# Ingineria Programării în Reţea (IPR)

Securitate. Securizarea aplicaţiilor de reţea

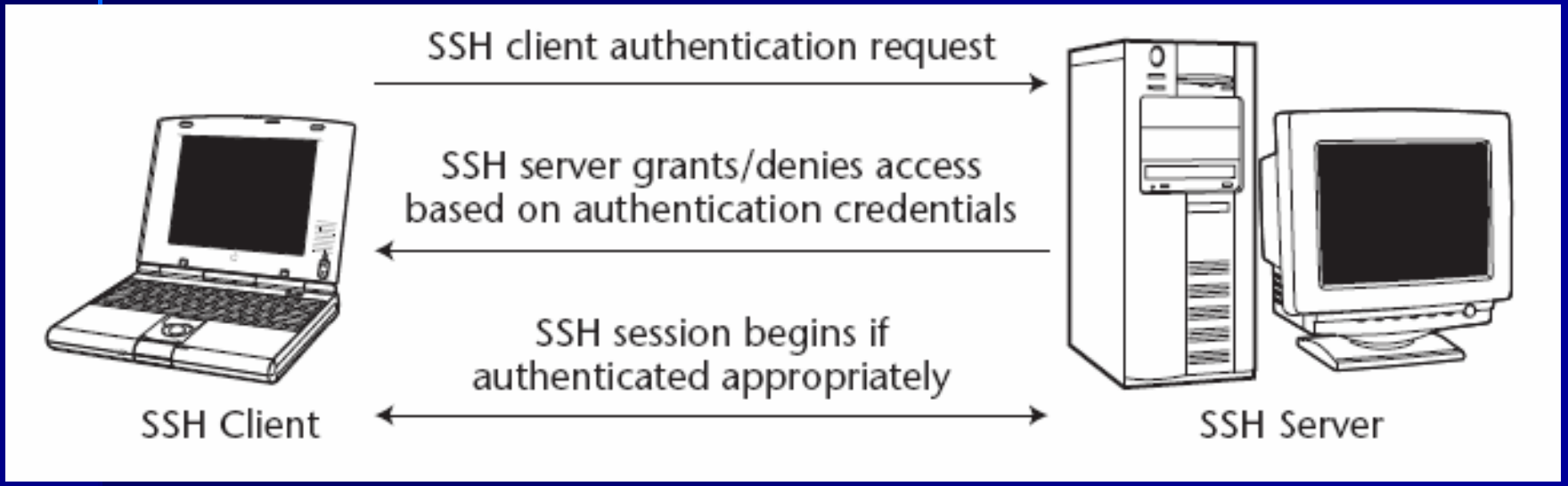
# Securitatea

- Securitatea reprezintă un punct important în cadrul unui proiect de dezvoltare de software pentru aplicaţii de reţea
- Dacă în trecut se foloseau protocoale "nesigure" (informaţia circulă în reţea necriptat) se tinde tot mai mult către înlocuirea lor. E.g. telnet este înlocuit de ssh, ftp de sftp şi http de https.
- Un alt aspect important îl constituie "rezistenţa" aplicaţiei/serverului la un atac

# SSH


- Protocol de reţea care permite schimbul de date printr-un canal sigur între două computere (informaţia circulă criptat)
- Oferă mai multe modalităţi de autentificare
  - Parole
  - Cheie publică
  - Certificat
  - Kerberos
  - RSA securID
  - PAM
- Protocoale asociate pentru transfer de fişiere SFTP sau SCP
- Portul standard TCP este 22

