e simboli
- No ripetizioni sequenziali (tipo paaassword o 121212aaaa)
- No dati contestuali (mariorossi88)
- Cambio Password frequente
- No stessa pwd per piu' account

PASSWORD: GROUP POLICY

Impostazioni di sistema

- ➔Criteri di Gruppo
- ➔Impostazioni di Sicurezza
- ➔Criteri…
- ➔Password
  - ➔Cronologia
  - ➔Lunghezza
  - ➔Complessità
  - ➔…



PWD: Tempo Cracking

- https://www.passwordmonster.com/
- https://www.security.org/how-secure-is-my-password/

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

TIME TO CRACK: MD5 Hashed Passwords

Number of characters	Numbers Only	Lowercase Only	Upper and Lower Case	Number, Upper, Lower	Number, Upper, Lower, Symbols
8	Instantly	Instantly	2 minutes	5 minutes	3 hours
9	Instantly	9 seconds	2 hours	5 hours	12 days
10	Instantly	4 minutes	2 days	14 days	3 years
11	Instantly	2 hours	132 days	3 years	279 years
12	Instantly	2 days	19 years	159 years	26.5 thousand years
13	Instantly	6 weeks	995 years	10 thousand years	3 million years
14	3 minutes	3 years	51 thousand years	608 thousand years	239 million years
15	26 minutes	82 years	2 million years	37 million years	22.7 billion years
16	5 hours	2136 years	140 million years	3 billion years	3 trillion years
17	43 hours	56 thousand years	8 billion years	145 billion years	205 trillion years
18	18 days	2 million years	379 billion years	9 trillion years	20 quadrillion years
19	6 months	38 million years	20 trillion years	557 trillion years	2 quintillion years
20	5 years	977 million years	2 quadrillion years	35 quadrillion years	176 quintillion years
21	49 years	26 billion years	54 quadrillion years	3 quintillion years	17 sextillion years
22	490 years	660 trillion years	3 quintillion years	133 quintillion years	2 septillion years

Password

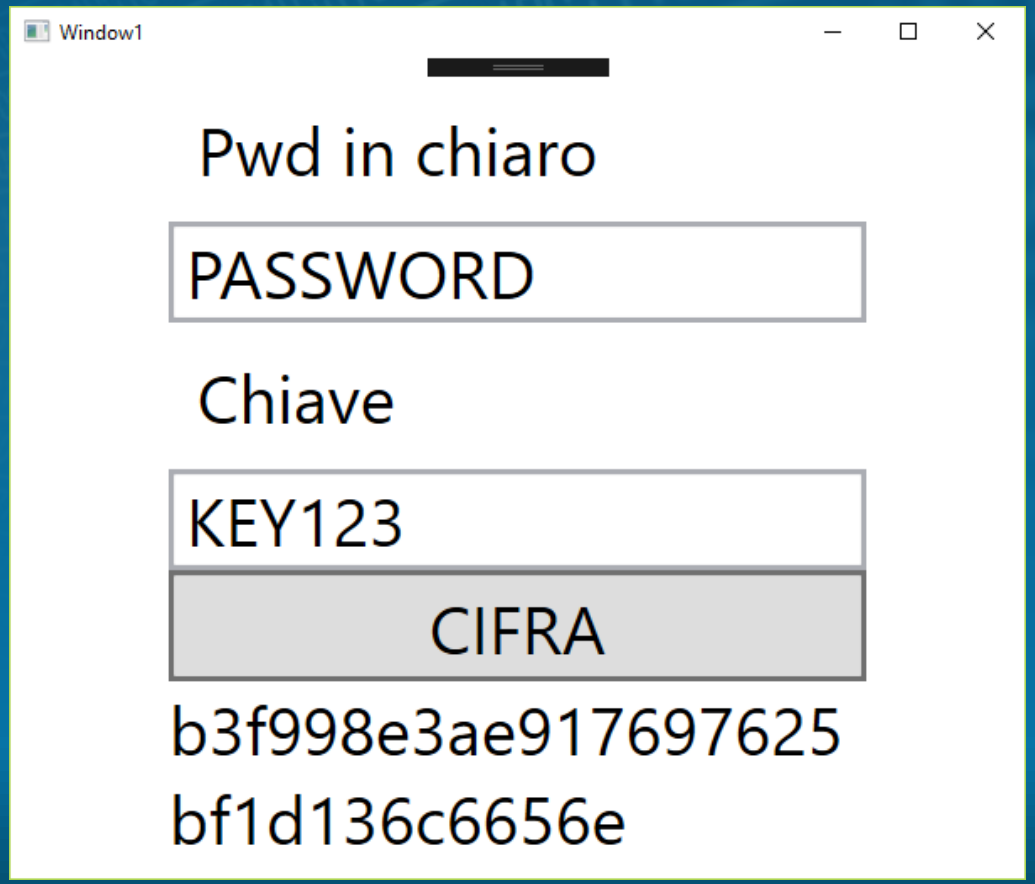
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

