

Autenticazione utente

Corso di Sicurezza
a.a. 2019-20

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

<http://www.di-srv.unisa.it/~ads>



Maggio 2020

Sommario

- Introduzione
- Password
- One-time password
- Challenge-Response
- Two-factor Authentication

Sistemi di autenticazione: principi



Pericoli



Sistemi di autenticazione: principi

Qualcosa che l'utente **POSSIEDE**

- cose fisiche o elettroniche, ...



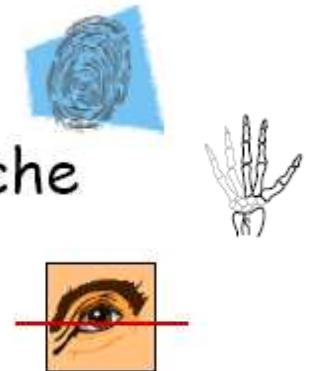
apriti
sesamo

Qualcosa che l'utente **CONOSCE**

- password, PIN,...

Qualcosa che l'utente **E'**

- **biometria**, cioè misura di proprietà biologiche

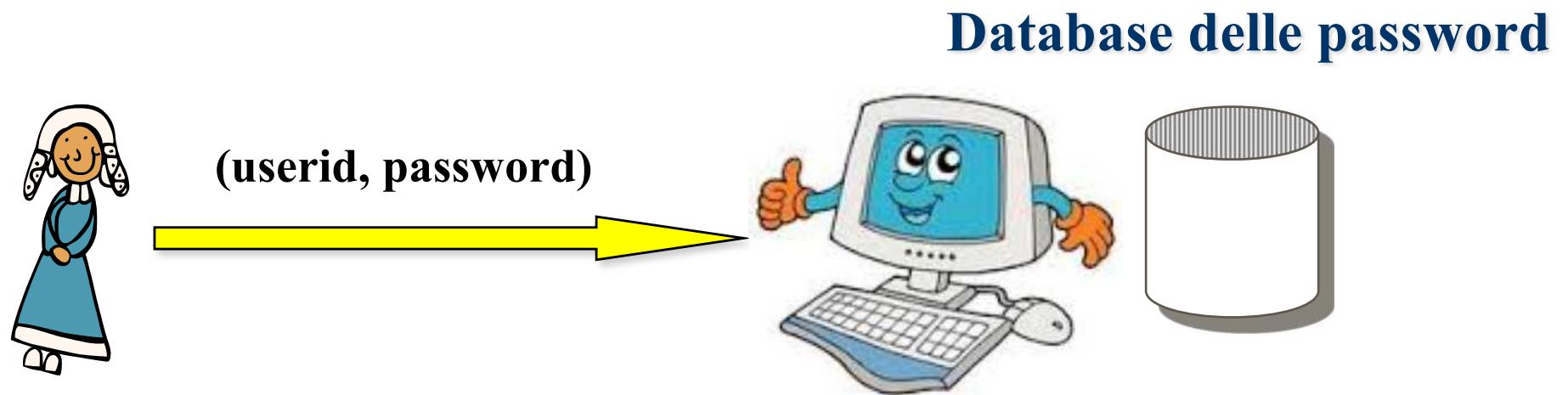


Caratteristiche

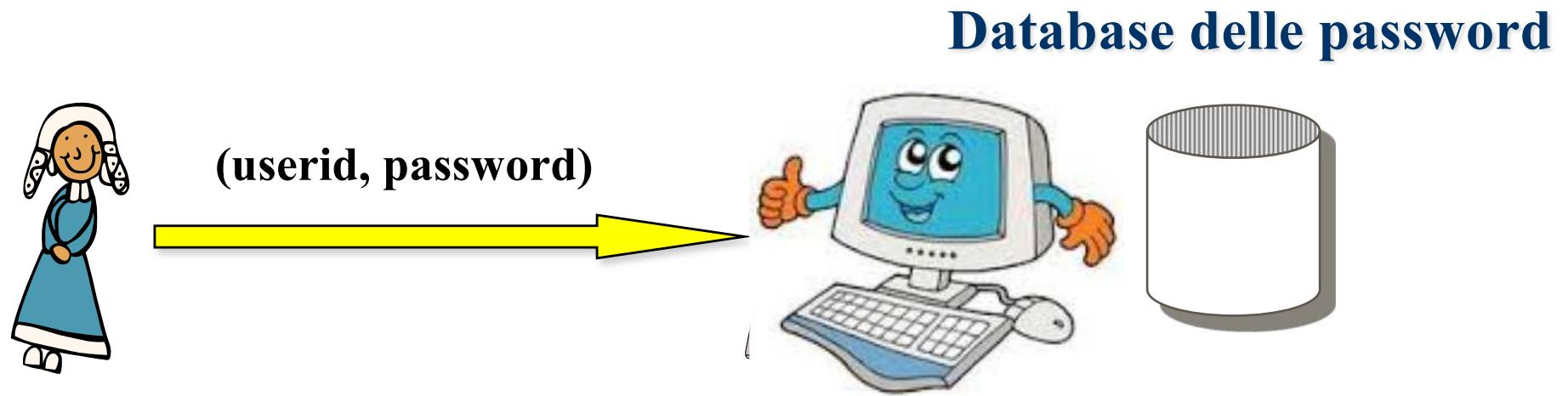
- Sicurezza
- Tempo dell'autenticazione (password, analisi DNA,...)
- Costo
- Complessità dell'update (riconoscimento vocale,...)
- Affidabilità e Mantenibilità
- Fattori psicologici:
accettabilità, facilità d'uso, ...



Password



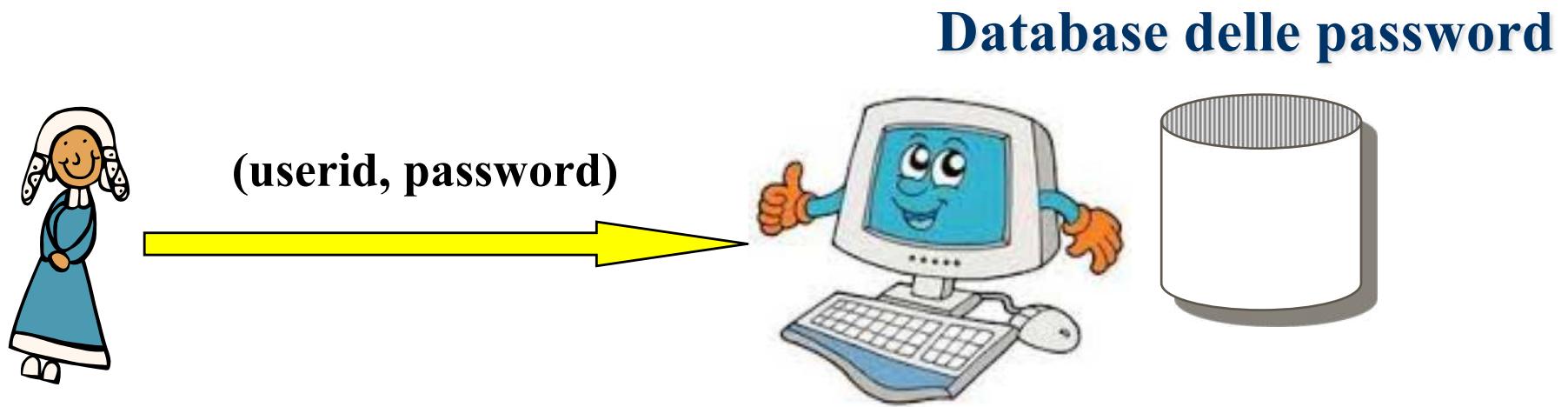
Password



Il sistema deve memorizzare una rappresentazione della password

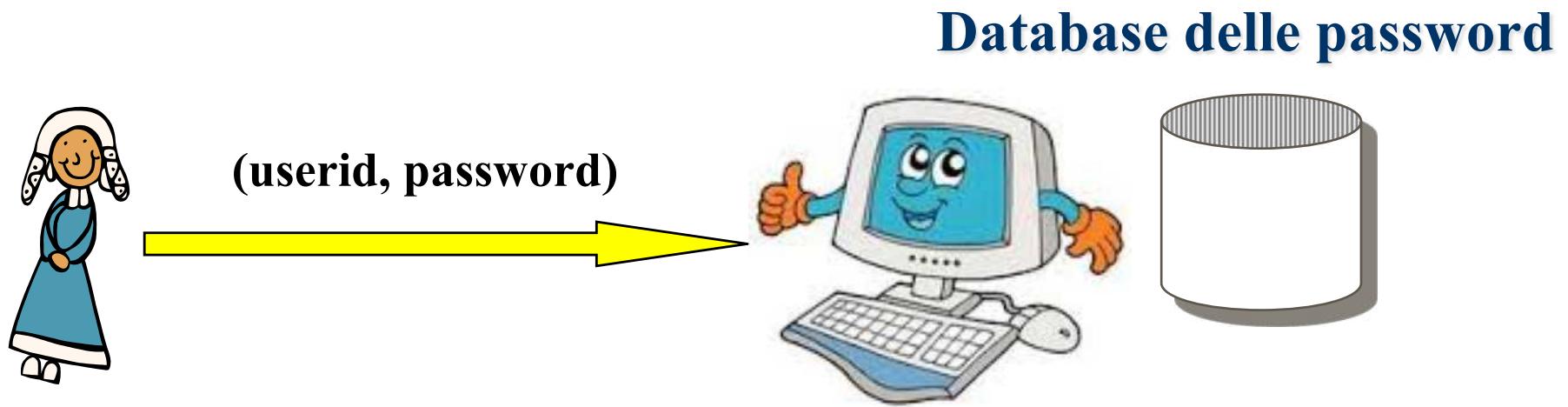


Password



Memorizzate in chiaro in un file protetto

Password



Memorizzate in chiaro in un file protetto

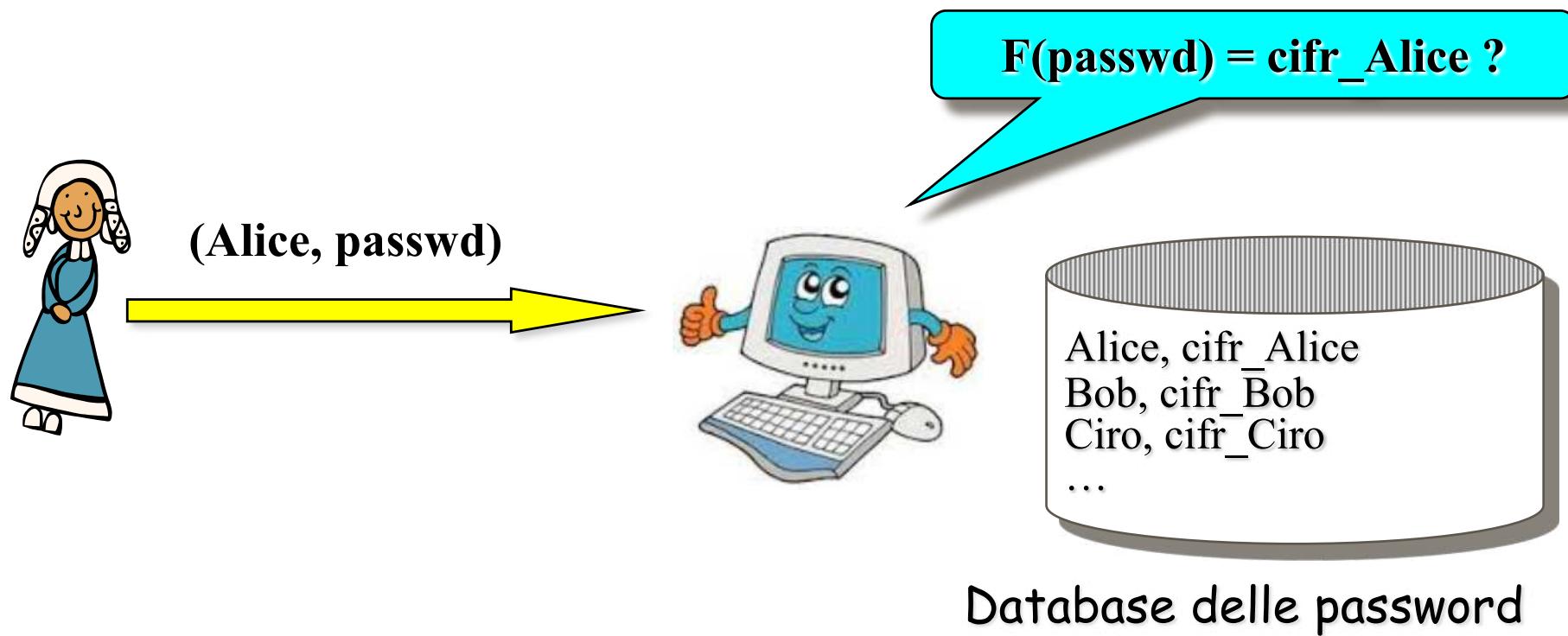
Problema:

nessuna protezione contro
chi riesce a leggere il file



Password

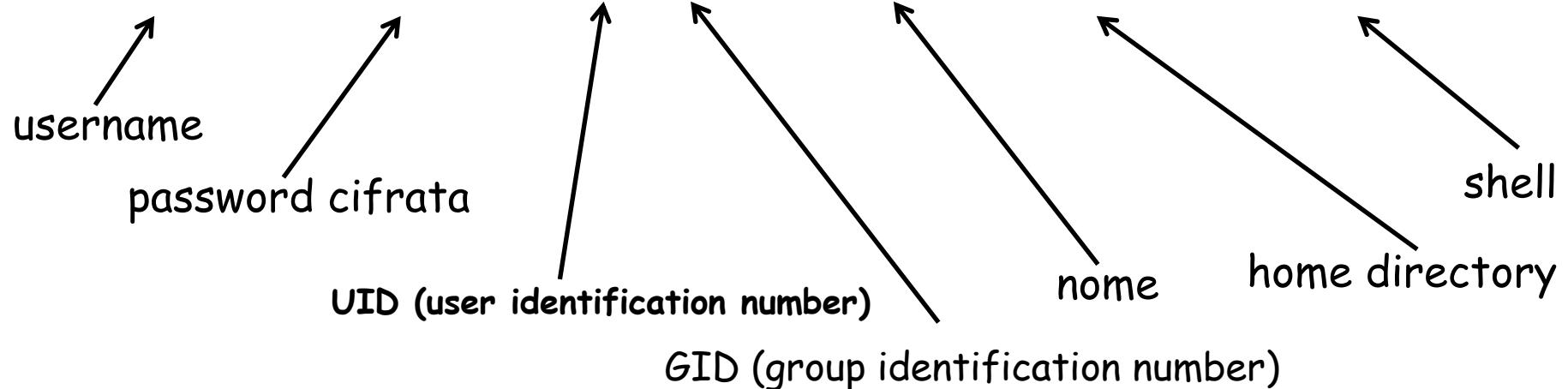
Memorizzate in forma cifrata



Password sotto UNIX

File */etc/passwd*

```
root:fi3sED95ibqR6:0:1:System Operator:/bin/ksh
daemon:*:1:1::/tmp
uucp:OORoMN9FyfNE:4:4:/var/spool/uucppublic:/usr/lib/uucp/uucico
ciro:eH5/.mj7NB3dx:181:100:Ciro Esposito:/u/ciro:/bin/ksh
```



Password sotto UNIX

Funzione di cifratura = variante del DES

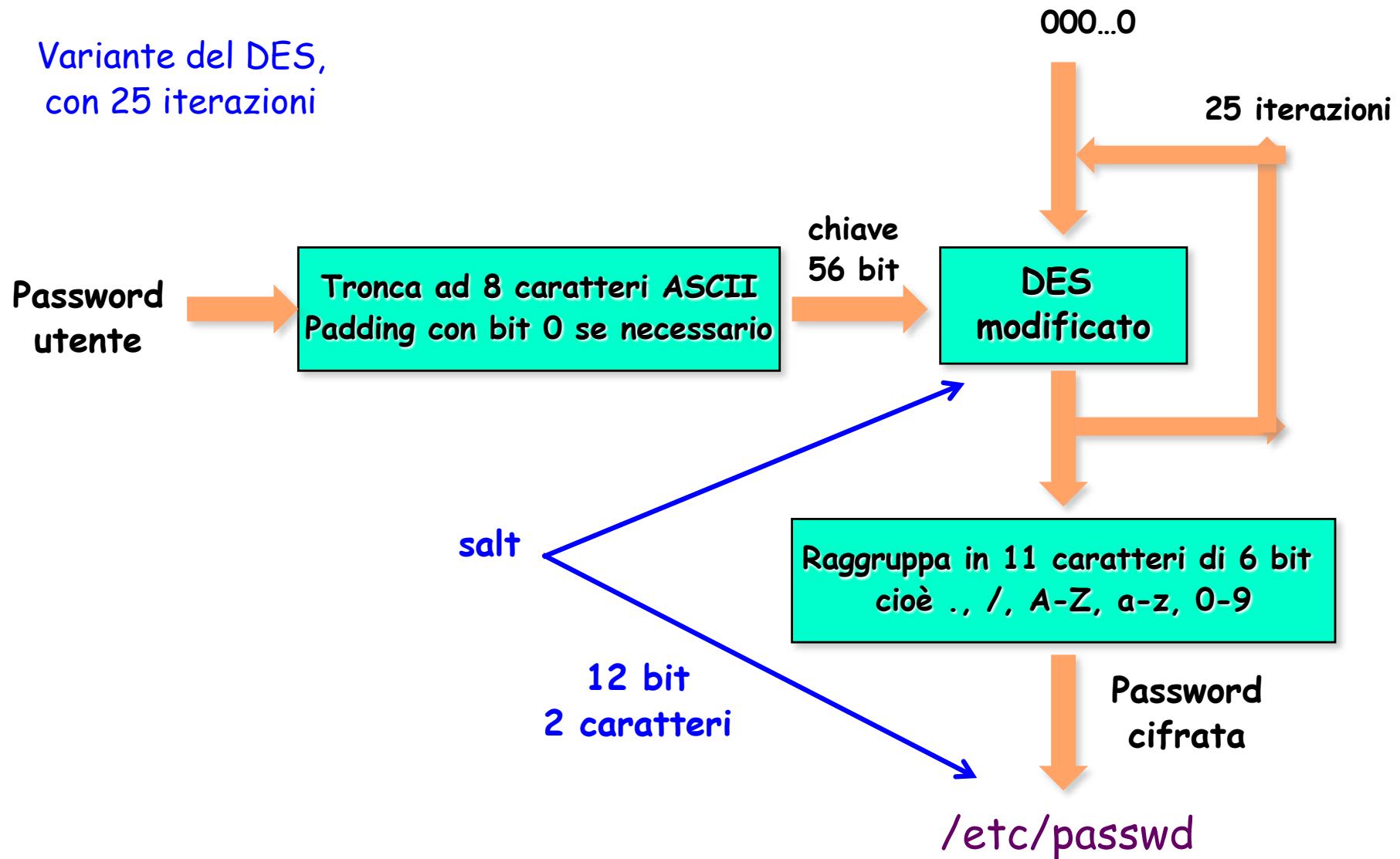
- Progettata da Robert Morris e Ken Thompson
- Evita la possibilità di usare chip DES disponibili commercialmente
- Evita che stesse password abbiano la stessa cifratura in diversi sistemi
- 25 iterazioni



