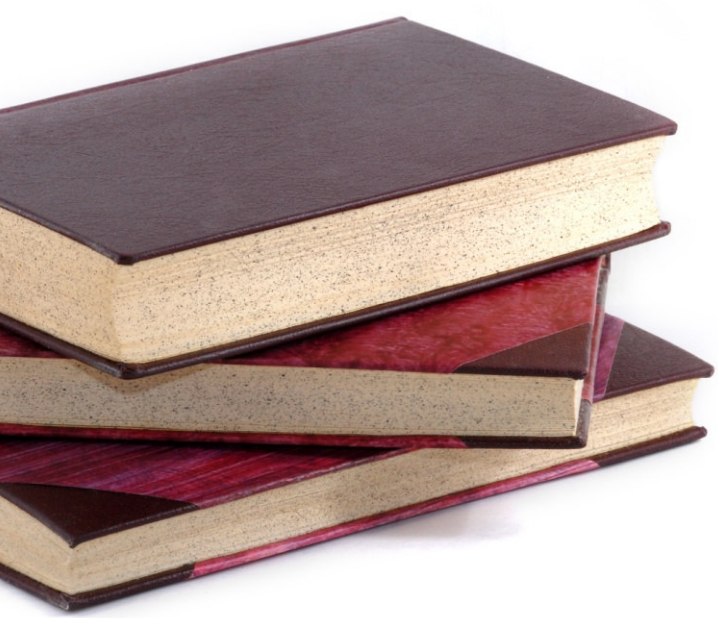
USO
just crunch it

Cursul 8



8

Principii de securitate

8 decembrie 2008

Motto

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Eugene H. Spafford

Problematica securității

- Protecția informațiilor prețioase (companii, instituții)
- Ce este un sistem sigur?
  - resursele sale sunt utilizate şi accesate în orice împrejurare aşa cum se doreşte
- Se poate obține un sistem sigur?
  - Da. Complet izolat de lumea exterioară.
- Are sens?
  - Nu. ☺ Nu este util şi flexibil.
- Ce înseamnă securizarea unui sistem de calcul?
  - folosirea de metode de protecție _suficient_ de mare
  - un potențial atacator va fi _descurajat_
  - compromiterea sistemului este _greu_ de realizat
- Securitatea este un proces nu o finalitate
- Veriga cea mai slabă indică securitatea sistemului

Niveluri de securitate

- La nivel de persoană
  - utilizatorii sunt aleşi cu grijă
  - reducerea probabilității ca un utilizator să permită accesului unei persoane neautorizate
- La nivel fizic
  - protecția încăperilor ce conțin sistemele de calcul
- La nivelul sistemului de operare
  - securizarea accesului (parole)
  - protecția resursele SO (memorie, fişiere)
- La nivelul rețelei
  - securizarea accesul 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, fişiere, procesor
- Cine asigură securitatea sistemului de operare?
  - nucleul SO
    - nivel intermediar între utilizator şi hardware
- Suport hardware
  - procesoarele oferă cel puțin două niveluri de privilegiu
    - unul pentru operații obişnuite (user mode)
    - altul pentru acces la instrucțiuni privilegiate (supevisor mode)
    - “rings” în x86
  - doar nucleul rulează în modul supervizor (kernel mode)

Securitatea sistemului de fişiere

- Aspecte importante
  - directorul HOME al fiecărui utilizator
    - drepturi depline
    - utilizatorul poate sau nu permite accesul altor utilizatori
  - Doar utilizatorul privilegiat are acces la anumite intrări
    - fişiere de configurare, programe executabile
- Cum se realizează securitatea fişierelor?
  - drepturi de acces (sau liste de acces)
  - opțiuni
    - pentru fiecare fişier se precizează drepturile pentru fiecare utilizator (liste de acces)
    - utilizatorul deține privilegii pentru acces la anumite fişiere (capabilități)