La DIFESA... Password

- MAI usare le stesse credenziali per servizi diversi
  - Per ricordarsele: programmi password-safe; per esempio, KeePass http://keepass.info/
  - Ma, da soli, non bastano: http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/
- Se usate Firefox, impostate la *master password*. Per approfondimenti su come i browser memorizzano le password: http://raidersec.blogspot.it/2013/06/how-browsers-store-your-passwords-and.html
- Cambiate SEMPRE le password di default dei dispositivi/programmi
- Ovunque possibile, abilitate l'autenticazione in due passi http://en.wikipedia.org/wiki/Two-step_verification
- Esempi:
  - https://www.google.com/landing/2step/
  - https://www.dropbox.com/help/363

Le Password

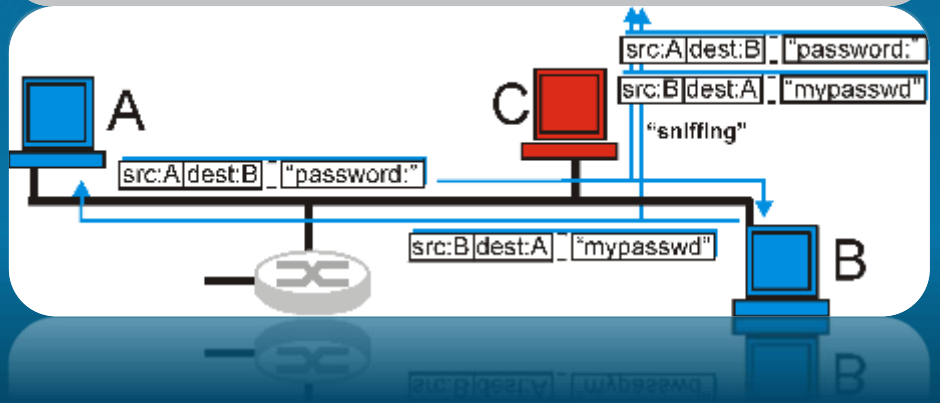
- Le password sono uno dei più antichi sistemi di autenticazione; i primi computer le conservavano in chiaro in un file
- Per migliorare al sicurezza ➔ **hashing** delle password: conservazione dei nomi utente e dell'hash delle relative password



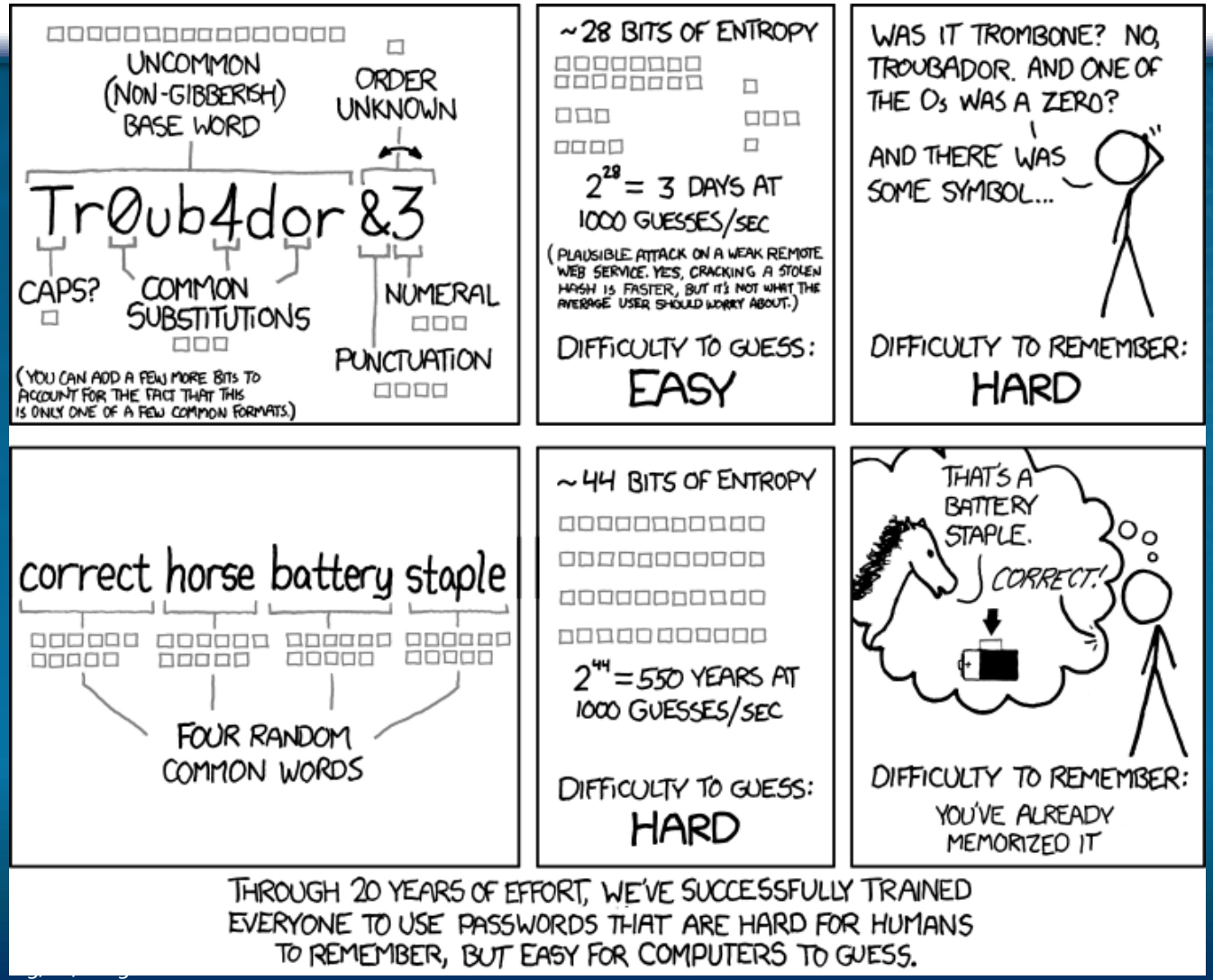
Le Password

- dall'hash è impossibile ricostruire la password

- Per catturare una pwd:
  - attacchi *brute force* o *dictionary based*
  - **keystroke sniffing**
  - **network sniffing**



