Ordine degli Ingegneri della provincia di Forlì-Cesena

RELATORE: Ing. Giorgio Sbaraglia

21 APRILE 2017

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. Attacchi hacker: alcuni casi famosi
4. Le reti WI-FI: problemi di sicurezza
5. Imparare ad usare le Password
6. L’autenticazione a due fattori (MFA)
7. Il Backup
8. Conclusioni

Cosa è la crittografia

Crittografia è una parola d'origine greca composta da κρυπτός (***kryptós***) che significa "nascosto", e γραφία (***graphía***) che significa "scrittura".
Da non confondere con la **Steganografia** che è una tecnica che si prefigge di **nascondere un messaggio** (invece nella Crittografia lo si rende **indecifrabile**).

I primi sistemi di crittografia risalgono a circa 3.000 anni fa.
Il sistema più antico è il cosiddetto **Codice di Atbash**, un impianto rudimentale nel quale la prima lettera dell'alfabeto era sostituita dall'ultima, la seconda dalla penultima e così via (come se l'alfabeto venisse scritto al contrario).

Storia della crittografia: il cifrario di Cesare

Il Cifrario di Cesare è un cifrario "a sostituzione": l'alfabeto cifrante è traslato di tre lettere rispetto all'alfabeto in chiaro (cifratura "monoalfabetica").

Chiaro (*C*):	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrato (*E*):	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

```
veni, vidi, vici
YHQL, YLGL, YLFL
```

Il Cifrario di Cesare non utilizza nessuna chiave, basta conoscere l'algoritmo per decifrarlo.
Non rispetta il Principio di KERCKHOFFS.

Il Principio di KERCKHOFFS

È stato enunciato nel lontano 1883 dal linguista franco-olandese August Kerckhoffs nel suo celebre articolo *“La cryptographie militaire”* apparso nel “Journal des sciences militaires". È il principio su cui si basa la crittografia moderna.

Principio di Kerckhoffs

“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione”.

La cifratura polialfabetica: il cifrario di Vigenère

Il Cifrario di Cesare era a cifratura “monoalfabetica”.

Idea del cifrario di Vigenère: usare più alfabeti cifranti monoalfabetici, cambiando l’alfabeto man mano che si procede con la crittazione. Elementi fondamentali:

1. Un insieme di alfabeti cifranti monoalfabetici.
2. Una chiave che determina, ad ogni passo, quale alfabeto cifrante deve essere usato.

Ideato dal dilomatico francese **Blaise de Vigenère nel XVI secolo**, per secoli è stato considerato inviolabile, al punto da guadagnarsi il nome di “chiffre indéchiffrable”.

In realtà fu violato, in maniera indipendente, da Babbage e Kasiski nel XIX secolo.

La macchina ENIGMA e Alan Turing

Era un dispositivo usato dai nazisti durante la seconda guerra mondiale per cifrare e decifrare messaggi.

Enigma usava 3 rotori in cascata, ognuno dei quali poteva avere 26 posizioni diverse. Realizzava una cifratura polialfabetica basata sull'uso di 26x26x26=17.576 alfabeti cifranti.

Combinazioni totali possibili:

1.764.486.127.404.000

La “Bomba” di Turing

I primi a capire il funzionamento della macchina Enigma furono i polacchi (M. Rejewski). Per decrittare Enigma gli inglesi allora radunarono a Bletchley Park, nel Bukinghamshire, i migliori crittoanalisti e matematici.

Fu **Alan Turing (**1912-1954) a dare il colpo di grazia a Enigma. Partendo dal metodo di Rejewski, Turing progettò una nuova macchina per decifrare Enigma.

La **“macchina di Turing”** (la “bomba”, poi “Colossus”) può essere definita il primo Computer della storia.
A partire dall'agosto 1940 gli inglesi riuscirono a decifrare i messaggi crittografati dei tedeschi.

La Crittografia moderna

Esistono due classi di algoritmi crittografici che si basano sull'utilizzo delle CHIAVI:

Crittografia simmetrica (a chiave privata) perché utilizza la stessa chiave k per le operazioni di cifratura e decifrazione. Un algoritmo di questo tipo è il DES (Data Encryption Standard).

Crittografia asimmetrica (a chiave pubblica o a doppia chiave) perché utilizza due chiavi differenti:

- la chiave di cifratura
- la chiave di decifratura.

Il più noto tra gli algoritmi a chiave asimmetrica è RSA.

Crittografia simmetrica (a chiave singola)

VANTAGGI: poco onerosa computazionalmente.

SVANTAGGI: il principale problema della crittografia simmetrica sta nella necessità di disporre di un canale sicuro per la trasmissione della chiave.

Crittografia asimmetrica a doppia chiave (Diffie-Hellman)

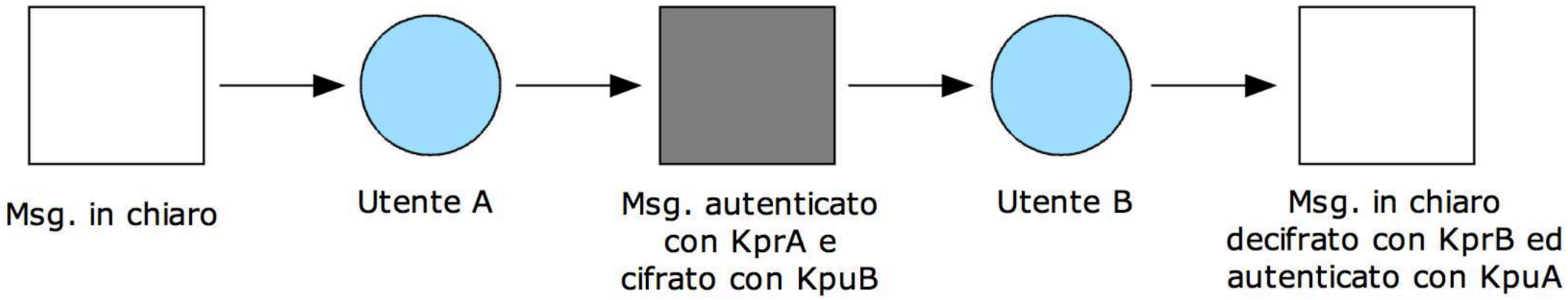
L'algoritmo Diffie-Hellman per lo scambio delle chiavi fu creato nel 1976 dai ricercatori Whitfield Diffie e Martin Hellman.

È il primo algoritmo a chiave pubblica della storia.

È stato creato per eliminare il problema dello scambio delle chiavi di cifratura su di un canale insicuro di comunicazione.

Non è un algoritmo di crittografia, ma esclusivamente un algoritmo di scambio delle chiavi.

Crittografia asimmetrica a doppia chiave (Diffie-Hellman)



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A
KprB = chiave privata dell'utente B
KpuB = chiave pubblica dell'utente B

VANTAGGI: lo scambio delle chiavi non è più critico (anzi può essere pubblica), sicurezza sull'autenticità del mittente.

SVANTAGGI: maggior onere computazionale.

RSA: algoritmo di crittografia asimmetrica

L'algoritmo **RSA** (dal nome degli inventori Rivest, Shamir e Adleman) è il più famoso algoritmo di **crittografia a chiave pubblica.**

Inventato nel 1977, poco dopo l'algoritmo di Diffie-Hellman, è uno degli algoritmi più usati per la cifratura di firme digitali.