Securitatea fişierelor în Unix

- Directorul HOME (drepturi depline)
  - De obicei acesta este /home/username
- Utilizatorii care accesează fişierul pot face parte din 3 entități
  - User (utilizatorul care deține fişierul)
  - Group (grupul care deține fişierul)
  - Others (ceilalți)
- Fiecare dintre cele 3 entități poate avea 3 drepturi
  - Citire (read - r)
  - Scriere (write - w)
  - Execuție (execute – x)
- Care este avantajul/dezavantajul acestei scheme?
  - puțin spațiu ocupat (avantaj)
  - flexibilitate limitată (dezavantaj)

Drepturi pe fişiere în Unix

- Drept de citire (read)
  - Fişiere
    - se poate citi conținutul fişierului
    - fişierul poate fi copiat în altă parte
  - Directoare
    - se poate afişa conținutul unui director
    - DAR, fără drept de execuție, NU se poate ajunge în director
  - Exemplu:

```
razvan@anaconda:~/junkcode$ ls -ld sing/
drwxr-xr-x  5 razvan razvan 4096 Aug 23 17:57 sing/
razvan@anaconda:~/junkcode$ ls sing/
cvs-project.zip  lza  module  papers.zip
```

Drepturi pe fişiere în Unix (cont.)

- Drept de scriere (write)
  - Fişiere
    - fişierul poate fi editat
    - fişierul poate fi şters
  - Directoare
    - se poate crea un nou fişier
    - se poate şterge un fişier
    - directorul poate fi şters
  - Observaţie
    - În Linux, ştergerea unui fişier este condiţionată de prezenţa dreptului de write pe directorul părinte
    - Nu este nevoie de de drept de write pe fişier
      - Soluţie: activarea *sticky bit*
  - Exemplu de eliminare a dreptului de write

```
razvan@anaconda:~/junk/uso7$ ls
razvan@anaconda:~/junk/uso7$ touch uso7_test.txt
razvan@anaconda:~/junk/uso7$ chmod 555 .
razvan@anaconda:~/junk/uso7$ rm uso7_test.txt
rm: cannot remove `uso7_test.txt': Permission denied
razvan@anaconda:~/junk/uso7$ ls -l uso7_test.txt
-rw-r--r--  1 razvan razvan 0 Nov 10 17:16 uso7_test.txt
razvan@anaconda:~/junk/uso7$ ls -ld .
dr-xr-xr-x  2 razvan razvan 4096 Nov 10 17:16
```

Drepturi pe fişiere în Unix (cont.)

- Drept de execuție (execute)
  - Fişiere
    - un fişier poate fi executat
  - Directoare
    - se poate descende într-un director
    - fără drept de execuție, un director nu poate fi inclus în nici o cale
  - Exemplu:

```
razvan@anaconda:~/junk$ mkdir -p uso7_dir/uso7_subdir
razvan@anaconda:~/junk$ touch
  uso7_dir/uso7_subdir/uso7_test.txt
razvan@anaconda:~/junk$ ls uso7_dir/uso7_subdir/
uso7_test.txt
razvan@anaconda:~/junk$ ls -ld uso7_dir/
drwxr-xr-x  3 razvan razvan 4096 Nov 10 17:17 uso7_dir/
razvan@anaconda:~/junk$ chmod 644 uso7_dir
razvan@anaconda:~/junk$ ls -ld uso7_dir/
drw-r--r--  3 razvan razvan 4096 Nov 10 17:17 uso7_dir/
razvan@anaconda:~/junk$ ls uso7_dir/uso7_subdir/
ls: uso7_dir/uso7_subdir/: Permission denied
```

Schimbarea drepturilor

- chmod
- Exemple

```
razvan@anaconda:~/junk$ ls -l hello.c
-rw-r--r--  1 razvan razvan 81 Oct  6 21:35 hello.c
razvan@anaconda:~/junk$ chmod o+x hello.c
razvan@anaconda:~/junk$ ls -l hello.c
-rw-r--r-x  1 razvan razvan 81 Oct  6 21:35 hello.c
razvan@anaconda:~/junk$ chmod u=rx hello.c
razvan@anaconda:~/junk$ ls -l hello.c
-r-xr--r-x  1 razvan razvan 81 Oct  6 21:35 hello.c
```