LA DIFESA... PASSWORD



https://xkcd.com/936/

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

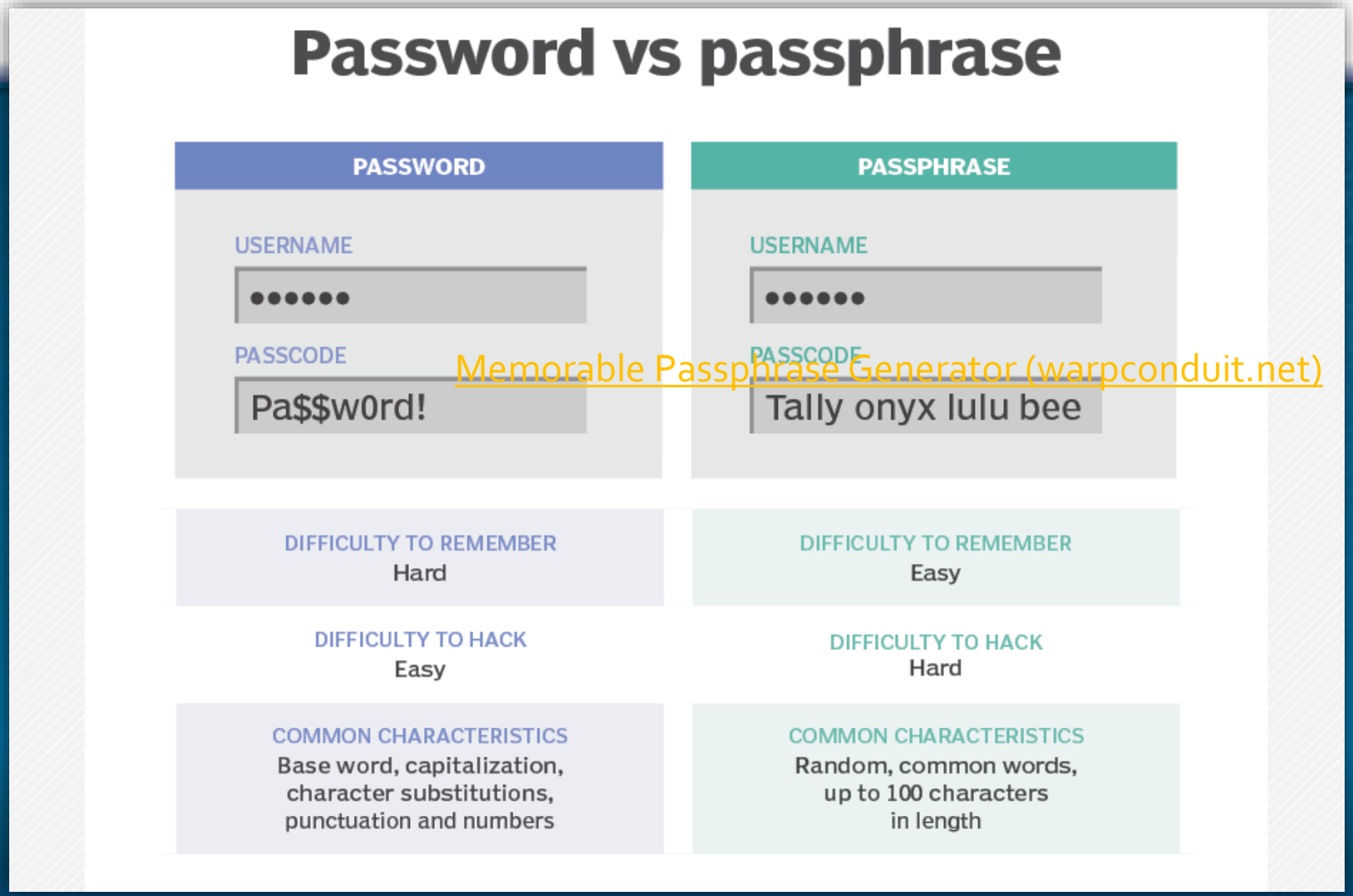
Most-Common-Passwords-of-2016-Keeper-Security-Study

LA DIFESA... PASSWORD

Basic Rules for creating passwords

1. **NEVER RESUSE A PASSWORD**
   Don't use the same password for all accounts
2. **DON'T USE PERSONAL INFORMATION**
   Using versions of your name, family members or DOB
3. **MIX IT UP**
   Use uppercase, lowercase, characters, and numbers.
4. **MAKE IT LONG**
   The longer the password the harder it is to guess
5. **CHANGE THEM FREQUENTLY**
   Set reminders to change them once a month
6. **DON'T SHARE THEM**
   This may be tricky to manage but important to teach
7. **USE A PASSWORD MANAGER**
   NordPass was rated the top password manager in Australia
8. **USE TWO-FACTOR AUTHENTIFICATION**
   Where possible this will add another layer of protection