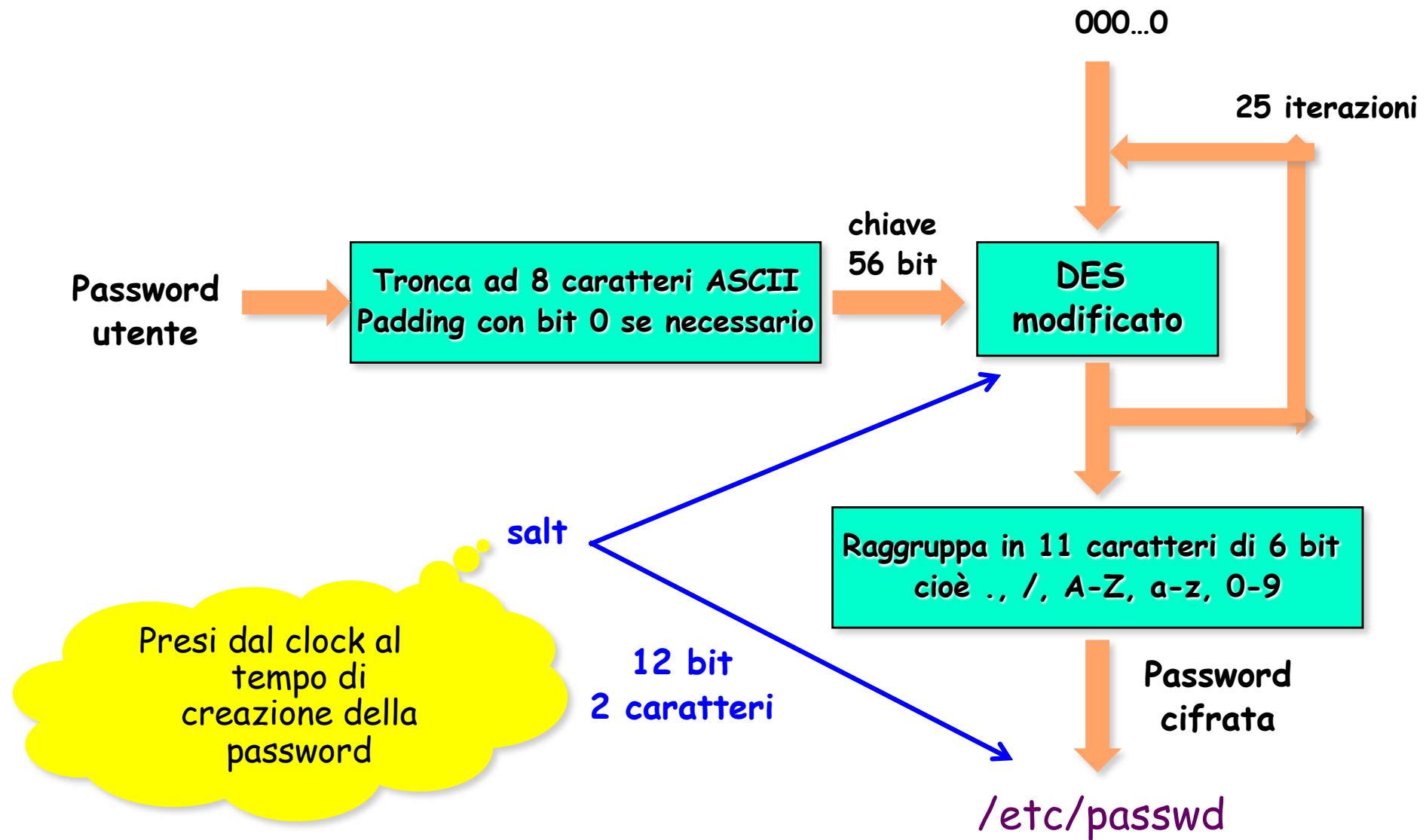
Maggiore difesa contro attacchi con dizionario

Funzione di cifratura crypt()

Variante del DES,
con 25 iterazioni



Funzione di cifratura crypt()



Password sotto UNIX

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

bit iniziali

bit dopo espansione

Espansione E
16 bit sono duplicati

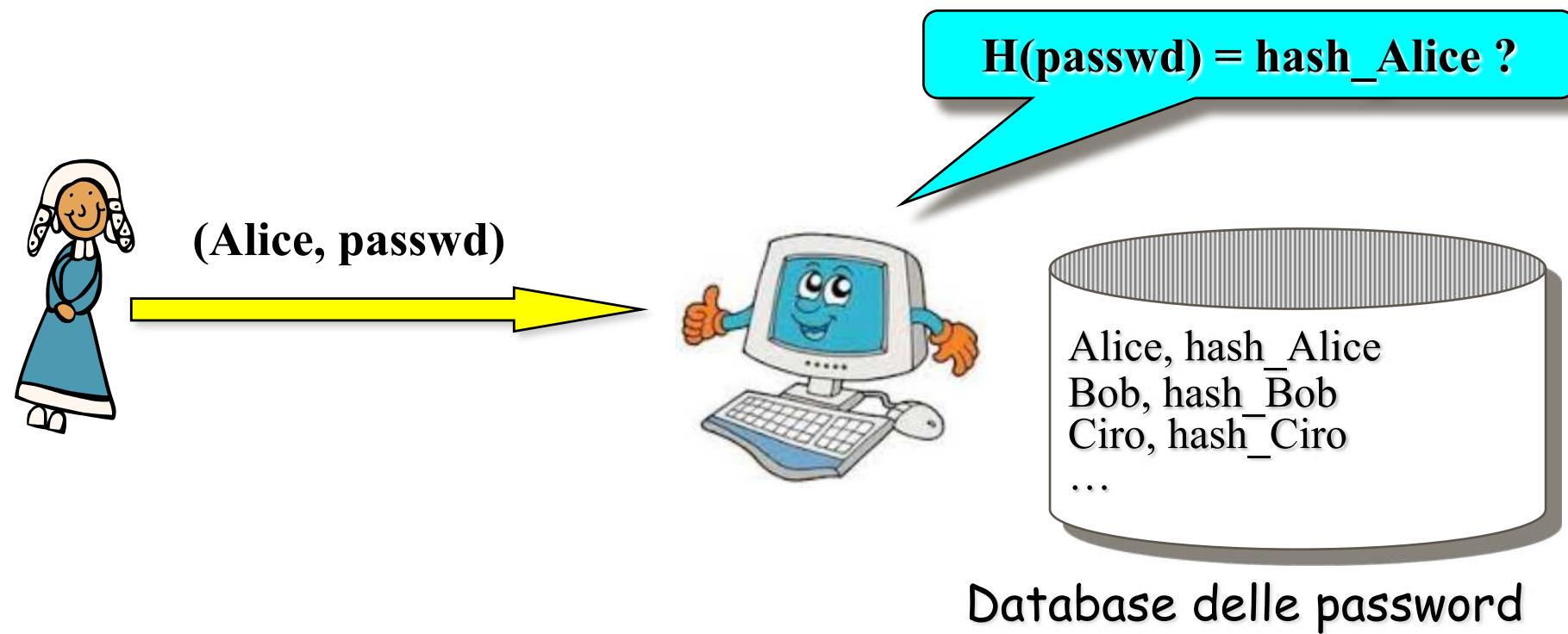
12 bit salt

- associati a 12 coppie (1,25), (2,26), (3,27),...
- Se bit salt =1 swap coppia corrispondente nei 48 bit output della tabella espansione E



Password

Memorizzato hash



Shadow Password

■

- Un cracker che ha in possesso il file delle password ha molte possibilità di intromettersi



- Difesa: utilizzare il sistema **shadow**:



- si sostituisce una 'x' alla password cifrata nel file "passwd"
- il file "shadow" contiene i cifrati ma è accessibile solo da root

Shadow password

```
masucci:x:500:100:Masucci Barbara:/home/masucci:/bin/bash
```

```
masucci:FeEQShVEhOlq6:10889:0:10000:::::
```

Ultima volta che la password è stata
cambiata, giorni trascorsi dal 1/1/1970

giorni dopo i quali la password
deve essere cambiata

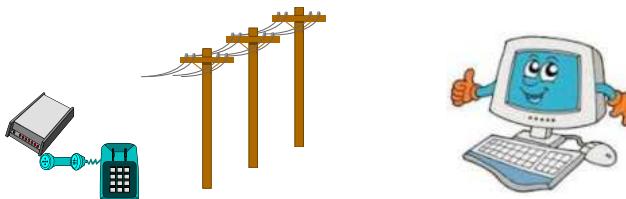
Giorni che devono trascorrere prima
che la password venga cambiata

Password: attacchi

Spiare durante la digitazione



Intercettazioni



Tentare a caso o sistematicamente

- In genere bassa entropia, quindi *deboli* password
- Attacchi con dizionario

Spiare password

- Video e poi riconoscimento automatico
- Successo 90% per Pin 4-digit da 3 metri
 - Anche se non visibili i punti di contatto
 - Google Glass, 83%
 - iPhone 5, 100%
 - \$72 Logitech webcam, 92%
- Successo 78% per password 8-caratteri su tastiera QWERTY di iPad

My Google glass see your password, Blackhat 2014

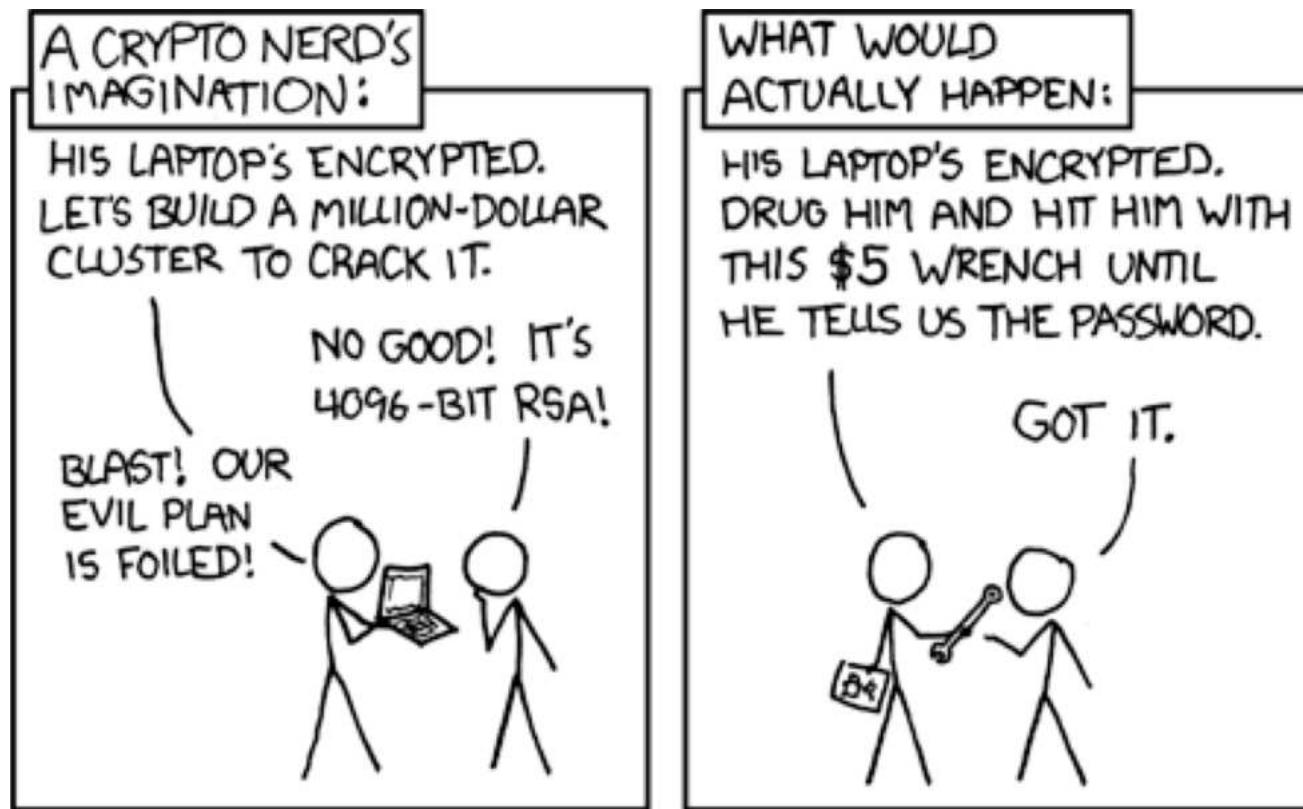
Spiare password

- \$700 Panasonic camcorder
- Successo 100% per pin di iPad



My Google glass see your password, Blackhat 2014

Altri attacchi



<http://xkcd.com/538/>

Altri attacchi



Drug dealer: Cops leaned me over 18th floor balcony to get my password

"This is *Training Day* for f—ing real."

by Nate Anderson · Apr 22, 2015 1:45pm CEST

[Share](#) [Tweet](#) 152

If you want access to encrypted data on a drug dealer's digital device, you might try to break the crypto—or you might just try to break the man.

According to testimony from a police corruption trial currently roiling the city of Philadelphia, officers from an undercover drug squad took the latter route back in November 2007. After arresting their suspect, Michael Cascioli, in the hallway outside his 18th floor apartment, the officers took Cascioli back inside. Although they lacked a search warrant, the cops searched Cascioli's rooms anyway. According to a [federal indictment](#) (PDF), the officers "repeatedly assaulted and threatened [Cascioli] during the search to obtain information about the location of money, drugs, and drug suppliers."

Cascioli kept \$800 of cash in his nightstand, which he told the cops about. The officers allegedly "took money from [Cascioli's] nightstand and used it to purchase pizza" for themselves.

Cascioli, who [gave an interview last October to the Philadelphia Daily News](#), said the cops wanted much more cash. (The trial has largely focused on allegations that members of the squad shook down drug suspects for money and valuables.) "I'm going to f—ing break your face if you don't tell us where the f— money is," Cascioli recalled one officer



[Enlarge](#) / Officer Thomas Liciardello, accused of being the ringleader of a corrupt undercover unit.

Ricerca esaustiva

Tempo richiesto per una ricerca esaustiva $T = c^n \cdot t \cdot y$

- c numero di possibili caratteri
- n lunghezza della password
- t numero di iterazione di hash/cifratura, $t = 25$
- y tempo richiesto per singola iterazione, $y = 1/125.000 \text{ sec}$

→ c	26	36 (minuscole)	62 (min. e maius.)	95
↓ n	(minuscole)	alfanumerici)	alfanumerici)	(caratteri tastiera)
5	0,67 ore	3,4 ore	51 ore	430 ore
6	17 ore	120 ore	130 giorni	4,7 anni
7	19 giorni	180 giorni	22 anni	442 anni
8	1,3 anni	18 anni	1385 anni	42.073 anni
9	34 anni	644 anni	85.852 anni	3.997.015 anni
10	895 anni	23.187 anni	5.322.801 anni	3.879.716.476 anni

Attacco con dizionario

- Si basa sulla possibilità che un utente utilizzi come password una parola di senso compiuto
- Tenta di “indovinare” una password utilizzando un file di parole (il dizionario)
- Il successo dipende dalla bontà del dizionario



Trovata passwd di Ken Thompson

- File /etc/passwd trovato nel 2014 con le passwd di Dennis Ritchie, Ken Thompson, Brian Kernighan, Steve Bourne, Bill Joy
- Passwd di Thompson cifrata con crypt(3): [ZghOT0eRm4U9s](#)
- Trovata la passwd: [p/q2-q4!](#)
- Insieme a Joe Condon costruì *Belle, chess computer world champion* nel 1980



From: Nigel Williams <nw@retrocomputingtasmania.com>
Cc: TUHS main list <tuhsm@minnie.tuhs.org>
Subject: Re: [TUHS] Recovered /etc/passwd files
Date: Wed, 9 Oct 2019 16:49:48 +1100
Message-ID: <CACCFpdx_6oeyNkgH_5jgfbxbWbZ6VtOXQNKOsO
In-Reply-To: <8088e5bd-3530-d3e1-8066-db6ea9389dea@k

ken is done:

ZghOT0eRm4U9s:p/q2-q4!

took 4+ days on an AMD Radeon Vega64 running hashcat at about 930MH/s during that time (those familiar know the hash-rate fluctuates and slows down towards the end).

Password Crackers

- Usano anche dizionari ed un insieme di regole modificabili dall'utente
- Richiede l'accesso al file delle passwd
- Il successo dipende dalla bontà del dizionario

Password Crackers

- Usano anche dizionari ed un insieme di regole modificabili dall'utente
- Richiede l'accesso al file delle passwd
- Il successo dipende dalla bontà del dizionario

Alcuni password crackers:

Crack

Brutus

RainbowCrack

Wfuzz

Cain and Abel

John the Ripper

Hashcat

Hydra

DaveGrohl

ElcomSoft

THC Hydra

Medusa

OphCrack

LOphtCrack

Aircrack-NG

Controllo della password

Per evitare cattive scelte come password

- Alcuni sys. admin. scelgono loro la password per gli utenti
- Uso di software per il controllo della scelta
Freeware per UNIX: npasswd, passwd+, anlpasswd,...
- Esempio vincoli:
 - min lunghezza
 - min numero caratteri alfabetici
 - min numero caratteri non-alfabetici
 - max numero caratteri ripetuti
 - elenco parole proibite
- **Password Crackers** per testare il file /etc/passwd

Vulnerabilità delle password

Morris e Thompson (CACM, 1979) esaminarono 3289 password trovandone 2831 (86%) vulnerabili tra cui:

- 15 erano un singolo carattere ASCII
- 72 erano una stringa di 2 caratteri ASCII
- 464 erano una stringa di 3 caratteri ASCII
- 477 erano una stringa di 4 caratteri alfanumerici
- 706 erano una stringa di 5 lettere tutte minuscole o tutte maiuscole
- 605 erano una stringa di 6 lettere tutte minuscole

Altre Vulnerabilità

Nomi comuni (Anna, Maradona,...)

Parole comuni (computer,...)

Specificità dell'utente (telefono, targa, date, indirizzi,...)

Permutazioni delle precedenti (a ritroso,...)

Il worm di Internet (novembre 1988) provava:

- nessuna password
- user name
- user name concatenato con se stesso
- cognome
- cognome a ritroso
- dizionario di 432 parole

Idee per scegliere una password

Usare minuscole e maiuscole

Usare numeri e lettere

Effettuare sostituzioni sistematiche, come $o \rightarrow 0$ $l \rightarrow 1$

Includere caratteri non alfanumerici

Scegliere lettere da una frase lunga

Lunga (7/8 caratteri)

Facile da ricordare (nessuna necessità di scriverla su carta!)

Esempi: DA.nMdCdNV qE'uC24o ...

