



# Autenticazione utente



Che bocca grande che hai!

Autenticazione

0



# Sistemi di autenticazione: principi

❑ Qualcosa che l'utente **POSSIEDE**  
- cose fisiche o elettroniche, ...



❑ Qualcosa che l'utente **CONOSCE**  
- password, PIN, ...

❑ Qualcosa che l'utente **E'** (o come si comporta)  
- **biometria**, cioè misura di proprietà biologiche



Autenticazione



# Caratteristiche

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



Autenticazione

2

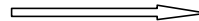


# Password

Database delle password



(userid, password)



Autenticazione

3

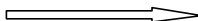


# Password

Database delle password



(userid, password)



Il sistema deve memorizzare una rappresentazione della password

Come?

Autenticazione

4

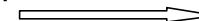


# Password

Database delle password



(userid, password)



Memorizzate in chiaro in un file protetto

Autenticazione

5

# Password

Database delle password

(userid, password)

Memorizzate in chiaro in un file protetto

Problemi:

- nessuna protezione contro chi riesce a leggere il file
- problemi anche per i backup

Autenticazione 6

# Password

Memorizzate in forma cifrata

(Annarella, passwd)

$F(\text{password}) = \text{cifr\_Annarella} ?$

Annarella, cifr\_Annarella  
Biagio, cifr\_Biagio  
Ciro, cifr\_Ciro  
...

Database delle password

Autenticazione 7

# Password: attacchi

- Spiare durante la digitazione
- Intercettazioni
- Tentare a caso o sistematicamente
  - In genere bassa entropia, quindi *deboli* password
  - Attacchi con dizionario

Autenticazione 8

# 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

Autenticazione 9

# 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

Autenticazione 10

# 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%
...	...	...	...

Autenticazione 11



## 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



## 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 dalla funzione di cifratura,  $t = 25$
- $y$  tempo richiesto per singola iterazione,  $y = 1/125.000$  sec

$\Rightarrow c$	26	36 (minuscole alfanumerici)	62 (min. e maius. alfanumerici)	95 (caratteri tastiera)
$\Downarrow n$	(minuscole)	(minuscole alfanumerici)	(min. e maius. 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



## 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 ...



## 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+, anpasswd,...

Esempio vincoli:

- min lunghezza
- min numero caratteri alfabetici
- min numero caratteri non-alfabetici
- max numero caratteri ripetuti
- elenco parole proibite

- **Password Crackers** (ad es., Crack) per testare il file /etc/passwd



## Shadow password

Cifratura password in un file separato e protetto

- Previene l'attacco di leggere/copiare il file e trovare password deboli
- SVR4 Unix: /etc/shadow protezione 400, proprietario root
- SunOs: /etc/security/passwd.adjunct dove /etc/security ha protezione 700
- File /etc/passwd contiene solo separatori speciali (oppure stringhe casuali per ingannare eventuali attaccanti!)
- Attenzione ai backup!



## Shadow password

- `ads:x:500:100:De Santis Alfredo:/home/ads:/bin/bash`
- `ads:FeEQShVEhOlq6:10889:0:11000:::`

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



## 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)

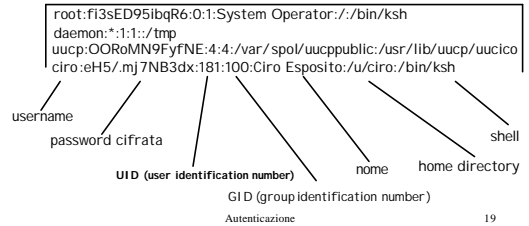
Autenticazione

18



## Password sotto UNIX

File `/etc/passwd`



Autenticazione

19



## Password sotto UNIX

Funzione di cifratura = variante del DES

- 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



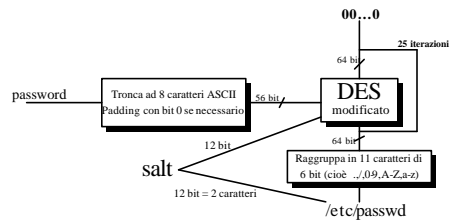
Autenticazione

20



## Password sotto UNIX

Funzione `crypt()` [Robert Morris e Ken Thompson, 1979]