Svantaggio: l'algoritmo RSA non è veloce, viene utilizzato soprattutto nei sistemi crittografici ibridi che utilizzano contemporaneamente sia algoritmi simmetrici che algoritmi a chiave pubblica (come ad esempio nei software PGP e GNUPG).

RSA: algoritmo di crittografia asimmetrica

È basato su tecniche di teoria dei numeri: prodotto di due numeri primi di dimensioni elevate (ad esempio **1024 bit**: $2^{1024}=1,797x10^{308}=>$circa 300 cifre decimali).

La sicurezza del sistema è basata sul fatto che è difficile fattorizzare un prodotto di due numeri primi di dimensioni elevate (allo stato attuale…).

La lunghezza delle chiavi di cifratura va da 1024 bit a 4096 bit (consigliato almeno 2048 bit).

Due componenti principali:

1. Algoritmo di generazione delle chiavi
2. Algoritmo crittografico vero e proprio

Advanced Encryption Standard (AES)

Conosciuto come **Rijndael** e sviluppato Joan Daemen e Vincent Rijmen. Questo algoritmo ha vinto la selezione per l'**Advanced Encryption Standard (AES)** il 2 Ottobre 2000.

Ufficialmente il Rijndael è stato adottato dalla National Institute of Standards and Technology (NIST) ed è diventato lo standard per la cifratura del XXI secolo. Ha sostituito il DES.

Il cifrario utilizza chiavi di lunghezza variabile: 128, 192, 256 bit (256 bit per i doc. “Top secret”).

Funzioni di HASH

Funzione crittografica di hash: è un algoritmo matematico che trasforma dei dati di lunghezza arbitraria (*messaggio*) in una stringa binaria di dimensione fissa (p.es. 160 bit) chiamata *valore di hash*, ***impronta*** *del messaggio* o ***checksum***. Gli algoritmi usati devono essere unidirezionali (one-way), quindi **non invertibili.**

CARATTERISTICHE della funzione di Hash:

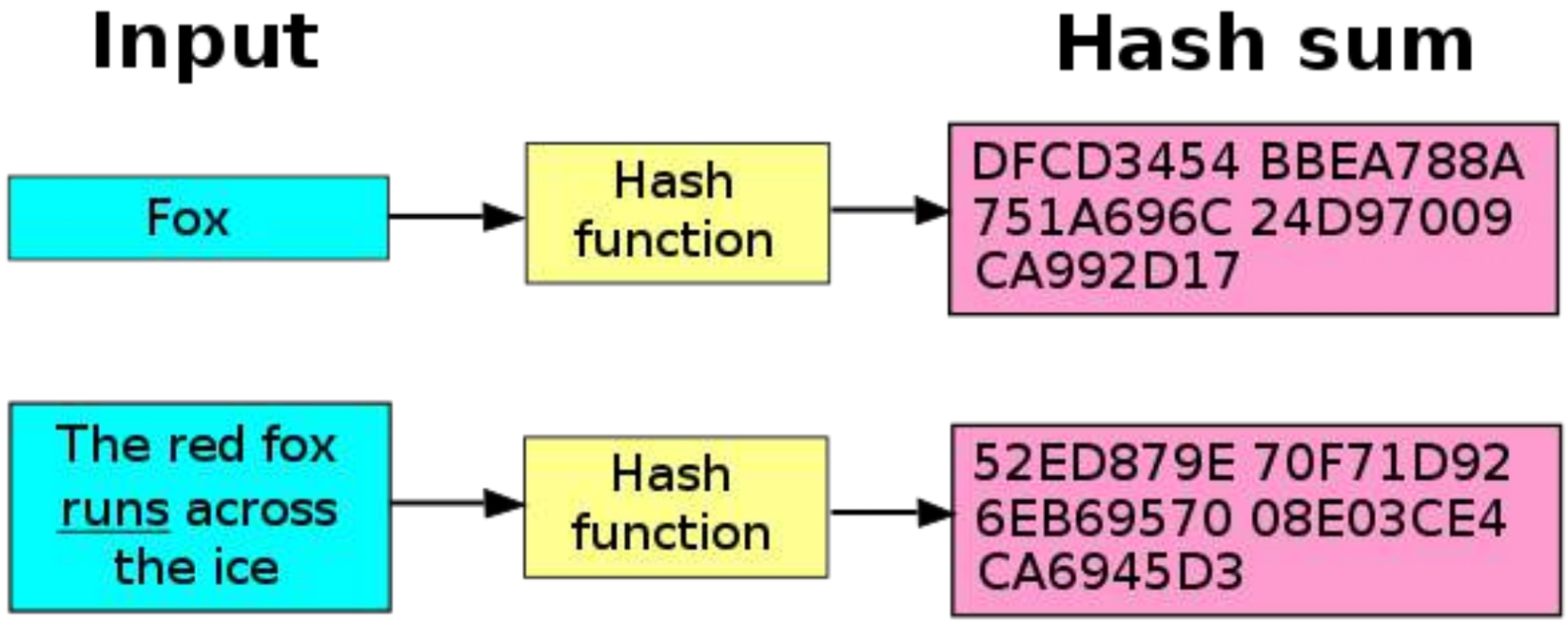
- **coerente** (quindi dare risultato univoco)
- **casuale** (impossibile da interpretare)
- **univoca** (la probabilità che due messaggi diversi generino lo stesso hash deve essere nulla, si parla di “resistenza alle collisioni”)
- **non invertibile** (deve essere impossibile risalire al messaggio originale)

Funzioni di HASH: MD5, SHA-1, SHA-2

Algoritmi di HASH utilizzati:

- **MD5** ("Message Digest"): genera una fingerprint da 128 bit (32 caratteri esadecimali). Sviluppato da Ronald Rivest. Ormai abbandonato, perché non sicuro.
- **SHA-1** ("Secure Hash Algorithm 1"): genera una fingerprint da 160 bit. È l'algoritmo di hash standard adottato dalla NSA (National Security Agency).
- **SHA-2** ("Secure Hash Algorithm 2"): è la varianti più sicura di SHA-1, con dimensioni dell'hash maggiori, da 256 (64 esadecimali) a 512 bit, contro i 160 di SHA-1.
- **SHA-3**: è in fase di progettazione, per diventare il nuovo standard.

Funzioni di HASH: esempio



Anche piccole modifiche ai dati di ingresso causano una notevole cambiamento dell'uscita: si tratta del cosiddetto **effetto valanga.**

Funzioni di HASH: utilizzo

Gli hash sono una sorta di "**impronta digitale**" a lunghezza fissa di un messaggio. Sono utili in diversi settori applicativi:

- **Controllo degli errori** ("checksum error")
- **Verifica dell'integrità di un messaggio:** per garantire che un messaggio non sia stato modificato da un eventuale attaccante, per controllare l'integrità dei file critici di un sistema operativo.
- **Firme digitali**: firmare l'intero documento è computazionalmente pesante => si firma solo un hash del documento.
- **Memorizzazione di password**: la password non viene salvata in chiaro per motivi di sicurezza, né viene cifrata per evitare che sia possibile risalire alla password originale. Si memorizza in questi casi l'hash della password.
- **Identificativo di File o Dati**: per identificare un file senza doverlo salvare per esteso.