Survey di Klein [1989]

Survey su circa 15.000 account

4 DECstation 3100

➤ ognuna provava 750 password al secondo

Dizionario di 62.727 parole

2.7% (cioè 368) trovate nei primi 15 minuti

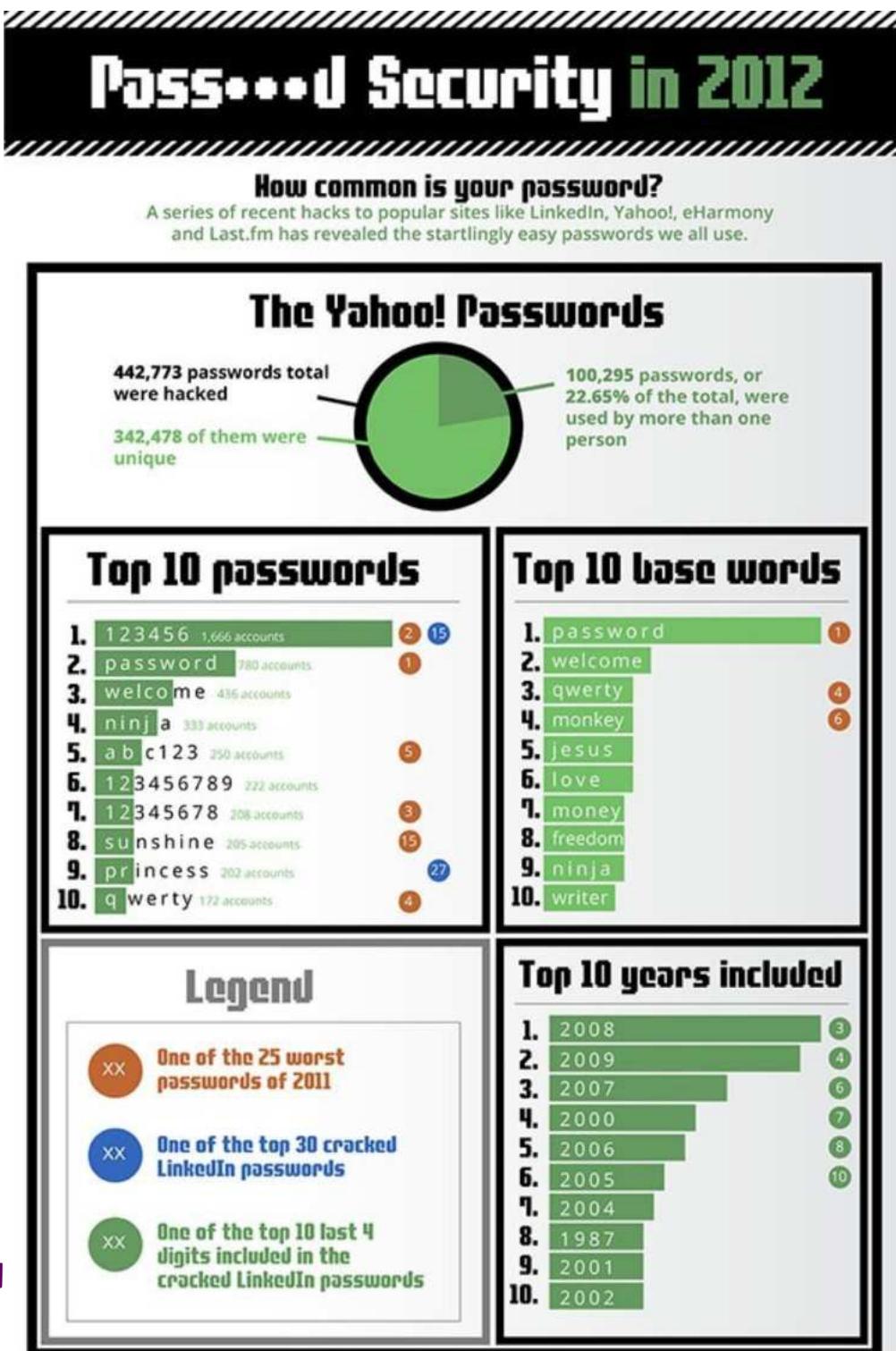
21% (circa 3000) trovate nella prima settimana

25% in 4 mesi

Password trovate

Tipo di password trovate	taglia	matches	% su totale
User/account name	130	368	2,7%
Sequenze caratteri	866	22	0,2%
Numeri	427	9	0,1%
Cinese	392	56	0,4%
Nome luoghi	628	82	0,6%
Nomi comuni	2239	548	4,0%
Nomi femminili	4280	161	1,2%
Nomi maschili	2866	140	1,0%
Termini sportivi	238	32	0,2%
Fantascienza	691	59	0,4%
Film e attori	99	12	0,1%
Cartoni animati	92	9	0,1%
Bibbia	7525	83	0,6%
...

Password facilitation



Password più frequenti nel 2019

Rank	Password
1	123456
2	123456789
3	qwerty
4	password
5	1234567
6	12345678
7	12345
8	iloveyou
9	111111
10	123123
11	abc123
12	qwerty123
13	1q2w3e4r
14	admin
15	qwertyuiop
16	654321
17	555555
18	lovely
19	7777777
20	welcome
21	888888
22	princess
23	dragon
24	password1
25	123qwe

SplashData, Dicembre 2019

<https://www.helpnetsecurity.com/2019/12/18/worst-passwords-of-2019/>

Password più frequenti nel 2019

Rank	Password
1	123456
2	123456789
3	qwerty
4	password
5	1234567
6	12345678
7	12345
8	iloveyou
9	111111
10	123123
11	abc123
12	qwerty123
13	1q2w3e4r
14	admin
15	qwertyuiop
16	654321
17	555555
18	lovely
19	7777777
20	welcome
21	888888
22	princess
23	dragon
24	password1
25	123qwe

And, just for reference, here were the 10 most common passwords of 2018:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

SplashData

<https://metro.co.uk/2019/12/19/10-worst-passwords-2019-revealed-nothing-changed-11932281>

Invecchiamento password

Cambiare la password migliora la sicurezza!

... non troppo spesso però! (immaginate ad ogni log in)

Fissare il tempo di vita di una password

- L'utente è costretto a cambiare password
- Migliora la sicurezza (se una password è compromessa...)

Per evitare il riutilizzo di vecchie password

- Memorizzare tutte le password di un utente
- Fissare un minimo tempo di uso per ogni password

SVR4 UNIX: **passwd -n 7 -x 50 ciro** (min 7 max 50 giorni)

Password-strength evaluators

Ci sono parecchie applicazioni che valutano la bontà della password ... prima che venga inserita

Password-strength evaluators

Email

Controlla la tua password: è complessa?

La protezione di conti online, file del computer e informazioni personali è maggiore se si utilizzano password complesse.

Verifica l'efficacia delle tue password: Digita una password nella casella di testo.

Password:

Strength:  Medium

Nota ciò non garantisce l'effettiva sicurezza della password. Si tratta di uno strumento fornito solo a scopo di riferimento.

security

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

Password-strength evaluators

Test Your Password		Minimum Requirements			
Password:	We5?\$\$a!				
Hide:	<input type="checkbox"/>				
Score:	100%				
Complexity:	Very Strong				
Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	$+(n*4)$	8	+ 32
✓	Uppercase Letters	Cond/Incr	$+((len-n)*2)$	1	+ 14
*	Lowercase Letters	Cond/Incr	$+((len-n)*2)$	2	+ 12
✓	Numbers	Cond	$+(n*4)$	1	+ 4
*	Symbols	Flat	$+(n*6)$	4	+ 24
*	Middle Numbers or Symbols	Flat	$+(n*2)$	4	+ 8
*	Requirements	Flat	$+(n*2)$	5	+ 10
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	$-(n*2)$	0	0
✓	Consecutive Lowercase Letters	Flat	$-(n*2)$	0	0
✓	Consecutive Numbers	Flat	$-(n*2)$	0	0
✓	Sequential Letters (3+)	Flat	$-(n*3)$	0	0
✓	Sequential Numbers (3+)	Flat	$-(n*3)$	0	0
✓	Sequential Symbols (3+)	Flat	$-(n*3)$	0	0
Legend					
*	Exceptional:	Exceeds minimum standards. Additional bonuses are applied.			
✓	Sufficient:	Meets minimum standards. Additional bonuses are applied.			
!	Warning:	Advisory against employing bad practices. Overall score is reduced.			
✗	Failure:	Does not meet the minimum standards. Overall score is reduced.			

Test Your Password		Minimum Requirements			
Password:	security				
Hide:	<input type="checkbox"/>				
Score:	10%				
Complexity:	Very Weak				
Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	$+(n*4)$	8	+ 32
✗	Uppercase Letters	Cond/Incr	$+((len-n)*2)$	0	0
*	Lowercase Letters	Cond/Incr	$+((len-n)*2)$	8	0
✗	Numbers	Cond	$+(n*4)$	0	0
✗	Symbols	Flat	$+(n*6)$	0	0
✗	Middle Numbers or Symbols	Flat	$+(n*2)$	0	0
✗	Requirements	Flat	$+(n*2)$	2	0
Deductions					
!	Letters Only	Flat	-n	8	- 8
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	$-(n*2)$	0	0
!	Consecutive Lowercase Letters	Flat	$-(n*2)$	7	- 14
✓	Consecutive Numbers	Flat	$-(n*2)$	0	0
✓	Sequential Letters (3+)	Flat	$-(n*3)$	0	0
✓	Sequential Numbers (3+)	Flat	$-(n*3)$	0	0
✓	Sequential Symbols (3+)	Flat	$-(n*3)$	0	0
Legend					
*	Exceptional:	Exceeds minimum standards. Additional bonuses are applied.			
✓	Sufficient:	Meets minimum standards. Additional bonuses are applied.			
!	Warning:	Advisory against employing bad practices. Overall score is reduced.			
✗	Failure:	Does not meet the minimum standards. Overall score is reduced.			

Telepathwo

Telepathwords

Preventing weak passwords by reading your mind



Microsoft Research

<https://telepathwords.research.microsoft.com>

Telepathwords tries to predict the next character of your passwords by using knowledge of:

- common passwords, such as those made public as a result of security breaches
- common phrases, such as those that appear frequently on web pages or in common search queries
- common password-selection behaviors, such as the use of sequences of adjacent keys

Is your password weaker than you thought?

To help you find out, the *Telepathwords* weak-password prevention system will try to guess each character of your password before you type it.

✗ indicates that the character you typed was one of Telepathwords guesses.

✓ indicates that the character you typed was one Telepathwords could not guess.

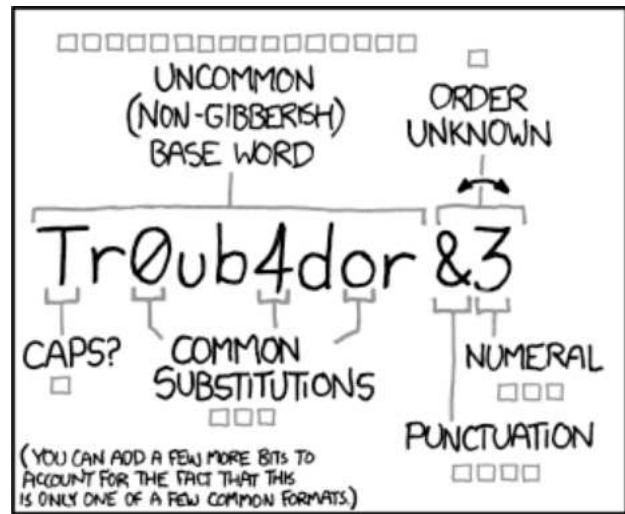
If your password has few characters that Telepathwords could not guess, attackers may also find your password easy to guess.

✓✓✓✓ (4 more ✓ marks needed)
newpa **S** as in newpagsword

Best guesses for the
next key you'll type

L as in newpaltz
P as in newpaper

Hide the keys that you type
 Show our guesses



~28 BITS OF ENTROPY

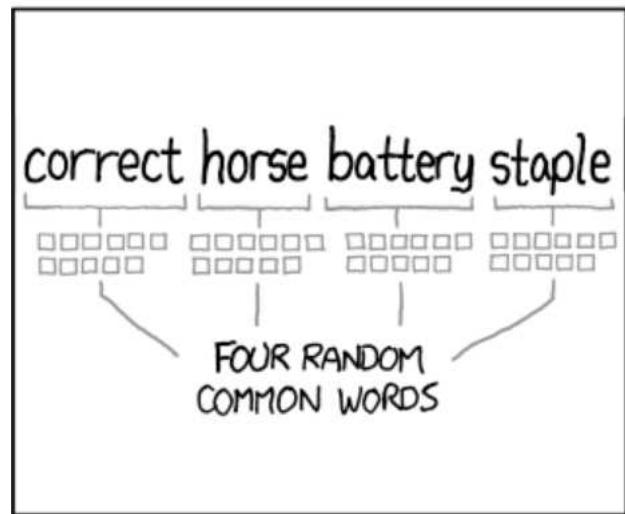
$2^{28} = 3$ DAYS AT 1000 GUESSES/SEC

(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.

<http://xkcd.com/936/>

CORRIERE DELLA SERA

10 aprile 2015

Gaffe della tv francese piratata da Isis Mandano in onda le password



13
13 HEURES

DAVID DE LOS

JOURNALISTE TV5 MONDE

Password di YouTube:
"lemotdepassedeyoutube"

La gaffe della tv francese piratata: tutte le password dietro all'intervistato

Certamente non era previsto: dopo l'attacco informatico di mercoledì sera alla televisione francese TV5Monde da parte di un gruppo di hacker che si richiama allo Stato Islamico, la redazione dell'emittente è incappata in una imbarazzante gaffe. Durante un'intervista col programma 13 Heures di France 2 (proprio sull'attacco hacker) un giornalista si è messo di fronte ad una parete sulla quale si vedono le password per il canale YouTube, Twitter e Instagram.

Social Engineering (People Are the Weak Security Link)



REUTERS

TOP NEWS

Exclusive: Snowden persuaded other NSA workers to give up passwords - sources

Thu, Nov 07 22:07 PM EST



By Mark Hosenball and Warren Strobel

WASHINGTON (Reuters) - Former U.S. National Security Agency contractor Edward Snowden used login credentials and passwords provided unwittingly by colleagues at a spy base in Hawaii to access some of the classified material he leaked to the media, sources said.

A handful of agency employees who gave their login details to Snowden were identified, questioned and removed from their assignments, said a source close to several U.S. government investigations into the damage caused by the leaks.

Snowden may have persuaded between 20 and 25 fellow workers at the NSA regional operations center in Hawaii to give him their logins and passwords by telling them they were needed for him to do his job as a computer systems administrator, a second source said.

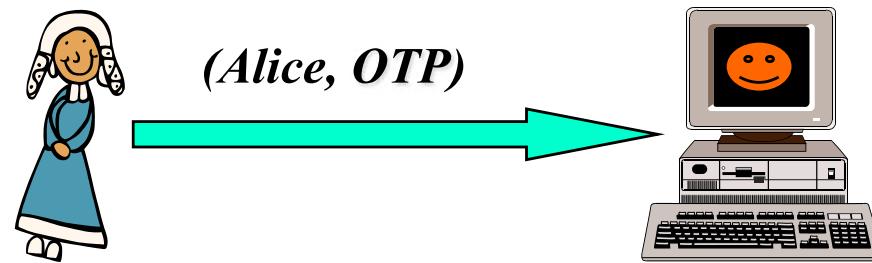
The revelation is the latest to indicate that inadequate security measures at the NSA played a significant role in the worst breach of classified data in the super-secret eavesdropping agency's 61-year history.

Sommario

- Introduzione
- Password
- One-time password
- Challenge-Response
- Two-factor Authentication

One-time Password

Ogni password è usata solo una volta!



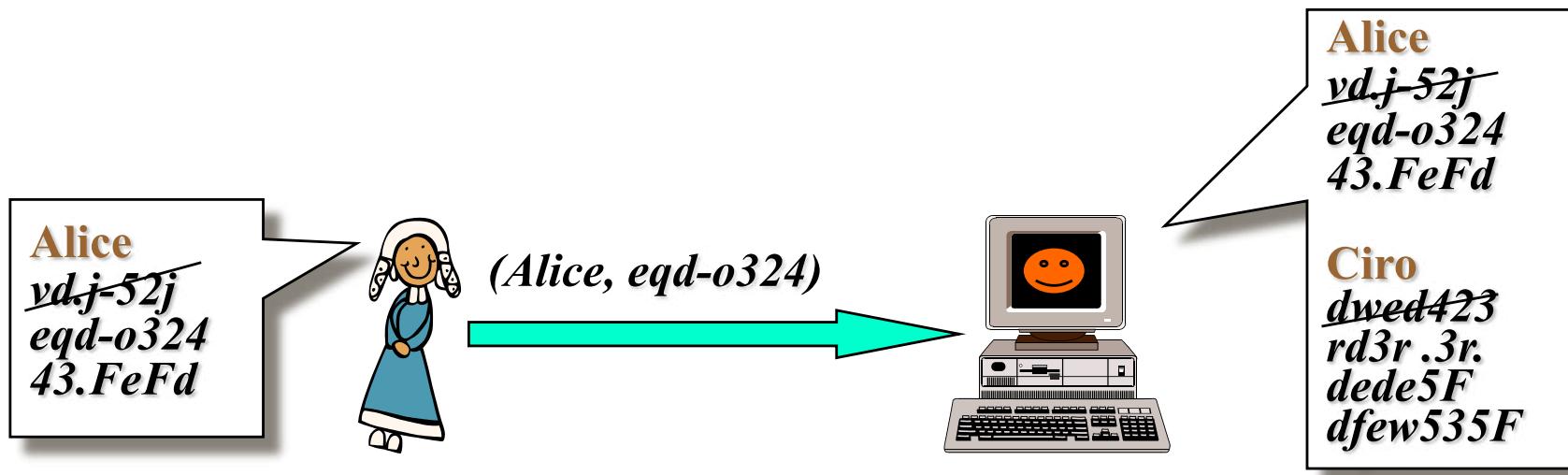
Vedremo:

- Lista condivisa
- Schema di Lamport
- HMAC-Based One-Time Password
- Time-Based One-Time Password

One-time Password

Ogni password è usata solo una volta!

Lista condivisa

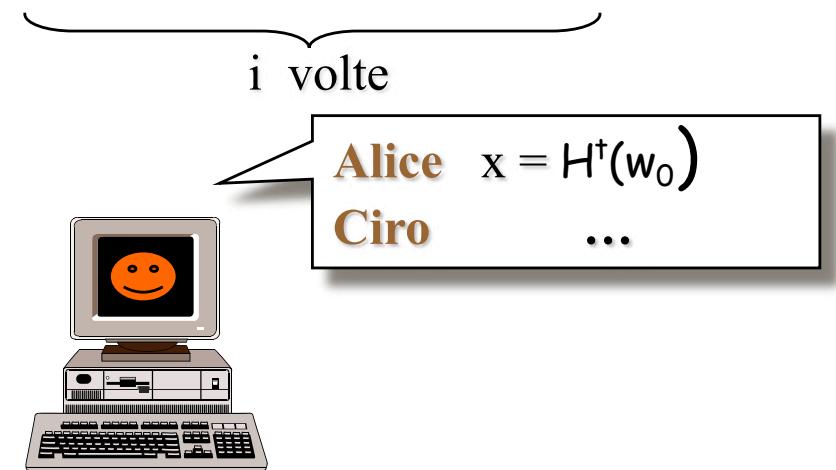
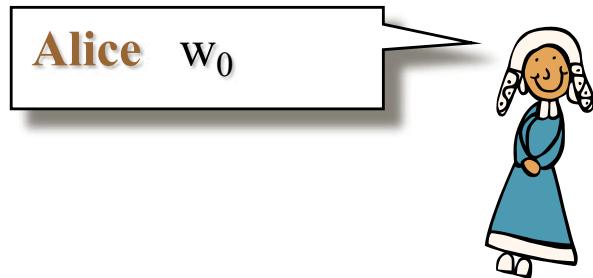


Schema di Lamport

Schema di Lamport per t autenticazioni (H funzione hash)

Alice sceglie w_0 . Sia $H^i(w_0) = H(H(\dots H(w_0)\dots))$

Inizializzazione



Schema di Lamport

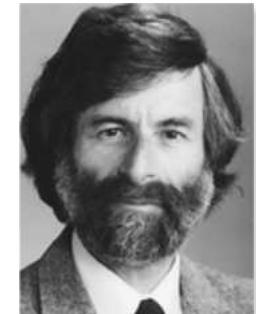
Schema di Lamport per t autenticazioni (H funzione hash)

Alice sceglie w_0 . Sia $H^i(w_0) = H(H(\dots H(w_0)\dots))$

Per l' i -esima autenticazione



Schema di Lamport



Leslie Lamport,

"Password Authentication with Insecure Communication"
Communications of the ACM, November 1981

