sicurezza nei sistemi di calcolo

sommario

- access control
- autenticazione e passwords
- vulnerability scanners
- hardening
- logging e log auditing

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"

autenticazione

- fase in cui si **identifca 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.

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	**non necessità accesso allo user db**	veloce, **parallelizzabile**, efficace, difficile da contrastare (dopo che il db è stato violato)
svantaggi	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 degli utenti può essere protetto mediante **controllo di accesso**
  - tale protezione può o meno essere sufficiente
    - **dipende dalla cura con cui si mitiga tale rischio**
  - defence in depth: si assume che possa essere rivelato all'attaccante
- se l'attaccante ha il database, la difesa deve prevedere **metodi crittografici**
  - trattati nel seguito del corso

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

vulnerability assessment

- studio automatizzato per individuare quali vulnerabilità sono presenti in un sistema: **configurazioni o bug software**
- caratteristiche
  - altamente automatizzato, fino alla creazione dei report
    - intervento umano limitato
  - eseguito su base periodica
  - efficace **solo per vulnerabilità già ben note per prodotti diffusi e per errori di configurazione tipici**
  - **inefficace per software custom**
  - poco costoso (rispetto al penetration test)
- strumenti con **database di vulnerabilità**
  - il db, per ogni software e relativa versione, fornisce le vulnerabilità note
- **le vulnerabilità ben note costituiscono il pericolo maggiore**
  - perché l'exploit è noto

penetration test

- procedura per individuare le vulnerabilità di un sistema usando tecniche di hacking
- caratteristiche
  - richiede un **pesante intervento umano**
  - svolto da **specialisti**
  - si usano **ambienti di sviluppo** per exploit specifici o esecuzione di exploit di libreria (es. metasploit)
  - potrebbe trovare **vulnerabilità non** note
  - **utile anche per software custom**
  - **molto costoso**
  - comunque **mai esaustivo**
- deve essere svolto all'interno di un **framework contrattuale che tutela sia if «pen-tester» e l'organizzazione** che ha richiesto il servizio
  - vincoli sui test (ora e perimetro di intervento), prove di successo, codice etico
- mai fare attacchi e poi proporsi all'organizzazione vittima mostrando le vulnerabilità senza avere un contratto
  - il rischio di denuncia è alto, per molte amministrazioni è un atto dovuto

vulnerability scanners

- nmap
  - scanning delle porte
  - versione OS, versione server, uptime
- nessus/OpenVAS
  - scanning delle porte
  - identificazione delle versioni dei server
  - matching su un db di vulnerabilità
  - check “locale” con login ssh
- moltissimi tool commerciali
  - http://sectools.org/vuln-scanners.html

hardening

- attività di **mitigazione del rischio di attacco**
- consiste nel **configurare** una macchina in modo da rendere difficili o impossibili certi attacchi tipici
- agisce principalmente sulla configurazione di sistema, servizi, applicazioni, utenze, privilegi, ecc.
- tipicamente abbinata a...
  - dei sistemi di log auditing
  - una corretta politica di mantenimento

hardening: metodologia

- l’hardening richiede
  - grosse competenze tecniche
  - un aggiornamento costante rispetto alle minacce
- basato spesso su “best practices”

hardening: gruppi e utenze

- avviare solo le utenze strettamente indispensabili appartenenti alle seguenti categorie
  - user accounts (gli utenti)
  - system accounts (account per amministrazione)
    - molto pericolosi (es. root)
    - preferibilmente non accessibili dall'esterno
  - application accounts
    - particolari system accounts con privilegi limitati
- bloccare il login di tutti gli account che non fanno capo ad una persona
- se ci sono più persone che devono compiere operazioni privilegiate usare il meccanismo dei gruppi

hardening: permessi

- elimina, se possibile, file e directory scrivibili da tutti gli utenti
  - sono fonte di potenziali interferenze tra gli utenti
  - questo controllo dovrebbe essere fatto periodicamente
    - si può usare un IDS come tripwire per automatizzare questa verifica

hardening: servizi

- solo i servizi strettamente indispensabili
- meno servizi → meno vulnerabilità
- attenzione maggiore a servizi di rete
- per i servizi rimasti considera...
  - ... di far girare un servizio con una utenza limitata
    - cioé un application account
  - ... jailing (vedi nel seguito) se possibile
  - ... considera il serivizio come “critico” e applica una politica adeguata
    - monitorare in maniera stringente i relativi security alert
    - tempestività nell'applicare le patch di sicurezza

hardening: servizi privilegiati

- i servizi/comandi privilegiati utilizzabili dall'utente sono pericolosi
- spesso il software gira con diritti maggiori rispetto a quelli dell'utente che lo usa
  - server (web, email, ecc.) permettono a "utenti remoti" di effettuare operazioni sul sistema in cui gira
  - programmi con diritti privilegiati (passwd, ping, ecc.) permettono di effettuare operazioni normalmente non ammesse per l'utente comune

hardening: servizi privilegiati

- è veramente necessario tali servizi/comandi siano privilegiati?
  - considerare l'uso di un application account con privilegi limitati
  - considera l'uso di wrapper di sicurezza che verificano e limitano gli input a tale comando/servizio
    - richiede programmazione, tipicamente in C

hardening: schema di un wrapper

Initialize string constants such as the full path to the real program, maximum string lengths, the allowed character mask, and the allowed environment variable list

Check that an environment exists (used by interactive programs)

Check that USER & uid can be found in user db (paranoid option)

For i=1 to argc

- rewrite each character using a character mask
- if string length > predetermined value, error out

For i=1 to length of envp

- drop any variable not in predetermined list
- rewrite each character using a character mask
- if string length > predetermined value, error out
- if variable is suppose to be the user name but isn't, error out (paranoid option)

Create the new environment variable array

Execve real program with new environment and safe argument strings

hardening: strumenti

- un hardening efficace è molto difficile fare manualmente
- si usano **strumenti automatici** che guidano/suggeriscono la configurazione del sistema
- tools famosi
  - lynis
  - bastille (obsoleto)
  - MBSA

hardening: security patches

- kernel, software di sistema e applicazioni sono sicuramente affetti da bug di sicurezza
  - un bug diventa problematico solo dopo che ne viene diffusa l'esistenza
- applicazione di pach di sicurezza o upgrade
  - fondamentale la tempestività rispetto all'annuncio
- la patch potrebbe tardare ad apparire, nel frattempo considera...
  - spegnimento del servizio
  - riduzione dei privilegi
  - wrapping

hardening: security patches

- per software open la patch è spesso più rapida da ottenere ma richiede la ricompilazione dell'applicazione
  - la preparazione di un pacchetto binario che include la patch può richiedere tempo
  - la compilazione di un pacchetto software può richiedere un po' di esperienza
- per software proprietari possiamo solo confidare nel vendor per una patch binaria

hardening: log auditing periodico

- attivare meccanismi di auditing che permettano di avere una verifica continua nel tempo
  - log auditing come logwatch, lire, swatch, logsurf
  - Intrusion Detection Systems

logging

- attività di registrazione di eventi relativi a...
  - comportamento degli utenti
  - servizi
  - applicazioni
  - anomalie
  - ecc.
- la registrazione è sempre **sollecitata** da…
  - **processi** che implementano servizi o applicazioni
  - **kernel** in presenza di anomalie o eventi particolari

logging e policy

- è necessario proteggere i log da manomissioni
  - obiettivo di un hacker è quello di essere invisibile quindi spesso sono oggetto di modifica
- una buona politica di sicurezza dovrebbe…
  - proteggere l'integrità dei log
    - monitoraggio della taglia, compressione, rotazione, consolidation in un log server, protezione dalla scrittura (hardening del log server).
  - far sì che vengano loggati tutti gli eventi "**interessanti**"
    - accurata configurazione del logging
  - far sì che le informazioni "**critiche**" contenute nei log vengano prontamente comunicate all'amministratore perché possa prendere adeguate misure reattive
    - log auditing

log auditing

- una attività di verifica periodica dei log in modo da individuare tentativi di intrusione
- il log auditing “a occhio” è improponibile
- tools automatici di reporting periodico
  - scanning periodico delle nuove righe dei log (a partire dall'ultimo scan)
  - email con report
  - possibilità di fare scanning su log da varie fonti
    - es. web server, firewalls, ecc.
- es. logwatch

SIEM: Security Information Event Manager

- il log auditing è ora parte di prodotti integrati: i SIEM
- integrano
  - collezionamento da moltissime fonti (scalano)
  - motore di correlazione di eventi
  - regole puntuali o statistiche per sollevare allarmi
  - strumenti di analisi (business intelligence)
- costo non trascurabile
  - di acquisizione e di gestione
- MSSP: Managed Security Service Provider
  - servizi che forniscono funzionalità SIEM outsourced