# SSH – Procesul de autentificare



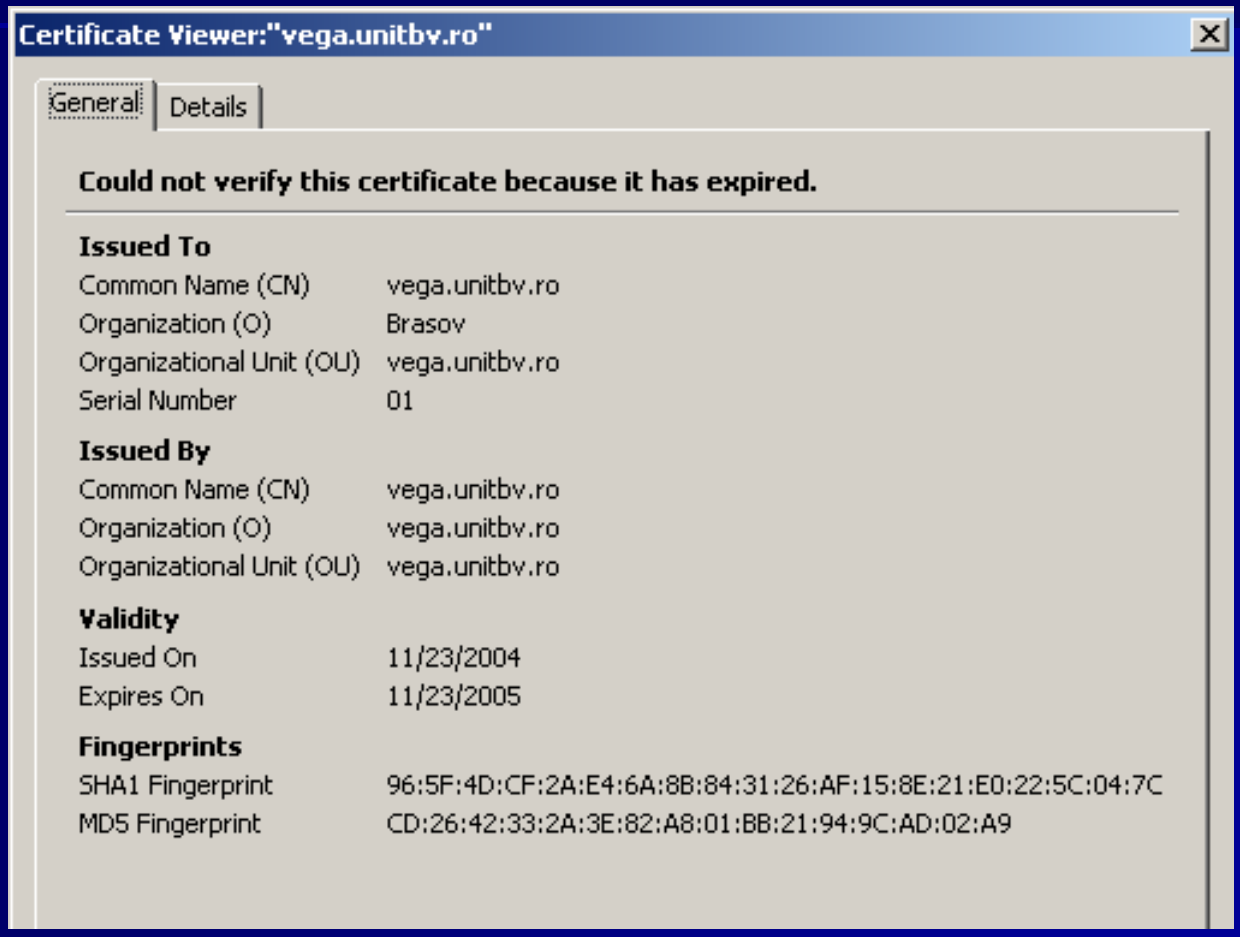
# Pachet de date tip SSH

# SSL

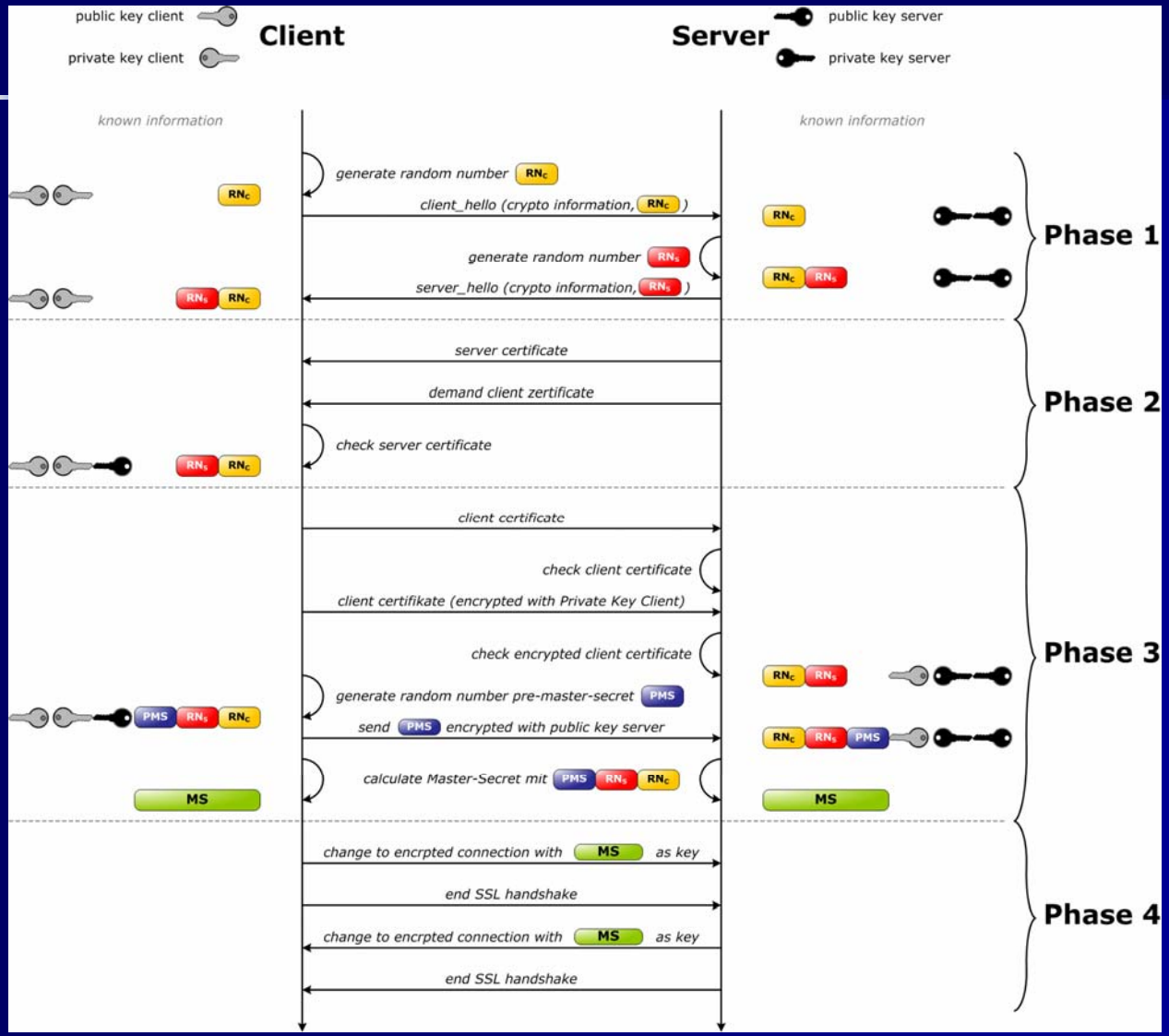
- SSL (Secure Sockets Layer) protocol dezvoltat de Netscape pentru trimiterea documentelor private via Internet
- Foloseşte un sistem cu două chei de criptare: cheia publică şi cea privată

# SSL – Pagină securizată

# SSL – Certificat



# SSL – Handshake



# DoS (Denial of Service)

- Un atac de tip Dos sau DDoS (Distributed Dos) reprezintă încercarea de face nedisponibilă o resursă din Internet (servere web bancare, servere DNS root, etc.)
- Moduri de implementare:
  - forţarea reset-ului sau consumarea resurselor pentru ca respectivul server să nu mai poată oferi servicii
  - obstrucţionarea mediului de comunicaţie între utilizatori şi victimă pentru a nu mai comunica corespunzător

# DoS – simptomele atacului

- Performanţă neobişnuit de scăzută în reţea
- Indisponibilitate a unui site web anume
- Indisponibilitate a oricărui site web
- Creşterea dramatică a numărului de mesaje de spam recepţionate (“mail bomb”)