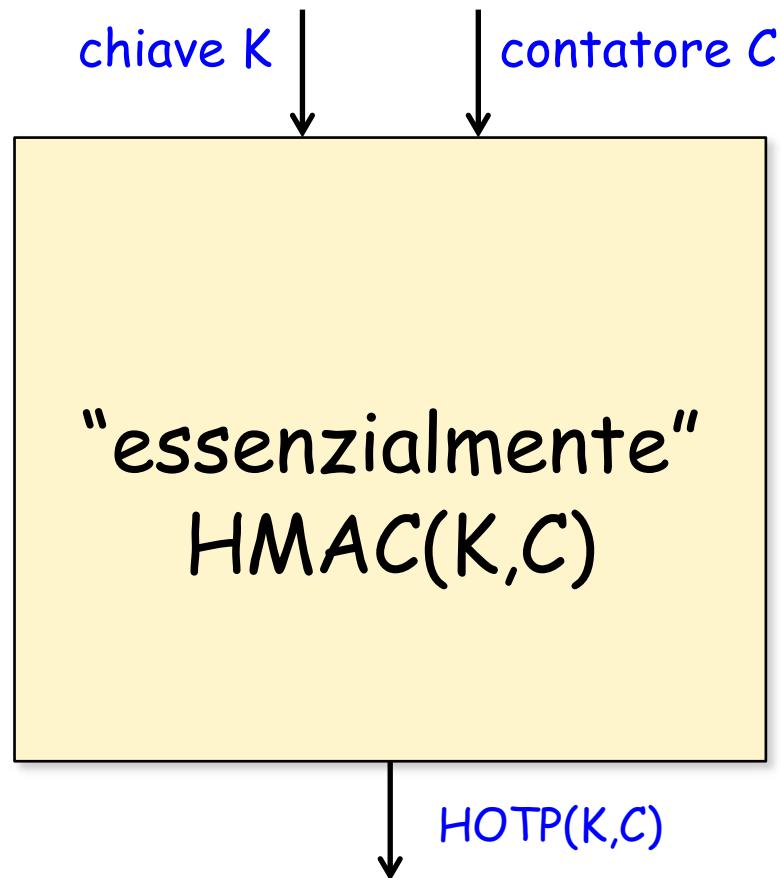
S/Key, sviluppato nei laboratori Bellcore

RFC 1760, The S/KEY One-Time Password System,
febbraio 1995

HMAC-Based One-Time Password Algorithm

Pubblicato come RFC 4226

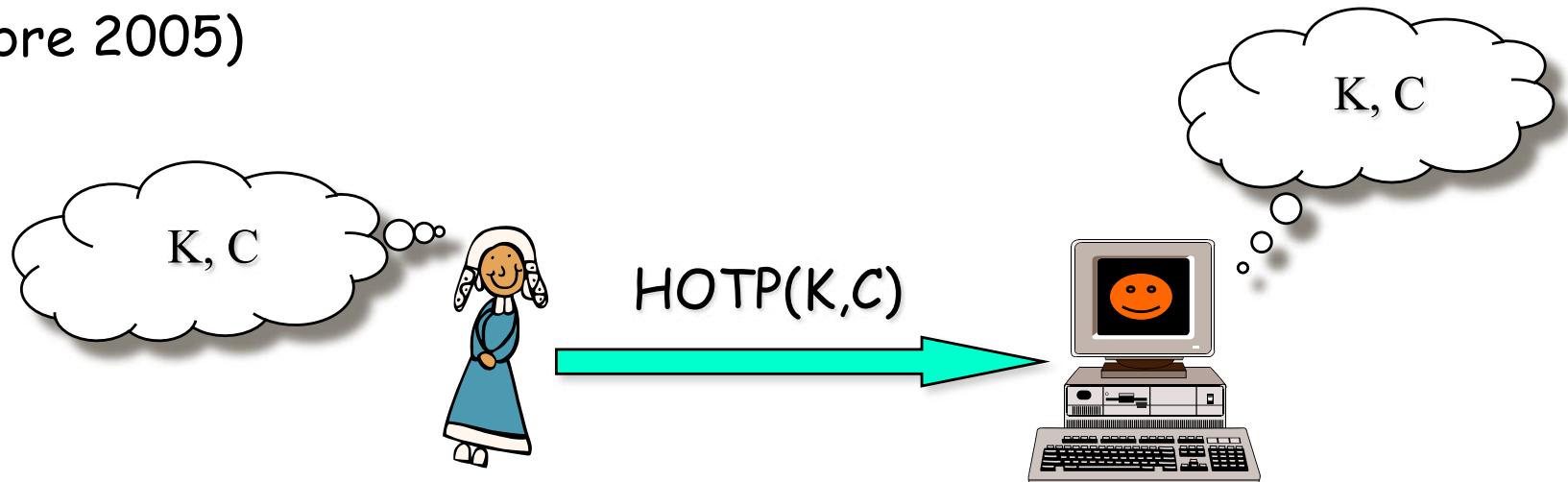
OTP: An HMAC-Based
One-Time Password Algorithm
(dicembre 2005)



HMAC-Based One-Time Password Algorithm

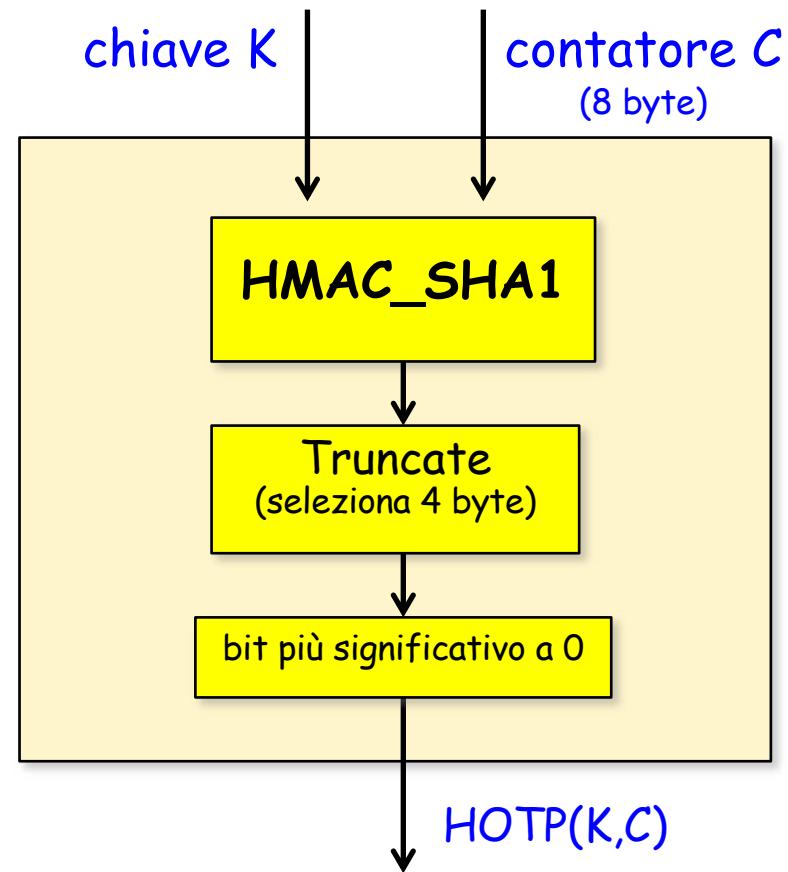
Pubblicato come RFC 4226

OTP: An HMAC-Based
One-Time Password Algorithm
(dicembre 2005)



HMAC-Based One-Time Password Algorithm

Pubblicato come RFC 4226
(dicembre 2005)

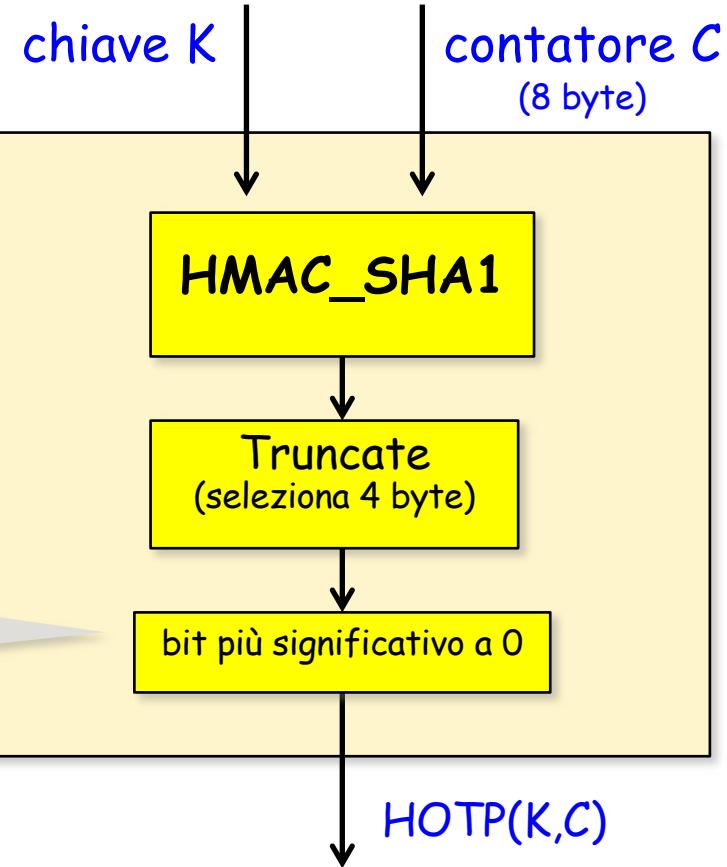


HMAC-Based One-Time Password Algorithm

Pubblicato come RFC 4226
(dicembre 2005)

AND con 0xFFFFFFFF

serve per evitare ambiguità
nella possibile interpretazione
come intero signed / unsigned



HMAC-Based One-Time Password Algorithm

Pubblicato come RFC 4226
(dicembre 2005)

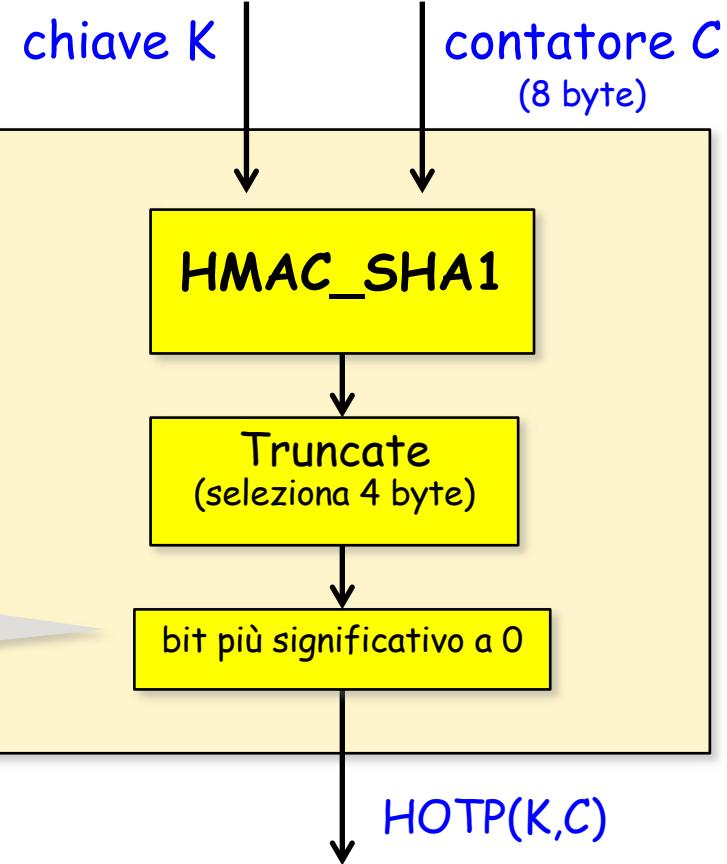
AND con 0xFFFFFFFF

serve per evitare ambiguità
nella possibile interpretazione
come intero signed / unsigned

Conversione in numero in $\{0, 1, \dots, 2^{31}-1\}$

Numero digit d scelto in $\{6, 7, 8\}$

Utile per una persona



$$\text{HOTP value} = \text{HOTP}(K,C) \bmod 10^d$$

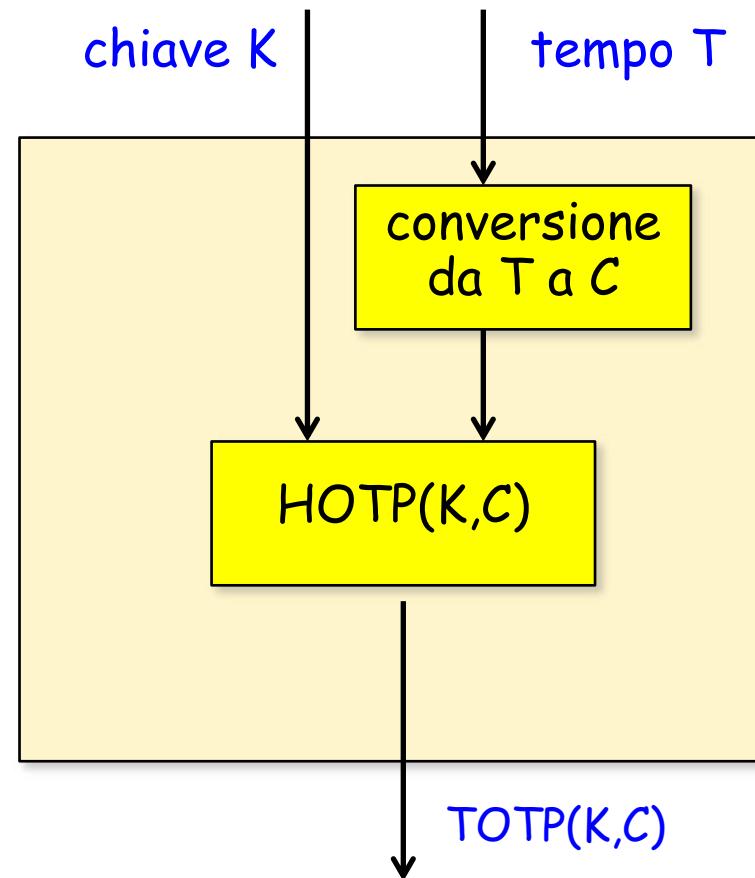
Time-Based One-Time Password Algorithm

Pubblicato come RFC 6238

TOTP: Time-Based

One-Time Password Algorithm

(maggio 2011)



Time-Based One-Time Password Algorithm

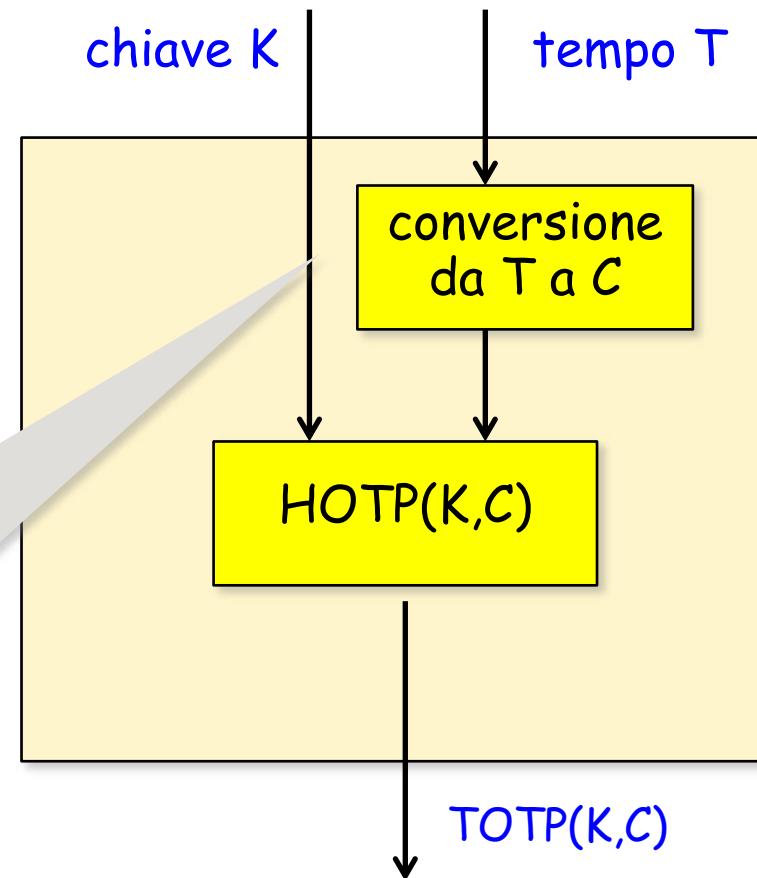
Pubblicato come RFC 6238

TOTP: Time-Based

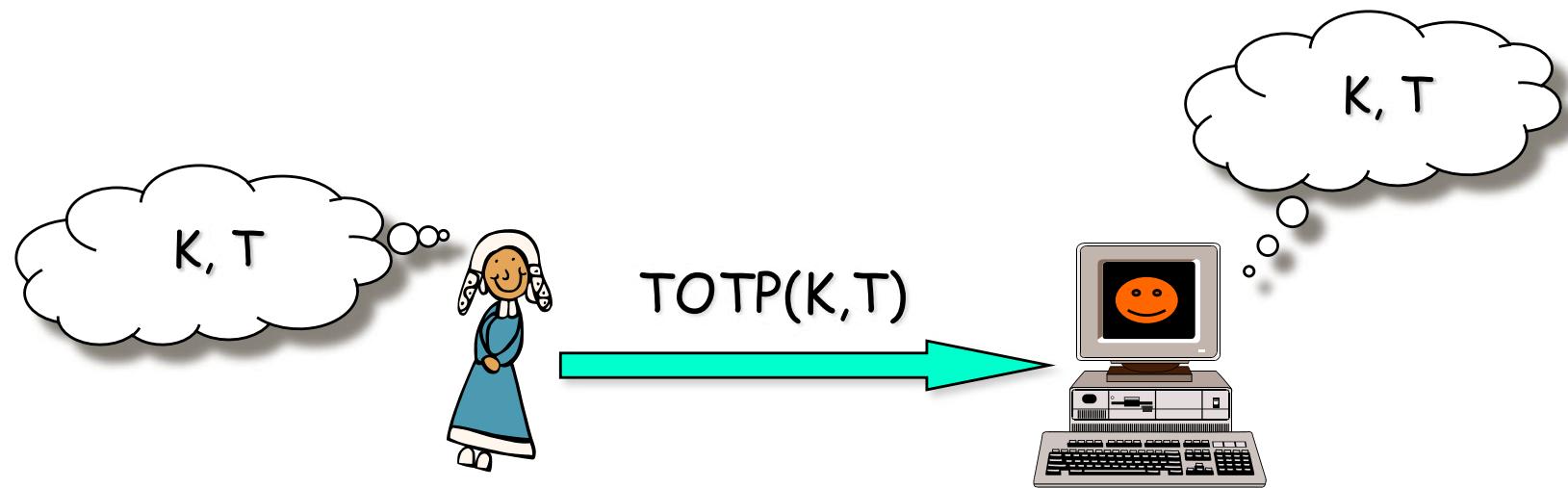
One-Time Password Algorithm
(maggio 2011)

$$C = \frac{\text{tempo corrente} - \text{tempo inizio}}{\text{time step}}$$

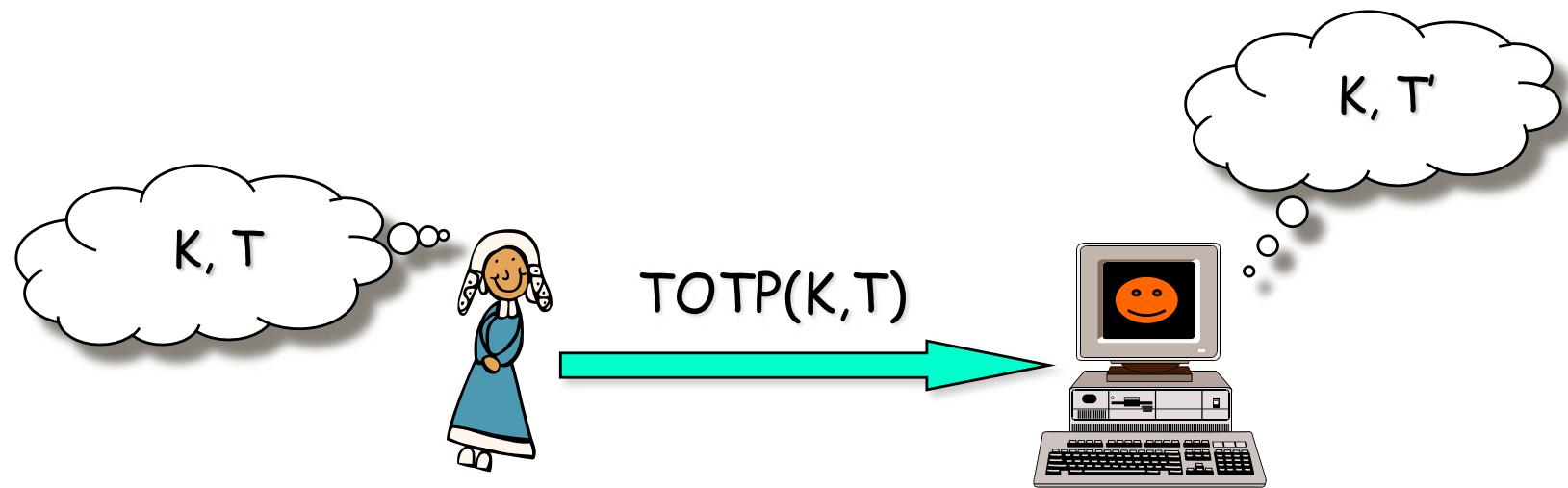
Tempo inizio concordato
Time step: default 30 secondi



