Securitatea sistemului

SO: Curs 13

Cuprins

- Principii de securitate
- Cel mai mic privilegiu
- Drepturi pe fișiere
- Autentificarea utilizatorilor

Suport de curs

- Operating Systems Concepts
  - Capitolul 14 – Protection
  - Capitolul 15 – Security
    - Secțiunile 15.1, 15.2, 15.5
- Modern Operating Systems
  - Capitolul 9 – Security
    - Secțiunile 9.4, 9.6

PRINCIPII DE SECURITATE

Principii de securitate

- Principiul celui mai mic privilegiu
- Cât mai puține caracteristici (feature creep)
- Controlul accesului
- Autentificare/autorizare
- Securizare (criptare)
- Defense in depth
- Risk management
- Sistemul trebuie să rămână utilizabil
  - Un sistem de securitate prea complicat va fi utilizat greșit => se obține efectul invers

Kernel Mode

- Instrucțiunile privilegiate sunt executate în spațiul kernel
  - accesul la I/O
  - alocarea de resurse
  - handler-ele de întrerupere
  - gestiunea sistemului
- Suportul procesorului
  - niveluri de privilegiu (rings)
  - x86: nivelul 0 (kernel), nivelul 3 (user)

Least Privilege

- Accesarea doar a acelor resurse/date necesare
- Aplicat la utilizatori, procese
- Privilege escalation
- Privilege separation
- Privilege revocation
- Sandboxing

Privilege separation

- componente separate au roluri separate
- cuplat cu principiul celui mai mic privilegiu
- exemplu: Postfix; master (root) + smtpd, pickup, cleanup, qmgr (postfix)
- folosirea utilizatorului nobody
- bitul setuid

Privilege escalation

- bug în aplicații - obținerea unor drepturi necuvenite
- de obicei sunt atacate conturile privilegiate
- sunt exploatate programele care rulează ca root - atenție specială executabilelor cu bitul setuid activat

Capabilities

- O cheie asociată unor acțiuni privilegiate sau unor drepturi de acces
- Pot fi interschimbate între entități
  - nu este un lucru obișnuit în sistemele de operare actuale
- Capabilități POSIX (IEEE 1003.1e)
  - CAP_NET_BIND_SERVICE
  - CAP_SYS_CHROOT
  - CAP_NET_RAW
- man 7 capabilities
  - nu se poate accesa un director/fișier din afara ierarhiei impuse de noul director rădăcină

setuid/setgid

- Real user ID
- Effective user ID
- Bitul setuid (chmod 4777)
  - permite configurarea euid ca utilizatorul ce deține executabilul
- setuid
  - total privilege revocation (real user ID, effective user ID)
- seteuid
  - temporary privilege revocation (effective user ID)

main() în ping.c

```
int
main(int argc, char **argv)
{
        struct hostent *hp;
        int ch, hold, packlen;
        int socket_errno;
        u_char *packet;
        char *target, hnamebuf[MAXHOSTNAMELEN];
        char rspace[3 + 4 * NROUTES + 1]; /* record route space */

        icmp_sock = socket(AF_INET, SOCK_RAW, IPPROTO_ICMP);
        socket_errno = errno;

        uid = getuid();
        if (setuid(uid)) {
                perror("ping: setuid");
                exit(-1);
        }
[...]
```

chroot

- Modifică directorul rădăcină asociat procesului.
  - nu se poate accesa un director/fișier din afara ierarhiei impuse de noul director rădăcină
  - chroot jail
- Comanda chroot
- Apelul chroot

```
chroot("/var/spool/postfix");
```

SECURITATEA FIȘIERELOR

Controlul accesului

- access control
- subiecți/obiecte
- matrice de control al accesului (access control matrix)

Controlul accesului (2)

- DAC - discretionary access control
  - decis de posesorul obiectului
  - posesor (owner) și drepturi de acces (access control rights)
  - ACL-based, capability-based
- MAC - mandatory access control
  - decis de sistem, nu de posesorul obiectului
  - subiecții și obiectele dispun de o etichetă
  - un subiect cu eticheta L1 poate accesa un obiect cu eticheta L2 dacă L1 > L2
- RBAC - role-based access control
  - decis de sistem
  - acces pe bază de roluri; un rol este un set de permisiuni

Drepturi pe fișiere

- Asocierea drepturilor de acces pentru utilizatori la fișiere
- Citire, scriere, ștergere, execuție
- Creare fișier, listare, ștergere fișier, parcurgere

