system security basics

access control

- eseguito dal kernel quando un processo (soggetto) intende accedere ad una risorsa (oggetto)
  - l‘accesso è richiesto tramite system call
  - input ad access control:
    - “credenziali” processo (soggetto)
      - la struttura delle credenziali varia a seconda dei kernel,
    - permessi della risorsa
      - in altre parole i “diritti”, ma visti dal punto di vista della risorsa
    - tipo di accesso richiesto (cioè l’operazione)
      - è dato dalla semantica della system call
  - risultato:
    - accesso concesso: system call eseguita con successo
    - accesso negato: la system call ritorna un errore
- windows e linux
  - i sistemi di permessi e credenziali di windows e linux realizzano Discretionary Access Control

access control nel filesystem

- controllo di accesso quando la risorsa è un file o una directory
- la struttura dei permessi dei file dipende dal sistema operativo
  - tipicamente basato su **access contro list**, ma con espressività limitata
  - per operazioni su file già esistenti (read/write) effettuato tipicamente **all'apertura del file**
- molto importante poiché…
  - gran parte dei dati risiedono su filesystem
  - in unix "tutto è un file"
- vedi parte dedicata a sistemi unix

autenticazione

- fase in cui si **identifica l'utente** e **si crea il primo processo** dell'utente
  - le credenziali contengono lo user-id
  - tipicamente contengono anche altro
    - dipende dal sistema operativo
- il processo che fa l'autenticazione è privilegiato e può **lanciare processi con le credenziali di utenze diverse**
  - tipicamente i processi regolari possono lanciare processi solo con le loro stesse credenziali

il database degli utenti

- il processo che esegue l'autenticazione effettua le **verifiche** rispetto ad un **database degli utenti**
- il db contiene lo **username**, lo **user-id**,…
- …altro che dipende da…
  - **…tipo di autenticazione** (vedi dopo)
  - …ulteriori aspetti legati alla autenticazione e al controllo di accesso
    - es. scadenza account, scadenza password, ruolo/i, gruppi, capabilities, ecc.

criticità del database degli utenti

- il password DB è un punto di vulnerabilità
  - chi vi accede può fare attacchi brute force, rainbow, basati su dizionario (vedi dopo)
- assolutamente da proteggere:
  - il DB stesso mediante configurazione di diritti
  - i processi che accedono al DB
    - questi devono avere i diritti di accesso al DB
    - … ma se sono vulnerabili (es. buffer overflow) l'intero DB può essere rivelato
    - es. comando passwd

approcci all’autenticazione

- qualcosa da **sapere**
  - password, pin, ecc.
- qualcosa da **possedere**
  - smart card, e-token, ecc.
- caratteristica biometrica (**essere**)
  - impronte digitali, iride, retina, viso, impronta della mano, impronta vocale, keystrokes timing
- **posizione** fisica
  - solo nella sala controllo, solo nel laboratorio, ecc.

vulnerabilità di password e login

- account e password di **default**
- password **troppo semplici**
  - vedi “easy-to-guess passwords”

- gli attacchi possono essere…
  - **on-line**: provare il login
  - **off-line**: possedendo il database egli utenti
  - tipicamente richiedono molti tentativi

attacchi on-line vs. off-line

	on-line	off-line
strumenti	script che automatizzano il normale login	password cracker (**brute force** + o – sofisticato), **dizionari**, **GPU** (per la crittografia)
scala temporale e quantità di password provate	poche password al secondo, migliaia di password al più	miliardi di password al secondo, dipende dal **budget** dell'attaccante (**uso di cloud**)
vantaggi dell'attacco e criticità lato difesa	**non necessità accesso allo user db**	veloce, **parallelizzabile**, efficace, difficile da contrastare (dopo che il db è stato violato)
Vantaggi lato difesa e criticità lato attaccante	facile da impedire con adeguata configurazione	**necessita accesso allo user db**

protezione da attacchi on-line

- autenticazione svolta dal normale programma di login
  - tipicamente configurabile
- semplici configurazioni
  - **log**
  - **ritardo** dopo ogni tentativo di login
  - ritardo a crescita esponenziale
  - max numero di tentativi falliti e **lock dell'account** per un tempo limitato o indefinitamente

protezione da attacchi off-line

- il database delle utenze può essere protetto mediante **controllo di accesso**
  - tale protezione può o meno essere sufficiente
    - dipende dalla criticità dell'applicazione
  - defence in depth: assumere che comunque l'attaccante possa riuscire ad accedere al db delle utenze
- se l'attaccante può accedere al database, la difesa deve considerare **strumenti crittografici**
  - tipicamente hashing, con salting contro attacchi a rainbow tables
  - questo tipo di protezione ha basso costo e alta efficacia
- **in ogni caso è importante che gli utenti scelgano buone password**
  - per contrastare gli attacchi brute force, che sono sempre possibili se l'attaccante riesce ad accedere al db delle utenze