Time-Based One-Time Password Algorithm



Time-Based One-Time Password Algorithm

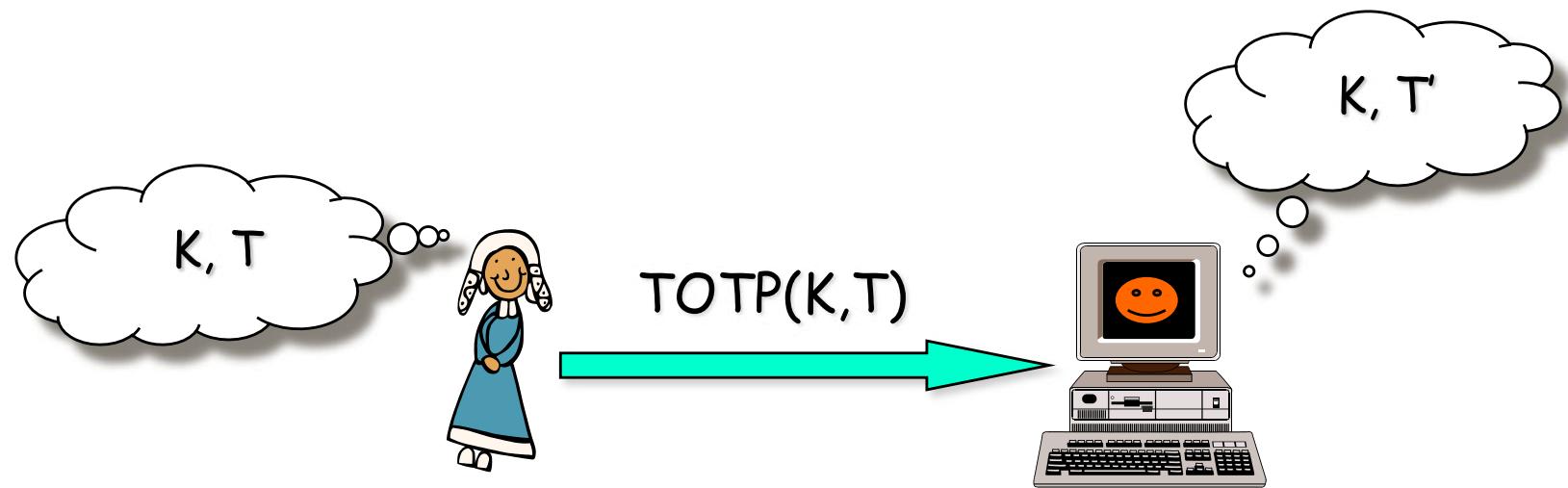


Il tempo potrebbe non essere lo stesso: $T \neq T'$

- Differenza tempo dei sistemi
- Ritardo input dell'utente



Time-Based One-Time Password Algorithm

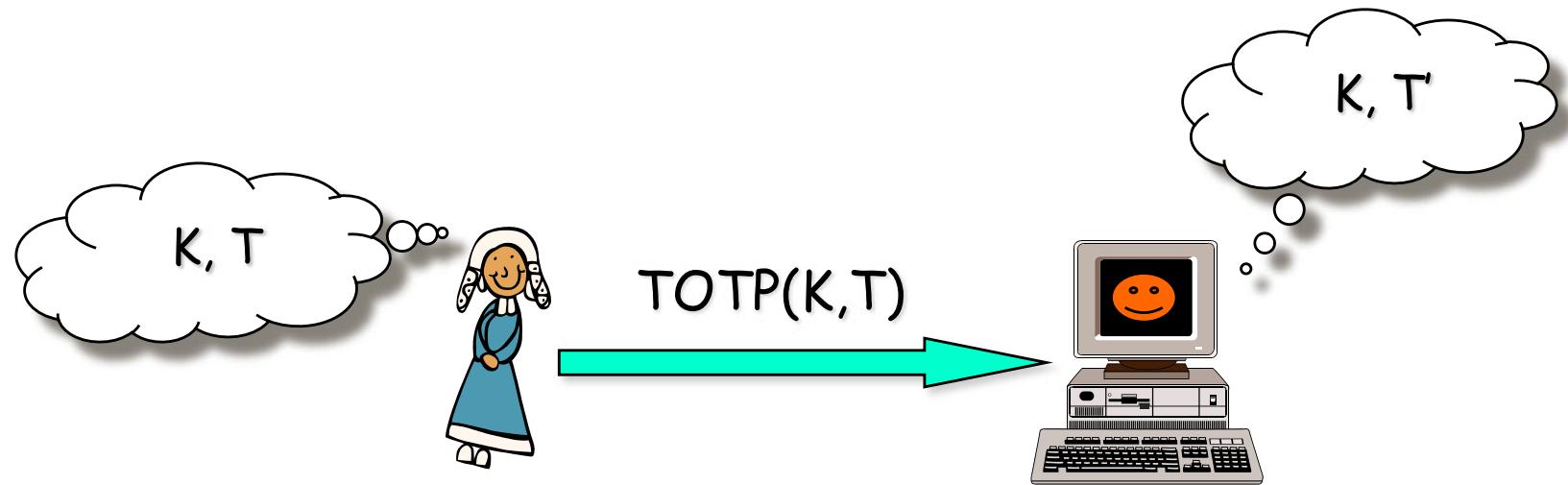


Il tempo potrebbe non essere lo stesso: $T \neq T'$

- Differenza tempo dei sistemi
- Ritardo input dell'utente

Server controlla
2 o 3 time windows

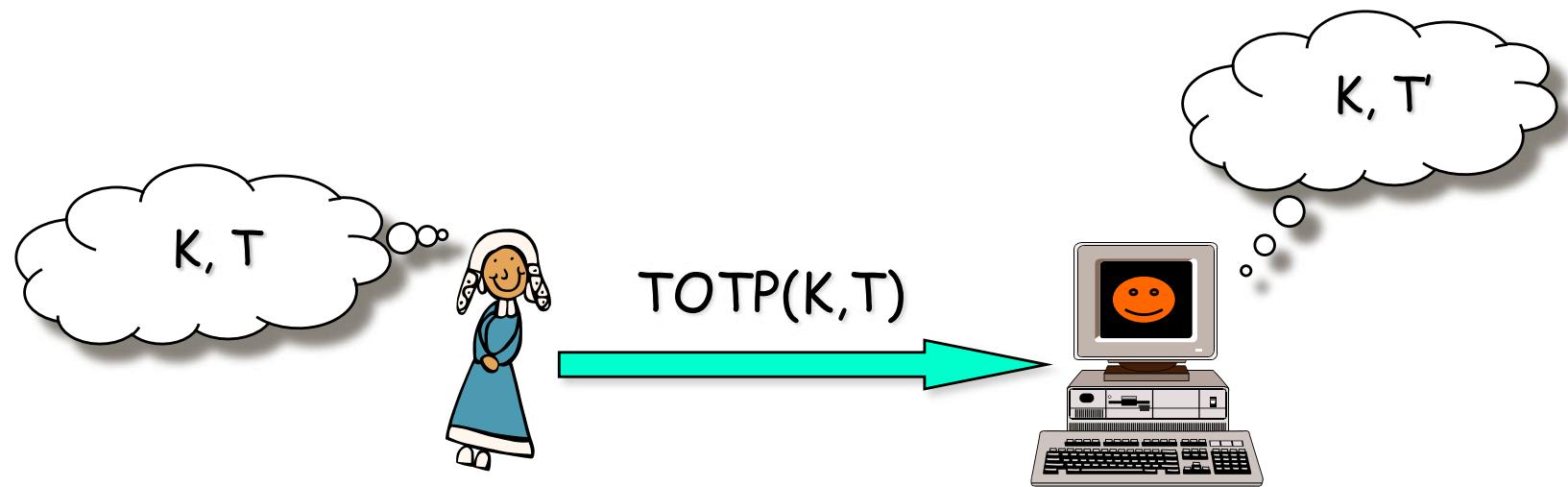
Time-Based One-Time Password Algorithm



Attacco di replay



Time-Based One-Time Password Algorithm



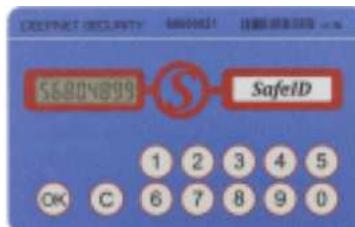
Attacco di replay



Server accetta ogni
password una sola volta



One-time Password Token



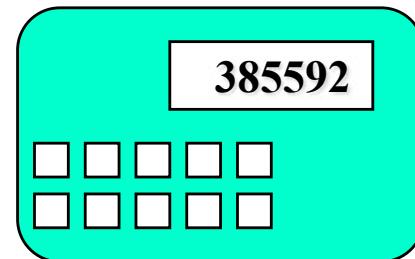
One-time Password computate

Computazione della prossima password

(in dipendenza di: tempo, funzione segreta, ID, serial number,...)

Token Card

- valore display → password
- protetta da un PIN
- Il valore cambia ogni 30-90 secondi ed è sincronizzato con il server
- Svantaggi: fragilità, costo, ...noiose

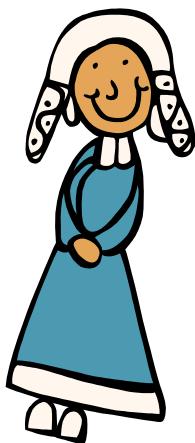


Sommario

- Introduzione
- Password
- One-time password
- Challenge-Response
- Two-factor Authentication

Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema

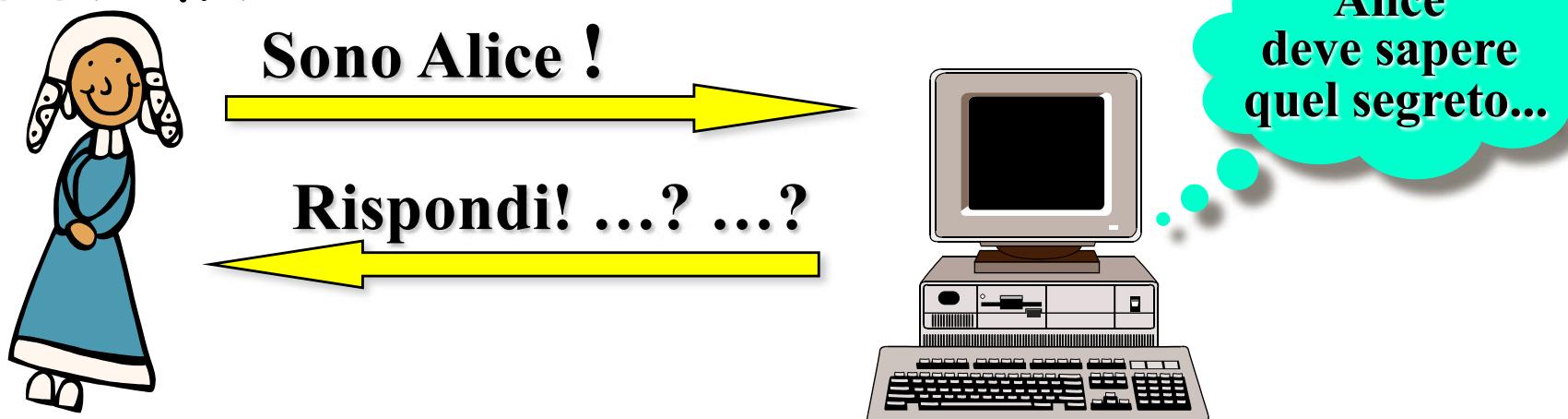


Sono Alice !



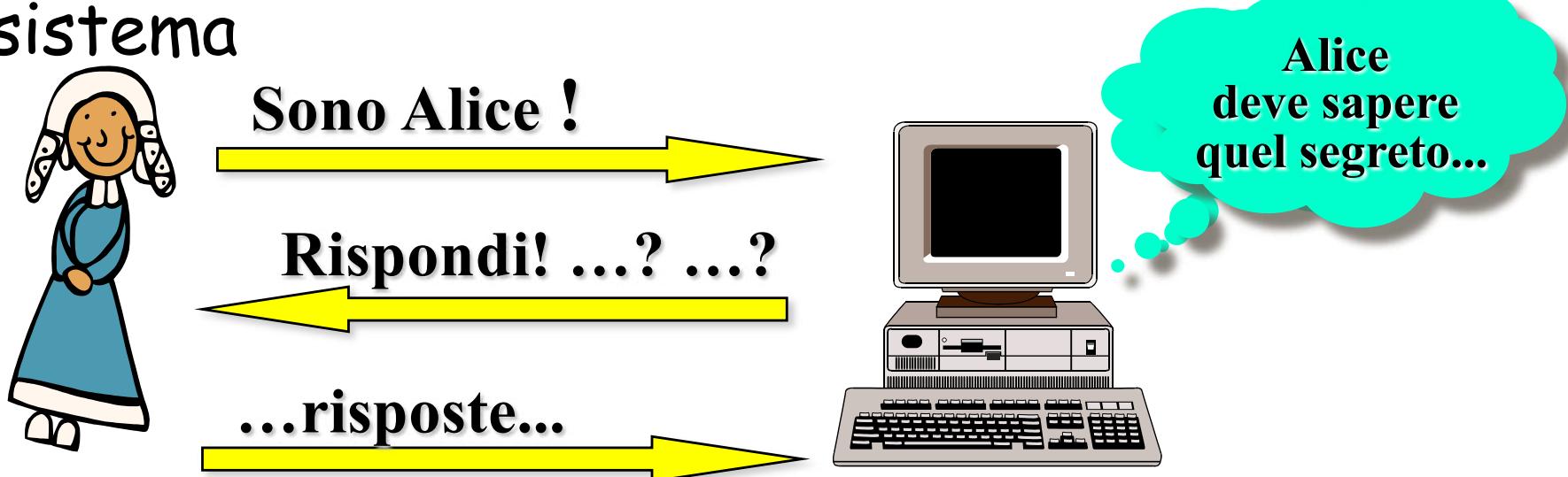
Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema



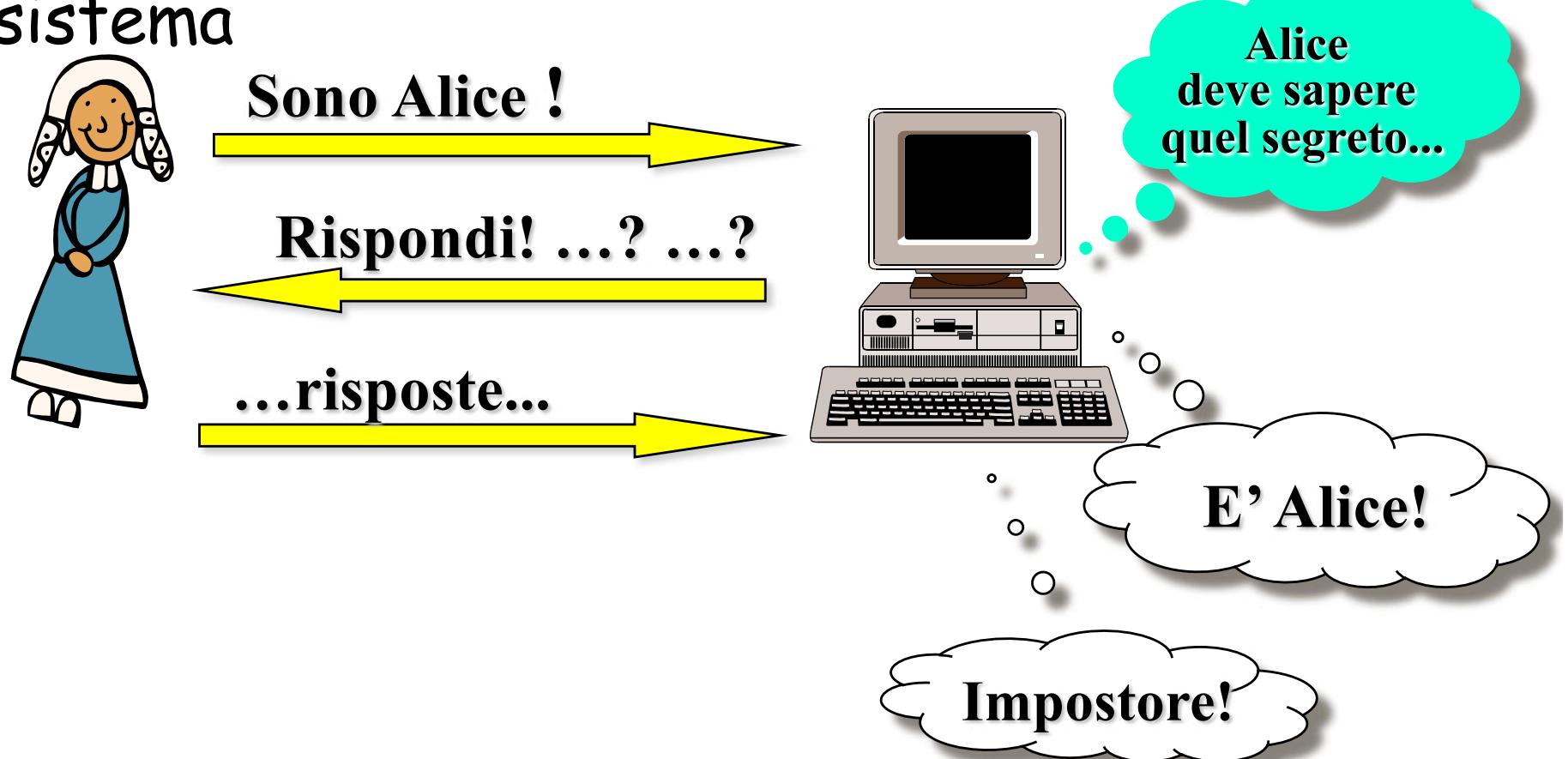
Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema

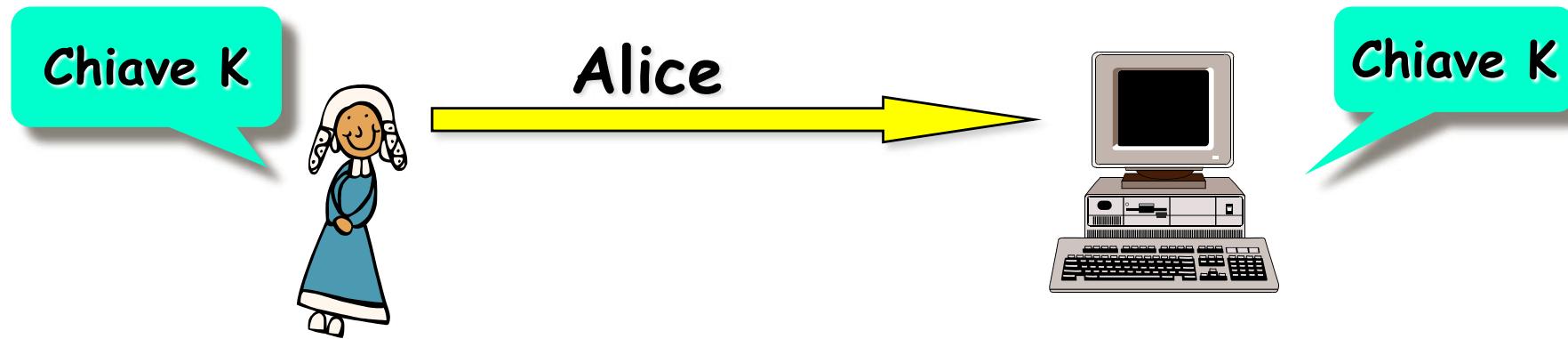


Challenge - Response

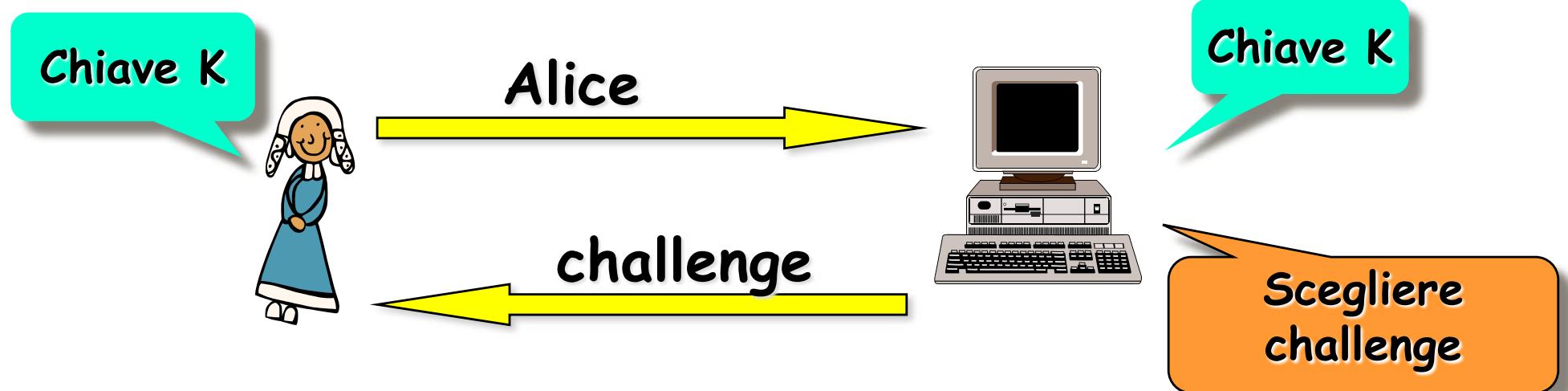
L'utente deve rispondere alle diverse sfide del sistema



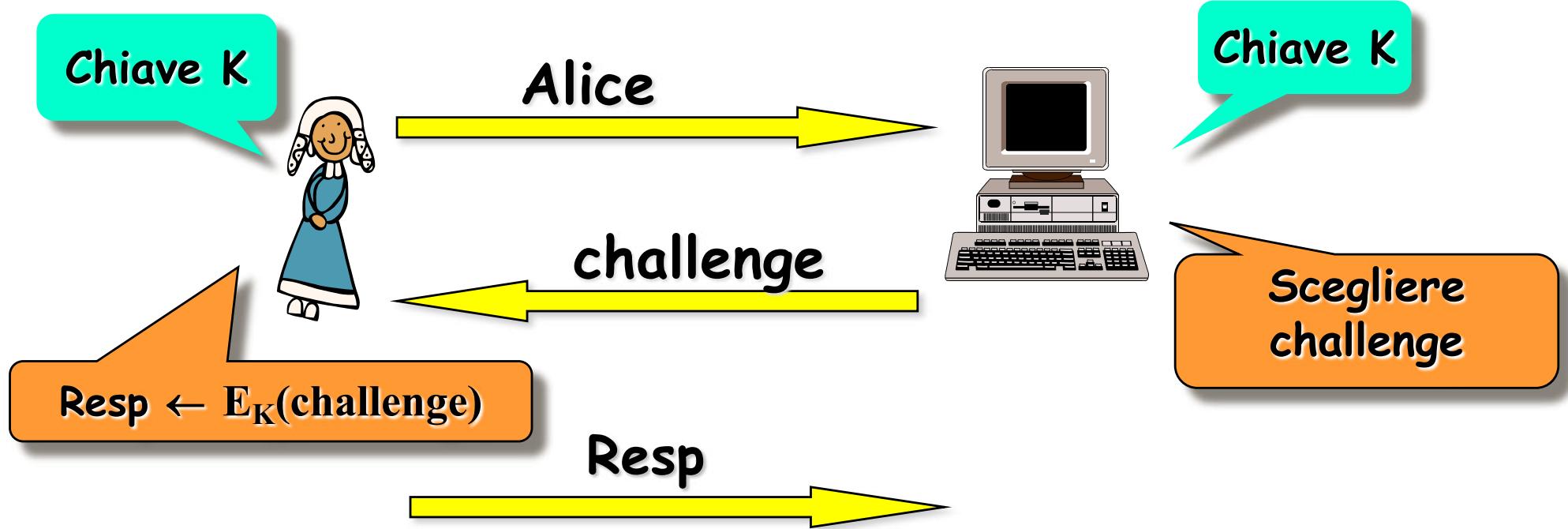
Protocolli per Challenge-Response



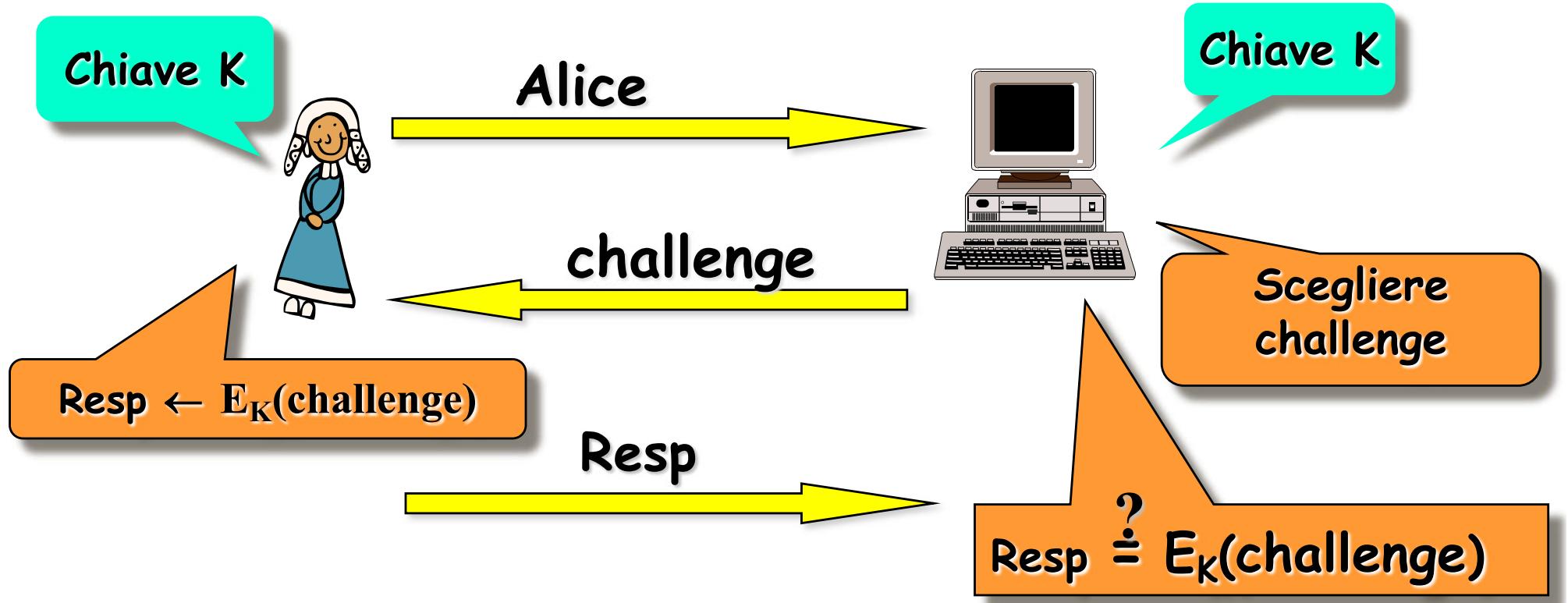
Protocolli per Challenge-Response



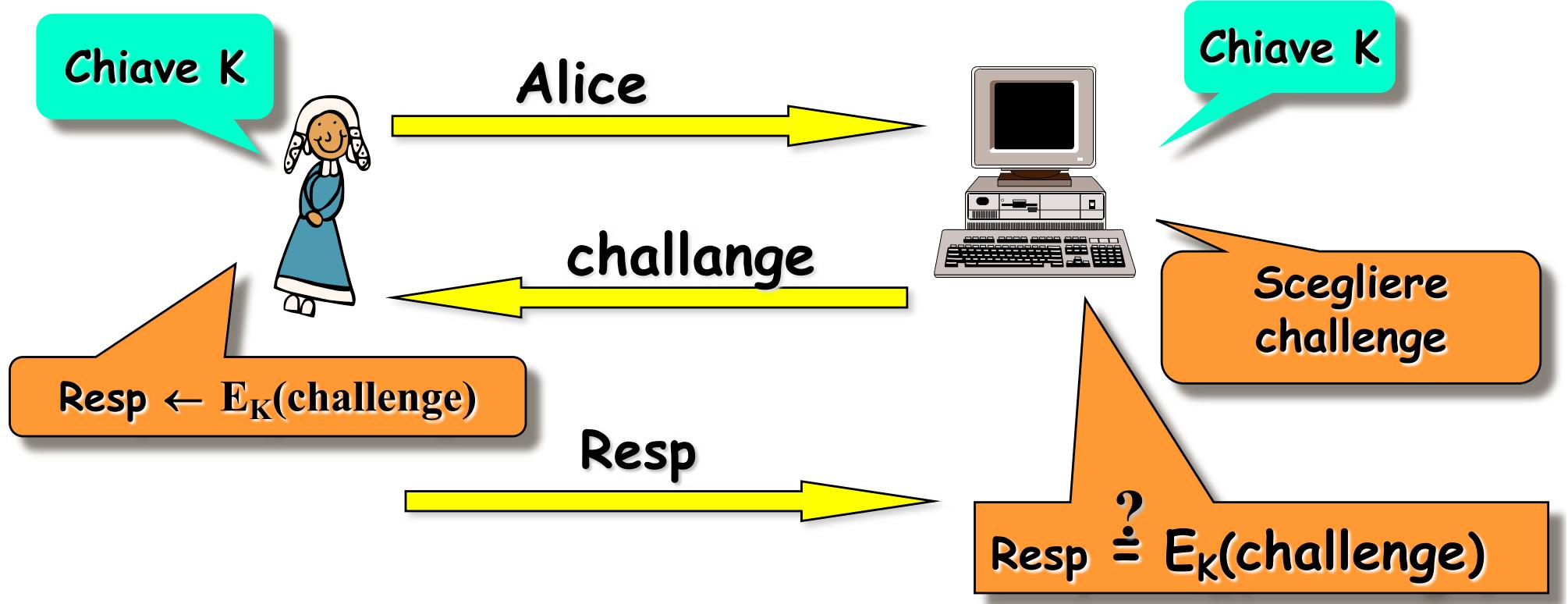
Protocolli per Challenge-Response



Protocolli per Challenge-Response



Protocolli per Challenge-Response



Caratteristiche di challenge
Possibili attacchi

Protocolli per Challenge-Response

Chiave K



2

$E_k(\text{challenge})$

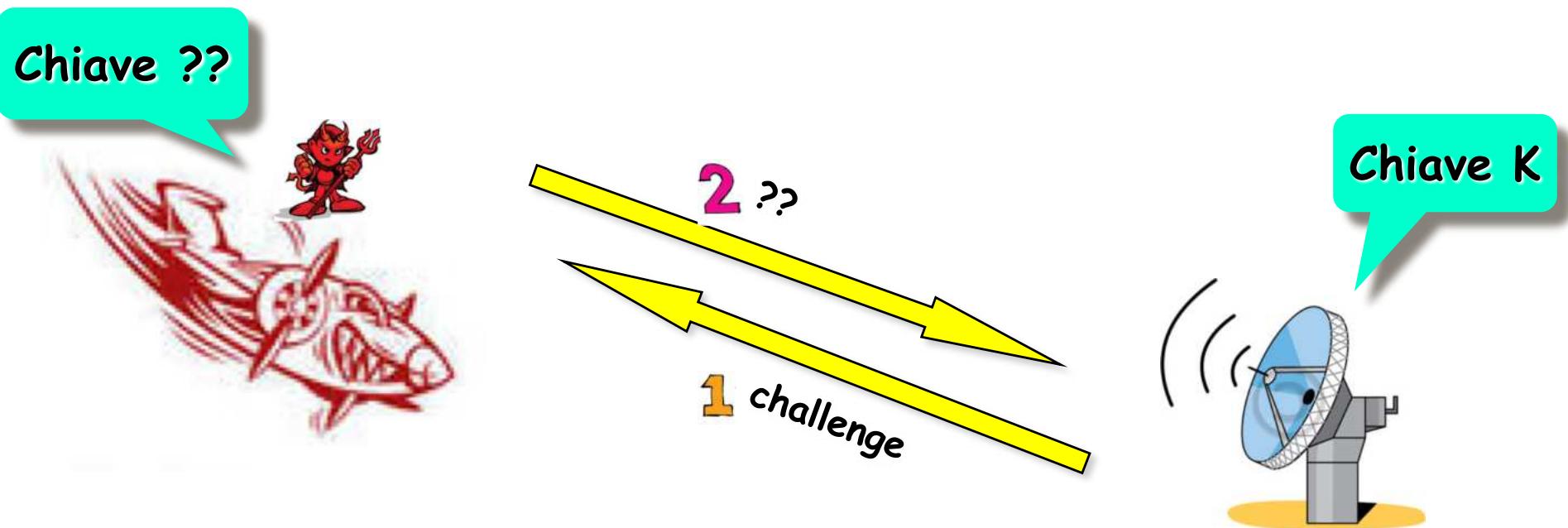
1

challenge

Chiave K



Protocolli per Challenge-Response



Protocolli per Challenge-Response

Chiave K



Chiave ??



Chiave ??



2 ??

1 challenge

Chiave K



Protocolli per Challenge-Response

Chiave K



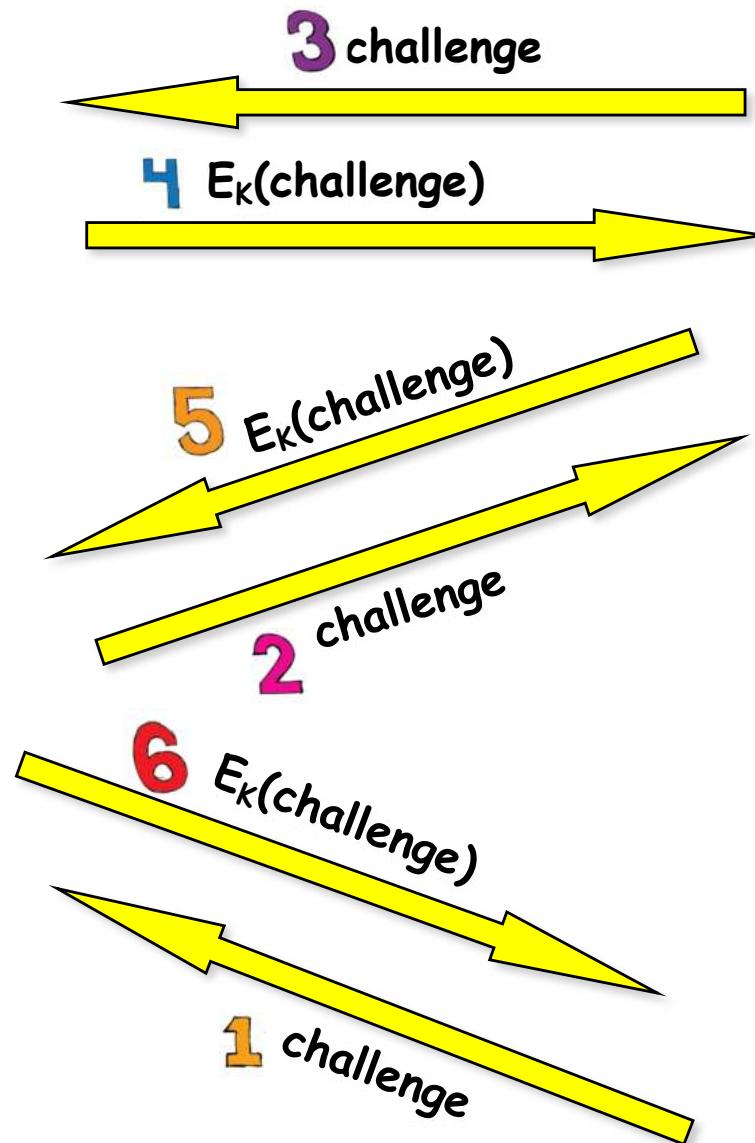
Chiave ??



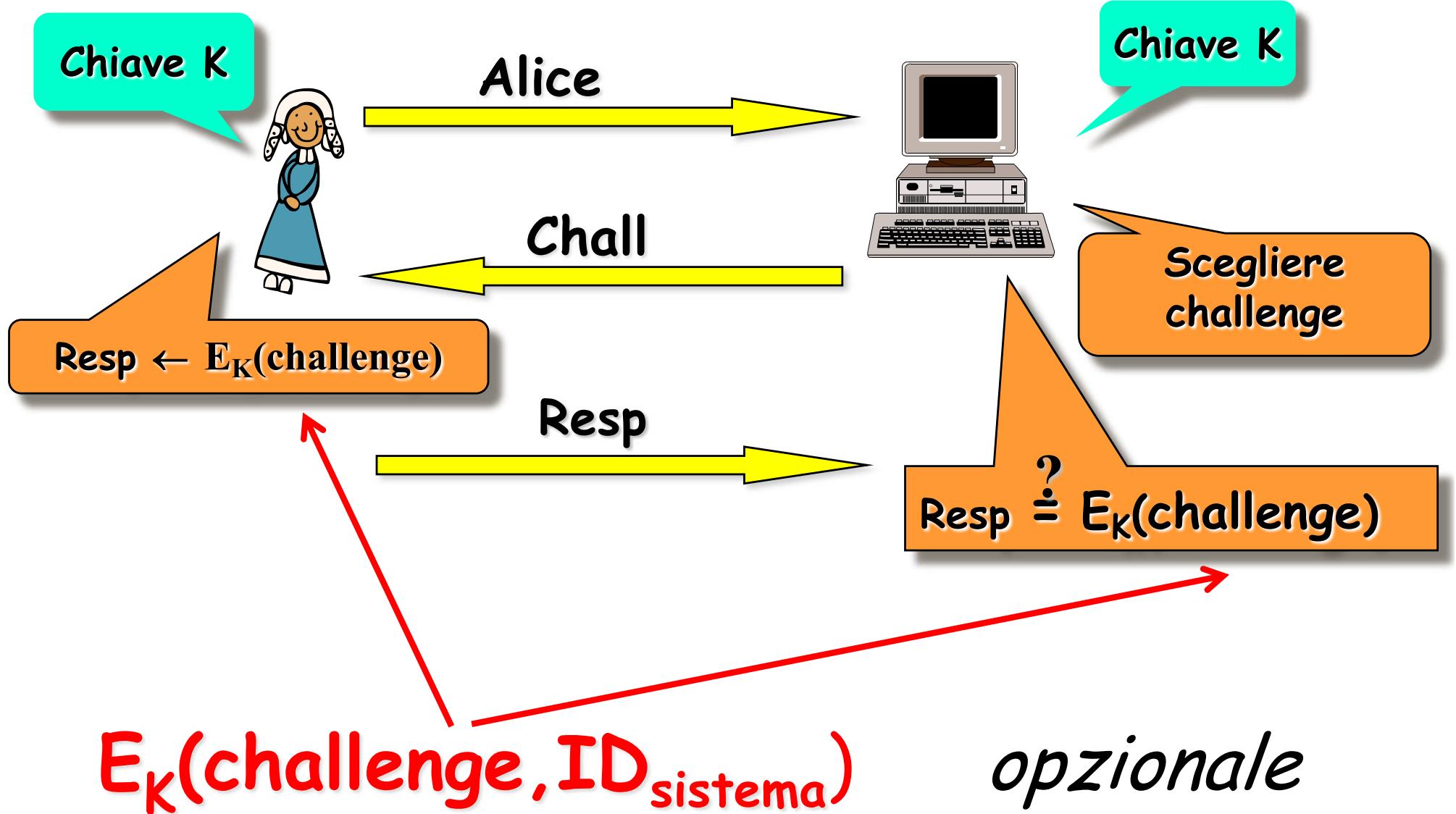
Chiave ??