PWD vs Passphrase



Memorable Passphrase Generator (warpconduit.net)

- **GENERATORI**
- PWD
  - LastPass
  - PasswordsGenerator
- PPH
  - PasswordGenerator
  - Random Passphrase Generator
  - WarpConduit

Passphrase

- Scegli una frase prendendola da un romanzo
- Prendi alcune parole ed uniscile

- Passphrase generator (WarpConduit)

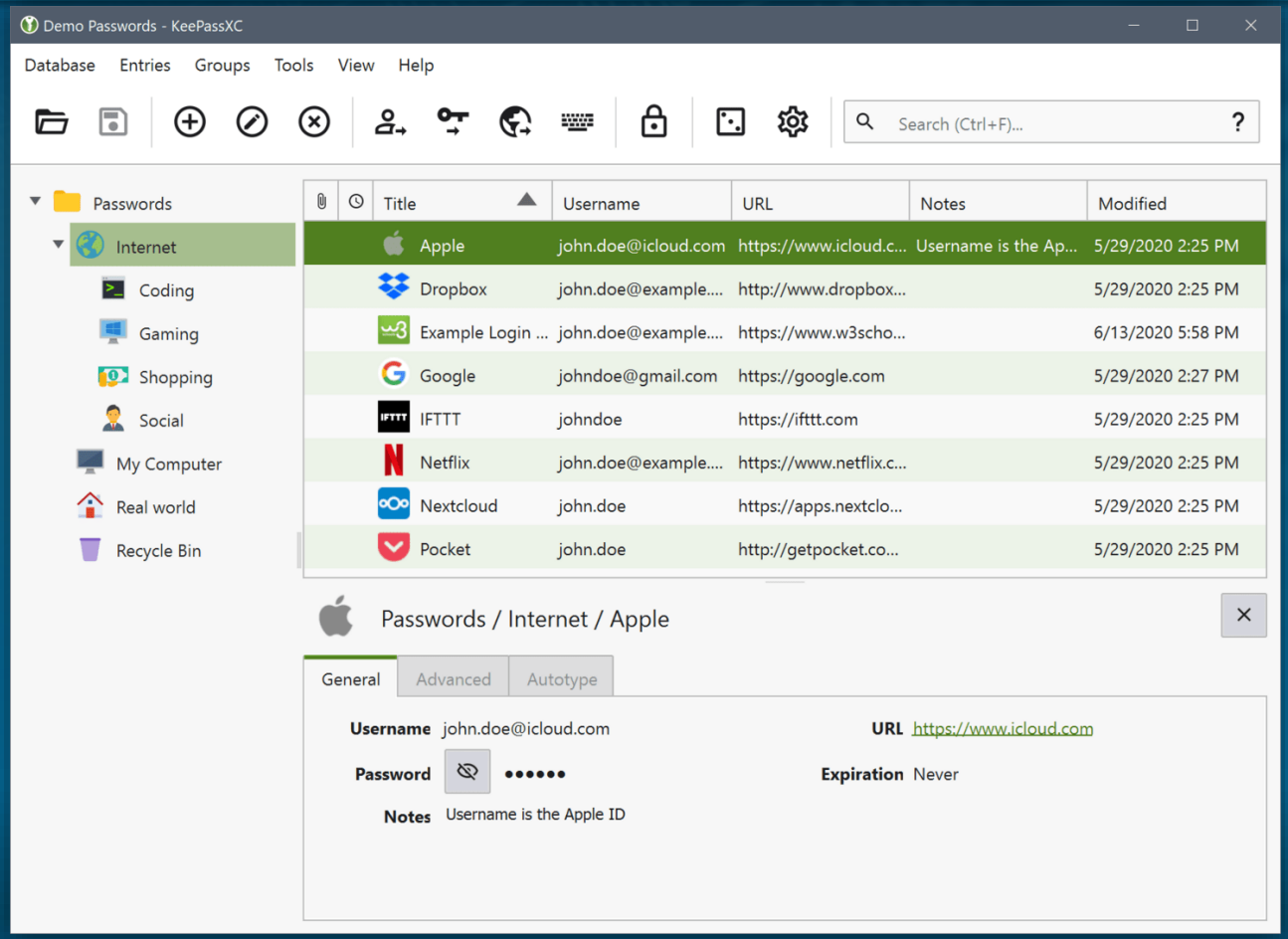
Password Manager

- ➔ Master Password
- ➔ accesso al software di gestione
- ➔ Password Multiple

- LASTPASS
- KeePass

Password Manager

- MasterPassword
- Il sw memorizza le altre pwd criptate
- Esempi
  - Lastpass
  - KeePass Password Safe
  - KeePassXC Password Manager