# DoS – Tipuri de atac

- Consumul resurelor: bandă, spaţiu pe disk sau timp de procesor
- Distrugerea unor informatii de configurare, ca de exemplu informatia de rutare;
- Distrugerea stării informaţiei, ca de exemplu resetarea nesolicitată a unei sesiuni TCP
- Blocarea comunicaţiei media (voce, text) între o terţă persoană şi victimă

# DoS – exemple (1)

- Atacul de tip “smurf” – bazat pe greşeli de configuraţie în reţea (ex. trimiterea pachetelor tuturor hosturilor dintr-o reţea prin broadcast; reţeaua devine un “smurf amplifier”)
- Ping flood – trimiterea unui număr mare de pachete ping (ex. `ping -f`)
- Atacuri de tip “teardrop” – trimiterea spre victimă a unor pachete suprapuse şi supradimensionate victimei. Crash-ul apare în momentul reasamblării pachetelor TCP/IP (bug prezent în Win 95, NT şi Kernel Linux < 2.1.63)

# DoS – exemple (2)

- "SYN Flood" - atacatorul trimite mai multe pachete TCP/SYN. Fiecare dintre aceste pachete este utilizat ca o cerere de conexiune (connection request), obligând serverul sa producă o semi-conexiune prin trimiterea înapoi a pachetelor TCP/SYN-ACK şi aşteptand răspunsul receptorului. Atacatorul nu va trimite nici un răspuns, astfel prin aceste semi-conexiuni se saturează numărul maximi de conexiuni pe care acel server le poate accepta şi menţine, fapt ce blocheaza alte requesturi legitime.

# DoS – exemple (3)

- Atacuri de tip peer-to-peer. Se încearcă conectarea la victimă cu ajutorul a zeci, sute sau chiar mii de computere care încearcă în acelaşi timp să îl contacteze.

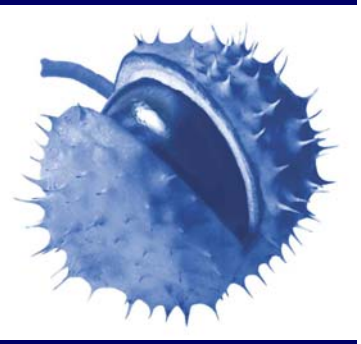
# Dos – Metode de prevenire şi răspuns

- Se recomandă a avea un set de IP-uri “de urgentă” pentru serverele critice
- Setarea atentă a unor filtre poate preveni un astfel de atac (ex. server FTP care refuză automat accesul de la un anumit IP/utilizator după 3-5 încercări de autentificare nereuşite)
- SYN Cookies modifică protocoalele folosite de server; acestea întârzie alocarea resurselor până cand adresa clientului nu este verificată (implementări în Solaris, Free BSD şi Linux )

# DoS – probleme la combatere

- Firewall-ul defineşte nişte reguli prea simple pentru a combate un DoS. (de exemplu dacă se atacă portul 80, nu ştie să facă diferenţa între traficul legitim şi atac)
- Intrussion-prevention systems - sunt eficiente dacă semnăturile atacului sunt valide, însă în general DoS au "conţinut legitim dar scop malefic"
- Routere şi switch-uri folosesc ACL-uri (acces control list) destul de limitate

# Securizarea aplicaţiior



- Ameninţări comune:
  - Input-ul şi flow-ul de date
  - Interfeţe software
  - Atacuri în funcţie de mediu (OS, arhitectură HW şi de reţea, file system, useri, baze de date)
  - Condiţii de excepţie

# Clasificarea vulnerabilităţiilor aplicaţiilor

- Vulnerabilităţi de proiectare
- Vulnerabilităţi de implementare
- Vulnerabilităţi de operare

# Vulnerabilitaţi de proiectare

- Aplicaţie care trimite date personale în format necriptat prin LAN/Internet
- Parole “hardcodate”
- Un sistem de log ....

```
20051018133106 Logon Failure: Bob
20051018133720 Logon Success: Jim
20051018135041 Logout: Jim
```

.... Defectuos ...

```
"Bob\n20051018133106 Logon Success: Greg"
```

# Vulnerabilitaţi de implentare

- Algoritmii de autentificare
- Inchiderea sesiuniilor
- Formatarea stringurilor
- SQL Injections
- Atacurile HTML Scripting

