

# I. SECURITATE ȘI CONFIDENȚIALITATE ÎN INTERNET

## 1. INTRODUCERE

### Importanța securității

De aproximativ 10 ani, infrastructurile de comunicații s-au extins de la nivelul intern al acestor organizații (Intranet) către conectarea globală la nivelul Internet-ului, în special în cazul companiilor întinse pe arii geografice largi. Această integrare este însoțită de riscuri ridicate de penetrare și compromitere. Utilizarea Internet-ului în domenii vitale (sănătate sau militar) precum și în scopuri comerciale (sisteme bancare sau comerț electronic) a crescut acest potențial de risc. Posibilitatea de accesare rapidă, în orice moment, a informației, precum și necesitatea de a asigura protecția acesteia împotriva furtului sau distrugerii au devenit cerințe care nu existau atunci când rețeaua și serviciile sale au fost create. Dependenta puternică de informație și comunicații duce la urmări de o gravitate crescută a cazurilor de furt, modificare sau distrugere a informației, precum și deteriorare sau întrerupere a canalelor de comunicație. Sistemele informatice, indiferent de natura acestora s-au dovedit de-a lungul timpului vulnerabile la atacuri, la accesări neautorizate ale informațiilor, la modificări ori distrugeri de informații, accidentale sau voite. Atenuarea și corectarea acestor vulnerabilități au devenit astăzi obligații ale oricărei organizații care deține calculatoare legate în rețea. Protejarea informației reprezintă așadar o activitate din ce în ce mai importantă, dar fiind faptul că ea poate circula printr-o rețea neprotejată cum este Internetul.

În urma implementării unor mecanisme de securitate într-o rețea de calculatoare, informațiile nu vor putea fi accesate sau interceptate de persoane neautorizate (curioase sau, eventual, chiar rău intenționate) și se vor împiedica falsificarea și / sau alterarea informațiilor transmise sau utilizarea clandestină a anumitor servicii destinate unor categorii specifice de utilizatori ai rețelelor.

Problemele de asigurare a securității rețelelor pot fi grupate în următoarele domenii interdependente:

- **confidențialitatea** se referă la asigurarea accesului la informație doar pentru utilizatorii autorizați și împiedicarea accesului pentru persoanele neautorizate;
- **integritatea** se referă la asigurarea consistenței informațiilor (în cazul transmiterii unui mesaj prin rețea, integritatea se referă la protecția împotriva unor tentative de falsificare a mesajului);
- **autentificarea** asigură determinarea identității persoanei cu care se comunică (aspect foarte important în cazul schimbului de informații confidențiale sau al unor mesaje în care identitatea transmitătorului este esențială);
- **ne-repudierea** se referă la asumarea responsabilității unor mesaje sau comenzi, la autenticitatea lor. Acest aspect este foarte important în cazul contractelor realizate între firme prin intermediul mesajelor electronice: de exemplu, un contract / comandă cu o valoare foarte mare nu trebuie să poată fi ulterior repudiat(ă) de una din părți (s-ar putea susține, în mod fraudulos, că înțelegerea inițială se referea la o sumă mult mai mică).

### Vulnerabilități în sistemul informatic

Vulnerabilitatea este o slăbiciune a unui sistem hardware sau software, care permite utilizatorilor neautorizați să obțină acces asupra sa sau a componentelor sale. Orice platformă are vulnerabilități, astfel că putem concluziona, fără a greși, că nu există vreun sistem 100% sigur. De multe ori, unele particularități ale sistemelor informatice care devin cunoscute utilizatorilor se pot transforma în vulnerabilități.

Există mai multe tipuri de vulnerabilități:

- Care permit refuzul serviciilor (*Denial of Service*);
- Care permit utilizatorilor locali cu privilegii limitate să-și mărească aceste privilegii fără autorizație;
- Care permit utilizatorilor externi (adică de pe calculatoare aflate la distanță) să acceseze rețeaua sau sistemul local în mod neautorizat.

Cauzele existenței vulnerabilităților sunt multiple; dintre acestea putem enumera:

- bug-urile existente în program, introduse de cele mai multe ori neintenționat;
- ignorarea sau nedocumentarea cu bună știință a bug-urilor cunoscute (securitatea prin obscuritate);
- configurarea necorespunzătoare a serverelor și a rețelelor;
- lipsa suportului din partea producătorilor (în general rezolvarea greoaie a bug-urilor);
- comoditatea sau necunoașterea problemelor de securitate din partea administratorilor de sistem sau a conducerii instituțiilor și a companiilor.

Există o bază de date a tuturor vulnerabilităților apărute de-a lungul timpului (**Common Vulnerabilities and Exposures**) care poate fi descărcată de la adresa <http://cve.mitre.org>.

## Abordarea problemei securității datelor într-o rețea

Abordarea problemei securității datelor într-o rețea presupune în primul rând **identificarea cerințelor de funcționare** pentru acea rețea, apoi identificarea tuturor amenințărilor posibile (împotriva cărora este necesară protecția). Această analiza constă în principal în 3 sub-etape:

- analiza vulnerabilităților - identificarea elementelor potențial slabe ale rețelei;
- evaluarea amenințărilor - determinarea problemelor care pot apărea datorită elementelor slabe ale rețelei și modurile în care aceste probleme interferă cu cerințele de funcționare;
- analiza riscurilor - posibilele consecințe pe care problemele le pot crea.

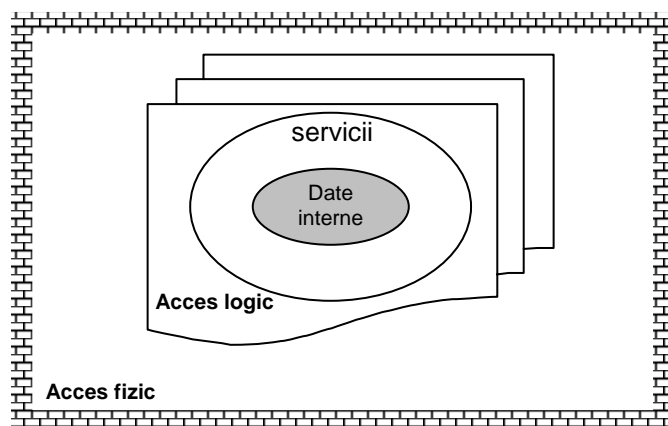
Următoarea etapă constă în **definirea politicii de securitate**, ceea ce înseamnă să se decidă:

- care amenințări trebuie eliminate și care se pot tolera;
- care resurse trebuie protejate și la ce nivel;
- cu ce mijloace poate fi implementată securitatea;
- care este prețul (financiar, uman, social etc.) măsurilor de securitate care poate fi acceptat.

Odată stabilite obiectivele politicii de securitate, următoarea etapă constă în **selecția serviciilor de securitate** - funcțiile individuale care sporesc securitatea rețelei. Fiecare serviciu poate fi implementat prin metode (mecanisme de securitate) variate pentru implementarea cărora este nevoie de așa-numitele funcții de gestiune a securității. Gestiunea securității într-o rețea constă în controlul și distribuția informațiilor către toate sistemele deschise ce compun acea rețea în scopul utilizării serviciilor și mecanismelor de securitate și al raportării evenimentelor de securitate ce pot apărea către administratorii de rețea.

## Modelul de securitate pentru un sistem

Modelul de securitate pentru un sistem (un calculator sau o rețea de calculatoare) poate fi văzut ca având mai multe straturi ce reprezintă nivelurile de securitate ce înconjoară subiectul ce trebuie protejat. Fiecare nivel izolează subiectul și îl face mai dificil de accesat în alt mod decât cel în care a fost prevăzut.



**Securitatea fizică** reprezintă nivelul exterior al modelului de securitate și constă, în general, în încuierea echipamentelor informatice într-un birou sau într-o altă incintă precum și asigurarea pazei și a controlului accesului. Această securitate fizică merită o considerație specială. Una dintre problemele mari o constituie salvările sub forma de copii de rezervă (backup) ale datelor și programelor, precum și siguranța păstrării suporturilor de salvare. Rețelele locale sunt, în acest caz, de mare ajutor, copiile de rezervă putându-se face prin rețea pe o singură mașină ce poate fi mai ușor securizată. O altă problemă importantă în securitatea unui sistem informatic o constituie pur și simplu sustragerile de echipamente. În plus, celelalte măsuri de securitate (parole, etc.) devin nesemnificative în cazul accesului fizic neautorizat la echipamente.

