Autenticazione utente

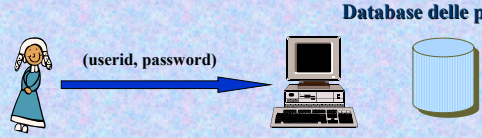
Sistemi di autenticazione: principi

- 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

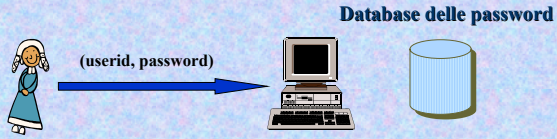
Caratteristiche

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

Password



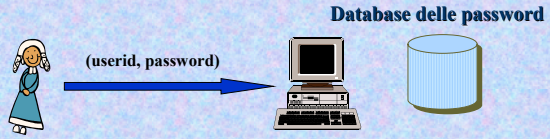
Password



Il sistema deve memorizzare una rappresentazione della password

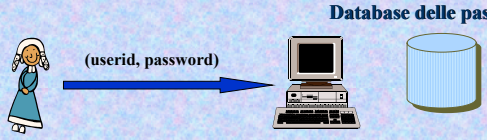
Come?

Password



Memorizzate in chiaro in un file protetto

Password



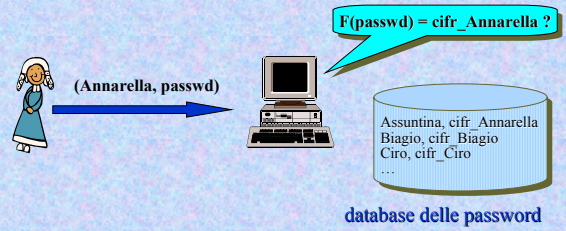
Memorizzate in chiaro in un file protetto

Problemi:

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

Password

Memorizzate in forma cifrata



Password: attacchi

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

Vulnerabiltà delle password

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

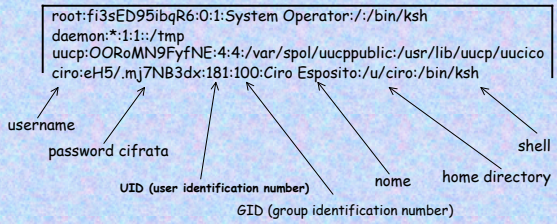
- 15 erano un singolo carattere ASCII
- 72 erano una stringa di 2 caratteri ASCII
- 464 erano una stringa di 3 caratteri ASCII
- 477 erano una stringa di 4 caratteri alfanumerici
- 706 erano una stringa di 5 lettere tutte minuscole o tutte maiuscole
- 605 erano una stringa di 6 lettere tutte minuscole

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

Password sotto UNIX

File /etc/passwd



Password sotto UNIX

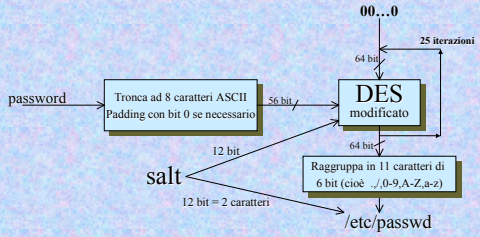
Funzione di cifratura = variante del DES

- 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

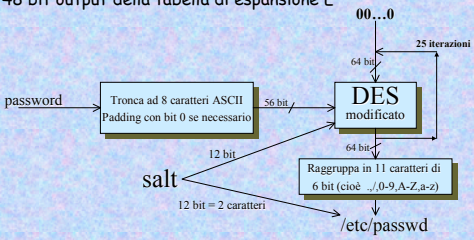
Password sotto UNIX

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



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
nei 48 bit output della tabella di espansione E



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

⇨ c / ⇩ n	26 (minuscole)	36 (minuscole alfanumerici)	62 (min. e maius. alfanumerici)	95 (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⇨0 ℓ⇨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+, anlpasswd,...
  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:FeEQShVEhOlq6:10889:0:10000::::`

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

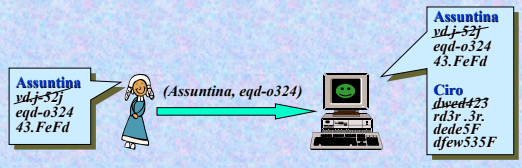
Invecchiamento password

- 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)