LA DIFESA... DEVICES PASSWORD

tp-links-wifi-defaults

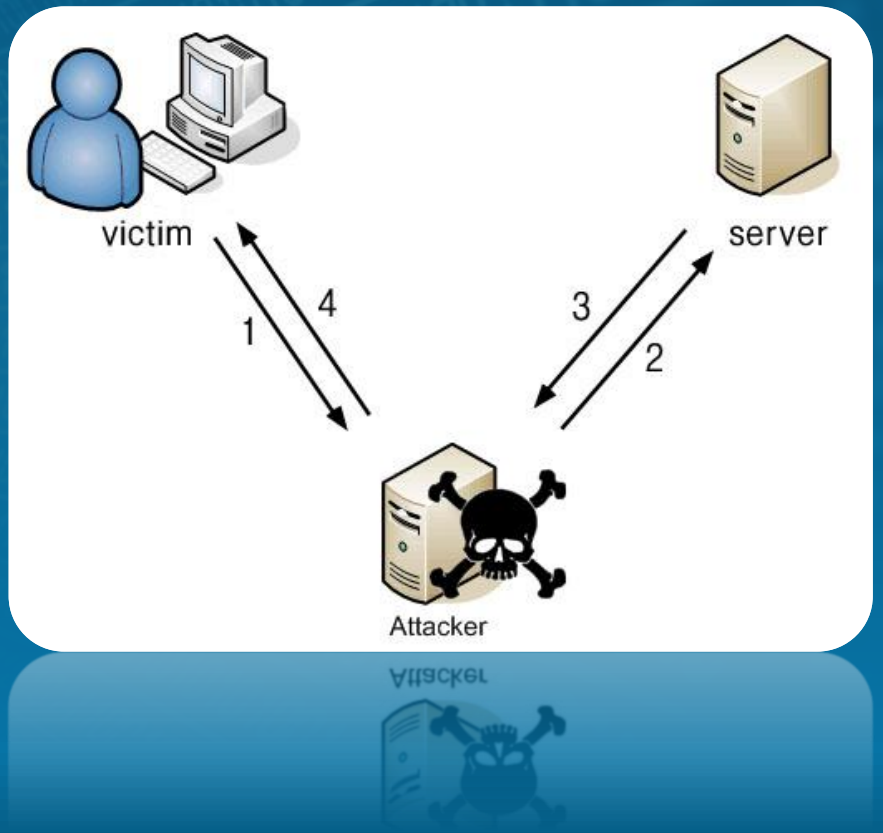
- cambiate le eventuali password di default su access point
- usate WPA2
- usate password lunghe (per evitare attacchi a dizionario)
- disabilitate WPS wi-fi-protected-setup-wps-is-insecure
- su Wi-Fi pubblici, considerate l'uso di una VPN
  - why-you-should-start-using-a-vpn

AUTORIZZAZIONE

- **Autorizzazione** è il *diritto accordato ad un'entità (hardware, software, individuo) di accedere ad un sistema e alle sue risorse secondo un profilo di permessi ben definito*.

AUTORIZZAZIONE

- Se un individuo riesce ad impersonare un utente valido (spoofing), non ci sono limiti al danno potenziale per la riservatezza e integrità delle informazioni, oltre agli eventuali danni economici.
- In qualche caso può persino essere compromessa la futura capacità di autenticazione degli utenti.