Agenda

1. La crittografia
2. **Email e sistemi di Messaggistica istantanea**
3. Attacchi hacker: alcuni casi famosi
4. Le reti WI-FI: problemi di sicurezza
5. Imparare ad usare le Password
6. L'autenticazione a due fattori (MFA)
7. Il Backup
8. Conclusioni

L’email NON è uno strumento sicuro

L’Email fu inventata nel 1972 da Ray Tomlinson.

Tutti noi la usiamo, ma è uno degli strumenti più antiquati e vulnerabili del web.

Ancora oggi l’email “tradizionale” utilizza il **protocollo SMTP (Simple Mail Transfer Protocol)** che è il protocollo standard per la trasmissione via internet delle email.

Si tratta di un **protocollo testuale**, relativamente semplice, creato negli anni ’80 e da allora rimasto sostanzialmente invariato.

L’email non è uno strumento sicuro: lo SPOOFING

Tra le molte limitazioni dell’SMTP c’è quella che non è in grado di gestire l’autenticazione del mittente.

Ciò rende possibile - ed anche abbastanza facile! - inviare email falsificando il mittente.

SPOOFING: Modifica di una informazione, ad esempio l’indirizzo mittente di un pacchetto IP

Una Email sicura: come fare?

Sarebbe possibile **crittografare** le email che si inviano e si ricevono, ma solo se ambedue i provider del servizio email supportano la crittografia TLS (con il protocollo HTTPS).

La crittografia del 100% delle email trasmesse su Internet richiederebbe la collaborazione di tutti i fornitori di servizi email online.

In realtà solo alcuni provider rispondono ai suddetti requisiti: uno di questi, il più noto, è Gmail di Google.

Una Email sicura: la crittografia PGP

PGP (PRETTY GOOD PRIVACY)

è stato originariamente creato nel 1991 da Philip R. Zimmermann.

Originariamente concepito come uno strumento per i diritti umani, da PGP è nato poi **OpenPGP**, che è uno standard Internet "open source" (definito secondo RFC4880) per l'interoperabilità dei messaggi protetti tramite **crittografia asimmetrica** (detta "**a chiave pubblica**"), basato sulla generazione di **una coppia di chiavi**, una "privata" ed una "pubblica" che non coincidono.

http://www.giorgiosbaraglia.it/lemail-ai-tempi-di-snowden-usare-la-posta-crittografata/

PGP (PRETTY GOOD PRIVACY)

VANTAGGI:

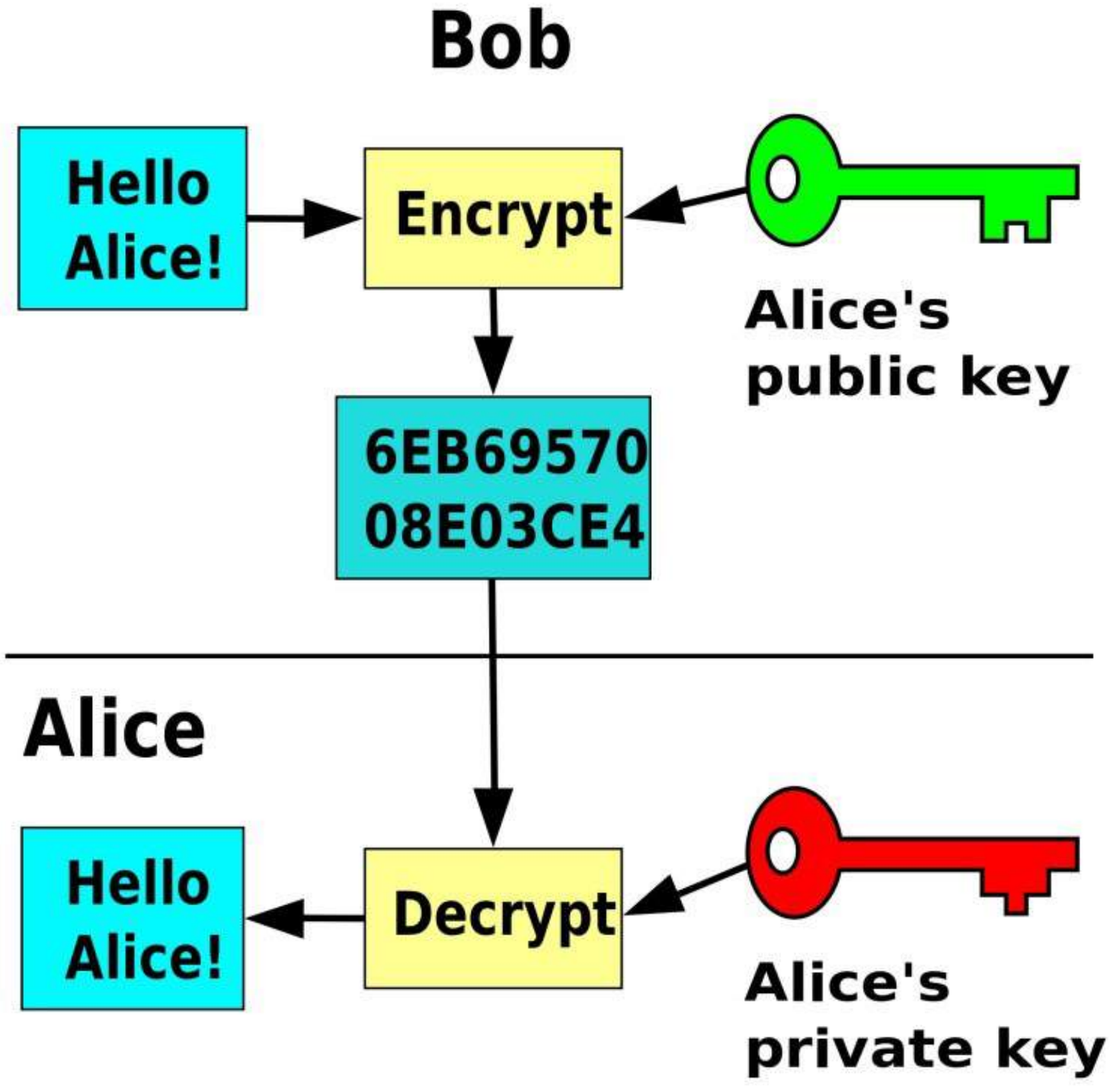
- **è un sistema "ibrido: a doppia chiave RSA** (non occorre una chiave segreta in possesso sia del mittente che del destinatario) e a **chiave simmetrica (DES)**.
- **riservatezza del contenuto**: il messaggio viene crittografato e reso illeggibile per un terzo che non possegga le chiavi.
- **autenticità del mittente**: ci dà la certezza della provenienza del messaggio.

SVANTAGGI:

- deve essere usato contemporaneamente da mittente e destinatario.

http://www.giorgiosbaraglia.it/lemail-ai-tempi-di-snowden-usare-la-posta-crittografata/

Come funziona PGP



Per usare la posta PGP

Non è difficile: basta installare un software che operi in PGP e che “lavori” per noi:

- **Gpg4win** (per Windows)
- **GPGTOOLS** (per macOS)
- **Enigmail** (per il client di posta Mozilla Thunderbird)
- **Guardian project** e **OpenKeychain** (per Android)
- **iPGMail** e **Hushmail** (per iOS)

Il sito ufficiale di OpenPGP: openpgp.org/software/
e quello di GnuPG: https://www.gnupg.org

La Messaggistica istantanea (IM)

Quando comunichiamo, sempre più spesso scegliamo le chat (gli sms sono quasi scomparsi).
E i sistemi di IM stanno iniziando a offrire un sistema di cifratura «end-to-end» integrato nella messaggistica.