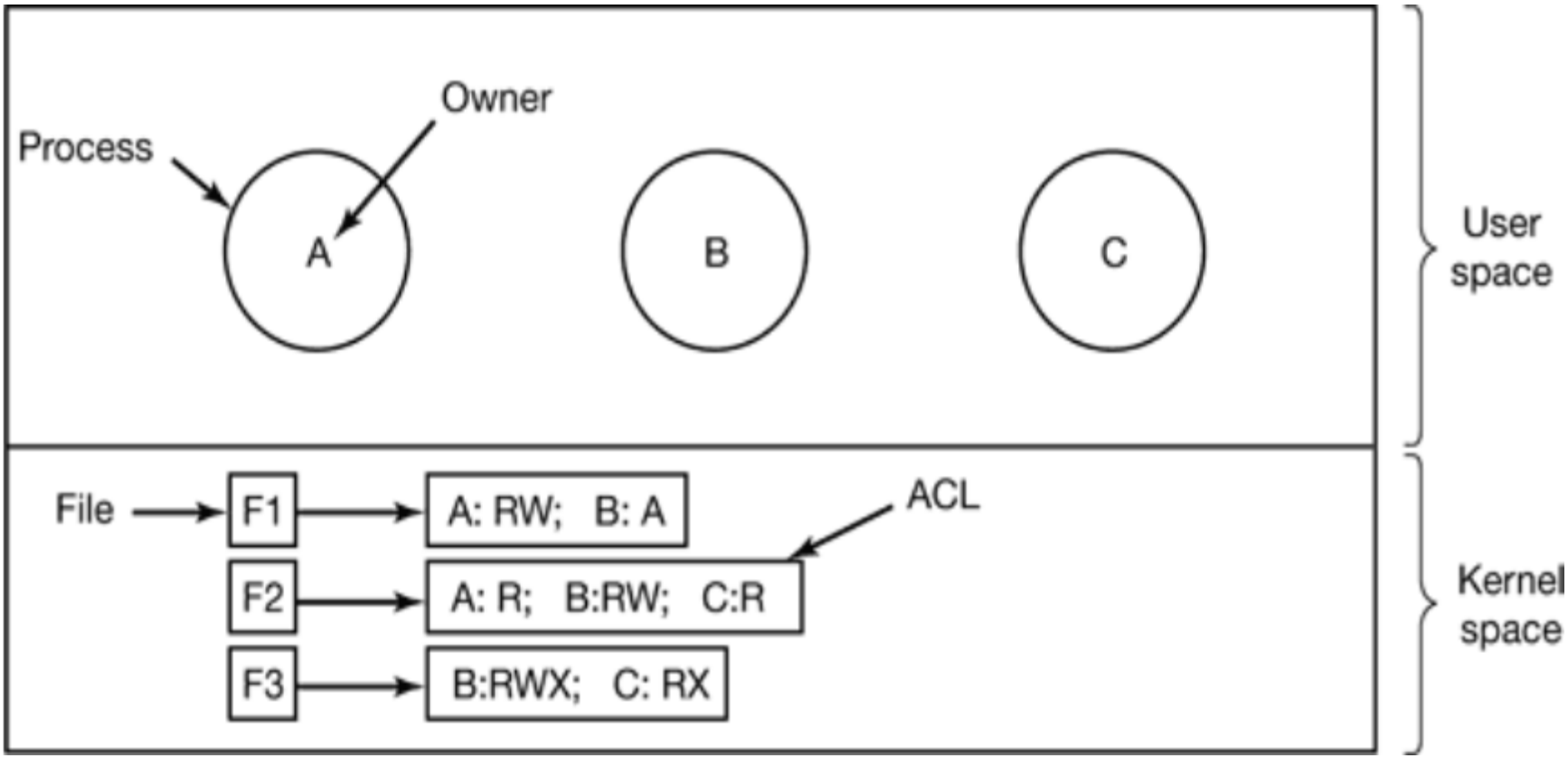
Matrice de acces

Domain	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

Drepturi pe fișiere în Unix

- Matrice de acces
- Domeniile sunt
  - utilizator (user) - deținătorul fișierului
  - grup (group) – grupul deținător al fișierului
  - alții (others)
- Drepturi
  - read (r) – citire, listare
  - write (w) – scriere, creare fișier
  - execute (x) – execuție, parcurgere

Liste de acces



Liste de acces (2)

- POSIX ACL
  - implementate pe sisteme de fișiere Linux cu extended attributes
  - getfacl, setfacl
- Drepturi pe fișiere în Windows
  - ACL pe NTFS
  - read, write, list, read and execute, modify, full control
- Role-based access control (RBAC)
  - sudo

Drepturi Unix

- DAC
  - există noțiunea de posesor (owner) (user, group)
  - chown, chgrp
- formă simplificată de ACL
- trei subiecți: utilizator (user), grup (group), ceilalți (others)
- chmod
  - deținătorul (user) poate schimba drepturile de access
  - read, write, execute
- umask
  - drepturile implicite pentru crearea unui fișier
  - ~umask & 666 pentru fișiere
  - ~umask & 777 pentru directoare

ACL vs. Capabilități

- ACL
  - listă de permisiuni atașate unui obiect
  - specifică subiecții (utilizatori, procese) care pot accesa obiectul
  - specifică operațiile posibile asupra subiectului
  - (andrei, read), (bianca, read & write), (cosmin, execute)
  - ACE (access control entries) în sisteme de fișiere
  - POSIX.1e ACL pe sisteme Unix
  - forma standard de drepturi Unix sunt o formă simplificată ACL
- Capabilități
  - token de autoritate
  - referă un obiect și acțiunile posibile asupra acestuia
  - un proces/utilizator trebuie să posede token-ul pentru a putea accesa obiectul
  - se permite transferul token-ului de la un subiect la altul (neimplementat în majoritatea sistemelor de operare)

SECURITATEA UTILIZATORILOR

Autentificarea utilizatorilor

- Accesul utilizatorilor în sistem
- Parolă
- Cheie publică
- Voice recognition, identificatori biometrici

/etc/passwd + /etc/shadow

- /etc/passwd
  - user:password_hash:uid:gid:...
  - problemă
    - accesul utilizatorilor (nevoie de informații diferite de password_hash)
- /etc/shadow
  - user:password_hash:...
  - security enforcing
    - număr de zile între schimbat parola
    - număr de zile după care contul este dezactivat
    - ....

Password hash în Unix

- man 3 crypt
- Implicit DES
- `$id$salt$encrypted`
- ID: 1 (MD5), 2a (Blowfish), 5 (SHA-256), 6 (SHA-512)
- salt este folosit pentru a adăuga un nivel suplimentar de criptare a parolei
  - un salt pe 12 biți înseamnă 4096 de posibilități de criptare

Autentificarea prin chei publice

- Cheie publică + cheie privată
- Cheia publică este pe sistem (server)
- Cheia privată este folosită pentru autentificare
- Legătură matematică
  - one way function
  - de fapt este two-way, insa nu este computațional fezabil să se calculeze inversul funcției (încă..)
- RSA, DSA

OTP

- One Time Password
- Time-synchronized OTP
  - RSA SecurID
- Algoritm matematic
  - s – initial seed
  - f – one-way function
    - cryptographic hash function
      - it is easy to compute the hash value for any given message,
      - it is infeasible to find a message that has a given hash,
      - it is infeasible to modify a message without changing its hash,
      - it is infeasible to find two different messages with the same hash.
  - f(f(f(f(...f(s)...))), ..., f(s)

ulimit

- comandă internă bash
- help ulimit
- limitează resursele shell-ului și a proceselor create
- limite soft și hard
  - resident set size
  - număr de descriptori de fișiere
  - dimensiunea stivei
  - dimensiunea memoriei virtuale
- informații dinamice

Cote

- limitări la nivelul sistemului de fișiere
- în Linux 4 valori de configurat la nivel de utilizator/grup
  - limitarea numărului de fișiere/inode-uri (soft/hard)
  - limitarea spațiului ocupat la nivel de blocuri (soft/hard)
- necesită suportul sistemului de fișiere

Dezactivarea accesului utilizatorilor

- împiedicarea accesului la cont
- /bin/false în loc de /bin/bash în /etc/passwd
- account expiration
- account locking
- password expiration

Expirarea contului

- echivalentă cu dezactivarea sa
- cel mai simplu: usermod -e 1 traian
- usermod -e 2013-10-31 traian
  - contul va fi dezactivat după data 31 octombrie 2013

Expirarea parolei și account locking

- nu mai funcționează autentificarea pe bază de parolă
- informații stocate în /etc/shadow
- passwd -l username
- usermod -L username
  - apare un semn ! în fața parolei criptate
  - contul va fi încuiat (locked)
  - usermod -U username (unlock)
- usermod -f 10
  - după 10 zile de la expirarea parolei contul este dezactivat
- /etc/default/useradd

Expirarea parolelor

- în Linux, informații stocate în /etc/shadow
- chage
- se poate configura intervalul de după expirare când contul este "locked"

Cuvinte cheie

- least privilege
- kernel-mode/user-mode
- setuid
- matrice de acces
- ACL
- capabilities
- /etc/passwd
- /etc/shadow
- drept de acces
- chmod, umask
- chroot
- ulimit
- cote
- expirarea contului
- expirarea parolelor