- Forma în octal a drepturilor
  - se asociază un bit fiecărui drept (r, w, x) al fiecărei entități
  - Exemplu:
    - `rw- = 110 = 6`
    - `-w- = 010 = 4`
    - `r-x = 101 = 5`
  - mai puțin intutivă, mai rapidă

umask

- Restricția drepturilor de creare a intrărilor în sistemul de fişiere
- Valori tipice pentru umask: 022, 027, 077
- Drepturi de creare implicite
  - 666 pentru fişier
  - 777 pentru director
- Drepturi de creare efective
  - ŞI logic între permisiunile implicite şi masca inversată
- Exemplu
  - Director: implicit 777
  - umask: `022 → 755 (rwx r-x r-x)`

```
razvan@anaconda:~/junk$ umask
0027
razvan@anaconda:~/junk$ mkdir uso7_dir1
razvan@anaconda:~/junk$ ls -ld uso7_dir1
drwxr-x---  2 razvan razvan 4096 Nov 10 17:29 uso7_dir1
razvan@anaconda:~/junk$ umask 077
razvan@anaconda:~/junk$ mkdir uso7_dir2
razvan@anaconda:~/junk$ ls -ld uso7_dir2
drwx------  2 razvan razvan 4096 Nov 10 17:29 uso7_dir2
razvan@anaconda:~/junk$
```

umask (cont.)

- Fişier: implicit 666
- Umask: `027 → 640 (rwx r-- ---)`

```
razvan@anaconda:~/junk$ umask
0022
razvan@anaconda:~/junk$ touch uso7_test1
razvan@anaconda:~/junk$ ls -l uso7_test1
-rw-r--r--  1 razvan razvan 0 Nov 10 17:28 uso7_test1
razvan@anaconda:~/junk$ umask 027
razvan@anaconda:~/junk$ touch uso7_test2
razvan@anaconda:~/junk$ ls -l uso7_test2
-rw-r-----  1 razvan razvan 0 Nov 10 17:28 uso7_test2
```

suid, sgid

- Aplicațiile care necesită resurse speciale pot fi rulate doar de superuser
  - ping, traceroute, passwd
  - orice utilizator trebuie să le poată rula
- Soluție
  - utilizarea unui bit special denumit **suid** (switch user id)
  - permite execuția unui program cu drepturile celui care îl deține (de obicei root)

```
razvan@anaconda:~/junk$ ls -l /bin/ping
-rwsr-xr-x  1 root root 30764 Dec 23  2003 /bin/ping
```

- Stabilirea bitului de suid/sgid: o valoare în octal suplimentară la chmod

```
razvan@anaconda:~/junk$ ls -l a.out
-rwxr-xr-x  1 razvan razvan 13564 Jul  9 20:49 a.out
razvan@anaconda:~/junk$ chmod 2755 a.out
razvan@anaconda:~/junk$ ls -l a.out
-rwxr-sr-x  1 razvan razvan 13564 Jul  9 20:49 a.out
razvan@anaconda:~/junk$ chmod 4755 a.out
razvan@anaconda:~/junk$ ls -l a.out
-rwsr-xr-x  1 razvan razvan 13564 Jul  9 20:49 a.out
```

- Potențial risc de securitate
  - un utilizator poate obține drepturi privilegiate

Securitatea utilizatorilor

- 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 şi o parola
  - posedă un atribut de utilizator (amprentă, retină, semnătură)

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
  - 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
    - numelui utilizatorului
    - unor nume/cuvinte cu legătură
      - nume de animale preferate, numele copiilor, zile de naştere
- Ar trebui să mă îngrijorez?
  - în 1997, în urma unui sondaj efectuat in Londra, 82% din parole puteau fi ghicite uşor pe baza unei analize sumare a vieții subiectelor.
  - 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/**