**Securitatea logică** constă din acele metode logice (software) care asigură controlul accesului la resursele și serviciile sistemului. Ea are, la rândul ei, mai multe niveluri împărțite în două grupe mari: **niveluri de securitate a accesului** și **niveluri de securitate a serviciilor**.

*Securitatea accesului* cuprinde:

- accesul la sistem, care este răspunzător de a determina dacă și când este rețeaua accesibilă utilizatorilor și în ce condiții. El poate fi răspunzător de asemenea și de gestionarea evidenței accesului. Accesul la sistem poate efectua și deconectarea forțată în anumite cazuri (ex. expirarea contului, oră de vârf, ...);
- accesul la cont care verifică dacă utilizatorul ce încearcă să se conecteze are un nume și o parolă validă;
- drepturile de acces (la fișiere, resurse, servicii etc.) care determină de ce privilegii dispune un utilizator (sau un grup de utilizatori) dat.

*Securitatea serviciilor* (care se află "sub" securitatea accesului) controlează accesul la serviciile unui sistem (calculator, rețea). Din acest nivel fac parte:

- *controlul serviciilor* care este responsabil cu funcțiile de avertizare și de raportare a stării serviciilor, precum și de activarea și dezactivarea diverselor servicii oferite de către sistemul respectiv;
- *drepturile la servicii* care determină exact cum folosește un anumit cont un serviciu dat (acces la fișiere, resurse, prioritate,...)

Odată stabilită conexiunea logică, subsistemul de securitate a accesului validează contul de acces. Subsistemul de securitate a serviciilor monitorizează activitatea utilizatorului și ia măsuri în cazurile în care cererile acestuia depășesc drepturile specificate în profilul utilizatorului (sau grupului de utilizatori) respectiv. Accesul într-un sistem sigur perfect ar trebui să se facă prin aceste niveluri de securitate descrise mai sus, de "sus" în "jos" fără să permită ocolirea vreunui din ele.

Securitatea la nivel de host (gazdă) urmează principiile enunțate mai sus. Mai concret (în cazul unui server Internet) distingem:

- entitățile ce au acces local la acea mașină (utilizatori, programe server, agenți locali) precum și drepturile acestora (ce are voie să facă un anumit utilizator, cu ce privilegii rulează un anumit proces, ce prioritate are un proces, ce drepturi are asupra fișierelor respective, asupra spațiului de stocare, ce resurse și între ce limite are voie să acceseze);
- serviciile oferite către exterior (publice sau pentru anumiți utilizatori; autentificare, monitorizare);
- sistemul de operare (tipul, distribuția, servicii implicite oferite - filtrarea sau dezactivarea celor de care nu e nevoie, bug-uri cunoscute, revizii (patches) etc.)

## Securizarea unei rețele

Securizarea unei rețele presupune **implementarea unor metode hardware și / sau software** astfel încât:

- informațiile să nu poată fi interceptate de persoane neautorizate;
  - să nu se poată modifica (altera, falsifica) aceste informații care circulă prin rețea;
  - să nu se poată realiza conexiuni ilegale la rețea, folosindu-se identitatea unor utilizatori sau calculatoare;
  - să nu se poată utiliza servicii destinate unor categorii specifice de utilizatori ai rețelei.
- Asigurarea securității constituie un atu competițional, pentru câștigarea încrederii partenerilor și clienților
  - Este necesară permanenta îmbunătățire a sistemului de securitate (un sistem sigur poate deveni nesigur la un moment dat). Trebuie luată în calcul apariția permanentă a noi pericole și vulnerabilități și starea de veghe permanentă, pentru repararea ("*patch*") breșelor de securitate.

Amenințările pot fi:

- neintenționate
  1. dezastre, calamități naturale
  2. defectări ale echipamentelor
  3. întreruperi ale energiei electrice
  4. greșeli umane de operare sau manipulare a datelor
- intenționate
  1. furtul echipamentelor
  2. atacuri - la nivel logic
    - din curiozitate
    - pentru testarea sistemelor de securitate
    - pentru furtul sau distrugerea unor informații

Amenințările intenționate (atacurile logice) se pot clasifica în:

I. după tipul atacului

- **atacuri pasive:** intrusul doar observă informația transmisă, fără a interveni asupra ei și fără a cunoaște conținutul acestei informații. Se face doar analiza traficului (surse, destinații, volum de date transmis, frecvență), încălcându-se totuși normele de confidențialitate.
- **atacuri active:** intrusul intervine în fluxul de date
  1. pentru obținerea în mod clandestin a unor informații (furt)
    - angajați care accesează servicii care în mod normal le-ar fi interzise
    - oameni de afaceri care încearcă să descopere strategiile adversarilor
    - persoane care realizează fraude financiare (furtul numerelor de identificare a cărților de credit, transferurile bancare ilegale etc.)
    - spioni militari sau industriali care încearcă să descopere secretele / strategiile adversarilor sau chiar teroriști care fură secrete strategice.

2. pentru distrugerea parțială (modificare, inserare), totală (ștergere) sau întârzierea unor mesaje
  - foști angajați care urmăresc să distrugă informații ca o formă de răzbunare
  - hackeri
  - viruși și alte programe malware

## II. după locul de unde vine atacul

- **atacuri din exteriorul organizației:** hackeri, malware, acțiuni DoS. Soluții: instalare, configurare și actualizare firewall, programe antivirus și antimalware;
- **atacuri din interiorul organizației ("insider threat"):** angajați cu sau fără drepturi sporite de acces, cu diverse nemulțumiri referitoare la companie (post ocupat, activitate desfășurată, salariu) pot sustrage în diverse scopuri informații sau crea intenționat breșe de securitate (dezactivare firewall, instalare malware). Sunt cele mai periculoase atacuri. Soluții: monitorizare activitate angajați, controlul accesului fizic, politica drepturilor de acces logic

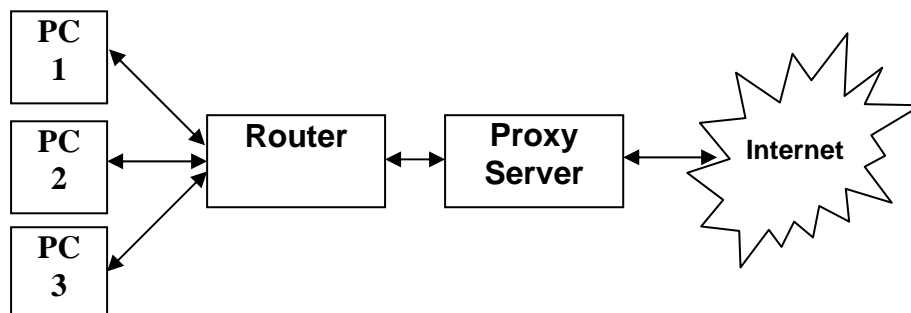
## Implementarea securității

- nivel fizic
  1. protecția sistemului de calcul împotriva pagubelor materiale (la calamități naturale)
  2. protecția sistemului de calcul împotriva căderilor de tensiune electrică (alimentarea prin surse neîntreruptibile de putere - UPS)
  3. restricționarea accesului fizic în perimetru, împotriva accesului nedorit - încuierea echipamentelor într-o sală, sisteme de supraveghere și autentificare (cartele magnetice, recunoaștere vocală, date biometrice - amprentă digitală, etc.)
  4. restricționarea fizică a accesului la servere (mecanisme hard de autentificare):
    - cititor de amprentă digitală,
    - eToken - dispozitiv USB pentru generarea și stocarea sigură a parolelor și certificatelor digitale, pentru autentificare, semnătură digitală și criptare;
    - "USB Computer Lock" - cheie USB prin care se limitează accesul la anumite informații
  5. restricționare acces fizic la stații de lucru (gestionarea accesului unui utilizator la o anumită stație de lucru, într-un anumit interval orar)
  6. protecția mediului de transmisie
- nivel logic
  1. firewall (atacuri din exterior)
  2. limitarea drepturilor de acces:
    - blocarea accesului din exterior și interior (login) pentru anumiți utilizatori
    - drepturi de scriere, citire, execuție particularizate pe grupuri de utilizatori
  3. criptarea datelor
  4. salvări regulate de date (*backup*), utilizarea tehnicii mirroring

## 2. WWW

În scopul unei expuneri cât mai reduse pe Internet, date fiind vulnerabilitățile localizate la mai multe niveluri (utilizator, browser, sistem de operare, site web, etc.) trebuie respectate câteva reguli care reduc din șansele ca un utilizator să fie victima unui atac cibernetic (în special furtul datelor confidențiale sau instalarea unor programe tip *malware* pe propriul sistem).