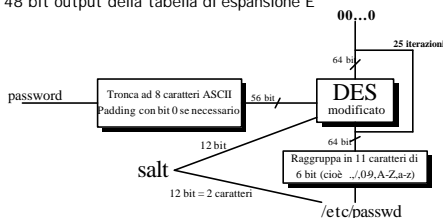
Autenticazione

21



## Password sotto UNIX

**salt**: 12 bit presi dal clock al tempo della creazione della password i bit sono associati a 12 coppie (1,25), (2,26), (3,27),... se 1 viene fatto lo swap della coppia corrispondente nel 48 bit output della tabella di espansione E



Autenticazione

22



## One-time password

- ❑ Ogni password è usata solo una volta!
- ❑ Lista condivisa



Autenticazione

23

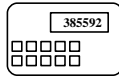


## One-time password compute

- Computazione della prossima password  
(in dipendenza di: tempo, funzione segreta, ID, serial number,...)

### Token Card

- valore display  $\Rightarrow$  password
- protetta da un PIN
- Esempio: **SecurID**



- Il valore cambia ogni 30-90 secondi ed è sincronizzato con il server
- Svantaggi: fragilità, costo, ...noiose



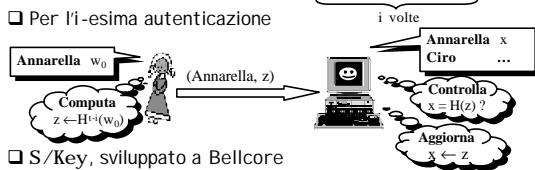
## Schema di Lamport [1981]

- Schema di Lamport per  $t$  autenticazioni ( $H$  funzione hash)
- Annarella sceglie  $w_0$ . Sia  $H^i(w_0) = H(H(\dots H(w_0)\dots))$
- Inizializzazione



## Schema di Lamport [1981]

- Schema di Lamport per  $t$  autenticazioni ( $H$  funzione hash)
- Annarella sceglie  $w_0$ . Sia  $H^i(w_0) = H(H(\dots H(w_0)\dots))$
- Per l' $i$ -esima autenticazione

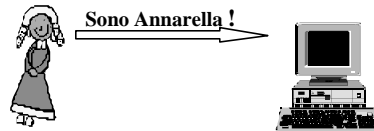


- S/Key, sviluppato a Bellcore



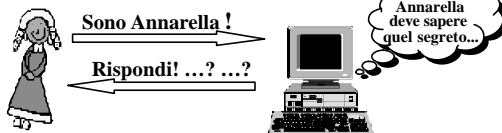
## Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema



## Challenge - Response

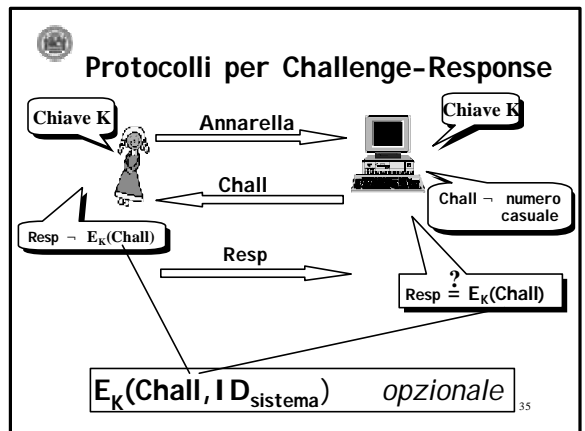
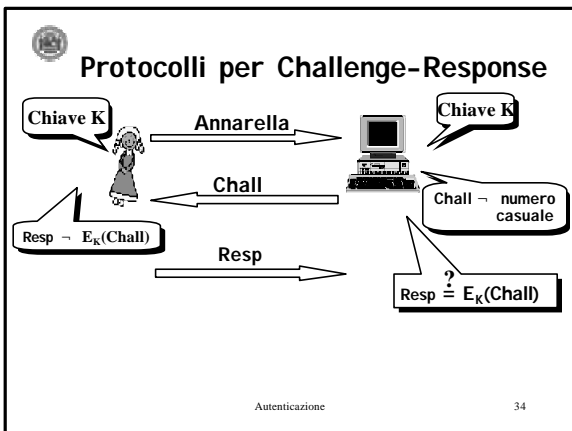
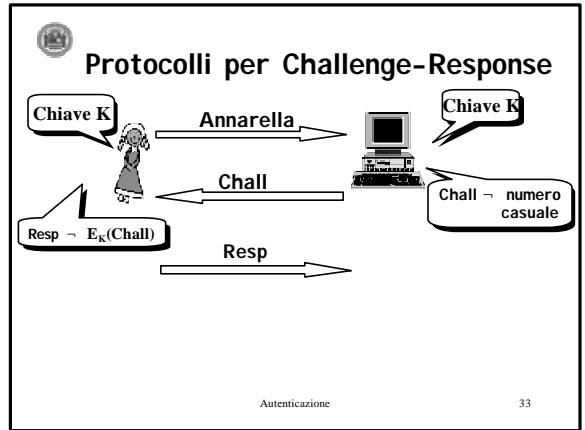
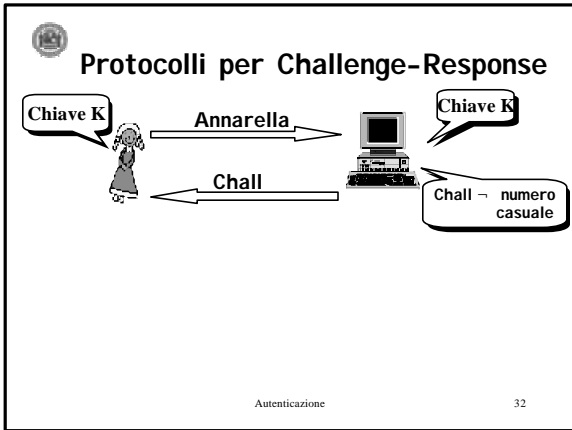
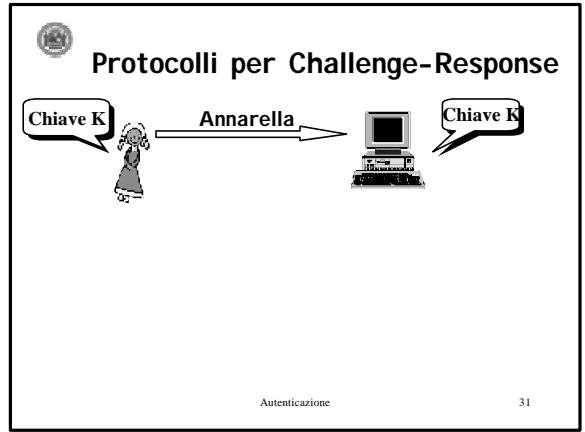
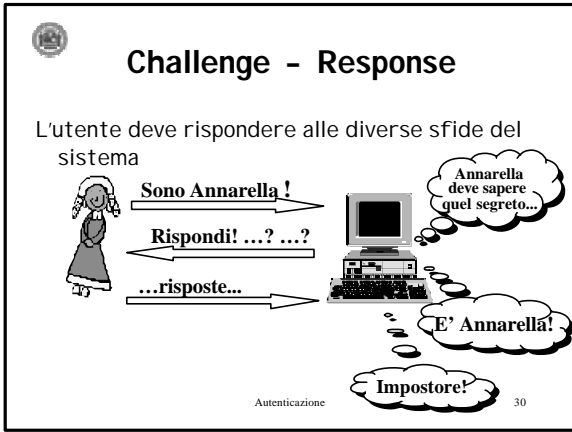
L'utente deve rispondere alle diverse sfide del sistema

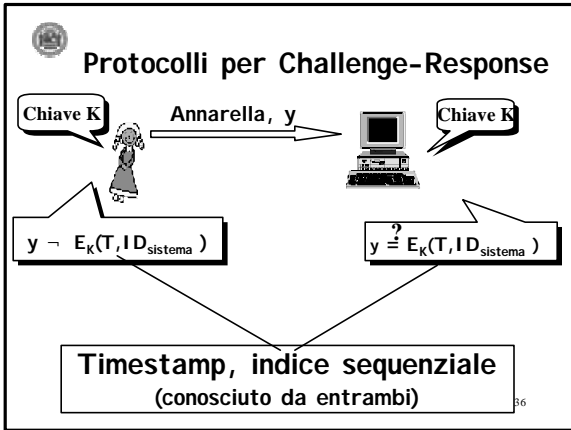


## Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema







**Standard ISO/IEC 9798**

Specifica meccanismi di autenticazione

ISO (International Organization for Standardization)  
IEC (International Electrotechnical Commission)

- 9798-2: basati su cifrari simmetrici
- 9798-3: basati su firme digitali
- 9798-4: basati su MAC
- 9798-5: basati su tecniche *zero-knowledge*

Autenticazione 37