Protecție la ghicirea parolelor

- Alegerea de parole bune
  - Minim 7 caractere, atât lower case cât şi upper case
  - Cel puțin un caracter special sau numeric
  - Nu trebuie să fie nume de persoane sau cuvinte din dicționar
  - Usor de reținut
  - Exemple:
    - I check my e-mail every 3 hours → Icme-me3h
    - My rusty car is 7 years old → Mrci7yo
- Utilizarea parolelor generate aleator de sistem (pot fi greu de retinut)
  - Exemplu program generat parole bune (**pwgen**)

```
razvan@anaconda:~/junk$ pwgen -n -c 5 1
ohN0e
```

- Verificarea periodică a parolelor utilizatorilor
- Password aging: forțarea schimbării parolei după o anumită perioadă
- Criptarea parolelor

Parole în Unix

- La început parolele se păstrau criptat în **/etc/passwd**
- Fisierul /etc/passwd conține şi alte informații
  - numele utilizatorilor
  - directorul home
  - shell-ul folosit

- Multe programe au nevoie de informațiile de mai sus
  - fişierul /etc/passwd este citibil de toți utilizatorii

```
razvan@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 în Unix (cont.)

- Fişierul **/etc/shadow**
  - accesibil numai de root
  - intrare în /etc/passwd

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

  - intrare în /etc/shadow

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

- Parola ar putea fi spartă prin încercări de login repetate
  - timeout între încercările de autentificare

Contul de root/Administrator

- Controlul absolut al sistemului
  - obținerea contului de superuser înseamnă spargerea sistemului
- Trebuie folosit _numai_ atunci când este nevoie
  - pentru operații obişnuite, folosiți contul _neprivilegiat_
  - o bună parte din atacurile pe Windows se bazează pe faptul că utilizatorii folosesc numai contul de Administrator
- sudo
  - permite unui utilizator obişnuit (dar de încredere) rularea unui set restrâns de comenzi cu privilegii de root
  - NU trebuie folosit pentru a permite accesul la lucrul cu shell
    - obținerea unui shell de root înseamnă accesul absolut la sistem

Evitarea accesului la contul de root

- Principiul “least privilege”
  - foloseşte numai atât cât este nevoie (fără privilegii suplimentare)
- Linux
  - folosirea **sudo** pentru rularea unui set restrâns de comenzi
    - fişierul de configurare **/etc/sudoers**
  - folosirea de **capabilități**
    - unele programe pot avea acces numai la o parte din privilegiile root
- Windows
  - folosirea **Power Users**