- **Navigarea cât mai anonimă**, utilizând eventual servere proxy pentru ascunderea adresei IP reale. Un "*proxy server*" acționează ca un intermediar între utilizator și resursa solicitată, având două roluri: **protejarea identității** (în scopuri de securitate) și **creșterea vitezei de acces** la o resursă prin crearea unei zone de memorie ("*cache*") - în special pentru accesarea rapidă a unor pagini web.



- **Evitarea download-ului inutil**: programe, toolbars-uri, screensaver-e distribuite cu generozitate, gratuit, pe Internet, pot fi surse de infectare cu diverse coduri nedorite care duc la încetinirea sistemului, distrugerea sau modificarea unor fișiere, instalarea unor programe pentru furtul identității sau monitorizarea activității. Unele pagini web, profitând și de lacunele de securitate întâlnite în sistem, pot instala coduri nedorite care afișează reclame sau urmăresc activitatea pe calculator.
- **Logarea**: intrarea într-un cont personal ("*login*") nu se va face cu salvarea datelor de identificare (în special pe calculatoare publice la care au acces mai mulți utilizatori), iar ieșirea din cont se va face prin "*logout*" (operație care închide sesiunea curentă de lucru și împiedică logarea altcuiva folosind eventualele date rămase în memoria cache a browserului).
- **Furnizarea datelor personale** (adresă, telefon, etc.) trebuie să se facă doar acolo unde este absolută nevoie de ele și se justifică divulgarea lor.
- **Evitarea adreselor de phishing**: copii fidele ale unor site-uri reale (în special din domeniul bancar, e-commerce sau licitații) înșală utilizatorii, îndemnându-i (pentru diverse motive) să divulge informații personale sensibile (cum ar fi numărul cardului bancar, codul de siguranță, codul PIN). Mesajele sosesc de obicei prin e-mail sau programe de mesagerie instant (I.M.) și folosesc tactici grave, emoționale (conțin termenul "urgent" pentru a invoca diverse motive - actualizarea bazelor de date, câștigarea unui premiu, o dobândă atrăgătoare, un mesaj important, etc.).
- **Verificarea autenticității paginii** în care se introduc datele personale. Termenul *forgery* reprezintă procesul de creare, adaptare sau imitare a unor obiecte sau documente cu scopul de a induce în eroare. Falsurile au loc la diverse niveluri: se falsifică bunuri (mărci ale unor producători, înregistrate ® - Registered Trade Mark sau încă neînregistrate ™ - Trade Mark), bancnote, înscrisuri oficiale, opere de artă, documente, etc. O altă abordare a fraudei prin falsuri o reprezintă furtul identității: tot mai multe site-uri – copii mai mult sau mai puțin fidele ale site-urilor originale (de obicei ale unor bănci) - solicită diverse informații confidențiale potențialilor clienți în scopul realizării unor carduri bancare clonate sau utilizării acelor date pentru achiziția online de bunuri sau servicii. Termenul utilizat pentru substituirea de identitate pe Internet este "*Web forgery*". Pentru realizarea tranzacțiilor financiare sigure se folosește **protocolul https** (*Hypertext Transfer Protocol Secure*), protocol creat de Netscape Communications în 1994 care folosește portul 443 și asigură criptarea documentelor web transmise, utilizarea semnăturilor digitale (printr-un certificat digital emis de o autoritate competentă și recunoscută) și a unui cod de autentificare pentru integritatea mesajelor.

### Mecanisme de protecție:

- Versiunile noi de Firefox (versiunea 2) și IE (versiunea 7) au diverse **mecanisme integrate**, astfel că utilizatorul este avertizat înainte de a accesa o pagină periculoasă. Aceste mecanisme pot fi:
  - Anti-phishing: previne furtul unor date bancare
  - Anti-malware: avertizează despre o pagină ce conține cod periculos pentru securitatea calculatorului. De obicei, scripturile Javascript acționează prin:
    - copierea pe hard-disk a unor secvențe de cod cu efecte nedorite
    - modificarea regiștrilor
    - modificarea setărilor browserului (în special Internet Explorer, care s-a dovedit a fi cel mai vulnerabil, deci și cel mai atacat)

- Google deține un serviciu de avertizare și raportare a paginilor suspecte.



- Tot Google, prin intermediul Google toolbar, protejează accesul la pagini cu potențial risc prin extensia de Firefox denumită *Google Safe Browsing*.



Una din firmele de referință în domeniul securității calculatoarelor, McAfee, oferă serviciul **McAfee Site Advisor**, prin care testează zilnic site-urile înscrise în program, împotriva a mii de vulnerabilități cunoscute. Prin intermediul unui plugin, site-urile sunt marcate cu un simbol care le clasifică din punctul de vedere al securității, în:

	<b>SAFE</b>	Site-uri fără riscuri sau cu riscuri foarte scăzute
	<b>CAUTION</b>	Site-uri cu riscuri minore
	<b>WARNING</b>	Site-uri cu riscuri ridicate
	<b>UNKNOWN</b>	Site-uri neverificate; accesare cu precauție

Site-urile de e-commerce sigure poartă emblema ("McAfee SECURE sites"), ce garantează atât autenticitatea lor, cât și că utilizarea lor este sigură.

### 3. Securitatea mesajelor e-mail

Un mesaj e-mail poate fi interceptat de persoane neautorizate, cu sau fără intenție, pe traseul expeditor -> server expeditor -> server destinatar -> destinatar. În ceea ce privește securitatea datelor se urmăresc patru scopuri:

#### 1. confidențialitatea (utilizatorii neautorizați să nu aibă acces la informație)

Accesul la căsuța poștală a unui utilizator se face printr-o parolă. Intimitatea (*privacy*) corespondenței însă nu se poate întotdeauna asigura. De aceea, transmiterea informațiilor confidențiale se poate face prin criptarea mesajului, implementările disponibile la acest moment fiind **S/MIME** (*Secure / Multipurpose Internet Mail Extensions*) - dezvoltat de RSA Data Security Inc., **PGP/MIME** (*Pretty Good Privacy*) și **OpenPGP**.

#### 2. autentificarea (determinarea identității partenerului înainte de a iniția un dialog cu el)

Una din problemele des întâlnite în mediul online este preluarea unei alte identități, în scopul ascunderii identității (fenomen denumit *spoofing*). Protejarea identității expeditorului unui mesaj se poate face prin semnătura electronică, un cod prin care, ca și semnătura pe diverse hârtii oficiale, se poate stabili identitatea semnatarului și garanta că nu a fost modificat conținutul. Se folosește criptografia cu chei publice pentru generarea unui cod ce va fi inclus în mesaj.

#### 3. nerepudiarea (dovedirea partenerului că el este cel care a trimis datele)

Recunoașterea originii este foarte importantă, astfel încât expeditorul să nu poată nega că el este autorul mesajului. Acest serviciu permite de exemplu ca un mesaj să fie trimis mai departe și altor destinatari (*forward*) care să poată identifica autorul mesajului original. O aplicație a acestui serviciu este în plasarea comenzilor on-line, a căror recepție să poată fi dovedită și care pot fi confirmate.

#### 4. integritatea (asigurarea că datele trimise nu au fost modificate)

Acest serviciu asigură că mesajul original este primit nemodificat, atât din punct de vedere tehnic (legătura prin rețea și trecerea prin diverse noduri nu va afecta conținutul), cât și al unui posibil atac informatic care să vizeze modificarea mesajului.