Quanto sono sicuri?

EFF Electronic Frontier Foundation, associazione che si occupa della difesa dei diritti della Rete li ha analizzati:

https://www.eff.org/node/82654

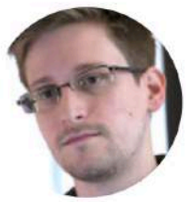
La Messaggistica istantanea (IM)

	Crittografia end-to-end	Crittografia: provider non può accedere	È verificata identità interlocutore?	Sicurezza in caso di furto chiavi	Il codice è accessibile per analisi?	C'è stata un'audit indipendente?
BBM (BlackBerry)	✅	🚫	🚫	🚫	🚫	🚫
Facebook Messenger	✅	🚫	🚫	🚫	🚫	✅
iMessage (Apple)	✅	✅	🚫	✅	🚫	✅
Signal (Open Whisper)	✅	✅	✅	✅	✅	✅
Skype (Microsoft)	✅	🚫	🚫	🚫	🚫	🚫
SnapChat	✅	🚫	🚫	🚫	🚫	✅
Telegram	✅	🚫	🚫	🚫	✅	✅
Viber	✅	🚫	🚫	🚫	🚫	✅
WhatsApp	✅	✅	✅	✅	🚫	✅

Il più sicuro è SIGNAL

Realizzato da Open Whisper Systems per iOS ed Android

Consigliato da:



“ Use anything by Open Whisper Systems.

— **Edward Snowden**, Whistleblower and privacy advocate

“ Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.

— **Laura Poitras**, Oscar winning filmmaker and journalist

“ I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.

— **Bruce Schneier**, internationally renowned security technologist

Gli SPYWARE su smartphone

Per il cybercrime è più utile spiare il dispositivo piuttosto che rubarlo.

SPYWARE: è un'applicazione di monitoraggio (spionaggio!) che viene installata su uno smartphone all'insaputa del proprietario.

Può essere installata:

1) con **accesso diretto al dispositivo.**

2) **da remoto:** le tecniche per riuscire ad installare l'app (con tutti i permessi necessari) passano ancora una volta attraverso il **phishing**, il **social engineering** e la **navigazione Web**. Spesso viene usato lo **spoofing** per scrivere a nome di un amico, collega, che consiglia l'utilizzo una "stupenda" app. Analogamente a come avviene per i Ransomware si spinge la vittima ad installare un'app.

Gli SPYWARE su smartphone

Tramite la connettività lo spyware invia all'esterno una serie di informazioni:

- Rubrica telefonica e email
- SMS ricevuti
- Contenuto della casella di posta
- Storico delle chat (es. WhatsApp)
- Registrazioni audio
- Registrazioni video
- Immagini da fotocamera
- Tutto ciò che viene digitato
- Ogni file presente in memoria

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. **Attacchi hacker: alcuni casi famosi**
4. Le reti WI-FI: problemi di sicurezza
5. Imparare ad usare le Password
6. L’autenticazione a due fattori (MFA)
7. Il Backup
8. Conclusioni

Gli attacchi Hacker hanno colpito anche società famose

- **Yahoo!:** 500 milioni di account rubati (marzo 2014, messi in vendita nel 2016 da hacker “Peace”)
- **Dropbox:** 68 milioni di account rubati (violazione 2012, pubblicazione agosto 2016)
- **Twitter:** 32 milioni di password rubate (giugno 2016, da hacker russi).
- **LinkedIn:** 117 milioni di password ed email sul Dark Web (2012, poi messi in vendita nel 2016)
- **Ashley Madison:** pubblicati su rete TOR 37 milioni di nomi, indirizzi e carte di credito (luglio 2015).
- **Hacking Team** : 400 GB di dati pubblicati online via torrent (luglio 2015)
- **Hyatt Hotel:** Carte di credito violate (fine 2015). Prima anche Hilton e Starwood
- **ESA** European Space Agency (2015)
- **Target:** violate 40 milioni di carte di credito e debito (2014)
- **Gmail, Google+** (settembre 2014)
- **Sony Pictures:** Corea del Nord? O hacker LulzSec? (fine 2014)
- **Ebay** (marzo 2014)
- **Spotify:** attacco hacker su Android (maggio 2014)
- **NASA** (hacker Gary McKinnon, 2012)

Alcuni dei principali furti di dati emersi di recente

SITO	N. profili coinvolti	Data presunta attacco/leak	Data diffusione dati leak	Protezione password
Last.fm	43.570.999	2012	agosto 2016	MD5 senza salt
Dropbox	68.680.737	2012	agosto 2016	SHA1 con salt/BCRYPT
Badoo	127.343. 437	/	giugno 2016	MD5 senza salt
MySpace	360. 213. 024	2013	maggio 2016	SHA1 con salt
LinkedIn	167.370. 910	2012	maggio 2016	SHA1 senza salt
Tumblr	65. 469. 298	2013	maggio 2016	SHA1 con salt

In rosso: i casi in cui la protezione della password (Hash) lasciava più a desiderare.

Fonti: https://haveibeenpwned.com
https://www.vigilante.pw

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. Attacchi hacker: alcuni casi famosi
4. **Le reti WI-FI: problemi di sicurezza**
5. Imparare ad usare le Password
6. L’autenticazione a due fattori (MFA)
7. Il Backup
8. Conclusioni

L'importanza del protocollo HTTPS

IMPORTANTE: I siti sicuri (quelli da usare per dati riservati o pagamenti on-line) devono operare con il protocollo **HTTPS** invece di HTTP.

HTTPS è un protocollo che integra il protocollo standard HTTP con un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS). Questa tecnica aumenta il livello di protezione contro attacchi tipo "**man in the middle (MITM)**".

Digitate username e password solo se state utilizzando una connessione sicura

Un minaccia: reti Wi-Fi “free”