    - utilizatori de sistem care au acces la câteva din privilegiile Administrator

Securitatea rețelelor

- 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
  - recunoaşterea
  - obținerea accesului
  - folosirea sistemului pentru generarea unui nou atac împotriva unui alte rețele

Recunoaşterea

- Recunoaşterea activă
  - **host, whois**
  - ping sweep
  - aplicații de scanare a porturilor
    - Nmap
- Recunoaşterea pasivă
  - interceptarea traficului din rețea
    - tcpdump
    - Wireshark
    - kismet

Ţinta atacurilor

- Până în 2000 atacurile erau lansate pentru obținerea accesului pe o maşină țintă
  - se urmăresc servicii incorect configurate sau vulnerabilități ale sistemelor
- Din 2000 au apărut atacurile DoS (Denial of Service)
  - atacul se bazează pe generarea unui număr foarte mare de cereri
- Din 2003 viruşi de tip “blaster”
  - atac indirect, prin generarea unui trafic foarte mare în rețeaua locală

Obținerea accesului

- Prin analiza traficului
  - obținerea parolei
  - alterarea traficului pentru schimbarea comportamentului unui serviciu
- man-in-the-middle attack
  - un atacator este capabil să citească, insereze şi modifice mesajele transmise între două entități fără ca aceste două entități să realizeze că legătura între ele a fost compromisă
- Social engineering
- Ascunderea identității atacatorului → spoofing

Man in the Middle

- Eavesdropping
  - interceptarea mesajului între două entități
  - e-mail sau instant messaging: mesajele sunt transmise în clar (plain-text)
  - criptarea traficului
- Replay attack
  - transmisia de date între entități este întârziată sau repetată fraudulos
  - două stații A şi B doresc să comunice
    - A doreşte sa se autentifice
    - A transmite (eventual criptat) o parolă
    - o stație C (MITM) capturează parola
    - C se va conecta la B folosind parola lui A
    - Cva căpăta acces la sistem
  - session-tokens
    - B transmite lui A un jeton (token) care e folosit de A pentru criptare
    - B face acelaşi calcul la primirea parolei şi verifică dacă valorile coincid
- DoS (Denial of Service)
  - pot fi inițiate de un atacator ce ascultă comunicația şi îşi poate ascunde identitatea (spoofing)

Phishing

- Formă cunoscută de social engineering
- Folosită pentru a obține parole, detalii ale cărții de credit, etc.
- Atacatorul invocă a fi o persoana de încredere în comunicația electronică
- De obicei se realizează prin e-mail, messaging sau telefonie