Câteva sfaturi în utilizarea serviciului e-mail:

1. Folosiți programe antivirus și anti-spyware actualizate, pentru protejarea de fișiere rău intenționate ce pot fi atașate mesajelor e-mail sau se pot instala, cu sau fără acceptul utilizatorului, în sistem;
2. Nu trimiteți date confidențiale prin e-mail (folosiți criptarea) sau pe site-uri nesigure, care vă cer acest lucru (nume utilizator, parolă, adresă, CNP, numărul cardului, PIN, etc.). O mulțime de mesaje nesolicitate (*spam*, *scam*) pot conține diverse informații mai mult sau mai puțin interesante, dar, mai ales, invitații la asociere în afaceri, intrarea în jocuri piramidale, instalarea unor programe gen worm care afectează siguranța datelor, logarea pe site-uri clone ale unor bănci sau webmail, link-uri ascunse către site-uri cu conținut malițios.
3. Utilizați adrese email diferite în funcție de specificul activității: adresa de serviciu numai în scopuri profesionale, o adresă personală pentru alte situații: corespondența cu prietenii, înscriere la newslettere, forumuri, concursuri, etc.
4. Atenție la deschiderea mesajelor și a fișierelor atașate, chiar dacă vin de la o persoană cunoscută:
  - a. Se poate disimula expeditorul real al mesajului, astfel încât mesajul să pară că vine din partea altcuiva;
  - b. Fișierele atașate pot avea extensii duble, astfel încât un fișier *image.jpg.exe* să fie executat de sistem, deci posibilă instalare a unui program nedorit în sistem;
  - c. În corpul mesajului pot exista legături (link-uri) către destinații disimulate, altele decât cele vizibile. Scopul redirectării poate fi:
    - creșterea traficului unei pagini (benefică pentru acea pagină dacă este înrolată în sisteme de publicitate - afișarea banner-elor duce la bani mai mulți încasați în urma reclamelor);
    - promovarea unor **pagini comerciale** (reclame mascate la diverse produse sau servicii) sau **cu conținut malițios** (crack, phishing, etc);
    - **rularea unor secvențe de cod** (*scripts*) cu un anumit efect asupra sistemului (modificare regiștri, instalare programe de monitorizare a activității - parole introduse, site-uri accesate, informații transmise, îngreunarea lucrului prin procese care ocupă memorie RAM sau pe disc din ce în ce mai multă)

Exemplu: <a href="adresă nedorită">adresa dorită</a>

## 4. Transferul fișierelor prin FTP

FTP este prin definiție o metodă nesecurizată de transfer fișiere, deoarece nu a fost gândită nicio metodă de criptare a datelor transferate, username-ului, parolei și comenzilor utilizate, toate acestea putând fi capturate prin utilizarea unor programe tip *sniffer* (program care urmărește pachetele de date ce trec printr-o rețea). Aceasta este una din problemele tuturor protocoalelor dezvoltate înainte de SSL (cum ar fi HTTP, SMTP, Telnet). Soluția ar fi utilizarea protocoalelor SFTP sau FTPS (FTP over SSL), protocoale ce permit criptarea SSL (*Secure Sockets Layer*) sau TLS (*Transport Layer Security*).

**SFTP** (*SSH File Transfer Protocol*, denumit și *Secure File Transfer Protocol*)

SFTP este folosit tipic cu protocolul SSH versiunea 2 (TCP port 22) pentru transferul securizat al fișierelor. Spre deosebire de mai vechiul protocol SCP (Secure Copy) ce permitea doar transfer securizat pentru fișiere, protocolul SFTP prezintă și alte avantaje: mai multe tipuri de operații asupra fișierelor la distanță (reluarea transferurilor întrerupte, listarea fișierelor din directoare, ștergerea fișierelor la distanță), este disponibil și pe alte platforme (nu doar pe UNIX)

**FTPS** (denumit și *FTP Secure* sau *FTP-SSL*)

FTPS este o extensie a protocolului FTP care oferă suport pentru protocoalele criptografice TLS și SSL, inclusiv pentru certificate de autentificare cu chei publice (pe partea de server și client), algoritmi de criptare AES (*Advanced Encryption Standard*), RC4, RC2, DES (*Data Encryption Standard*), Triple DES și funcțiile hash SHA, MD5, MD4 și MD2.



## 5. Conexiuni sigure la distanță ("remote")

La apariția protocolului Telnet (1969), utilizatorii rețelelor inter-conectate proveneau din mediul militar, academic și guvernamental, servicii unde nu se pune la acel moment problema de securitate a datelor. Odată cu dezvoltarea explozivă a Internetului, după 1990, s-a impus necesitatea apariției unor metode criptate pentru lucrul la distanță ("*remote*") pe servere. Protocolul **SSH** (*Secure Shell*) apărut în 1995 este un protocol ce permite schimbul datelor printr-un canal securizat, astfel încât datele sensibile (de obicei parole) să nu poată fi interceptate într-o rețea nesecurizată cum este Internet-ul. Tipic, protocolul SSH este utilizat pentru conectarea la distanță pe o mașină Linux și executarea unor comenzi pe acea mașină. Utilizarea protocolului SSH necesită un server SSH (care rulează pe mașina Linux, de obicei pe portul TCP 22) și un client prin care utilizatorul contactează daemon-ul SSH de pe calculatorul unde se dorește conectarea.

Versiunea inițială SSH-1 avea câteva puncte slabe ce o făceau vulnerabilă (de exemplu, atacurile de tip "*man in the middle*" prin care atacatorul își plasează mașina la nivel logic între alte două mașini care comunică, de unde interceptează mesajele transmise și lansează atacuri asupra celor două mașini țintă). Versiunea folosită curent este SSH-2, ce aduce multiple îmbunătățiri versiunii originale (securitate superioară, posibilitatea de a rula mai multe sesiuni printr-o singură conexiune).

## 6. Asigurarea securității sistemului informatic

Pentru asigurarea securității rețelei este importantă implementarea unor mecanisme specifice pornind de la nivelul fizic (protecția fizică a liniilor de transmisie), continuând cu proceduri de blocare a accesului la nivelul rețelei (firewall), până la aplicarea unor tehnici de codificare a datelor (criptare), metodă specifică pentru protecția comunicării între procesele de tip aplicație care rulează pe diverse calculatoare din rețea.

### Tehnici de codificare / criptare

Împiedicarea interceptării fizice este în general costisitoare și dificilă; ea se poate realiza mai facil pentru anumite tipuri de medii (de exemplu, detectarea interceptărilor pe fibre optice este mai simplă decât pentru cablurile cu fire de cupru). De aceea, se preferă implementarea unor mecanisme de asigurare a securității la nivel logic, prin tehnici de codificare / criptare a datelor transmise care urmăresc transformarea mesajelor astfel încât să fie înțelese numai de destinatar; aceste tehnici devin mijlocul principal de protecție a rețelelor.

### Criptografia tradițională

Modelul clasic de criptare presupune transformarea unui text sursă ("plain text") printr-o funcție dependentă de o cheie ("key"), transformare în urma căreia rezultă textul cifrat ("ciphertext"). Înainte de apariția rețelelor de calculatoare, acesta era transmis printr-un curier sau prin radio. În cazul interceptării mesajelor cifrate, ele nu puteau fi decodificate prea ușor în absența cheii de criptare. Uneori, "intrușii" puteau nu numai să asculte canalele de comunicație (intruși pasivi), ci și să înregistreze mesajele și să le retransmită mai târziu, să introducă propriile mesaje sau să modifice mesajele legitime înainte ca ele să ajungă la receptor (intrus activ).

Domeniul care se ocupă de spargerea (decodificarea) cifrurilor se numește criptanaliză ("cryptanalysis") iar conceperea cifrurilor (criptografia) și spargerea lor (criptanaliza) sunt cunoscute global sub numele de criptologie ("cryptology").

Într-o încercare de formalizare matematică a proceselor de criptare și decriptare, se pot folosi următoarele notații: S - textul sursă, CK - funcția de criptare, dependentă de o cheie K, R - codul rezultat și DK - funcția de decriptare. Cu aceste notații, criptarea este exprimată prin formula

$R = CK(S)$  iar decriptarea - prin  $S = DK(R)$ .

Se observă că  $DK(CK(S)) = S$ .

O regulă de bază în criptografie stabilește necesitatea cunoașterii metodei generale de criptare de către orice criptanalist. Acest principiu are la bază constatarea că pentru a inventa, testa și instala o nouă metodă de criptare este necesară o cantitate prea mare de efort pentru ca acest procedeu să fie practic. În consecință, cel mai important element devine cheia de criptare.

Cheia constă într-un șir de caractere care definește / selectează una sau mai multe criptări potențiale. Spre deosebire de metoda generală, care, în mod tradițional, se schimbă doar la câțiva ani, cheia putea fi schimbată oricât de des era necesar.