Pineapple Mark V

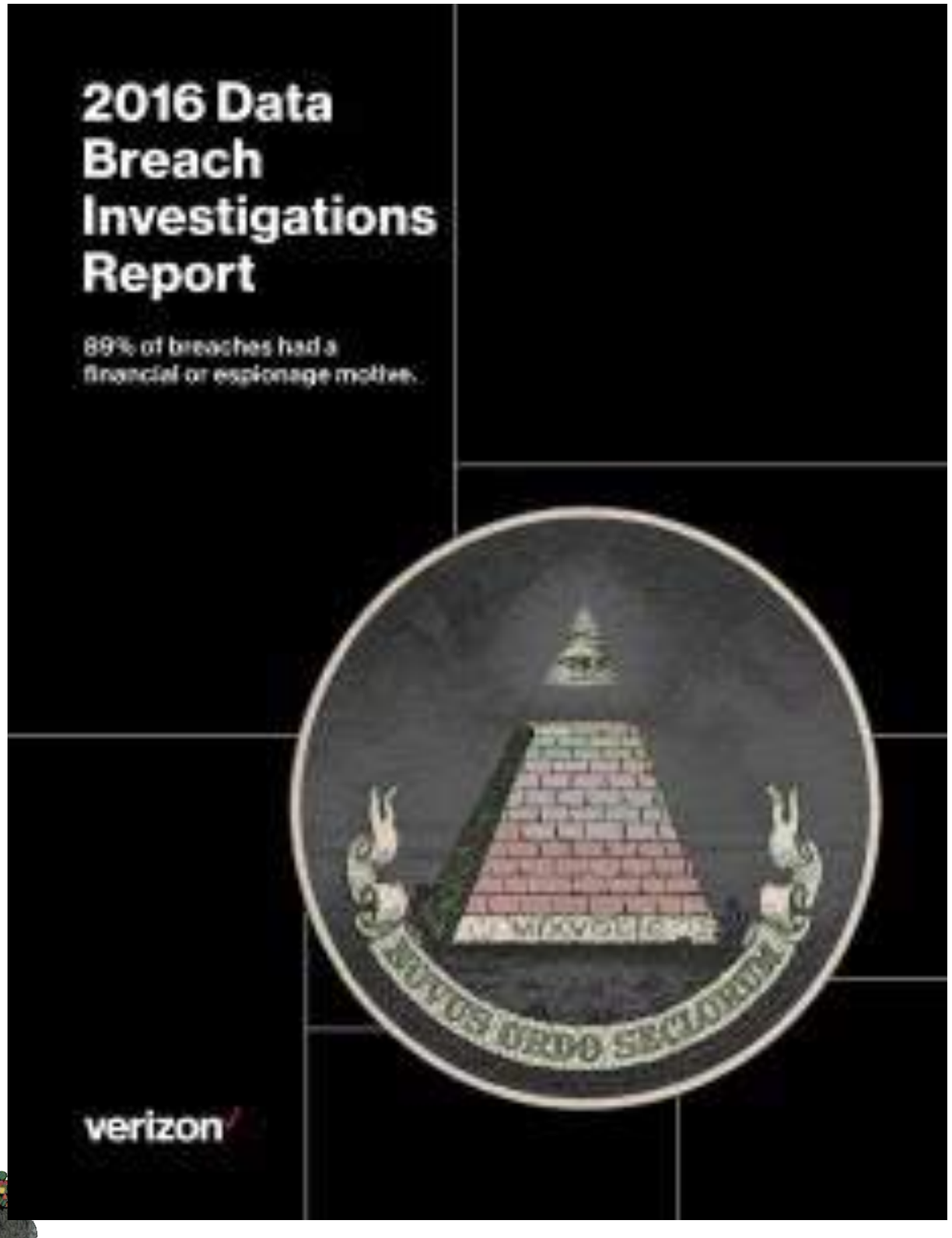
Pineapple Mark V è un dispositivo prodotto da Hak5, acquistabile per 99,99 $. Dotato di due schede di rete Wifi e semplici tools: Kali Linux e Wireshark (per catturare i pacchetti di dati), permette all’hacker di creare un **fake access point** (“free” e malevolo!). Si possono eseguire attacchi tipo **Man In the Middle** (MITM) in modalità Wifi ed eseguire phishing e furto di credenziali.

Le vittime sono gli utenti che si collegano alla rete Wifi creata da Pineapple ed i cui dati vengono “sniffati”.

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. Attacchi hacker: alcuni casi famosi
4. Le reti WI-FI: problemi di sicurezza
5. **Imparare ad usare le Password**
6. L’autenticazione a due fattori (MFA)
7. Il Backup
8. Conclusioni

Verizon Data Breach Investigations Report 2016



Le **password deboli** sono la causa del **63%** delle violazioni degli account

Ma le persone continuano ad usare password molto banali

La classifica delle password più utilizzate nel mondo (ed anche le peggiori!) nel 2016:

(Fonte: SPLASH DATA azienda statunitense specializzata in software di gestione di password, che ha esaminato dati che contenevano oltre 3,3 milioni di parole chiave rubate.)

1. **123456** *(al primo posto dal 2013)*
2. password
3. 12345
4. 12345678
5. football
6. qwerty
7. 1234567890
8. 1234567
9. princess
10. 1234
11. login
12. welcome
13. solo
14. abc123
15. admin
16. 121212

Le password più usate nel mondo negli ultimi anni

	2011	2012	2013	2014
1°	password	password	123456	123456
2°	123456	123456	password	password
3°	12345678	12345678	12345678	12345
4°	qwerty	abc123	qwerty	12345678
5°	abc123	qwerty	abc123	qwerty
6°	monkey	monkey	123456789	123456789
7°	1234567	letmein	111111	1234
8°	letmein	dragon	1234567	baseball
9°	trustno1	111111	iloveyou	dragon
10°	dragon	baseball	adobe123	football

Alcuni nostri Account sono più importanti e critici

- ☑ Internet Banking e Carte di Credito
- ☑ Servizi Cloud
- ☑ Account E-mail
- ☑ ID Apple o Account Google

Se vengono violati, possiamo subire danni importanti:

- ☑ **Furto e/o distruzione di dati personali**
- ☑ **Blocco di servizi (E-mail, smartphones inutilizzabili…)**
- ☑ **Danno reputazionale (molto grave per le aziende)**
- ☑ Furto di identità

Caratteristiche di una PASSWORD

1. **NUMERO** di caratteri usati: da 1 a 20 (non serve andare oltre)
2. **TIPI** di caratteri usati:

   ☑ Numeri (0-9) = **10**

   ☑ Lettere (a-z, A-Z) = **52** (26 minusc. + 26 maiusc.)

   ☑ caratteri speciali da tastiera (# &%?^ ecc.) = **33**

TOTALE = 95 caratteri (codici ASCII dal 32 al 126)

Purtroppo in alcuni siti – irragionevolmente - vengono imposte delle LIMITAZIONI al numero dei caratteri e NON sono permessi i caratteri speciali

Quante sono le combinazioni possibili?

Consideriamo – per semplicità - una **Password di 4 caratteri:**

Solo NUMERI: 10^4 = 10.000 combinazioni

Solo LETTERE MINUSC.: 26^4 = 456.976 combinazioni

LETTERE MIN.+MAIUSC.: 52^4 = 7.311.616 combinazioni

NUMERI+LETTERE: 62^4 = 14.766.366 combinazioni

NUM.+LETT.+CAR.SPEC.: 95^4 = 81.450.625 combinazioni

Aumentando i tipi dei caratteri, il numero delle combinazioni cresce in modo ESPONENZIALE

Quanto tempo serve per scoprire una password con attacco “Brute Force”?

Con un computer in grado di provare
un miliardo di chiavi al secondo:

Password di 8 caratteri:	**Combinazioni**	**Tempo**
Solo Numeri (10^8)	1,0E+08	< 1 sec.
Lettere+numeri (62^8)	2,2E+14	2,5 giorni
Lett.+num.+car.spec. (95^8)	6,6E+15	1.576 giorni

Password di 12 caratteri:	**Combinazioni**	**Tempo**
Solo Numeri (10^{12})	1E+12	16 minuti
Lettere+numeri (62^{12})	3,2E+21	1.023 secoli
Lett.+num.+car.spec. (95^{12})	5,4E+23	17 milioni anni

L'ENTROPIA di una PASSWORD

I Crittografi usano il termine **ENTROPIA** (nozione introdotta nel 1948 da **Claude Shannon**) per riferirsi ad una misura matematica della complessità di una password. Una password con una maggiore entropia è più difficile da indovinare.