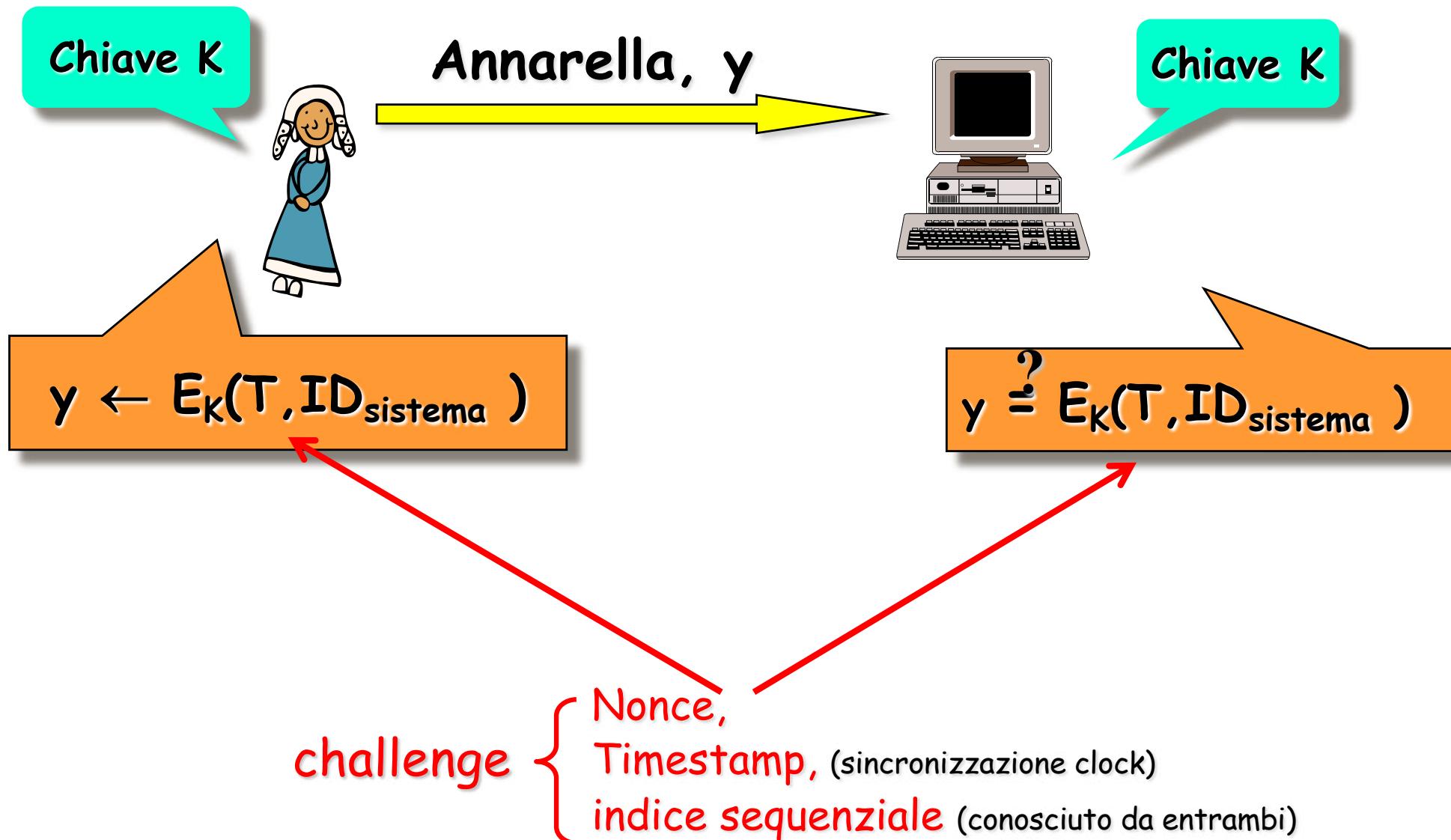
Chiave K



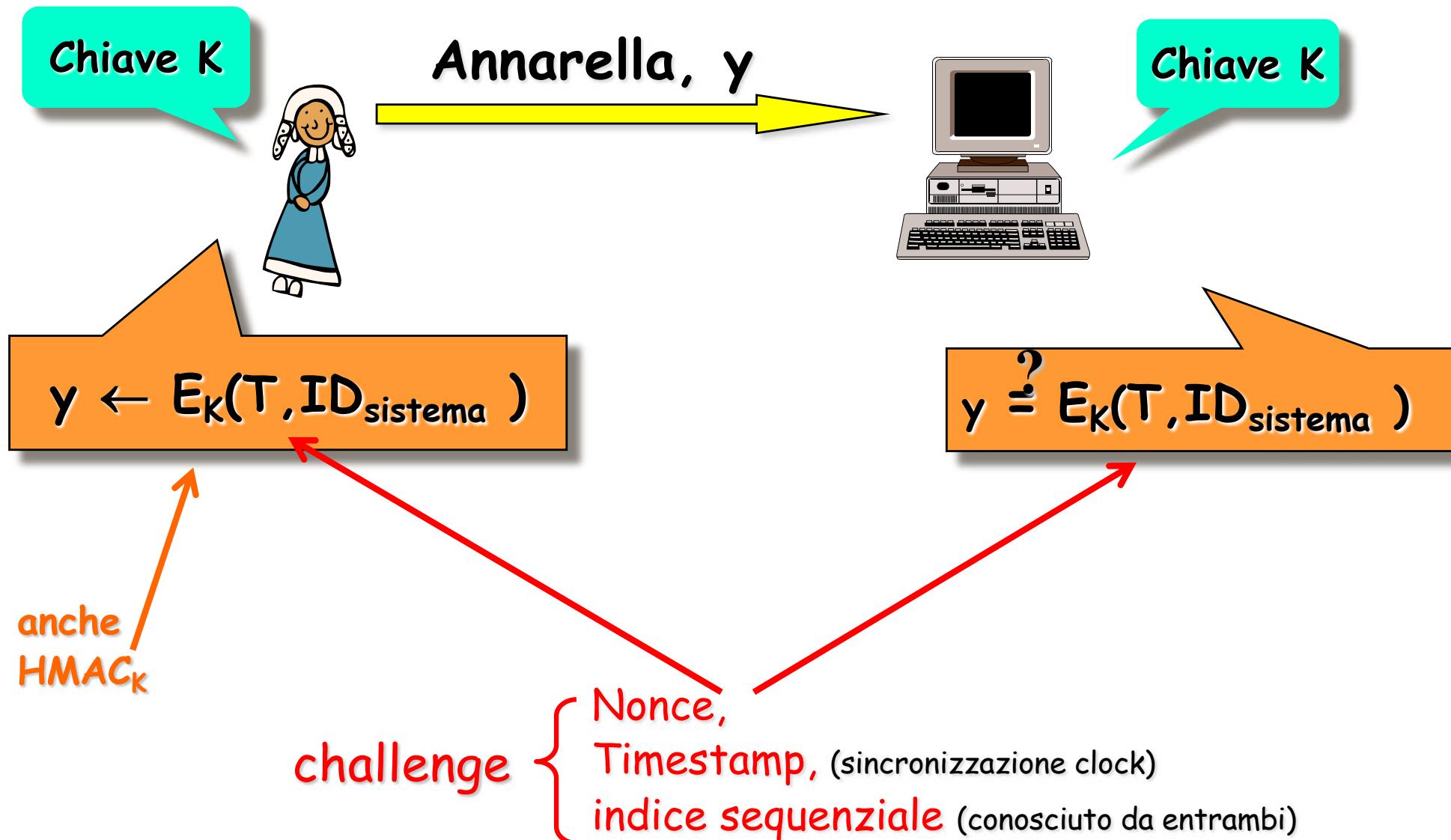
Protocolli per Challenge-Response



Protocolli per Challenge-Response



Protocolli per Challenge-Response



Sommario

- Introduzione
- Password
- One-time password
- Challenge-Response
- Two-factor Authentication

Two-factor authentication

Due fattori per verificare identità

Qualcosa che l'utente **POSSIEDE**

- cose fisiche o elettroniche, ...



Qualcosa che l'utente **CONOSCE**

- password, PIN,...



Qualcosa che l'utente **E'**

- biometria, cioè misura di proprietà biologiche

Multi-factor authentication

Almeno due dei tre fattori per verificare identità

Two-factor authentication

Due fattori per verificare identità

Automated teller machine (ATM)



Two-factor authentication

Due fattori per verificare identità

The image shows a red-bordered screenshot of the Google Two-factor Authentication setup process. It consists of three main sections:

- Top Left:** A "Sign in" form with fields for "Email" and "Password". An arrow labeled "password" points from this section to the "Google Verifica in due passaggi" page.
- Bottom Left:** A "Enter the verification code sent to your phone" form with a "Enter code:" input field and a "Verify" button. An arrow labeled "codice via sms" points from this section to the "Google Verifica in due passaggi" page.
- Top Right:** The "Google Verifica in due passaggi" landing page, which includes:
 - A title: "Maggior sicurezza per il tuo account Google".
 - An illustration of a castle-like structure with Google services (G+, YouTube, Gmail) inside.
 - Three buttons: "Perché è utile", "Come funziona", and "Come ti protegge".
 - Text: "L'accesso al tuo account sarà leggermente diverso".
 - Two numbered steps:
 - Dovrai inserire la password:** "Ogni volta che esegui l'accesso a Google, devi inserire nome utente e password come al solito."
 - Ti verrà chiesto qualcosa' altro:** "Dopodiché verrà inviato un codice al tuo telefono tramite SMS, telefonata o la nostra app per dispositivi mobili. In alternativa, se hai un token di sicurezza, puoi inserirlo nella porta USB del computer."

Two-factor authentication

Due fattori per verificare identità

The diagram illustrates the process of two-factor authentication (2FA). It shows a comparison between a standard Google sign-in page and a Google 2FA landing page, along with images of FIDO2 tokens.

Google Sign-in Page: Shows the standard Google sign-in interface with fields for Email and Password, and a "Sign In" button.

Google 2FA Landing Page: Shows the "Google Verifica in due passaggi" (Two-step verification) landing page, which emphasizes increased security for the account.

FIDO2 Tokens: Two physical hardware tokens are shown: a blue USB token labeled "Token usb" and a white card-based token labeled "Security KEY".

Annotations:

- An arrow points from the "password" field on the sign-in page to the "Google Verifica in due passaggi" page, indicating that the password is the first factor.
- An arrow points from the "Token usb" and "Security KEY" tokens to the "interazione con Google Chrome" (Interaction with Google Chrome) section, indicating that these tokens are used for the second factor.
- Text at the bottom:** "da ottobre 2014" (since October 2014), indicating when the integration with Google Chrome began.

Two-factor authentication

Due fattori per verificare identità

The diagram illustrates the Two-factor authentication (2FA) process. It shows a sequence of three components:

- Google Sign-in Page:** A screenshot of the Google sign-in interface. It features fields for "Email" and "Password", a "Sign in" button, and a "Stay signed in" checkbox. An arrow labeled "password" points from this screen to the Google 2FA landing page.
- Google 2FA Landing Page:** A screenshot of the "Google Verifica in due passaggi" (Two-step verification) page. The page highlights "Maggior sicurezza per il tuo account Google" (Greater security for your Google account). It includes sections for "Perché è utile" (Why it's useful), "Come funziona" (How it works), and "Come ti protegge" (How it protects you). Another arrow points from this page to the Google Authenticator screenshots.
- Google Authenticator Screenshots:** Two screenshots of the Google Authenticator app on an Android device. The top screenshot shows a verification code (246174) and an email address (alice.work@gmail.com). The bottom screenshot shows a QR code with the text "With 2-step verification, whenever you sign in to your Google Account you will need:" followed by "1 Your password" and "2 A code that this app will generate for you".

Annotations:

- An arrow labeled "password" points from the Google Sign-in page to the Google 2FA landing page.
- An arrow points from the Google 2FA landing page to the Google Authenticator screenshots.
- A large arrow labeled "TOTP del Google Authenticator" points from the Google Authenticator screenshots back to the Google Sign-in page.

Google 2-Step Verification

[Get Started](#)[Home](#) **Features** [Help](#)

Get codes via text message

Google can send verification codes to your cell phone via text message. Your carrier's standard messaging rates may apply.



Want a phone call instead?

Google can call your cell or landline phone with your verification code.



No connection, no problem

The Google Authenticator app for Android, iPhone, or BlackBerry can generate verification codes. It even works when your device has no phone or data connectivity.



Keep your account even more secure

Instead of using verification codes, you can insert a [Security Key](#) into your computer's USB port for even more protection against phishing.



Backup phone numbers

Add backup phone numbers so Google has another way to send you verification codes in case your main phone is unavailable.



Backup codes

You can print or download one-time use backup codes for times when your phones are unavailable, such as when you travel.



Register your computers

During sign-in, you can choose not to use 2-Step Verification again on your computer. We'll still ask for codes or Security Key on other computers.



Mac

iPad

iPhone

Watch

TV

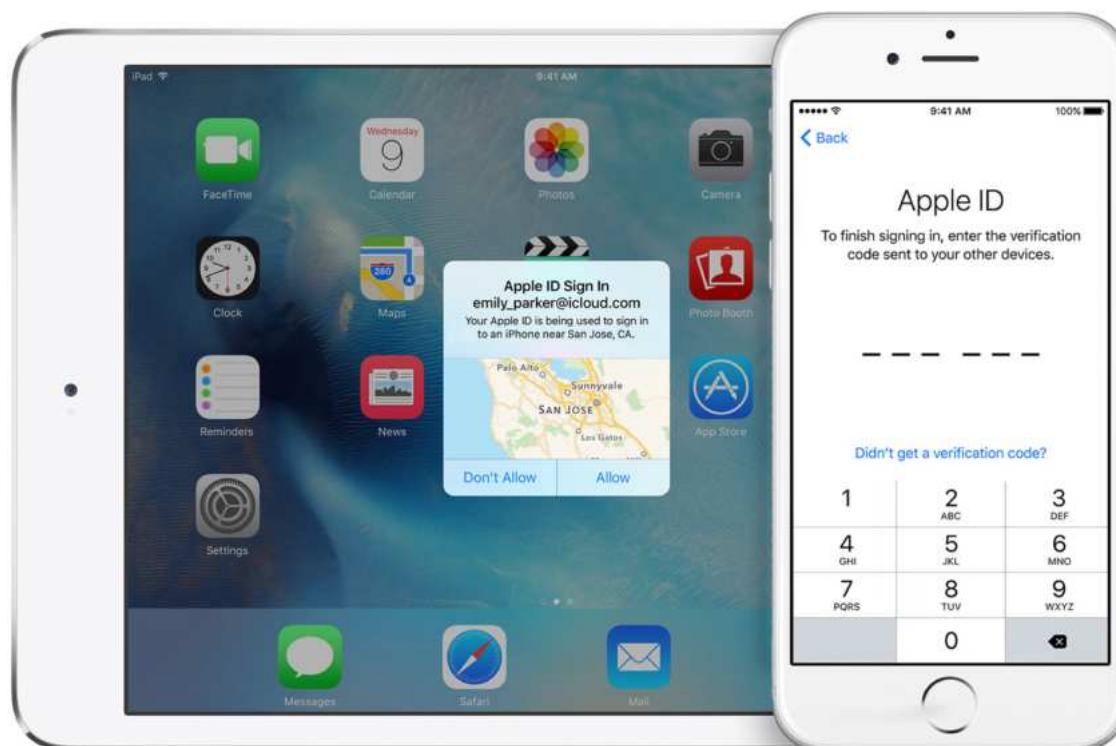
Music

Support



Two-factor authentication for Apple ID

Two-factor authentication is an extra layer of security for your Apple ID designed to ensure that you're the only person who can access your account, even if someone knows your password.



Two-factor authentication

Due fattori per verificare identità

Web service che usano two-factor authentication



Two-factor authentication

Siti Web

Lista siti web che supportano two-factor authentication



<https://twofactorauth.org>

Two Factor Auth (2FA)

List of websites and whether or not they support 2FA.
Add your own favorite site by submitting a pull request on the [GitHub repo](#).

Search websites

Category	Icon	Description
Backup and Sync	Cloud storage icon	Dropbox, Google Drive, OneDrive, etc.
Banking	Dollar sign icon	Bank of America, Chase, Wells Fargo, etc.
Cloud Computing	Cloud icon	AWS, Google Cloud, Microsoft Azure, etc.
Communication	Speech bubble icon	Facebook, LinkedIn, Twitter, etc.
Cryptocurrencies	Coin icon	Bitcoin, Ethereum, Litecoin, etc.
Developer	Code editor icon	GitHub, Stack Overflow, etc.
Domains	Globe icon	Google Domains, Namecheap, etc.
Education	Notebook icon	Khan Academy, Coursera, etc.
Email	Envelope icon	Gmail, Outlook, etc.
Entertainment	Music note icon	Netflix, Hulu, etc.
Finance	Money bag icon	Robinhood, Acorns, etc.
Food	Coffee cup icon	GrubHub, Uber Eats, etc.
Gaming	Controller icon	Epic Games, Steam, etc.
Health	Hospital icon	WebMD, Mayo Clinic, etc.
Hosting/VPS	Server icon	Amazon AWS, DigitalOcean, etc.
Identity Management	User icon	OneLogin, Okta, etc.
Investing	Cash icon	Robinhood, Acorns, etc.
Other	Robot icon	IFTTT, Zapier, etc.
Payments	Credit card icon	PayPal, Venmo, etc.
Remote Access	Monitor icon	LogMeIn, TeamViewer, etc.
Retail	Shopping cart icon	Amazon, Walmart, etc.
Security	Lock icon	TwoFactorAuth.org
Social	People icon	Facebook, LinkedIn, etc.
Transport	Car icon	Uber, Lyft, etc.
Utilities	Phone icon	Twilio, Twinkl, etc.