# Vulnerabilitaţi de implentare – exemple (1.1)

```
#include <stdio.h>
#include <stdlib.h>
int main( int argc, char *argv[] )
{
   if( argc != 2 )
   {
      printf(“Error - supply a format string please\n”);
      return 1;
   }

   printf( argv[1] );
   printf( “\n” );

   return 0;
}
```

# Vulnerabilitaţi de implentare – exemple (1.2)

- Complilare cod: `cc fmt.c -o fmt`
- Rulare: `./fmt "%x %x %x %x"`
- Practic apelăm printf astfel:

```
printf( "%x %x %x %x" );
```

- Rezultatul ... :

```
4015c98c 4001526c bffff944 bffff8e8
```

.... O parte din stivă ...

# Un exemplu din “viaţa de zi cu zi” Bug descoperit în wu-ftpd (v<2.6.0)

```
[root@attacker]# telnet victim 21 (21 = port FTP)
Trying 10.1.1.1...
Connected to victim (10.1.1.1).
Escape character is ‘^]’.
220 victim FTP server (Version wu-2.6.0(2) Wed Apr 30 16:08:29 BST 2003) ready.
user anonymous
331 Guest login ok, send your complete e-mail address as password.
pass foo
230 User anonymous logged in.
site exec %x %x %x %x %x %x %x %x
200-8 8 bfffcacc 0 14 0 14 0
200 (end of ‘%x %x %x %x %x %x %x %x’)
site index %x %x %x %x %x %x %x %x
200-index 9 9 bfffcacc 0 14 0 14 0
200 (end of ‘index %x %x %x %x %x %x %x %x’)
quit
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 448 bytes in 0 transfers.
221-Thank you for using the FTP service on vulcan.ngssoftware.com.
221 Goodbye.
Connection closed by foreign host.
```

# Vulnerabilitaţi de implentare – exemple (2.1)

- Cod original PHP:

```
<SCRIPT> SomeCode…
var strEmailAdd = 'attacker data';
MoreCode…

</SCRIPT>
```

- Cod manipulat de atacator (trimite ca date: *'; alert('Hi!'); //* )

```
<SCRIPT> SomeCode…
var strEmailAdd = ''; alert('Hi!'); //';
MoreCode…
</SCRIPT>
```

# Vulnerabilitaţi de implentare – exemple (2.2)

- Explicaţie: atacatorul nu initializează variabila `strEmailAdd` prin folosirea `‘` . Apoi prin `;` urmează codul arbitrar `alert('Hi!');` . `//` după codul arbitrar comenteză restul liniei pentru că input-ul e întotdeauna urmat de `‘;` în output-ul HTML şi nu se doreşte obţinerea unei erori de sintaxă

# Vulnerabilitaţi de operare

- "Insecure defaults" – multe sisteme lasate cu setările default, fără a fi customizate pentru nevoile specifice (servicii, porturi deschise fără a fi nevoie de ele)
- Sisteme fără update-uri (patch-uri, hotfix-uri, service pack-uri pentru OS şi aplicaţii)
- Alte erori umane

...

# Câteva link-uri utile ...(1)

- Threat models:

*http://msdn2.microsoft.com/en-us/security/aa570411.aspx*

- ActiveX Control Test Container:

*http://msdn2.microsoft.com/en-us/library/f9adb5t5(vs.71).aspx*

- BoundsChecker:

*http://www.compuware.com/products/devpartner/visualc.htm*

- C/C++ Code Analysis:

*http://msdn2.microsoft.com/en-us/library/d3bbz7tz(en-US,VS.80).aspx*

- Forty's Source Code Analysis:

*http://www.fortifysoftware.com/products*

# Câteva link-uri utile ...(2)

- LCLint (Static code analysis tool that looks through the code for common cases of buffer overruns ):

*http://lclint.cs.virginia.edu*

- Strace (Traces which system calls are made by a specific process. ):

*Pentru UNIX:*

*http://sourceforge.net/project/showfiles.php?group_id=2861*

*Pentru Windows:*

*http://www.bindview.com/Services/RAZOR/Utilities/Windows*