Se la password viene scelta con le stesse probabilità per ogni simbolo, ci sono N^L password possibili *(ove N=numero simboli possibili; L=lunghezza password).*

L'entropia H di una password è quindi:

➡ $H=\log_2(N^L) = L \times \log_2(N)$, *(ove $\log_2$=logaritmo in base 2).*

➡ Ovvero: H = L x (LogN/Log2) *(ove Log=logaritmo in base 10).*

Se si usano tutti i Simboli ASCII scrivibili/stampabili (che sono 95: codici decimali dal 32 al 126):

ENTROPIA H = L x 6,56986 **ove: $6{,}56986=\log_2(95)$**

L'ENTROPIA H si misura in BIT.

Per un corretto livello di sicurezza, la Password deve essere di almeno 64 bit di entropia.

Oltre 128 bit non è più necessario aumentare la dimensione della password in quanto l'aumento di sicurezza sarebbe "inutile".

Le regole per una PASSWORD SICURA

✅ **SEMPRE DIVERSA:** Non utilizzare la stessa password in account diversi (*"non puoi evitare che il tuo provider venga violato, ma puoi evitare che tutti i tuoi account vengano hackerati in un colpo solo a causa dell'utilizzo di una sola password"*).

✅ **LUNGA**: utilizzare almeno dodici caratteri.

✅ **MISTA:** lettere maiuscole e minuscole, numeri e caratteri speciali.

✅ **SENZA SENSO:** Non utilizzare nomi, parole o parti di parole che possono essere ritrovati automaticamente in un dizionario.

The only secure password is the one you can't remember

(https://www.troyhunt.com/only-secure-password-is-one-you-cant/)

Errori comuni da EVITARE

Password contenenti:

- Parole presenti su un dizionario in qualsiasi lingua.
- Sequenze o caratteri ripetuti. Esempi: 12345678, 222222, abcdefg, o lettere adiacenti sulla tastiera (qwerty).
- Parole scritte al contrario, errori comuni di ortografia e abbreviazioni.
- Modificazioni ovvie alla password.
- Informazioni personali o di familiari: nome, compleanno, numero di patente e di passaporto o informazioni analoghe.

The only secure password is the one you can't remember

Strumenti per testare la Robustezza di una Password

Se si vuole avere un'idea di quanto siano complesse le password che utilizziamo, si possono usare ***tool online*** per verificarne il livello di robustezza. Eccone alcuni:

KASPERSKY SECURE PASSWORD CHECKER

https://blog.kaspersky.com/password-check/

PASSWORD CHECKER di Microsoft

https://www.microsoft.com/it-it/security/pc-security/password-checker.aspx

PASSWORD METER

http://www.passwordmeter.com/

BetterBuys

https://www.betterbuys.com/estimating-password-cracking-times/

HOW SECURE IS MY PASSWORD?

https://howsecureismypassword.net/

***UN CONSIGLIO**: trattandosi di servizi online, fidarsi è bene, ma non fidarsi è meglio. Pertanto suggerisco di provare la password cambiando tutti o alcuni caratteri, senza alterare la "geometria" della password. La sicurezza della nostra vera password sarà uguale a quella verificata. ma non sarà stata messa in rete.*

NON usare le DOMANDE di (in)SICUREZZA

Alcuni siti utilizzano le

DOMANDE DI SICUREZZA PER IL RECUPERO DELLA PASSWORD

Esempi (reali!) di domande di “sicurezza” proposte dai siti:

- *Qual era il cognome da nubile di tua madre?*
- *Qual era il nome della scuola elementare?*
- *Il nome del tuo primo animale?*
- *La tua squadra del cuore?*

Le domande semplici non sono mai sicure (le risposte in genere sono molto facili) e chi ci conosce bene potrebbe facilmente sapere la risposta.

Oppure potrebbe bastare controllare l'account Facebook o Twitter di una persona e scoprire la risposta alla domanda di sicurezza.

Oppure: Domande difficili => risposte dimenticate!

Qual è la SOLUZIONE?

The only secure password is the one you can't remember *(TROY HUNT)*

Se – come abbiamo spiegato – l'unica password sicura è quella che non si può ricordare, qual è il modo più pratico e sicuro per gestire le proprie passwords?

Usare un PASSWORD MANAGER

I PASSWORD MANAGER

Generare password sicure non è mai semplice, ricordarle è ancora più difficile. Con il password manager, però, tutto diventa semplice e sicuro.

COSA SONO:

programmi e App che archiviano in modo sicuro e crittografato le credenziali di accesso ai servizi web in una sorta di cassaforte (VAULT) virtuale, rendendola disponibile all'utente quando ne avrà bisogno.

I PASSWORD MANAGER (2)

✅ I migliori PM sono “multipiattaforma”: disponibili per i sistemi Mac, Windows, iOS ed Android. Questo permette (ma non è un obbligo) di sincronizzare attraverso il Cloud (p.es. Dropbox) le password su ogni dispositivo su cui sono installati (computer, laptop o smartphone che sia).

✅ Protetti da una MASTER PASSWORD, che diventa perciò l’UNICA password che occorre ricordare.

I vantaggi dei PASSWORD MANAGER

- L'UNICA password che occorre ricordare è la **MASTER PASSWORD** per aprirli.
- Si possono memorizzare: username, password, dati delle carte di credito e molti altri dati.
- I dati memorizzati vengono crittografati con sistema di cifratura AES 256 bit (*Advanced Encryption Standard*), una tecnologia crittografica utilizzato come standard dal governo USA e che la NSA ritiene adatta per proteggere i documenti TOP SECRET.
- Proteggono dai Keylogger.
- Hanno la capacità di generare automaticamente password sicure e complesse.
- Hanno un sistema intelligente di riempimento automatico dei moduli nei siti web (non occorre perciò fare "copia/incolla" delle password).

Gli svantaggi dei PASSWORD MANAGER

I migliori PM sono affidabili e facili da usare.

L'unico vero inconveniente è:

SE DIMENTICHIAMO LA MASTER PASSWORD

A differenza degli altri account, non sarà possibile cliccare sul solito pulsante "Recupera password" per recuperare la chiave d'accesso!

PROPRIO PER RAGIONI DI SICUREZZA NON HANNO PROCEDURE DI RECUPERO DELLA MASTER PASSWORD DIMENTICATA (tranne qualche eccezione)

***Consiglio**: **appuntarsi la master password.** Potrà sembrare sbagliato, ma se si teme di dimenticarla, sarà meglio annotare la master password da qualche parte e riporla in un luogo sicuro e (possibilmente) inviolabile.*

I MIGLIORI PASSWORD MANAGER

Sono molti i PM disponibili, gratuiti o a pagamento.