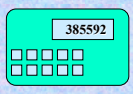
One-time password

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



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

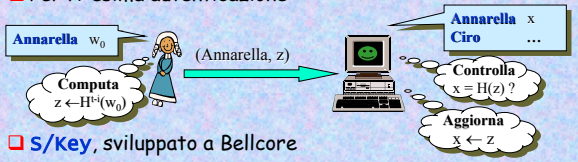


Schema di Lamport [1981]

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

Schema di Lamport [1981]

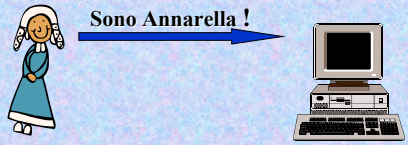
- Schema di Lamport per t autenticazioni (H funzione hash)
- Annarella sceglie w_0. Sia $H^i(w_0) = H(H(\ldots H(w_0)\ldots))$ (i volte)
- Per l'i-esima autenticazione



- S/Key, sviluppato a Bellcore

Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema

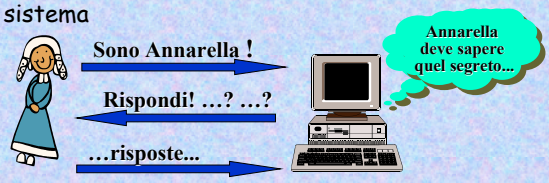


Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema

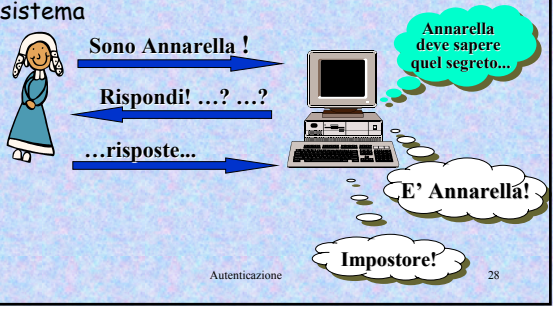
Challenge - Response

L'utente deve rispondere alle diverse sfide del sistema

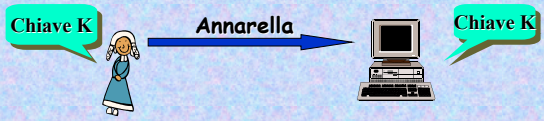


Challenge - Response

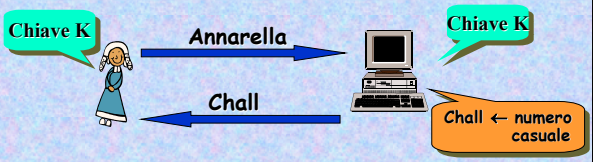
L'utente deve rispondere alle diverse sfide del sistema