Când un criptanalist trebuie să decodifice un text, el se confruntă cu una din următoarele probleme:

- problema textului cifrat ("ciphertext only problem"), când are la dispoziție o cantitate de text cifrat și nici un fel de text sursă;
- problema textului sursă cunoscut ("known plaintext problem"), când are la dispoziție un text sursă și textul cifrat corespunzător;
- problema textului sursă ales ("chosen plaintext problem"), dacă poate cripta la alegere zone din textul sursă (poate afla criptarea unui anumit text).

Există două metode tradiționale de criptare: **cifruri cu substituție** și **cifruri cu transpoziție**. Aceste tehnici de bază sunt folosite, în forme evolute, și în sistemele moderne de criptare.

### Criptografia modernă

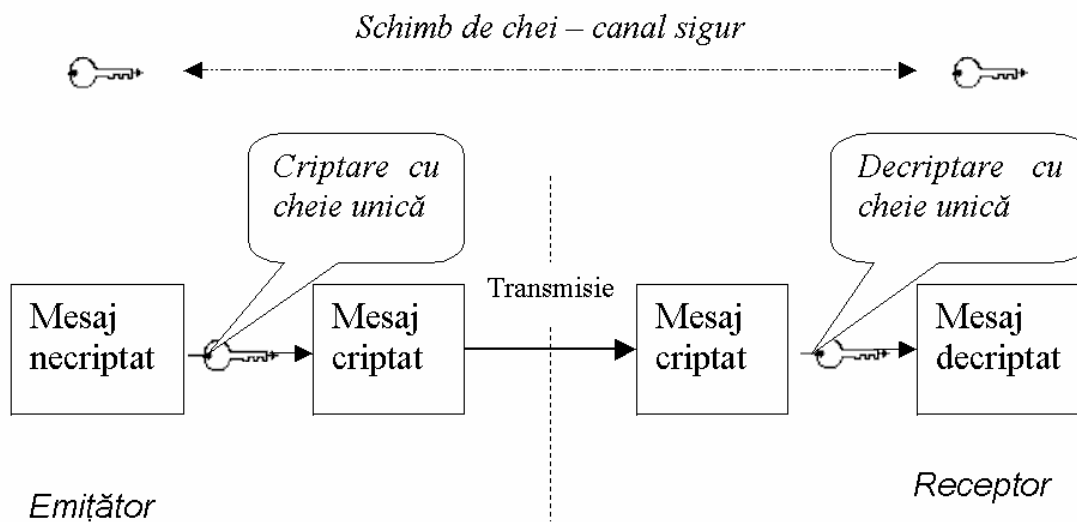
Având în vedere faptul că transmisia de date în Internet este neprotejată, a apărut necesitatea dezvoltării tehnicilor de criptare în direcția automatizării acestora și a implementării lor în rețele de calculatoare. Astfel, utilizarea unor algoritmi pentru criptarea informațiilor transmise va deveni principalul mijloc de rezolvare a problemelor de interceptare în rețele.

În descrierea unei transmisii de date prin rețea se obișnuiește să se numească generic "**mesaj**" un ansamblu de date trimis de un "emițător" unui "receptor". Printr-o metodă de criptare, mesajele vor fi transformate, pe baza unei chei de criptare, astfel încât să poată fi înțelese doar de destinatar.

Unul din principiile mai recent apărute în criptanaliză constă în utilizarea unei alte chei pentru decodificarea mesajului decât cea folosită la codificare; această tehnică este mai eficientă dar complică puțin procedeu general și de aceea se preferă când criptarea / decriptarea se realizează automat. Evident, dimensiunea unei chei de criptare (exprimate în general în biți) este o măsură a nivelului de securitate dat de acea cheie, ea indicând rezistența mesajului cifrat la încercările de descifrare de către cineva care nu deține cheia de descifrare potrivită.

Principiile de criptare din algoritmi cu cheie secretă au evoluat odată cu apariția calculatoarelor; ele continuă însă să se bazeze pe metodele tradiționale, cum ar fi **transpoziția și substituția**. Algoritmi cu cheie secretă sunt caracterizați de faptul că folosesc aceeași cheie atât în procesul de criptare, cât și în cel de decriptare (vezi figura de mai jos). Din acest motiv, acești algoritmi mai sunt cunoscuți sub numele de algoritmi simetrici; pentru aplicarea lor este necesar ca înaintea codificării / decodificării, atât emițătorul cât și receptorul să posede deja cheia respectivă. În mod evident, cheia care caracterizează acești algoritmi trebuie să fie secretă.

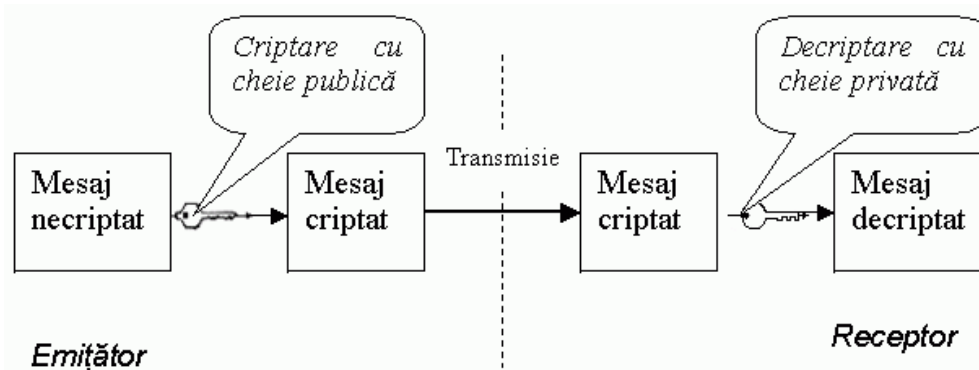
Principalul dezavantaj al algoritmilor simetrici constă în faptul că impun un schimb de chei private înainte de a se începe transmisia de date. Altfel spus, pentru a putea fi utilizați, este necesar un canal cu transmisie protejată pentru a putea fi transmise cheile de criptare / decriptare.



Schema de aplicare a unui algoritm simetric

Ulterior, vor apărea și algoritmi cu cheie publică, caracterizați prin faptul că criptarea și decriptarea folosesc chei diferite (vezi figura de mai jos). Această caracteristică a dat algoritmilor cu cheie publică și numele de algoritmi asimetrici. În acest caz, una dintre chei poate fi publică (general cunoscută - poate fi distribuită oricui) iar cealaltă va trebui să fie privată / secretă (cunoscută doar de cel care o folosește). Fiecare dintre aceste chei poate cripta mesajul, dar un mesaj criptat cu o anumită cheie nu poate fi decriptat decât cu cheia sa pereche.

Astfel, în cazul utilizării unui algoritm asimetric în comunicarea dintre un emițător și un receptor, fiecare dintre aceștia va deține câte o pereche de chei - publică și privată. Emițătorul poate cripta mesajul cu cheia publică a receptorului, astfel încât doar acesta să poată decripta mesajul cu cheia sa privată. În cazul unui răspuns, receptorul va utiliza cheia publică a emițătorului astfel încât decriptarea să se poată face exclusiv de către emițător (cu cheia sa pereche, privată).



Schema de aplicare a unui algoritm asimetric

Cheile algoritmilor asimetrici sunt obținute pe baza unei formule matematice din algebra numerelor mari, pentru numere prime între ele, iar din valoarea unei chei nu poate fi dedusă valoarea cheii asociate. Remarcăm faptul că aplicarea în informatică a calculelor modulo numere prime s-a dovedit extrem de benefică pentru mulți algoritmi moderni.

Tradițional, criptograful foloseau algoritmi simpli asociați cu chei de securitate foarte lungi. Azi se urmărește crearea unor algoritmi de criptare atât de complexi încât să fie practic ireversibili, chiar dacă un criptanalist achiziționează cantități foarte mari de text cifrat.

O altă caracteristică a criptografiei moderne constă în automatizarea tehnicilor clasice, prin folosirea unor dispozitive special concepute. Transpozițiile și substituțiile vor fi implementate cu circuite simple, de viteză mare, care vor fi conectate în cascadă astfel încât dependența ieșirii de intrare devine extrem de complicată și dificil de descoperit.