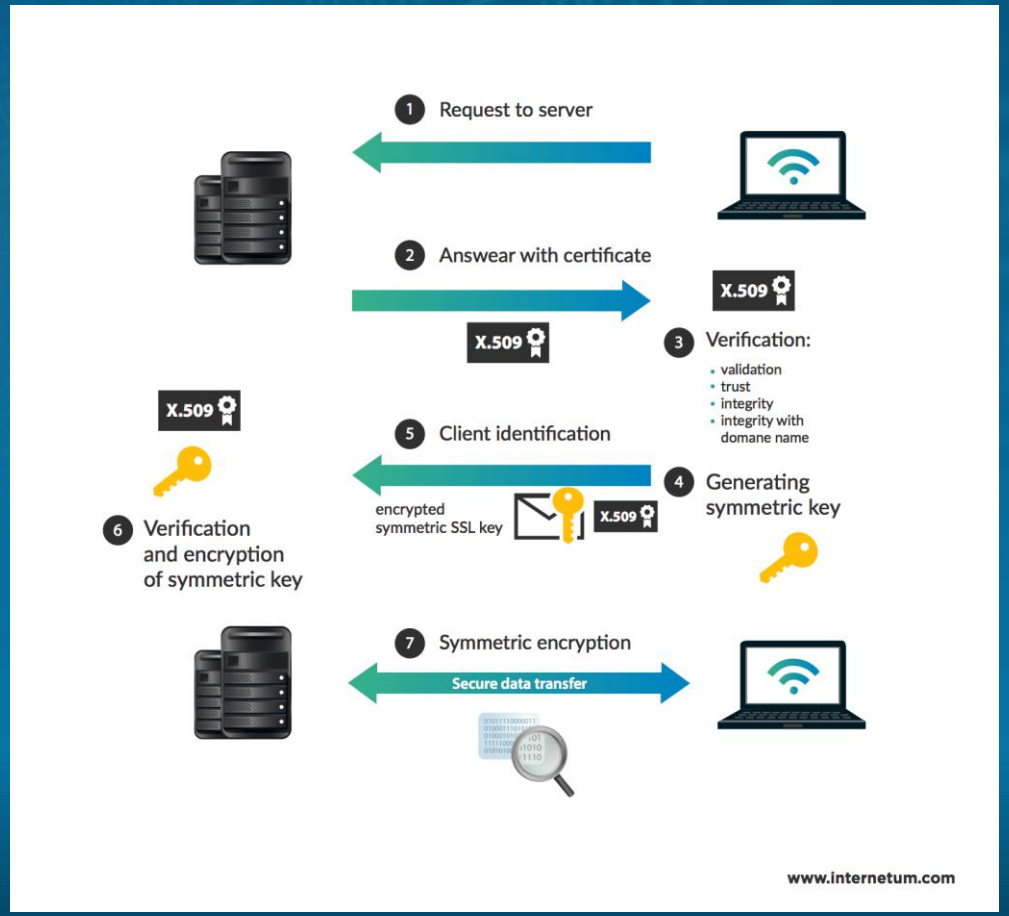


AUTORIZZAZIONE: METODI

- password
- certificati digitali
- dispositivi biometrici
- token fisici
- smart card
- …

Modelli di autenticazione

- Autenticazione locale
- Autenticazione diretta
- Autenticazione indiretta
- Autenticazione off-line



Schemi di Autenticazione

Elementi comuni dei sistemi di autenticazione:

- l'entità da autenticare;
- le caratteristiche distintive su cui si basa l'autenticazione;
- un proprietario o amministratore del sistema di sicurezza;
- un meccanismo di autenticazione che verifica le caratteristiche distintive.
- il meccanismo di controllo dell'accesso

Schemi di Autenticazione

Elementi comuni dei sistemi di autenticazione:

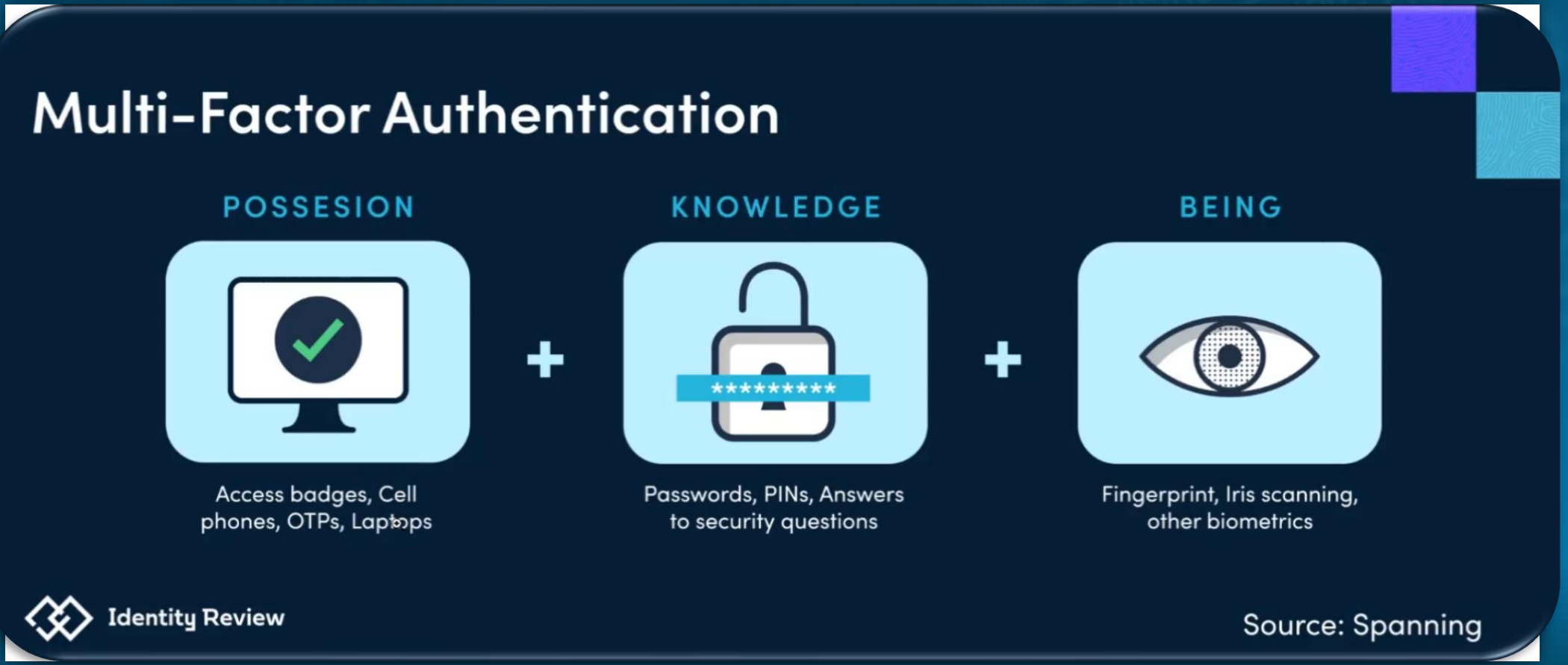
- l'entità da autenticare;
- le caratteristiche distintive su cui si basa l'autenticazione;
- un proprietario o amministratore del sistema di sicurezza;
- un meccanismo di autenticazione che verifica le caratteristiche distintive.
- il meccanismo di controllo dell'accesso