- Se poate pierde accesul la căsuța de e-mail sau la sume de bani importante
- În SUA, în 2004-2005 s-au înregistrat pierderi de 929 milioane $ din cauza phishing
- Anti-phishing
  - user training
  - browser-ele actuale sunt capabile de a identifica forme de phishing de pe diverse site-uri
  - spam-filters reduc mesajele spam care pot fi folosite pentru phishing

DoS Attacks

- Denial of Service
- Împiedicarea accesului utilizatorilor la o resursă
- Poate însemna consumul resurselor unui sistem
  - exemplu: deschiderea unui număr mare de procese
- Congestionarea traficului în rețele
  - devine dificilă comunicația între stațiile din rețea
- Exemple:
  - SYN floods
  - ICMP floods
  - UDP floods
  - Teardrop attack
  - Application level floods
  - Nukes
  - DDoS

Spam

- Unsolicited mail
- Open mail relay
  - server de e-mail ce permite retransmiterea (relaying) mesajelor de poştă de electronică sosite din Internet
- majoritatea ISP-urilor folosesc DNSBL (DNS based Blocking Lists))
- http://www.cnn.com/2006/WORLD/europe/11/27/uk.spam.reut/index.html -> 9 din 10 mesaje sunt spam

Prevenirea atacurilor

- Stabilirea unor politici clare de securitate
  - separarea ariilor cu nivel de securitate diferit
  - definirea clară a drepturilor ficărui utilizator
  - definirea serviciilor ce trebuie oferite de fiecare componentă a rețelei
- Configurarea politicilor de filtrare a pachetelor
- Configurarea criptării traficului important
- Configurarea programelor antivirus

Detectarea atacurilor

- stabilirea unui nivel de referință pentru performața rețelei
- monitorizarea traficului din rețea
  - automat
    - configurarea unui NIDS (Network Intrusion Detection System)
  - manual
    - prin stabilirea unor limite de încărcare la nivelul dispozitivelor de rețea
- jurnalele
  - politică de colectare, păstrare şi prelucrare a jurnalelor pentru serverele importante din rețea

Firewall

- Firewall software
  - aplicație ce implementează o listă de acces
  - protecția rețelelor locale cu cerințe medii de securitate
  - protecția sistemelor individuale

- Firewall **hardware** sau **dedicat**
  - implementarea deliste de acces
  - criptarea traficului
  - cost ridicat
  - rețele cu cerințe ridicate de securitate
  - PIX, CheckPoint

Firewall software

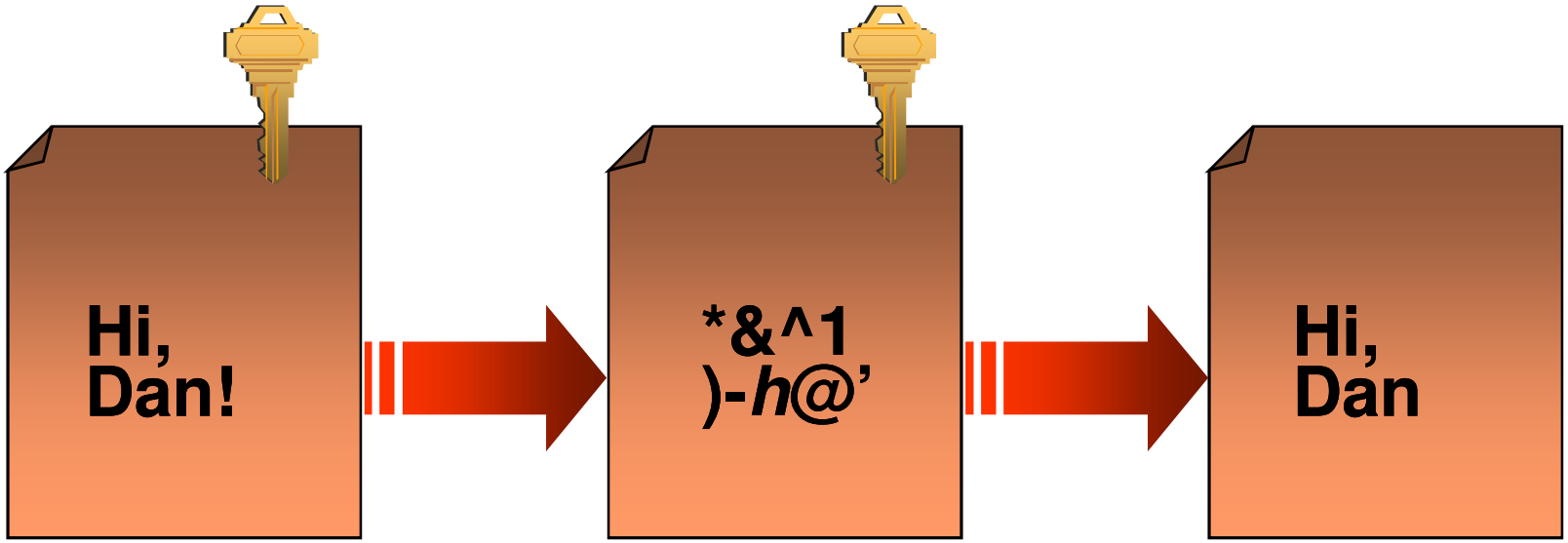
- Firewall integrat pe ruter
  - număr mai redus de conexiuni față de un firewall dedicat
  - poate gestiona topologii mai complexe
  - Cisco ACL