În 1977, guvernul SUA a adoptat ca standard oficial pentru informațiile nesecrete un cifru produs și dezvoltat de IBM, numit DES (Data Encryption System), care a fost larg adoptat în industrie. DES este cel mai popular algoritm cu cheie secretă;

el continuă să stea la baza unor sisteme folosite în mod curent. DES folosește (uzual) o cheie de 56 de biți; aceasta a fost în cele din urmă adoptată în locul uneia de 128 de biți, neagreată de NSA (National Security Agency), agenția "spărgătoare de coduri a guvernului", care dorea supremația în domeniul criptografic.

Din 1977, cercetătorii în criptografie au încercat să proiecteze mașini pentru a sparge DES. Prima asemenea mașină (1977) a fost concepută de Diffie și Hellman, avea nevoie de mai puțin de o zi iar costul ei a fost estimat la 20 de milioane de dolari. După aproape 2 decenii, costul unei astfel de mașini a ajuns la 1 milion de dolari iar timpul necesar spargerii codului a scăzut la 4 ore. Ulterior, s-au dezvoltat și alte metode, cum ar fi folosirea unui cip DES încorporat (loteria chinezească).

În scopul decriptării s-ar mai putea folosi mecanisme soft specifice (cum ar fi algoritmul asimetric Diffie-Hellman) și resursele libere ale unor calculatoare cu destinație universală. Astfel, s-a demonstrat că rularea pe mai multe calculatoare a unor programe distribuite de criptare (uzual, pe un număr mare de mașini, de ordinul miilor sau chiar zecilor de mii) crește considerabil eficiența procesului de decriptare.

Un alt cifru renumit este IDEA (International Data Encryption Algorithm), realizat de doi cercetători la Politehnica Federală din Zürich (ETHZ). Acest algoritm folosește o cheie de 128 de biți și este inspirat din metodele anterioare - DES și cele imaginate pentru spargerea DES.

Un alt algoritm performant a fost descoperit de un grup de cercetători de la MIT - Ronald Rivest, Adi Shamir, Leonard Adelman - și s-a numit cu inițialele creatorilor lui: RSA. Algoritmul de criptare RSA folosește o cheie publică.

Se observă că utilizarea unor astfel de algoritmi de criptare a datelor asigură transmisii confidențiale de date în rețele neprotejate, rezolvând problema interceptării. De fapt, riscul de interceptare / modificare nu dispare cu totul, din cauză că orice mesaj criptat poate fi în general decriptat fără a deține cheia corespunzătoare, dacă se dispune de suficiente resurse materiale și de timp.

Evident, dimensiuni variate ale cheii asigură diferite grade de confidențialitate iar perioada de timp necesară pentru decriptare poate fi prevăzută în funcție de mărimea cheii utilizate. Totuși, dacă procesul de decriptare este lent, este posibil ca în momentul în care s-ar obține datele dorite, acestea să nu mai fie actuale sau utile.

Timpul de decriptare depinde în mod natural și de puterea procesoarelor utilizate în acest scop, astfel încât utilizarea distribuită a unui foarte mare număr de procesoare poate duce la o micșorare considerabilă a timpului necesar. Din acest motiv, pentru transmisii de date în care este necesară o confidențialitate strictă se utilizează chei de dimensiuni mult mai mari, chiar pentru algoritmul DES (de 256, 512, 1024 și chiar 2048 sau 4096 de biți), știut fiind că timpul necesar decriptării crește exponențial cu dimensiunea cheii de criptare / decriptare.

Pentru utilizatorii obișnuiți ai Internet-ului, cei mai convenabili algoritmi de criptare sunt cei cu cheie publică fiindcă folosirea lor nu implică schimbul preliminar de chei pe canale de transmisie protejate, ca în cazul algoritmilor cu cheie secretă. Cheia publică poate fi distribuită fără restricții pe Intranet (rețeaua locală) sau Internet, iar mesajele criptate cu această cheie de un emițător vor putea fi decriptate numai utilizând cheia privată, care este deținută exclusiv de către destinatar. Astfel, nici măcar expeditorul nu ar putea realiza decriptarea mesajului trimis.

## Autentificarea

Un alt domeniu în care a evoluat criptografia modernă este cel al creării unor protocoale de autentificare - tehnica prin care un proces verifică dacă partenerul de comunicație este cel presupus și nu un impostor. Verificarea identității unui proces de la distanță este dificilă și necesită utilizarea unor protocoale complexe, bazate pe tehnici criptografice.

Problema poate fi imaginată intuitiv sub forma a doi parteneri care comunică și a altuia care dorește să se introducă fraudulos în comunicație, simulând pe oricare din partenerii de discuție. Ca o metodă de protecție, cei doi utilizatori pot stabili, de exemplu, o cheie secretă de sesiune, dar această metodă presupune transmiterea cheii printr-un canal sigur; de aceea, se preferă, ca și în cazul împiedicării interceptărilor, utilizarea criptărilor cu chei publice.

Unul din protocoalele de autentificare folosit în sistemele în timp real se numește Kerberos (omonimul câinelui paznic al lui Hades, care îi ținea pe cei nedoriți afară). Conectarea securizată la un server aflat la distanță cu ssh folosește pentru autentificare un alt protocol, bazat pe algoritmul cu cheie publică RSA.

Problema autentificării impune găsirea unui corespondent electronic pentru semnăturile autorizate de pe documentele legale. Un asemenea corespondent se numește semnătură digitală (vezi figura de mai jos) și presupune existența unui sistem prin care una din părți să poată transmite mesaje "semnate" celeilalte părți, astfel încât:

- receptorul să poată verifica identitatea pe care pretinde că o are emițătorul. Această cerință este necesară, de exemplu, în sistemele financiare: calculatorul trebuie să se asigure că un ordin de cumpărare sau de plată aparține companiei cu al cărei cont bancar se va opera.
- transmițătorul să nu poată renega ulterior conținutul mesajului. Această necesitate asigură protejarea băncilor împotriva fraudelor: un client necinstit ar putea acuza banca implicată în tranzacție, pretinzând, de exemplu, că nu a emis un anumit ordin (de plată).
- receptorul să nu poată pregăti el însuși mesajul. În cazul unei tranzacții financiare cu o bancă, această cerință protejează clientul dacă banca încearcă să-i falsifice mesajul.

Ca semnături digitale, se pot folosi semnături cu cheie secretă sau publică dar, așa cum s-a explicat anterior, de obicei se preferă cheile publice.

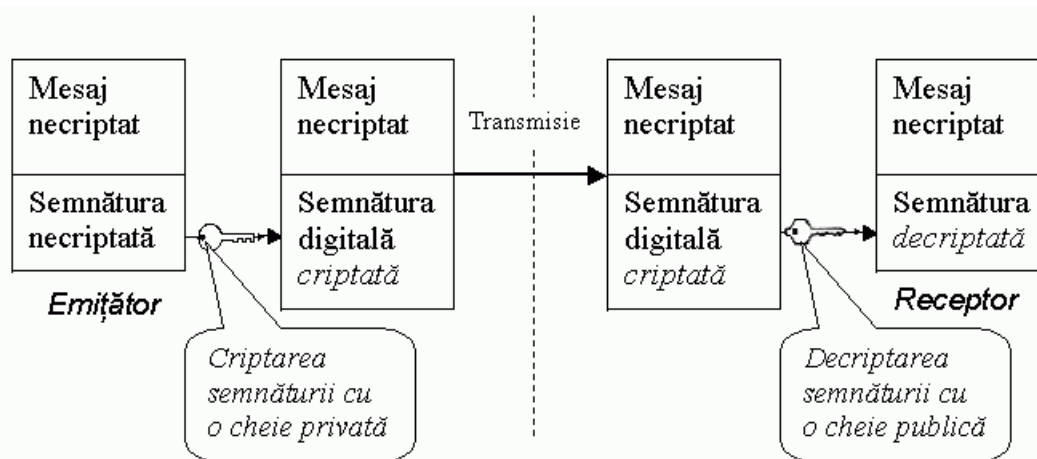
În cazul mesajelor transmise prin poștă electronică, riscul legat de impersonificarea expeditorului este destul de mare fiindcă standardele utilizate pentru transmiterea poștei electronice sunt simple și în plus au fost făcute publice (ceea ce înseamnă ca oricine are acces la ele și poate să le studieze). Standardul de e-mail nu are la bază nici un sistem pentru

verificarea identității celui care trimite un mesaj de poștă electronică, bazându-se pe o încredere reciprocă între utilizatori. Acest neajuns ar putea fi fructificat de către persoane răuvoitoare pentru a trimite mesaje de poștă electronică de pe adrese false, sau chiar de pe adrese existente, pretinzând că sunt utilizatorii care dețin acele adrese de poștă electronică. Practic, este (aproape) imposibilă identificarea unei persoane care a emis astfel de mesaje fiindcă în Internet există servere care asigură transmiterea anonimă a mesajelor ("anonymous remailers"), trimițându-le de la un server la altul de mai multe ori înainte de a le direcționa către adevărata destinație.