SCHEMI DI AUTENTICAZIONE : 2FA

Fattori di autenticazione di un utente:

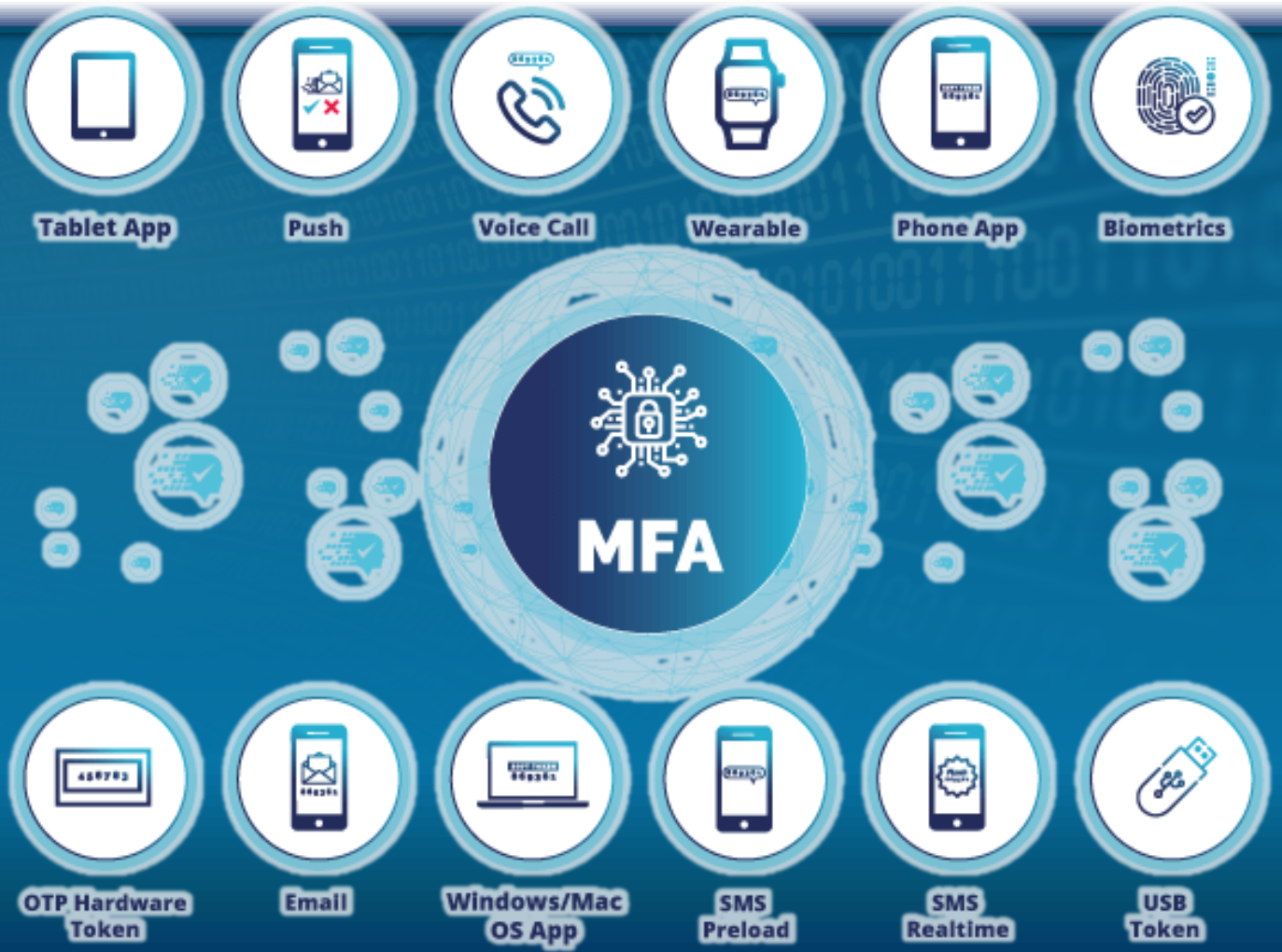
- qualcosa che **sai** (password, PIN, …);
- qualcosa che **hai** (token, Smart card, …);
- qualcosa che **sei** (impronta digitale, retina, iride, volto, voce,)

MFA – 2FA


Multi-Factor Authentication
POSSESION
KNOWLEDGE
BEING
****
Access badges, Cell phones, OTPs, Laptops
Passwords, PINs, Answers to security questions
Fingerprint, Iris scanning, other biometrics
Identity Review
Source: Spanning

MFA – 2FA

- P.Es. FACEBOOK o GOOGLE
- Accesso al Pannello di controllo
  ➔ Gestione Account
- Abilitarla SEMPRE



MFA – 2FA


Fractional
CISO
MULTI-FACTOR AUTHENTICATION
Password
Verification
Access


Multi factor authentication
Something you have
Something you are
Something you know

MFA – 2FA


Something You Have
ATM Card
Security Token
ID Badge
Mobile Phone
Something You Know
Password
PIN
Security Question
Transaction Number
Something You Are
Fingerprint
Face
Voice
Retina
Somewhere You Are
GPS Signal
IP Address
Physical or
MAC Address

SCHEMI DI AUTENTICAZIONE

Fattori di autenticazione di un utente:

- qualcosa che **sei: Punti deboli**
  - maggiore **costo**;
  - possibilità di **intercettazione**;
  - identificazione **non certa**;
  - **variabilità** nel tempo;
  - **trafugamento**

SCHEMI DI AUTENTICAZIONE

Non esiste

un metodo di autenticazione

Perfetto

è sempre più comune

utilizzare meccanismi

di protezione multipli

Social engineering

- l'attaccante si fa aiutare da un dipendente, inconsapevole, convincendolo a rivelare le informa z ioni (come username e password) necessarie ad entrare nel sistema.