- Firewall de server
  - pachet software peste un sistem de operare
  - în general rulează în spațiul kernel
  - iptables (netfilter), shorewall, Microsoft ISA Server, Novell Border Manager
- Firewall personal
  - în general rulează în spațiul utilizator
  - performanțe reduse pentru trafic ridicat
  - Symantec, McAfee, ZoneAlarm

Criptografia

- Studiul ascunderii mesajelor
- Criptarea este procesul de transformare a unui text clar într-un text cifrat
- Decriptarea este procesul invers
- Criptarea/decriptarea necesită
  - Un algoritm, o cheie şi date
- Două tipuri
  - Cu cheie simetrică şi asimetrică (publică)

Criptarea cu chei simetrice

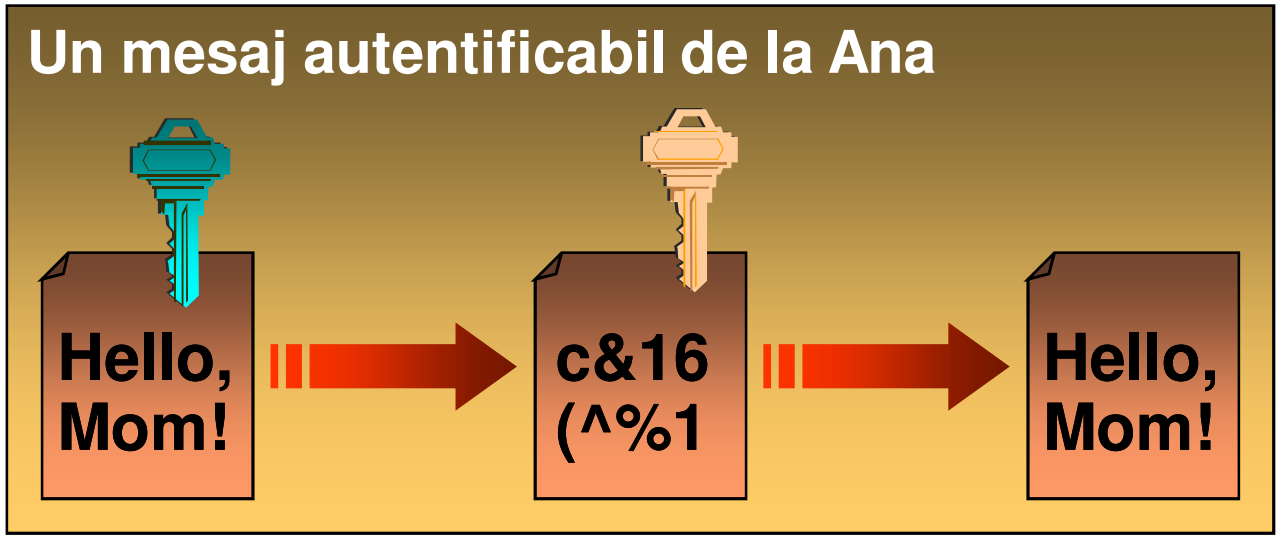
- O cheie secretă partajată între două entități
- Rapidă
  - Numita şi criptografie de masă (bulk cryptography)
- Exemple de algoritmi de criptare simetrică
  - DES
  - 3DES
  - RC4
  - AES



Criptarea cu chei publice

- O pereche de chei – key pair
  - cheie publică
  - cheie privată
  - în relație matematică
  - numere foarte, foarte, foarte mari
  - nefezabil să se determine una din cealaltă
- Cheia publică este ... publică
- Mai lentă
  - nepotrivită pentru criptarea de masă
- Exemple de algoritmi:
  - RSA
  - Diffie-Hellman
  - curbe eliptice

Criptarea cu chei publice (cont.)



Certificate

- Asociere între o identitate (subiect) şi o cheie publică

- Certificatele conțin
  - cheia publică a subiectului
  - detalii despre subiect
  - detalii despre emițătorul certificatului
  - data de expirare
  - o semnatură digitală peste conținutului certificatului

- Certificatul este semnat de o AC emitentă
- Folosite pentru a certifica identitatea subiectului

Viruşi, viermi, troieni

- Un program, o secvență de cod care se ataşează altor fişiere executabile fără cunoştința utilizatorului de sistem

- Un virus “adevărat” realizează cel puțin două lucruri
  - se execută
  - se replică
- Clasificare după rezultate şi modul de replicare
  - boot sector virus
  - e-mail virus
  - logic bomb
  - macro virus
  - cross-site scripting virus
  - sentinels
  - trojan horse
  - worm

Cuvinte cheie

- problematica securității
- drepturi de acces
- chmod
- umask
- suid, sgid
- parole
- John the Ripper
- /etc/passwd
- /etc/shadow
- pwgen
- sudo

- man in the middle
- phishing
- DoS
- spam
- NIDS
- firewall
- criptare
- chei simetrice/asimetrice
- certificat
- viruşi, viermi, troieni

Link-uri 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/

The End

?