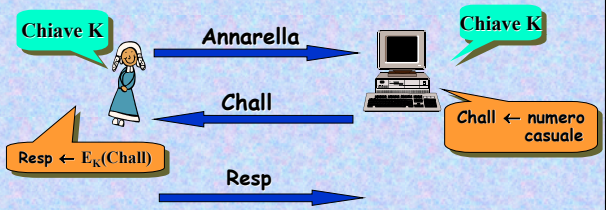
Protocolli per Challenge-Response



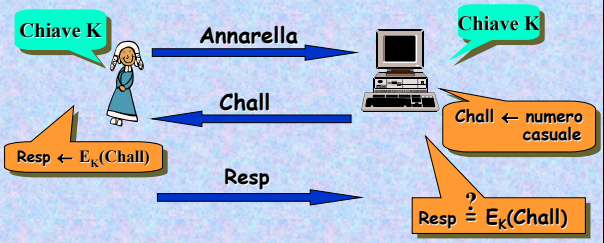
Protocolli per Challenge-Response



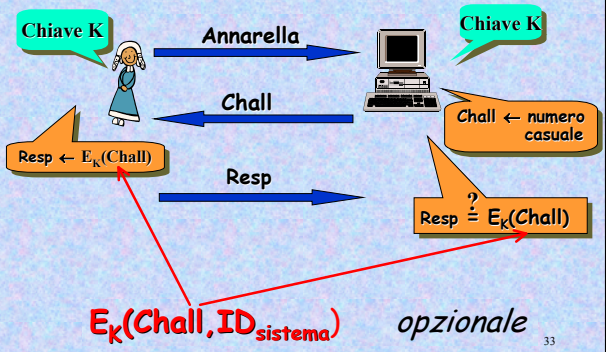
Protocolli per Challenge-Response



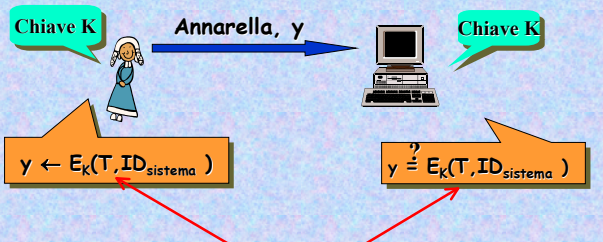
Protocolli per Challenge-Response



Protocolli per Challenge-Response



Protocolli per Challenge-Response



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*

Biometria: un po' di storia

- Sistema Bertillon, usato dal 1870 per quasi 40 anni
  - *antropometria*: lunghezza braccio e dita, altezza e larghezza testa, lunghezza piedi, ...
  - Nel 1903 negli Stati Uniti furono trovati 2 Willie West con identiche misure. Il giorno dopo ...
- Impronte digitali
  - suggerito verso il 1880
  - adottato dalla polizia londinese verso il 1900

Riconoscimento della Voce

- Training lungo
- L'efficacia dipende dal livello di rumore
- La voce cambia col tempo e ... con le malattie
- A molti non piace parlare ad un computer
- Computazione complicata (trasformata di Fourier,...)
- Attacchi di replay
  - Difesa: cambiare ogni volta la frase da leggere!

Dinamica della firma

- Semplice confronto della firma
  - facile da falsificare
  - molti hanno diverse variazioni nella firma

- In aggiunta al controllo delle coordinate: controllo pressione, tempo, velocità, accelerazione
- Per maggiore sicurezza:
  - cambiare ogni volta la frase da scrivere!

Impronte digitali: caratteristiche

- **Immutabilità:** configurazione e dettagli sono permanenti
- **Unicità:** la probabilità di trovare due impronte coincidenti, anche tra gemelli omozigoti, è minore di 10^{-20}
- **Classificazione:** le possibili variazioni sono limitate

Impronte digitali: anatomia

- Formate da insieme di linee dette **creste** (ridge lines)
- **Minuzie**: punti in cui le creste terminano o si biforcano
  - Furono introdotte da Francis Galton (1882-1916)
  - Classificazione ANSI (1986): terminazioni, biforcazioni, triforcazioni o crossover e indeterminate

Impronte digitali: acquisizione

- Inchiostratura e rullatura delle dita (metodo ben noto!)
- Prisma di vetro su cui viene appoggiato il polpastrello

luce immessa da una faccia del prisma

Impronte digitali: problemi

- Pulizia del trasduttore
- Accuratezza dipende dal dito da identificare
- Associate all'identificazione dei criminali

Geometria della mano

- Misura delle caratteristiche fisiche della mano:
  - lunghezza dita
  - larghezza mano
  - spessore dita

- Tra i migliori sistemi come accuratezza e accettabilità

Retina

- Simon e Goldstein nel 1935 mostrarono che la forma delle vene nella retina sono uniche per ogni individuo
- **template** in sistemi commerciali di 35 byte
- Scansione dell'occhio con raggio infrarosso

- Altro problema: allineare la testa rispetto allo scanner

scarsa accettabilita'

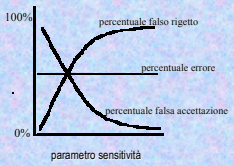
Altre tecniche biometriche

- Segno delle labbra
- Segno della pianta dei piedi 
- Forma delle vene nella mano o nel polso
- Risposta dello scheletro ad uno stimolo fisico

scarsa accettabilita'

Accuratezza

- **Falsa accettazione:** utente *non* autorizzato che passa il controllo
- **Falso rigetto:** utente autorizzato che non passa il controllo



Tecniche biometriche: conclusioni

- Studio Sandia National Labs, su sistemi commerciali

tecnica	errore
voce	2%
firma	2%
retina	0,40%
mano	0,10%
impronta	9% falso rigetto
	nessuna falsa accettazione

caratteristica	migliore	peggiore
accettabilita	mano	voce
falso rigetto	mano	impronta
falsa accettazione	mano, retina, impronte	voce
throughput	mano, retina, impronte	voce, firma
Difficolta di imitazione	retina	voce, firma
Grandezza template	retina	voce
costo	voce	retina

- Alta percentuale di errore
- Bene usarle insieme alle password!

il sistema controlla ciò che l'utente è + quello che sa