I migliori PM “multipiattaforma” sono:

LastPass (https://lastpass.com/it/)

dashlane (https://www.dashlane.com/it)

Kaspersky (http://www.kaspersky.com/password-manager)

KeePass (open source) (http://keepass.info/)

keeper (https://keepersecurity.com/it_IT/)

PasswordBox (https://www.passwordbox.com/)

oneSafe (http://www.onesafe-apps.com/)

Ma il MIGLIORE PASSWORD MANAGER è: (IMHO…)

"I can say that 1Password is still the most well-rounded password manager on the market" *(Robert Mcginley Myers)*

Fonte: ***thesweetsetup.com***

1Password

Realizzato dalla canadese **AgileBits** (https://agilebits.com/onepassword)

- ☑ ha tutte le funzionalità richieste per un PM, ottimamente sviluppate e perfettamente integrate con i principali browser;
- ☑ ha un elevato grado di sicurezza (**AES 256 bits**) e “slow hash” con algoritmo di derivazione della chiave **PBKDF2** (Password Based Key Derivation Function 2);
- ☑ può sincronizzare i dati (le “Casseforti”) tra i differenti dispositivi attraverso Dropbox (o iCloud);
- ☑ supporta “one-time passwords (OTP)” utile per gli account che richiedono l’autenticazione a due fattori;
- ☑ Offre “**1Password for Teams**” per le aziende;
- ☑ offre un efficiente servizio di supporto ed un Blog (AgileBits Blog) che dà risposte agli utilizzatori.

“Liberating yourself from the tyranny of passwords”

(https://www.troyhunt.com/only-secure-password-is-one-you-cant/)

Liberatevi dalla tirannia delle password...
(con un Password Manager)

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. Attacchi hacker: alcuni casi famosi
4. Le reti WI-FI: problemi di sicurezza
5. Imparare ad usare le Password
6. **L’autenticazione a due fattori (MFA)**
7. Il Backup
8. Conclusioni

AUTENTICAZIONE A DUE FATTORI (MFA: Multi-Factor Authentication)

Rappresenta un'ulteriore sicurezza, probabilmente il sistema di protezione attualmente più sicuro.

Per autenticarsi a sistemi digitali (computer, bancomat o altro) ci sono tre diversi metodi:

1. **"Una cosa che sai"**, per esempio una password o il PIN.
2. **"Una cosa che hai"**, come uno smartphone o un token di sicurezza.

3. **"Una cosa che sei"**, come l'impronta digitale, il timbro vocale, l'iride, o altre caratteristiche biometriche.

Come funziona:

la MFA utilizza almeno due dei tre fattori sopra elencati

Dopo aver inserito la password del proprio account, sarà richiesto di digitare un **secondo *pin*** o ***codice personale*** da ottenere grazie allo smartphone (sotto forma di sms o tramite un'apposita applicazione) o tramite un token.

*A differenza della password, questo secondo codice è di fatto **inattaccabile**, perché generato in maniera casuale secondo un algoritmo ed ha una durata molto limitata nel tempo (solitamente 30÷60 secondi).*

I principali siti che offrono l'Autenticazione a due fattori

- Amazon
- Apple ID
- Dropbox
- Evernote
- Facebook
- Google
- LinkedIn
- Microsoft
- PayPal
- Twitter
- Yahoo! Mail
- Wordpress

Consigliabile utilizzarla per i servizi più importanti.

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. Attacchi hacker: alcuni casi famosi
4. Le reti WI-FI: problemi di sicurezza
5. Imparare ad usare le Password
6. L'autenticazione a due fattori (MFA)
7. **Il Backup**
8. Conclusioni

31 Marzo:
Giornata Mondiale del BACKUP

31 Marzo:
Giornata Mondiale del BACKUP

30% of people
have never backed up [1]

113 phones
lost or stolen every minute [2]

29% of disasters
are caused by accident [3]

1 in 10 computers
infected with viruses each month [4]

L'importanza del BACKUP

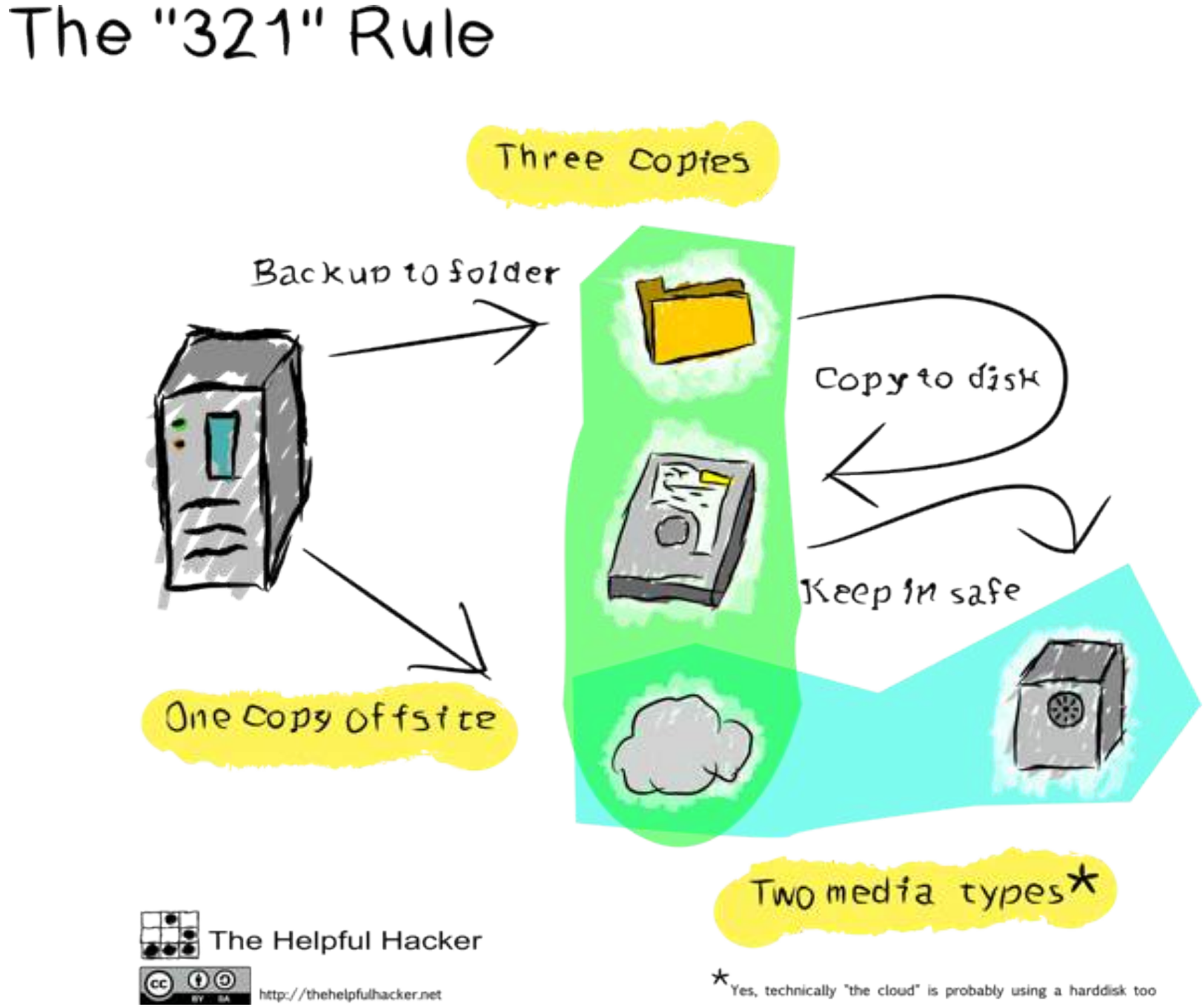
Per prevenire perdite di dati per qualsiasi ragione, fare sempre **copia di sicurezza dei propri dati (almeno il 30% degli utenti NON lo fa!).**

Un buon metodo:

3-2-1 Backup Strategy

- ✅ **3** copie di ogni dato che si vuole conservare (L'errore più frequente è la presenza di un'unica copia di backup)
- ✅ **2** copie "onsite" ma su storage differenti (HD, NAS, Cloud,…)
- ✅ **1** copia in sito remoto "off-site" (ev. Cloud)

3-2-1 Backup Strategy



NAS e sistemi RAID

NAS (Network Attached Storage) sono dei **veri e propri computer** (dotati solitamente di un sistema operativo basato su Linux) che collegandosi alla rete (casa, ufficio, ecc.) **permettono di archiviare e condividere dati e file con gli altri dispositivi**.