Two-factor authentication con smartphone

Codice inviato/generato con sms/app

Vantaggi:

- User friendly
- Facile configurazione
- Non occorrono token aggiuntivi



Two-factor authentication con smartphone

Svantaggi:

- Privacy del numero telefono, (e forse spam)
- sms sono insicuri
- sms possono avere ritardi di ricevimento

Two-factor authentication con smartphone

Svantaggi:

- Privacy del numero telefono, (e forse spam)
- sms sono insicuri
- sms possono avere ritardi di ricevimento

Pericoli:

- Smartphone usati anche per email
- Account recovery
 - Reset password ed invio per email
- Furto smartphone
 - Utente in genere loggato nella propria email
 - Accesso ad email per recupero
- Come se fosse un solo fattore e non due



Furto smartphone

- Nel 2013: 3,1 milioni americani vittime di furto di smartphone
- 68% non l'hanno riavuto



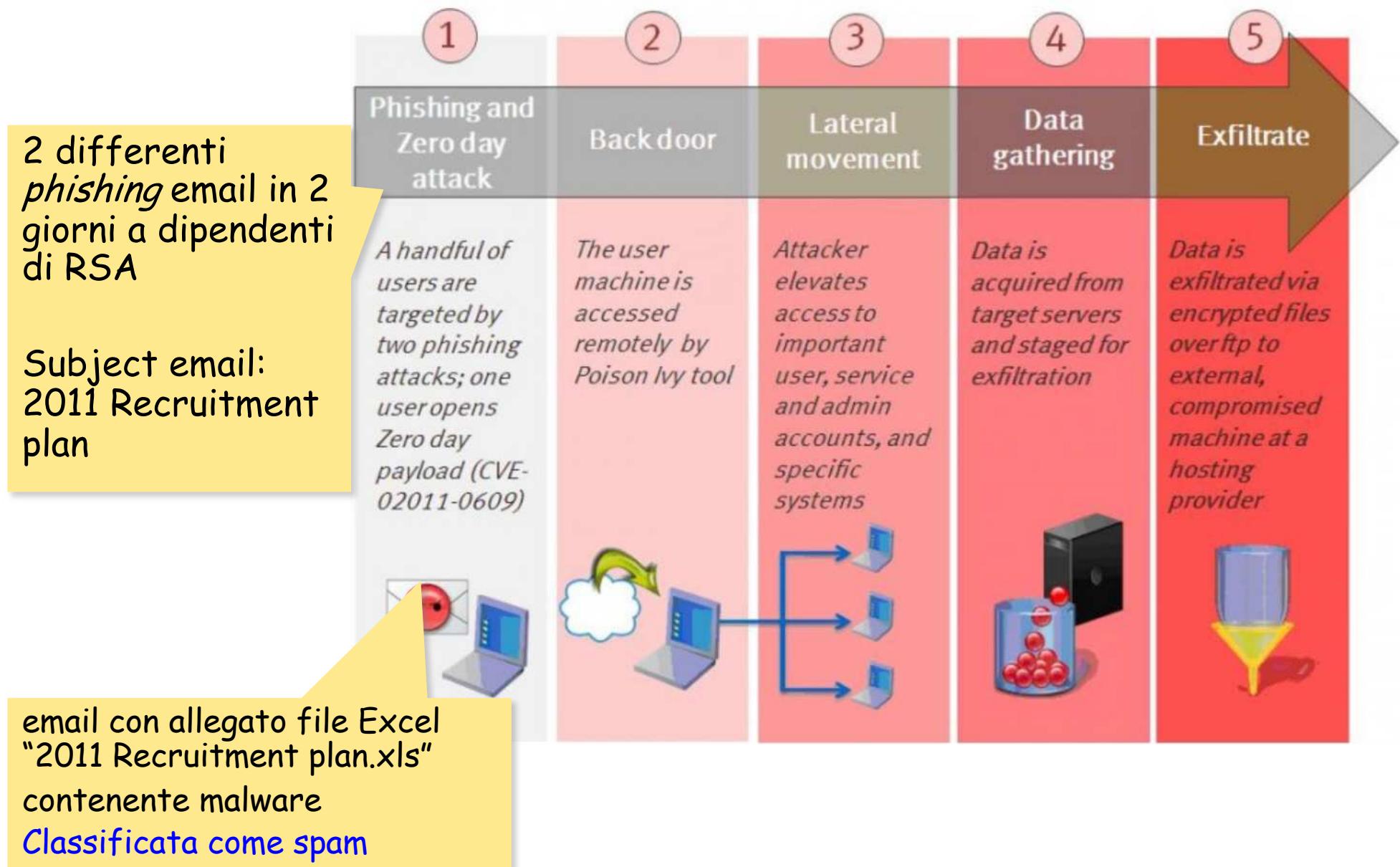
Source: Lookout and IDG Research survey of 500 American victims of smartphone theft. March 2014.

 Lookout

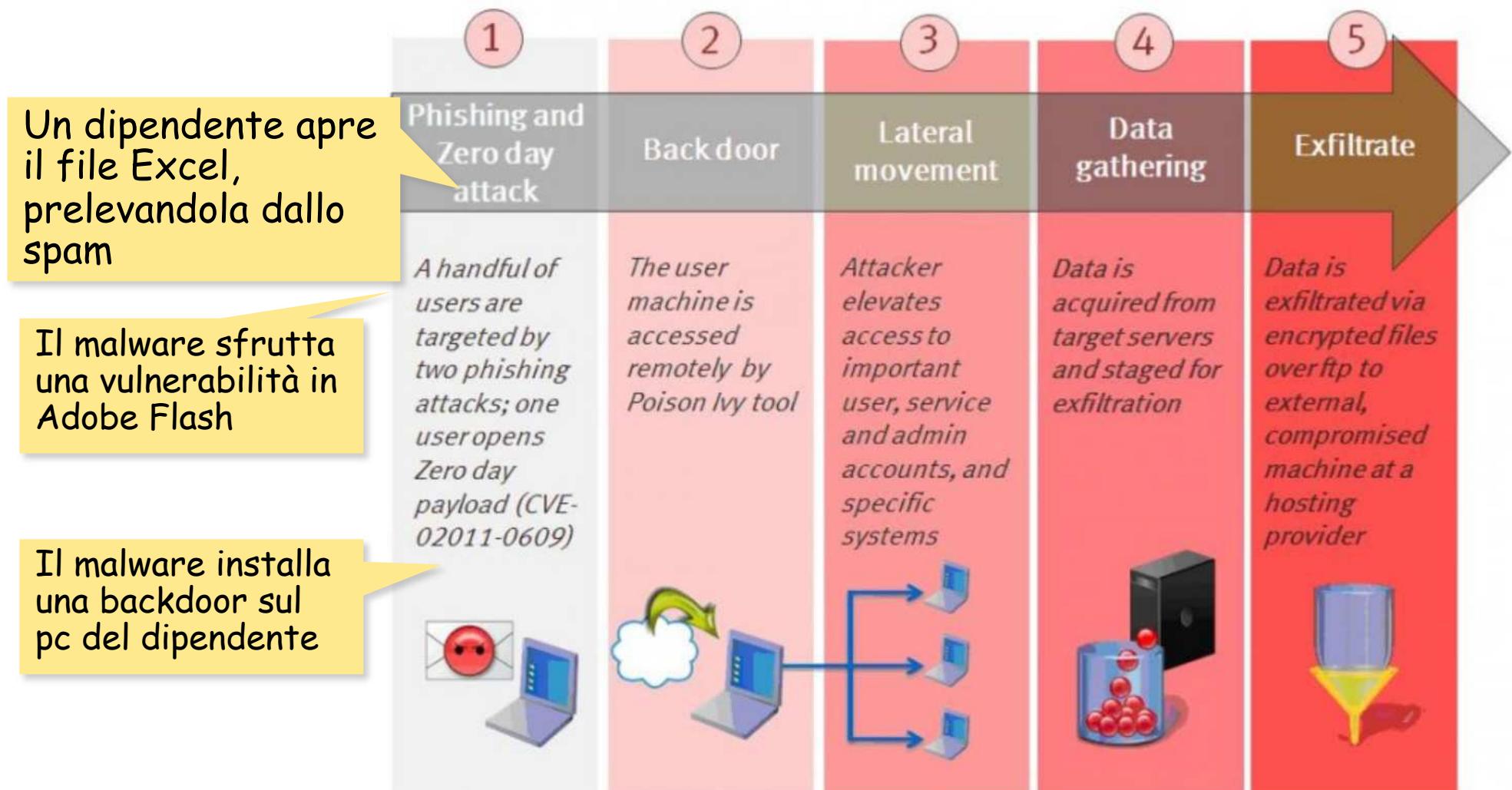
Attacco ad RSA, marzo 2011

- RSA annuncia di essere stata vittima di "an extremely sophisticated cyber attack", 17 marzo 2011
- Problemi con SecureID
- "this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation"
- RSA offre sostituzione del SecureID a 30.000 clienti, 6 giugno 2011
- Valutazione della perdita economica \$66.3 million
- Vediamo l'attacco (RSA non ha fornito tutti i dettagli ...)
 - <http://blogs.rsa.com/anatomy-of-an-attack/>

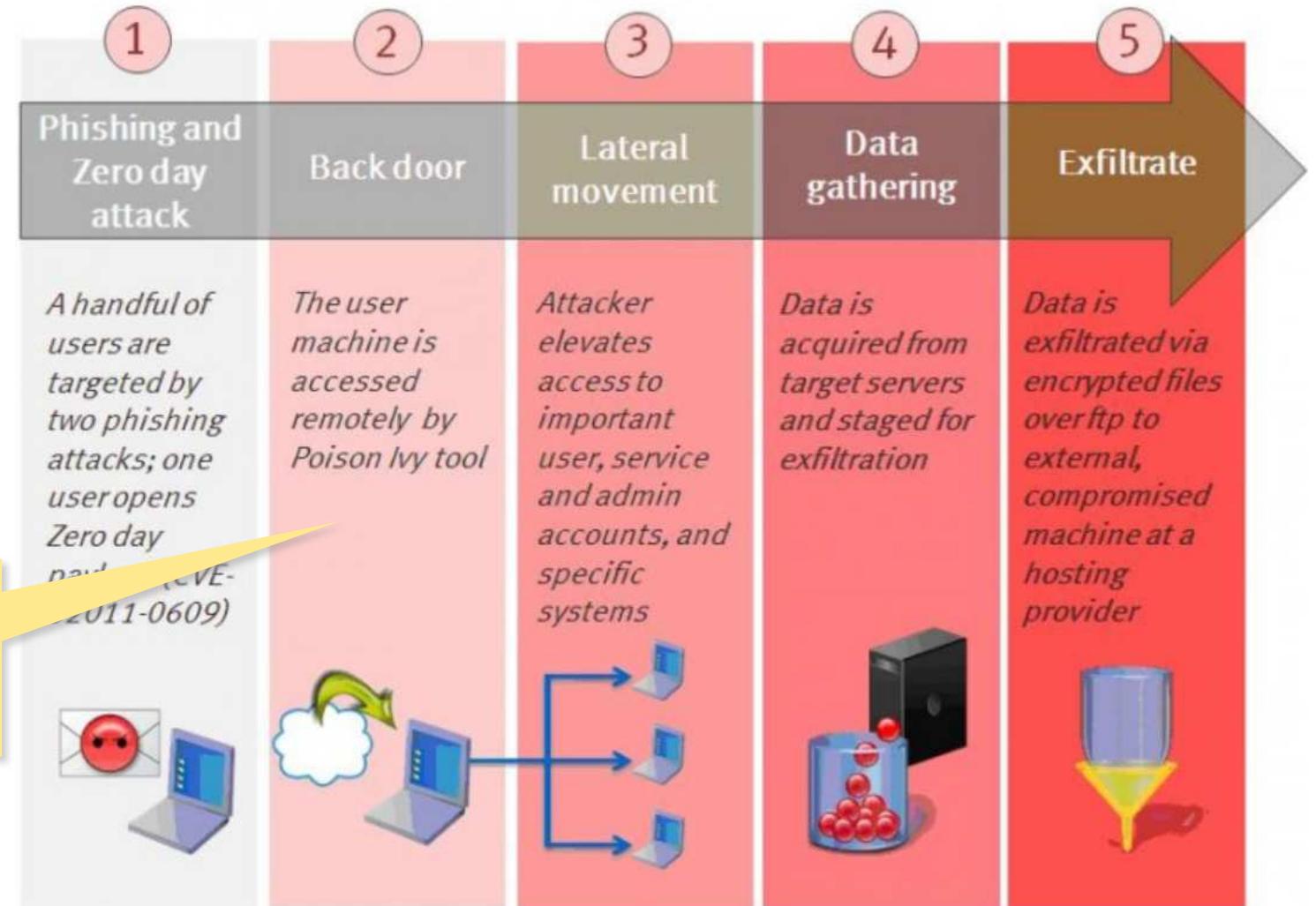
Anatomia dell'attacco



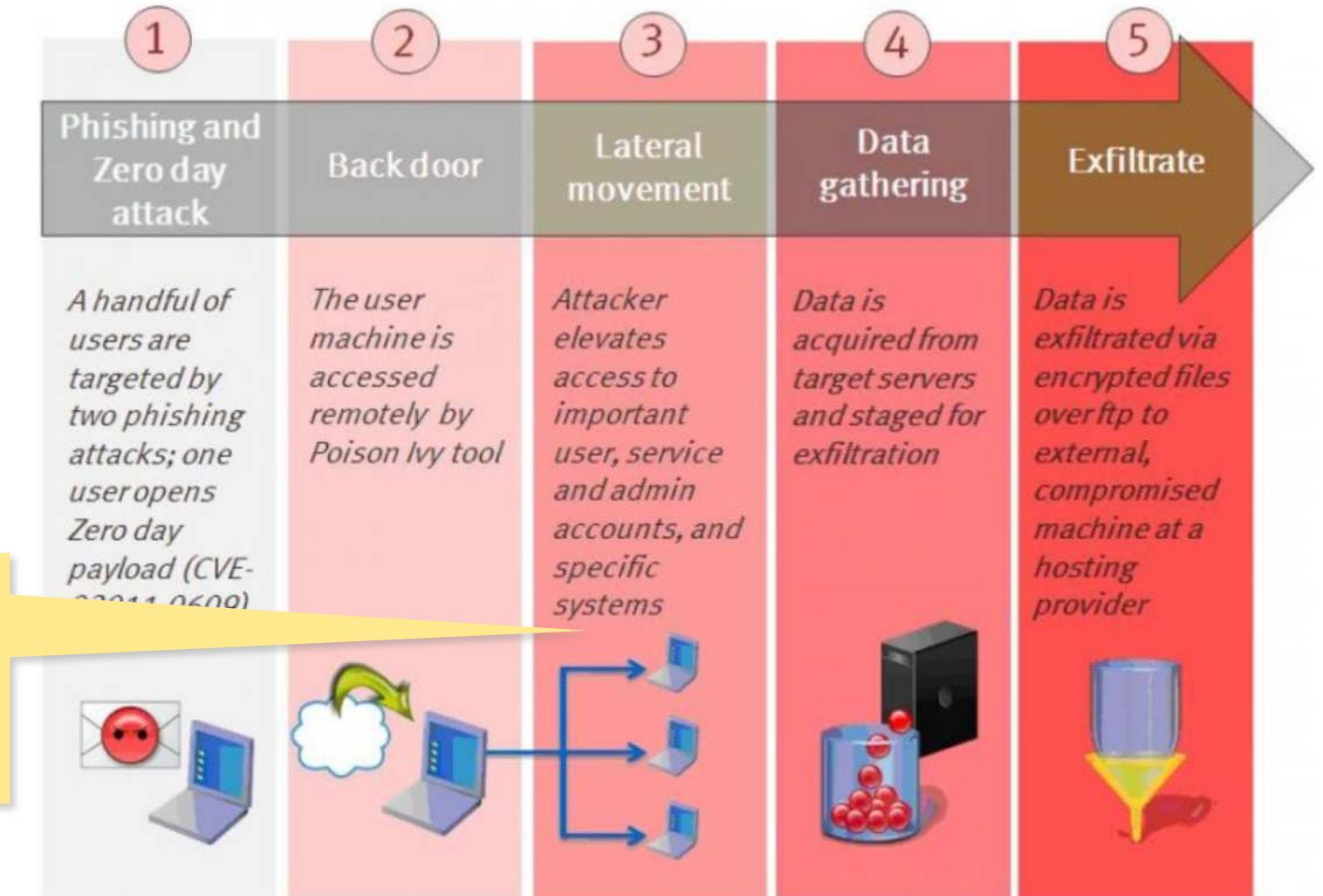
Anatomia dell'attacco



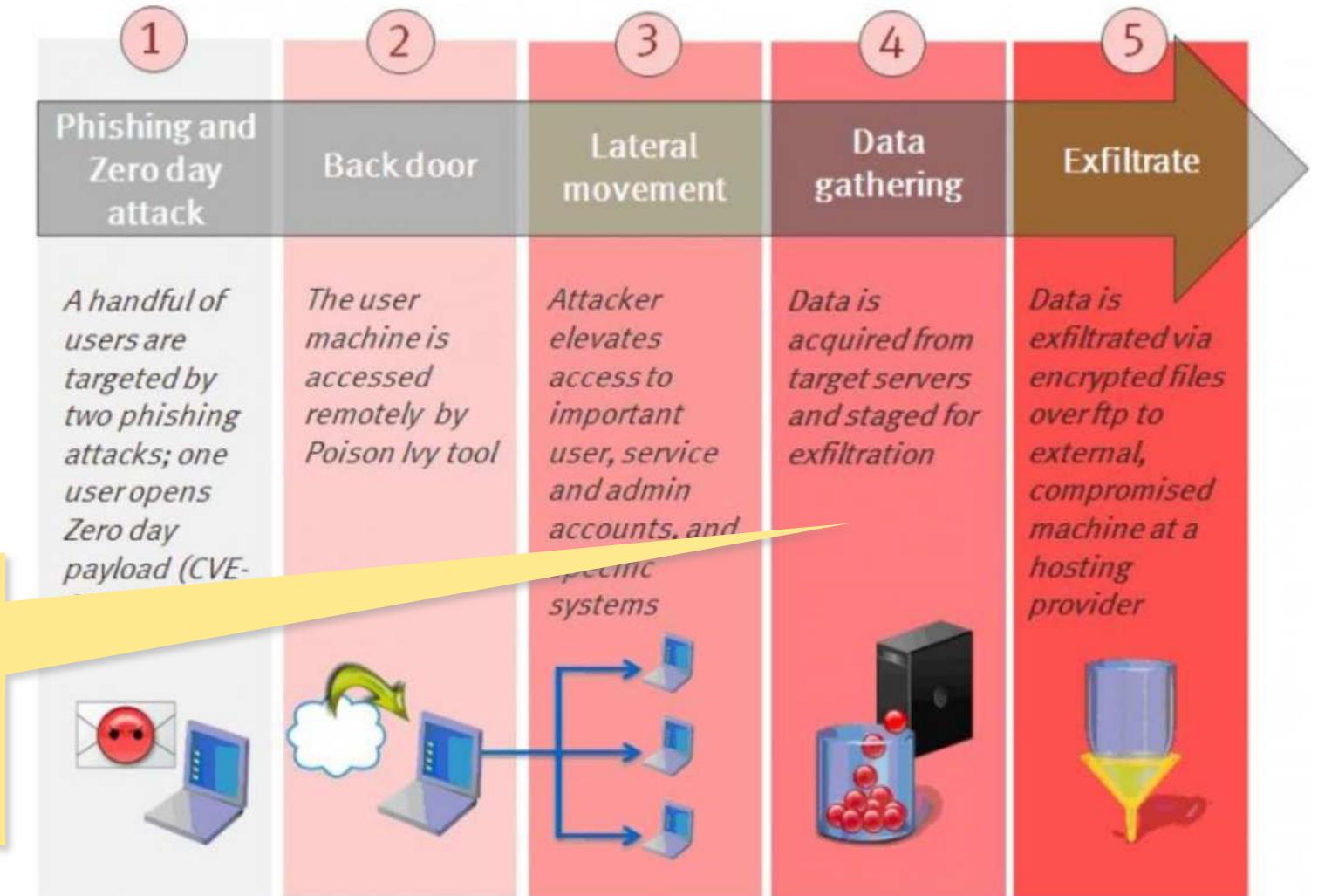
Anatomia dell'attacco



Anatomia dell'attacco



Anatomia dell'attacco



Bibliografia

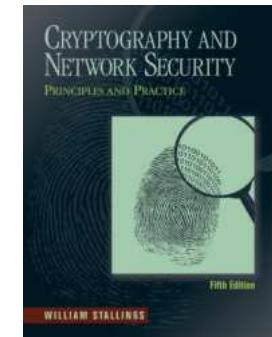
➤ Cryptography and Network Security

by W. Stallings, 2010

➤ cap. 18

➤ Tesina di Sicurezza su reti

➤ Autenticazione utente + password



Domande?