PASSWORD INTERNE ED ESTERNE

- interni (personale dell'azienda ➔ non forniscono un alto livello di protezione
  ➔ **mediare tra usabilità e sicurezza**:)
- esterni (come i clienti che si collegano via Internet ➔ **più complessa, protetta con metodi crittografici e modificata di frequente**).

Password Interne

- Usare password mnemoniche
- Disabilitare la scadenza della password
- Incoraggiare gli utenti a cambiare password
- Tenere i ser ver e i dispositivi di rete sotto chiave.
- Separare posti di lavoro dedicati ad applicazioni critiche
- ATN ai sistemi single sign-on
- Le password degli amministratori

Password Esterne

- **Connessioni remote**
  - ➔ trattamento diverso rispetto alle connessioni interne
  - ➔ filtrate da un dispositivo di sicurezza (*firewall*, *VPN*)
- **gestione informazioni di particolare valore**
- **NO re-routing**
- **NO «Dizionario»**
- **Cambio Periodico**
- **PC Portatili**

Password Esterne : criteri di scelta

1. **Scegliere una password a caso**
2. **Scegliere una seconda password a caso**
3. **Scegliere a caso una cifra o segno** di punteggiatura come carattere intermedio.
4. **Costruire la password forte concatenando le stringhe**

Ud1nE+33I00

D@n+C3l-1966

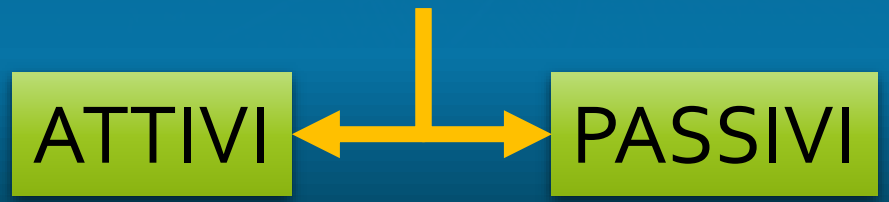
http://www.corriere.it/tecnologia/cyber-cultura/15_gennaio_21/password-cambiare-suggerimenti-0o8ea4do-a15b-11e4-8f86-063e3fa7313b.shtml?refresh_ce-cp

https://www.key4biz.it/cybersicurezza-ecco-le-25-peggiori-password-piu-usate/146851/

AUTENTICAZIONE TRAMITE TOKEN

- **Proprietà fondamentali:**

1. il titolare dev'essere in **possesso fisico**
2. **difficile da duplicare**;
3. **perdere l'accesso** a risorse critiche (smarrimento);
4. **inventario dei token**.



1. elimina l'**onere** di dover ricordare password complicate;
2. può contenere un dato segreto molto più **complesso** di quanto sia memorizzabile da una persona;
3. è spesso associato ad un **secondo fattore** di autenticazione, come ad es. un PIN;
4. un token attivo può generare un **output diverso** in diverse circostanze oppure ad ogni utilizzo.

BIOMETRIA

- La **biometria** (*bios*=vita e *metron*=misura) è la *scienza e tecnologia dell'autenticazione misurando le caratteristiche fisiologiche o comportamentali di una persona*.
  - **Impronte digitali**
  - **Geometria delle mani**
  - **Retina / Iride**
  - **Riconoscimento del volto**
  - **Impronta vocale**
  - **Firma autografa**
  - **Dinamica della digitazione su tastiera**

AUTENTICAZIONE IN RETE

- Per autenticare un soggetto (utente o processo) in un **contesto di rete** occorre trovare un compromesso fra
- *modalità operative* ragionevolmente semplici,
- un *onere amministrativo* non eccessivo (per i sistemisti)
- un *livello di sicurezza* accettabile.

AUTENTICAZIONE IN RETE

- In ambiente **Windows** è possibile semplificare le cose organizzando i server in un unico "dominio"
- l'autenticazione in rete avviene attraverso lo scambio di messaggi tra client e server
- **protezione crittografica**

Protocolli per l'autenticazione utente

PAP (Password Authentication Protocol)

CHAP (Challenge Handshake Authentication Protocol*)

Protocolli per l'autenticazione Processi

- l'autenticazione in rete avviene attraverso lo scambio di messaggi tra client e server
- scambio di messaggi tra le due parti in causa è modellato come una serie di Remote Procedure Calls (RPC)

ARCHITETTURE SINGLE SIGN-ON

- Elevato numero di servizi → molte password : problema Utente
- Elevato numero di utenti → problema Admin

- database unico, centralizzato, per tutti i profili (username, password e altri dati) al quale le applicazioni possano accedere attraverso un'interfaccia standard (p.es. LDAP -Lightweight Directory Access Protocol)
- Unica autenticazione per l'utente