CAPACITÀ DI ARCHIVIAZIONE

Dipende dal numero di “Bay” (baie) che sono presenti sul NAS, ciascuna alloggia un HD. Un NAS può avere 2, 4, 6 o anche più alloggiamenti.

Lo spazio totale di archiviazione è inferiore alla somma dello spazio dei dischi inseriti (per il principio della Ridodanza).

NAS e sistemi RAID

RIDODANZA:

Uno dei principali strumenti dei NAS per evitare la perdita dati è la configurazione detta **RAID (Redundant Array of Independent Disks):** è un sistema usato in varie configurazioni per condividere o replicare informazioni tra un gruppo di dischi rigidi.

Va da RAID 1 (conf. minima) a RAID 6.
Permette di gestire senza perdita di dati l'avaria di 1 o 2 dischi.

La configurazione in RAID può ridurre lo spazio totale anche del 50%.

Agenda

1. La crittografia
2. Email e sistemi di Messaggistica istantanea
3. Attacchi hacker: alcuni casi famosi
4. Le reti WI-FI: problemi di sicurezza
5. Imparare ad usare le Password
6. L'autenticazione a due fattori (MFA)
7. Il Backup
8. **Conclusioni**

DIECI regole per la sicurezza

- ✅ Controllare che il sito sia in **HTTPS.**
- ✅ Impostare Password forti e sempre diverse.
- ✅ Non trascrivere le Password in foglietti o files.
- ✅ Non memorizzare le password nel browser.
- ✅ Utilizzare un PASSWORD MANAGER.
- ✅ Cambiare periodicamente le password.
- ✅ Non usare le “Domande di Sicurezza”.
- ✅ Usare l’Autenticazione a due fattori.
- ✅ Fare il BACKUP dei propri dati.

E soprattutto:

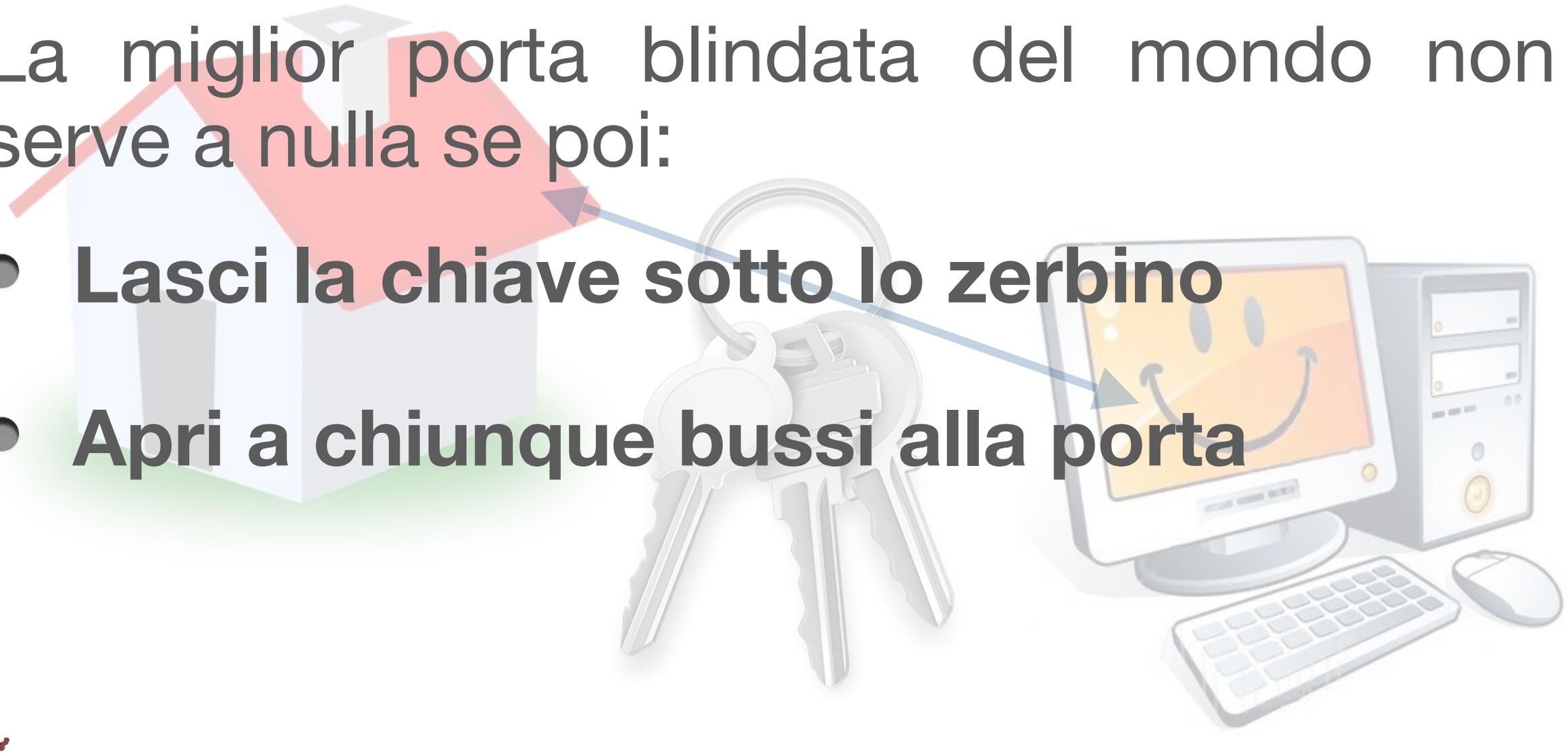
NON COMUNICARE LE PASSWORDS A NESSUNO

(amici, email di phishing, ecc…)

In Sintesi:
Sicurezza Computer come sicurezza Casa

La miglior porta blindata del mondo non serve a nulla se poi:

- **Lasci la chiave sotto lo zerbino**
- **Apri a chiunque bussi alla porta**



Il succo del discorso…

In ogni cyber attacco c’è sempre almeno un ERRORE UMANO

PEBKAC: “Problem Exists Between Keybord And Chair”

Grazie per l'attenzione

e … un consiglio:

8$U2dM:9H46@\qr!

giorgio@giorgiosbaraglia.it

334 6712113

www.giorgiosbaraglia.it

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica