SISTEME DE OPERARE (SO)

CURS 11

Lect. Univ. Dr. Mihai Stancu

Elemente de securitate

Departamentul de Informatică

- Suport (Introducere în sisteme de operare)
  - Capitolul 10 – Elemente de securitate

Cuprins

- Noțiuni de securitate
- Securitatea sistemului de operare
- Parole
- Securitatea rețelelor

Problematica securitatii

- protecția informațiilor prețioase (companii, instituții)
- Ce este un sistem sigur?
  - resursele sale sunt utilizate și accesate în orice împrejurare așa cum se dorește
- Se poate obține un sistem 100% sigur?
  - Da. Complet izolat de lumea exterioară.
  - nu este util, nici flexibil
- Ce înseamnă securizarea unui sistem de calcul?
  - folosirea de metode de protecție **suficient** de puternice
  - un potențial atacator va fi **descurajat**
  - compromiterea sistemului este **greu** de realizat
- Securitatea este un proces nu o finalitate

Notiuni de securitate

- obiective: confidențialitate, integritate, disponibilitate, autenticitate
- privilegii
  - principiul celui mai mic privilegiu
  - escaladare (escalation)
  - revocare (revocation)
  - separare (separation)
- principii
  - security through obscurity vs. security by design
  - cea mai slabă verigă
  - simplitate (feature creep)
  - defense in depth
  - analiza riscurilor
- securitate vs. uzabilitate

Niveluri de securitate

- la nivel de persoană
  - utilizatorii sunt aleși cu grijă
  - educarea utilizatorilor
- la nivel fizic
  - protecția încăperilor ce conțin sistemele de calcul
- la nivelul sistemului de operare
  - securizarea accesului (parole)
  - protecția resurselor SO (memorie, fișiere)
  - securizarea aplicațiilor
- la nivelul rețelei
  - securizarea accesului de la distanță
  - filtrarea pachetelor de compromitere a rețelei

Securitatea sistemului de operare

- sistem de operare sigur: resursele acestuia sunt accesate în mod valid
- zone de memorie, dispozitive de I/E, fișiere, procesor
- Cine asigură securitatea sistemului de operare?
  - nucleul SO
- suport hardware
  - procesoarele oferă cel puțin două niveluri de privilegiu
    - unul pentru operații obișnuite (user mode)
    - altul pentru acces la instrucțiuni privilegiate (supevisor mode)
      - doar nucleul rulează în modul supervizor (kernel mode)
  - separarea privilegiilor

UMASK

- restricția drepturilor de creare a intrărilor în sistemul de fișiere
- valori tipice pentru umask: 022, 027, 077
- drepturi de creare implicite
  - 666 pentru fișier
  - 777 pentru director
- drepturi de creare efective
  - ȘI logic între permisiunile implicite și masca inversată

UMASK – CONTINUARE

- fișier: implicit 666
- umask: 027 → (666 & ~027) = 640 (`rw- r-- ---`)

umask pe fișiere

```
alin@anaconda:~/junk$ umask
0022
alin@anaconda:~/junk$ touch so7_test1
alin@anaconda:~/junk$ ls -l so7_test1
-rw-r--r-- 1 alin alin 0 Nov 10 17:28 so7_test1
alin@anaconda:~/junk$ umask 027
alin@anaconda:~/junk$ touch so7_test2
alin@anaconda:~/junk$ ls -l so7_test2
-rw-r----- 1 alin alin 0 Nov 10 17:28 so7_test2
```

UMASK – CONTINUARE

- director: implicit 777
- umask: 077 → (777 & ~077) = 600 (`rwx --- ---`)

umask pe directoare

```
alin@anaconda:~/junk$ umask
0027
alin@anaconda:~/junk$ mkdir so7_dir1
alin@anaconda:~/junk$ ls -ld so7_dir1
drwxr-x--- 2 alin alin 4096 Nov 10 17:29 so7_dir1
alin@anaconda:~/junk$ umask 077
alin@anaconda:~/junk$ mkdir so7_dir2
alin@anaconda:~/junk$ ls -ld so7_dir2
drwx------ 2 alin alin 4096 Nov 10 17:29 so7_dir2
```

Securitatea accesului

- se permite **numai** accesul utilizatorilor autorizați
- autentificare
  - permiterea accesului utilizatorilor privilegiați
- Când este un utilizator autentic?
  - posedă o unitate de identificare (cheie, card)
  - posedă un nume de utilizator și o parola
  - posedă un atribut de utilizator (amprentă, retină, semnătură)

Autentificare, autorizare, controlul accesului

- autentificare (*authentication*)
  - permiterea utilizatorului în sistem pe baza credențialelor (parola, semnatură biometrică, certificat digital etc.)
- autorizare
  - acordarea de drepturi de acces la resurse pentru utilizator
- controlul accesului
  - verificarea drepturilor de acces la resurse; se permite sau nu se permite accesul

Parole

- formă de autentificare (username/password)
  - se compară parola introdusă cu cea stocată de sistem
  - dacă cele două coincid se permite accesul
- modul echo off sau “cu steluțe”
  - împiedicarea *shoulder surfing*
- neajunsurile folosirii parolelor
  - păstrarea secretă a parolei
    - sticky-note care este lipit pe monitor
    - stocată în telefonul mobil
    - recomandare: folosiți aplicații de stocare securizată (keyring)
  - ghicirea parolei
  - transferul parolei de la un utilizator autorizat la unul neautorizat

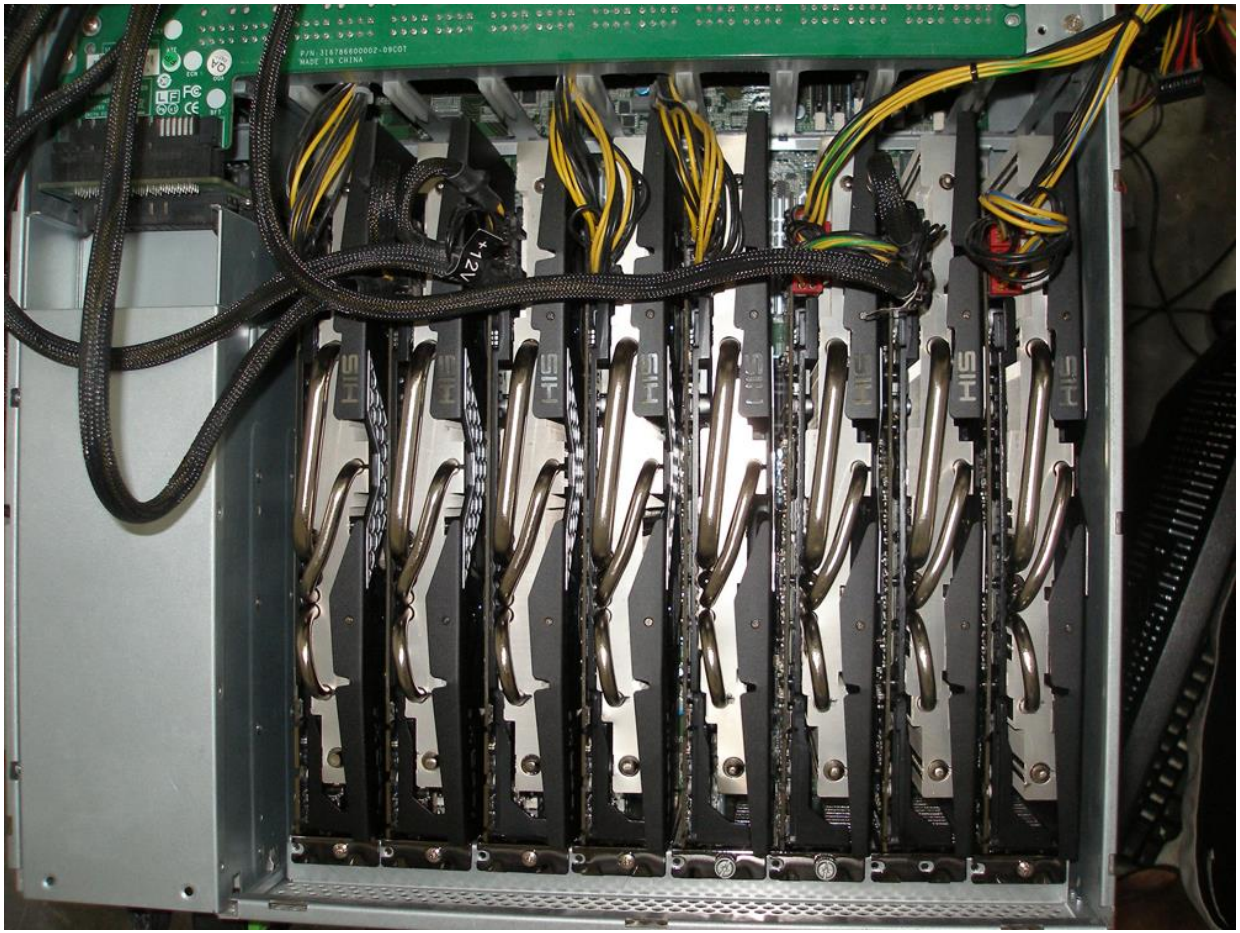
Ghicirea unei parole

- metode
  - încercări automatizate (brute force)
  - se încearcă ghicirea parolei pe baza unui dicționar
- Ar trebui să mă îngrijorez?
  - în 1997, în urma unui sondaj făcut în Londra, 82% din parole puteau fi ghicite ușor pe baza unei analize sumare a vieții subiecților
    - animale de casă, date de naștere, nume de rude
  - utilizarea forței brute
    - o parola cu 4 cifre are 10000 de posibilități
    - dacă s-ar încerca o parolă la fiecare milisecundă, în 10 secunde s-ar putea ghici parola
- John the Ripper – http://openwall.com/john/
  - dicționare (wordlist)

Protectie la ghicirea parolelor

- alegerea de parole bune
  - minim 10 caractere, atât lower case cât și upper case
  - cel puțin un caracter special sau numeric
  - nu trebuie să fie nume de persoane sau cuvinte din dicționar usor de reținut
- utilizarea parolelor generate aleator de sistem
  - pwgen
- verificarea periodică a parolelor utilizatorilor
- *password aging*: schimbarea parolei după o anumită perioadă
- folosirea de *passphrase*-uri: *I wake up at 7AM!*
- passphrase nepotrivit: *One does not simply walk into Mordor* – frază celebră, ușor de ghicit

Password Cracking



- Project Erebus v2.5
- AMD Radeon HD7970: 8.2 billion password combinations each second
- 8xAMD Radeon HD7970: 12 hours to brute force entire keyspace for any eight-character passwords (upper- or lower-case letter, digits or symbols)

Parole in Unix

- la început parolele se păstrau criptat în /etc/passwd
- fișierul /etc/passwd conține și alte informații
  - numele utilizatorilor
  - directorul home
  - shell-ul folosit
- multe programe au nevoie de informațiile de mai sus
  - fișierul /etc/passwd este citibil de toți utilizatorii

Drepturi de acces pe /etc/passwd

```
alin@anaconda:~/junk$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2147 Nov 4 15:35 /etc/passwd
```

- Parola criptată este vizibilă
  - potențial risc de spargere prin încercări

Parole in Unix – continuare

- fișierul /etc/shadow –accesibil numai de root
- parola ar putea fi spartă prin încercări de login repetate
  - timeout între încercările de autentificare

/etc/passwd

```
alin@anaconda:~/junk$ cat /etc/passwd | grep guest
guest:x:1001:1001:Guest,EF 303,,,Test:/home/guest:/bin/bash
```

/etc/shadow

```
alin@anaconda:~/junk$ cat /etc/shadow | grep guest
cat: /etc/shadow: Permission denied
anaconda:/home/alin/junk# cat /etc/shadow | grep guest
guest:$1$jv4hP2au$BSrUDS0J7LhJv8PrCFltU/:13124:0:99999:7:::
```

Contul privilegiat

- controlul absolut al sistemului
  - obținerea contului de superuser înseamnă spargerea sistemului
- trebuie folosit **numai** atunci când este nevoie
  - pentru operații obișnuite, folosiți contul **neprivilegiat**
  - o bună parte din atacurile pe Windows se bazează pe faptul că utilizatorii folosesc numai contul `Administrator`
- `sudo`
  - permite unui utilizator obișnuit (dar de încredere) rularea unui set restrâns de comenzi cu privilegii de `root`
  - *privilege separation*

- două tipuri de amenințări într-o rețea
  - vulnerabilități
    - la nivelul aplicațiilor sistemului (exploit)
    - la nivelul protocolului de comunicare folosit (SYN flood)
    - la nivelul dispozitivelor de rețea (ARP poisoning)
  - configurări necorespunzătoare
- în general există 3 faze ale unui atac
  - recunoașterea
  - obținerea accesului
  - escaladarea accesului (cont root) / folosirea sistemului pentru generarea unui nou atac împotriva unui alte rețele

Recunoasterea

- recunoașterea activă
  - host, whois
  - *ping sweep*
  - aplicații de scanare a porturilor
  - firewall – blocarea operațiilor
  - configurarea aplicațiilor să ofere detalii minime (versiune)
- recunoașterea pasivă
  - interceptarea traficului din rețea
    - tcpdump
    - Wireshark
    - Kismet
  - folosirea unor canale fizice sigure
  - criptarea traficului

Obținerea accesului

- prin analiza traficului
  - eavesdropping
  - obținerea parolei
  - criptare
- *man-in-the-middle attack*
  - un atacator este capabil să pretindă identitatea unei entități de încredere fără ca entitatea comunicantă să realizeze că legătura este compromisă
  - integritate (hashing: MD5, SHA), autentificare
- *social engineering*
  - educație

Atacuri Denial of Services

- împiedicarea accesului utilizatorilor la o resursă
- poate însemna consumul resurselor unui sistem
  - deschiderea unui număr mare de procese (fork bomb)
- congestionarea traficului în rețele
  - devine dificilă comunicația între stațiile din rețea
- *Distributed Denial of Service* (DDoS)

Prevenirea atacurilor

- stabilirea unor politici clare de securitate
- configurarea politicilor de filtrare a pachetelor
- configurarea criptării traficului important
- configurarea programelor antivirus
- detectarea atacurilor / problemelor
  - monitorizare
  - IDS (*Intrusion Detection System*)

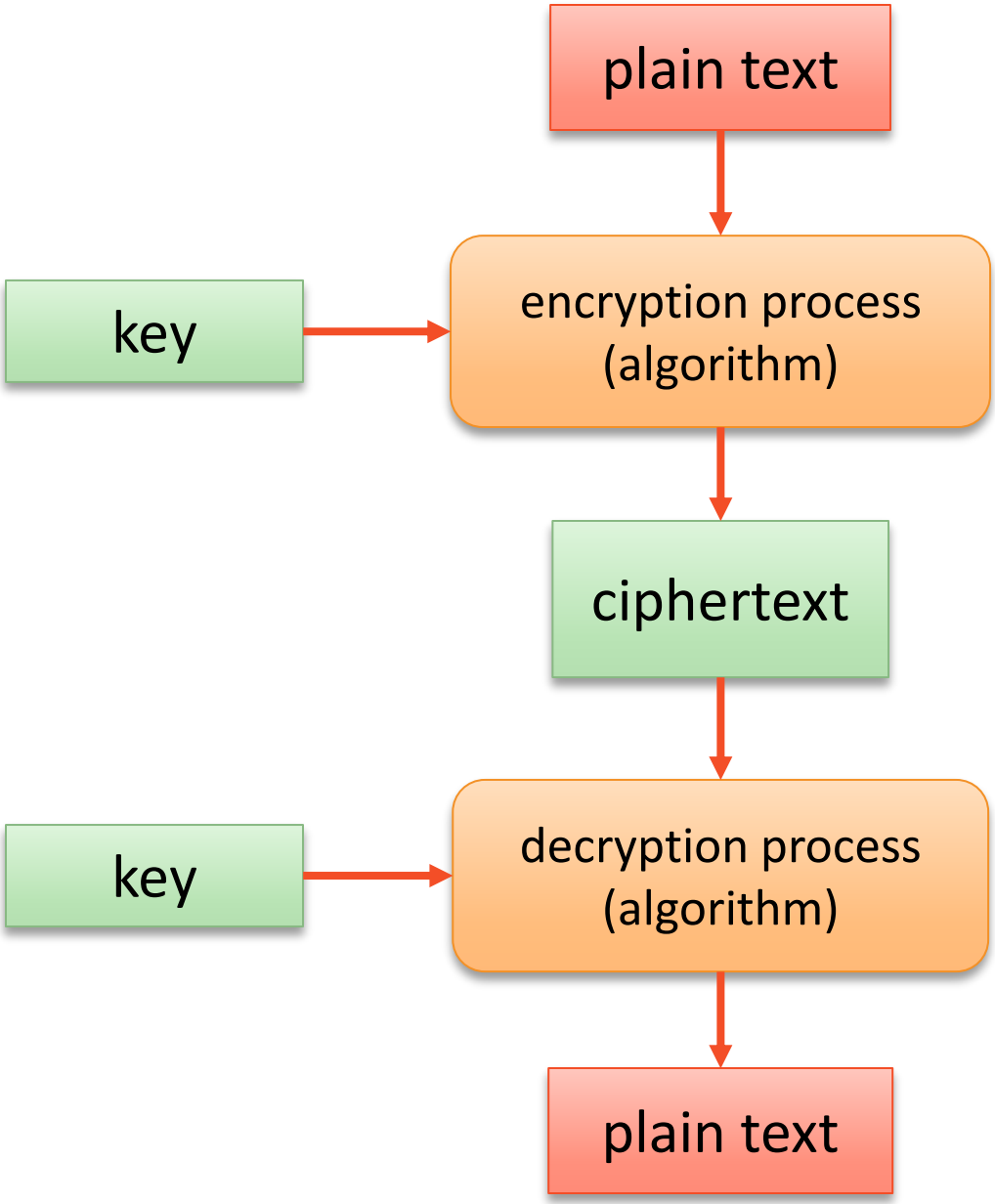
Firewall

- firewall software
- firewall hardware sau dedicat
- reguli de acces pentru pachetele de retea
- pot fi filtrate (dropped, rejected) pe baza criteriilor
  - tipuri de protocol
  - adresa IP sursa
  - adresa IP destinatie
  - port sursă
  - port destinație

Criptografie

- studiul ascunderii mesajelor
- criptarea este procesul de transformare a unui text clar (plain text) într-un text cifrat
- decriptarea este procesul invers
- criptarea/decriptarea necesită
  - un algoritm
  - o cheie
  - date/mesaj

Criptare si decriptare

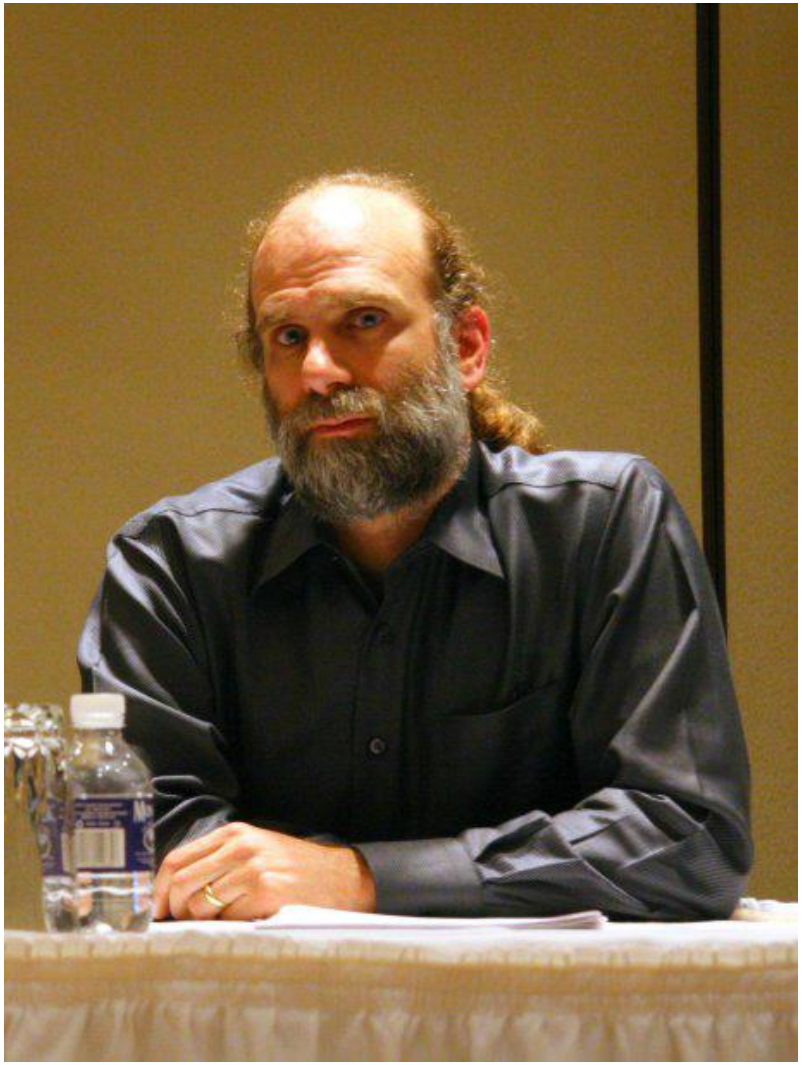


Security Engineering

- *Security Engineering: A Guide to Building Dependable Distributed Systems*
  - Ross Anderson
  - 2nd Edition, 2010
  - prima ediție poate fi descărcată gratis
  - o privire în ansamblu a securității sistemelor și rețelelor
  - atacuri și apărare
  - bogată în povestiri reale
  - ușor de citit
  - conține formalisme, dar insistă pe aspecte practice

Rusty Russell

- autorul mai multor cărți de securitate
- algoritmi de criptografie
- Bruce Schneier on security (blog) (http://www.schneier.com)
- Bruce Schneier Facts



RSA

- numele de la fondatorii: Ron Rivest, Adi Shamir, Led Adleman
- înființată în 1982
- algoritmul de criptare cu chei publice RSA
- token-uri de autentificare (RSA SecurID security tokens)
- RSA Factoring Challenge

AES

- Advanced Encryption Standard
  - adoptat de guvernul US ca standard de criptare în noiembrie 2001
  - inițial denumit Rijndael după numele unuia dintre inventatori
  - înlocuiește algoritmul DES (Data Encryption Standard) din 1977
  - procesul de alegere a avut loc între 1997 și 2000 – destinat comunității criptografice
  - inițial aleși 15 algoritmi, apoi 5 finaliști, apoi doar 1 (Rijndael)

Cuvinte cheie

- problematica securității
- principii de securitate
- umask
- autentificare
- autorizare
- controlul accesului
- parole
- /etc/passwd
- /etc/shadow
- root
- sudo
- recunoaștere
- man in the middle
- denial of service
- firewall
- criptare

Resurse utile

- http://en.wikipedia.org/wiki/Computer_security
- http://www.unixtools.com/security.html
- http://en.wikipedia.org/wiki/Ring_(computer_security)
- http://en.wikipedia.org/wiki/Network_security
- http://insecure.org/
- http://www.linuxsecurity.com/
- http://www.openbsd.org/
- http://www.schneierfacts.com/