Pentru autentificarea expeditorului unui mesaj (de poștă electronică sau un ansamblu de date transmis prin Internet în alte scopuri) se folosește cel mai adesea un sistem cu cheie publică. Astfel, dacă expeditorul criptează mesajul cu cheia privată proprie, datele pot fi decriptate doar utilizând cheia publică pereche (vezi figura de mai jos), deci oricine poate verifica faptul că mesajul a fost transmis într-adevăr de expeditor, și nu de o persoană ce pretinde a fi expeditorul (după cum s-a explicat deja, mesajul criptat cu o cheie poate fi decriptat doar utilizând cheia pereche acesteia și se presupune că expeditorul este singurul care are acces la cheia sa privată).

Evident că este posibil să se realizeze o criptare a mesajelor în paralel cu autentificarea, astfel încât inclusiv datele transmise să fie codificate. În acest caz, se vor utiliza perechile de chei privată, publică nu numai pentru autentificare, ci și pentru criptarea, respectiv decriptarea mesajelor transmise. Practic, pentru codificarea și semnarea digitală a unui mesaj emis, se va realiza o criptare cu cheia privată a emițătorului și apoi o criptare cu cheia publică a destinatarului. Astfel, destinatarul va putea decripta mesajul și autentifica proveniența sa în condiții de securitate.

Având în vedere faptul că algoritmi de criptare cu cheie publică consumă foarte mult timp, în general se implementează o tehnică puțin diferită: se utilizează o criptare cu cheie publică pentru transmiterea unei chei secrete generate aleator (deci cheia secretă este criptată și eventual se poate utiliza și autentificarea expeditorului), după care datele propriu-zise vor fi transmise criptate cu un algoritm simetric utilizând cheia secretă schimbată anterior. Această metodă îmbunătățește considerabil viteza de transmisie și de criptare / decriptare.



*Semnarea digitală a mesajelor necripte*

Practic, pentru o identificare cât mai riguroasă a expeditorului se utilizează un sistem complex, bazat pe certificare, în care fiecare utilizator deține un certificat (ce are atașată o cheie publică și o cheie privată, secretă). Acesta este emis de o autoritate de certificare recunoscută, în urma examinării, pe bază de acte, a identității reale a persoanei. În momentul în care se dorește identificarea unei persoane, o căutare în baza de date a organizației respective va indica identitatea expeditorului (pe baza cheii publice a acestuia, care este unică în lume).

Acest sistem este implementat sub forma unei structuri în care fiecare autoritate de certificare poate împuternici la rândul ei alte organizații să emită certificate de autentificare, astfel încât originea unui certificat poate fi verificată în mod complet testând validitatea certificatului, apoi validitatea certificatului deținut de organizația care a emis certificatul respectiv, și așa mai departe.

Sistemul de certificate digitale este utilizat nu numai pentru protejarea comunicațiilor, ci și pentru certificarea originii programelor. Astfel, prin folosirea unei criptări a programului de instalare cu cheia publică a firmei producătoare, utilizatorul poate verifica relativ ușor că acel program a fost creat într-adevăr de o anumită firmă și pentru a decide dacă să instaleze sau nu programul. Aceasta este practic cea mai bună soluție de rezolvare a problemei rulării de programe / coduri dăunătoare.

## Canale de comunicații securizate

**SSH (Secure Shell)** e un program pentru logare la distanță și pentru executarea comenzilor pe un calculator de la distanță. A fost făcut pentru a înlocui programele rlogin și rsh și pentru a asigura comunicațiile criptate între 2 gazde neîncrezătoare dintr-o rețea nesigură. Prin canalul oferit pot fi forwardate și conexiunile X11 și porturile arbitrare TCP/IP.

Pachetul SSH este compus din server (*sshd*), client (*ssh*) și alte câteva utilitare pentru manevrarea cheilor. În general *sshd*-ul se pornește din scripturile de inițializare ale sistemului și rulează tot timpul în background. La fiecare conexiune nouă, serverul face fork. Fiecare mașină are o cheie RSA: host key (în mod normal pe 1024 de biți). În plus, când e pornit programul daemon <sup>1</sup>, el generează automat o cheie: server key (pe 768 de biți). Aceasta e regenerată din oră în oră dacă a fost folosită și nu e păstrată niciodată pe disc. De fiecare dată când un client vrea o conexiune, daemonul îi trimite host key și server key (publică). Clientul compară host key cu cea din baza lui de date, pentru a verifica dacă nu s-a schimbat. Apoi clientul generează un număr aleator de 256 de biți. Crijtează acest număr folosind host key și server key și trimite numărul criptat la server. În continuare ambele părți vor folosi numărul acesta aleator ca o cheie de criptare. Sunt suportate următoarele metode de criptare: IDEA, DES, 3DES, ARCFOUR și TSS. Implicit se folosește IDEA. Apoi serverul folosește una din următoarele metode pentru a autentifica clientul:

Mai întâi, dacă mașina de pe care se loghează utilizatorul e scrisă în fișierul */etc/hosts.equiv* sau */etc/shosts.equiv* de pe mașina de la distanță și numele utilizatorului e același pe ambele mașini, acesta se loghează imediat. În plus, dacă în directorul home al utilizatorului de pe mașina de la distanță există fișierul *.rhosts* sau *.shosts* și conține o linie cu numele mașinii client și numele utilizatorului pe acea mașină, acesta se loghează imediat. În mod normal, doar această metodă de autentificare nu e permisă, fiind nesigură.

A doua metodă de autentificare e metoda rhost sau *hosts.equiv* combinată cu autentificarea prin RSA. Adică logarea se poate face doar dacă e permisă prin *.rhosts*, *.shosts*, */etc/hosts.equiv* sau */etc/shosts.equiv* și în plus se verifică și cheia gazdei.

Ca o a treia metodă de autentificare, *ssh* suportă autentificarea RSA. Fiecare utilizator își creează o pereche de chei: publică și privată. Serverul cunoaște cheia publică și doar utilizatorul cunoaște cheia privată. În fișierul *\$HOME/.ssh/authorized\_keys* se află lista cheilor publice care se pot loga. Când utilizatorul se loghează, programul *ssh* spune serverului care pereche de chei va fi folosită pentru autentificare. Serverul verifică dacă această cheie se află printre cele cărora li se permite logarea și, în caz afirmativ, trimite utilizatorului (de fapt programului *ssh* din spatele utilizatorului) o întrebare, un număr aleator, criptat cu cheia publică a utilizatorului. Această întrebare poate fi decriptată doar cu cheia privată potrivită. Utilizatorul decriptează întrebarea folosind cheia potrivită, dovedind astfel că e corect. *Ssh*-ul implementează protocolul de autentificare RSA automat. Utilizatorul își creează perechea de chei RSA automat, rulând *ssh-keygen*. Acesta pune cheia privată în *.ssh/identity* și cheia publică în *.ssh/identity.pub* în directorul home al utilizatorului. Utilizatorul trebuie să copieze *identity.pub* în *.ssh/authorized\_keys* în directorul home de pe mașina de la distanță (fișierul *authorized\_keys* corespunde cu fișierul convențional *.rhosts*, având o cheie pe o linie, chiar dacă liniile sunt foarte lungi). Apoi utilizatorul se poate loga fără parolă. Autentificarea prin RSA e mult mai sigură decât cea prin *rhosts*. Cel mai convenabil mod de a folosi autentificarea prin RSA e un agent de autentificare, *ssh-agent*.