Klein's easy-to-guess passwords

1. Passwords based on account names
   - Account name followed by a number
   - Account name surrounded by delimiters
2. Passwords based on user names
   - Initials repeated 0 or more times
   - All letters lower-or uppercase
   - Name reversed
   - First initial followed by last name reversed
3. Passwords based on computer names
4. Dictionary words
5. Reversed dictionary words
6. Dictionary words with some or all letters capitalized
7. Reversed dictionary words with some or all letters capitalized
8. Dictionary words with arbitrary letters turned into control characters
9. Dictionary words with any of the following changes: a 2 or 4, e 3, h 4, i 1, l 1, o 0, s 5 or $, z 5.
10. Conjugations or declensions of dictionary words
11. Patterns from the keyboard
12. Passwords shorter than six characters
13. Passwords containing only digits
14. Passwords containing only uppercase or lowercase letters, or letters and numbers, or letters and punctuation
15. Passwords that look like license plate numbers
16. Acronyms (such as "DPMA," "IFIPTC11," "ACM," "IEEE," "USA," and so on)
17. Passwords used in the past
18. Concatenations of dictionary words
19. Dictionary words preceded or followed by digits, punctuation marks, or spaces
20. Dictionary words with all vowels deleted
21. Dictionary words with white spaces deleted
22. Passwords with too many characters in common with the previous (current) password

proactive password selection

- si costringe l'utente a scegliere buone passwords
  - es. quando l'utente aggiorna la password si fa girare un ***password cracker*** ed eventualmente si rifiuta la password
    - il password cracker è configurato per eseguire un attacco brute force blando ma rapido
  - es. si fornisce un **feedback sulla "bontà"** della password

- problemi con password lunghe, complesse, da cambiare frequentemente:
  - contro il principio di usabilità
  - gli utenti vedono i vincoli come un problema
    - **password scritte su post-it attaccati al monitor o sotto la tastiera**
  - si deve trovare un **compromesso** anche in base alla criticità dell'account e al tipo di utenti

gestione personale delle password: password manager

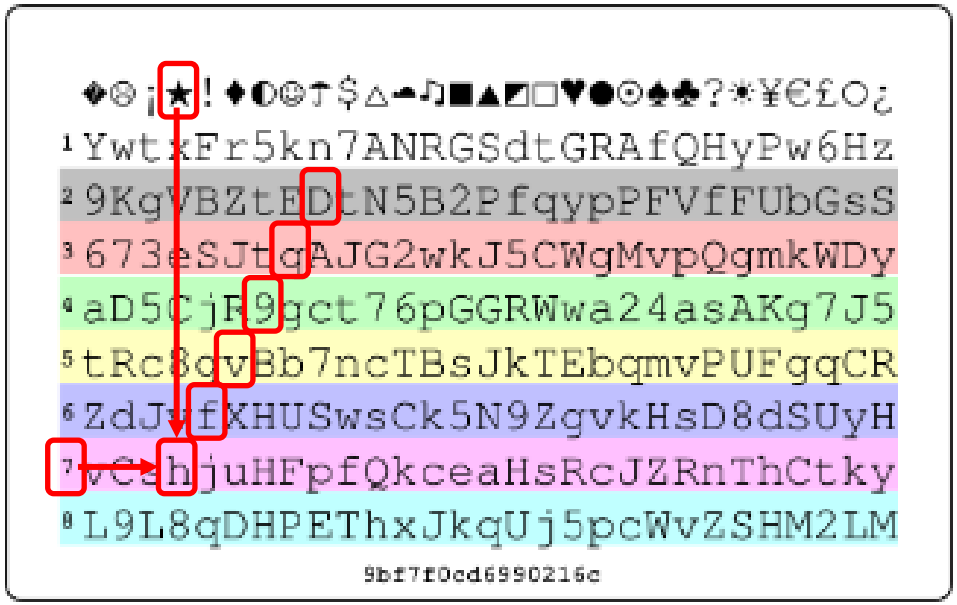
- software che memorizza username e password in maniera cifrata
  - basta una sola password per accedere a tutte le altre
  - es. keepass, gorilla, etc.
- features
  - configurable iterated encryption
    - to face brute force attacks
  - copy-paste, autotype, autofill with browser plug-in, metadata (url)
  - password strength metric, random password generation
  - open vs. closed source
  - multiplatform, mobile (?)
  - Cloud based, sync DB with cloud account
  - random key on memory sticks as (co-)master password
  - DB-less Hash-derived passwords (generate via hash da url e master password)

password manager: criticalities

- published DB (e.g., cloud) + weak master password
  - we can add random “key file” stored on local devices
- unlocked DB + unlocked desktop
- another software can attach to the password manager as a “debugger”
  - … and get the DB and/or the master password
  - recent OSes have protection against this
- untrusted software as password manager

alternatives: passwordcard

- https://www.passwordcard.org/
  - randomly generated by a key (not needed to be keept confidential)
  - choose your private (e.g. 6 chars NW)
  - just remember starting coordinates for each password



alternatives: “mnemotechnics”

- useful for master passwords of a password manager
- seeds
  - chose a quote of your infancy
    - with “words” that are not in the dictionary
  - chose a song, poetry, or other easy to remember
- apply a rule
  - e.g., second letter of each word

altri strumenti importanti

- hardening and patching
- logging
- auditing
  - SIEM
  - vulnerability assessment
  - penetration test