Ca o a 4-a metodă, *ssh*-ul suportă autentificarea printr-un server TIS. Ideea e ca *ssh*-ul cere serverului de autentificare TIS să autentifice utilizatorul. Uneori, numele utilizatorilor din baza de date TIS nu poate să fie același cu cel de pe mașina locală. Aceasta se întâmplă când utilizatorul se autentifică cu un smartcard sau Digipass. În acest caz, numele utilizatorului din baza de date e cunoscut ca numărul serial a device-ului de autentificare. Fișierul */etc/sshd\_tis.map* conține maparea între utilizatorii locali și numele corespunzător lor din baza de date TIS. Dacă fișierul nu există sau utilizatorul nu e găsit, numele corespunzător din baza de date TIS e presupus același.

Dacă o altă metodă de autentificare eșuează, *ssh*-ul cere utilizatorului o parolă. Parola e trimisă gazdei de la distanță pentru verificare, criptată. Când identitatea utilizatorului a fost acceptată de server, acesta fie execută comanda dată, fie se loghează și transmite utilizatorului un shell normal pe mașina de la distanță. Toate comunicațiile sunt criptate automat.

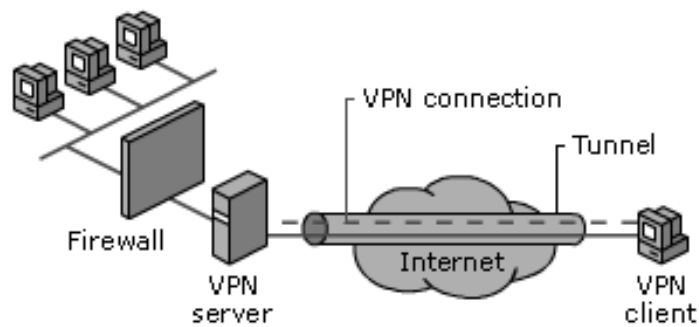
## Rețele private virtuale

O rețea privată virtuală (Virtual Private Network - VPN) asigură o modalitate de stabilire a unor comunicații securizate prin intermediul unei rețele nesigure în alte condiții. Cu ajutorul unei conexiuni VPN, cele două părți ale unei conexiuni pot comunica în aceleași condiții de siguranță ca și cele furnizate de rețeaua locală a unei firme. Pentru aceasta, o conexiune VPN oferă, de obicei, următoarele funcționalități:

- **Autentificare** - utilizând parole sau alte procedee, cele două părți ale unei comunicații își pot demonstra identitatea înainte de a accepta o conexiune. O dată conexiunea instalată, comunicația se poate desfășura în ambele direcții prin intermediul conexiunii respective.
- **Codificare** - prin codificarea tuturor datelor trimise între cele două puncte ale rețelei publice, pachetele transmise se pot vedea dar nu pot fi citite de un hacker. Acest procedeu este cunoscut sub numele de *tunneling*.

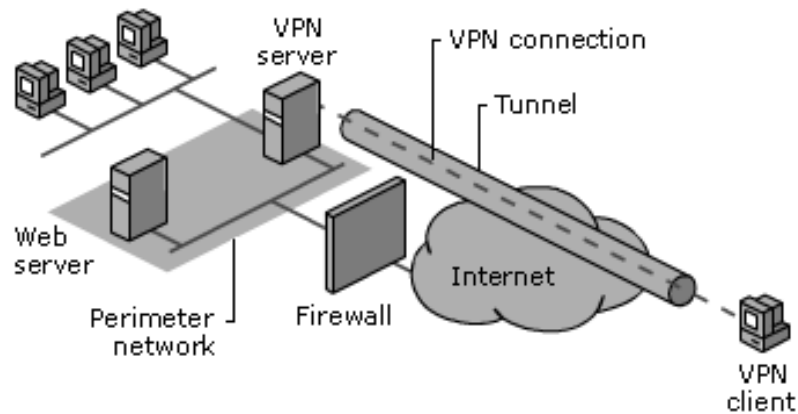
---

<sup>1</sup> daemon – program din sistemul de operare Unix ce rulează în fundal



În sistemul de operare Unix există mai multe modalități de configurare a conexiunilor VPN:

- **Internet Protocol SECurity (IPSEC)** - IPSEC este un standard creat de Internet Engineering Task Force (IETF) ca metodă obligatorie de codificare atunci când IP versiunea 6 va deveni protocolul Internet standard (în prezent versiunea standard este IPV4). În prezent există numeroase pachete software ce implementează IPSEC prin IPV4.
- **PPP over OpenSSH** - prin utilizarea acestei metode se poate configura o interfață PPP astfel încât să utilizeze SSH în vederea codificării tuturor datelor care traversează interfața PPP.
- **Crypto IP Encapsulation (CIPE)** - prin intermediul acestei metode pachetele IP sunt direcționate prin interfețele IP selectate sub formă de pachete UDP codificate. CIPE implică o suprasarcină mai redusă decât PPP over OpenSSH, deci este de așteptat obținerea unor performanțe superioare.



## II. MALWARE. VIRUȘI ȘI ALTE PROGRAME DĂUNĂTOARE

Cuvântul malware ("*malicious software*") este folosit de regula pentru a descrie orice forma de software periculos, care poate prelua controlul asupra PC-ului și produce daune sau cel puțin comportări neplăcute. Principalele categorii de malware sunt reprezentate de viruși, viermi (Worms) și troieni (Trojans). În general, se greșeste numindu-se "virusi" toate programele create în scopuri daunatoare: virusii sunt doar un tip de malware.

Un program care poate fi privit ca malware dacă face cel puțin una din următoarele:

- replicare prin rețea sau sistem de fișiere fără cunoscința utilizatorului
- permite controlul de la distanță neautorizat al unei persoane
- trimite informații sau fișiere la un alt sistem fără consimțământul utilizatorului
- trimite informații la un sistem pentru întreruperea activității normale.

**Căi de transmitere a programelor malware și câteva soluții:**

### 1. Vulnerabilități ale sistemului de operare și ale aplicațiilor folosite pentru accesarea paginilor web

Metode de protecție:

Înainte de conectarea la Internet (atât pentru un server Windows / Linux, cât și pentru o stație de lucru):

- Instalarea unei versiuni actualizate a sistemului de operare, cât mai stabil și cu breșe de securitate minime;
- instalarea și configurarea unui firewall
- instalarea, configurarea și actualizarea periodică a unui antivirus
- instalarea, configurarea și actualizarea periodică a unui program anti-spam (pe serverul de mail) și anti-malware (pe stația de lucru)

După conectarea la Internet: (în special pentru o stație de lucru Windows):

- actualizarea periodică a sistemului de operare și a browserului folosit
- utilizarea unor programe de șters urmele activității pe Internet (cookies, history, memoria cache)
- în browser (utilizarea și configurare, mai ales pentru calculatoare publice, folosite de mai mulți utilizatori):
  - o setarea parametrilor de securitate (Security) pentru cookies, rulare scripturi, ActiveX, Java;
  - o setarea parametrilor de intimitate ("Privacy"):
    - configurarea browserului astfel încât să nu memoreze nume de utilizator ("*username*") sau parole ("*passwords*") completate în diverse formulare de date (pentru login) sau alte câmpuri din formulare;
    - ștergerea periodică a datelor stocate local: cookies, history, memoria cache - fișiere temporare, formulare și parole salvate

Vulnerabilitățile serverelor (de web sau de e-mail) au reprezentat dintotdeauna o țintă pentru hackeri. Spargerea sistemului de securitate a site-urilor de e-commerce (magazine virtuale) conduce la obținerea datelor clienților (atât financiare - permit achiziții online folosind datele cardurilor bancare -, cât și adrese, numere telefon, adrese e-mail - ce pot fi utilizate ulterior în diverse scopuri: reclame comerciale, spam, etc).

### 2. E-mail

Este calea cea mai facilă pentru ca anumite informații să ajungă, cu sau mai ales fără acceptul destinatarului, în căsuța sa poștală. Reclame la produse ieftine sau gratuite, ascunderea unor adrese de phishing, materiale destinate adulților sunt doar câteva din problemele care afectează timpul, inbox-ul și câteodată chiar portofelul utilizatorilor.

Metode de protecție:

- program anti-spam - configurarea acestor programe este bine să se facă astfel încât mesajele considerate spam să ajungă totuși în inbox-ul destinatarului, eventual într-un folder special (astfel încât mesajele considerate greșit spam să fie totuși citite)
- reguli de filtrare - clienții moderni de e-mail permit stabilirea unor reguli de filtrare în funcție de numele expeditorului, adresă, subiect, cuvinte cheie, etc., astfel încât mesajele să poată fi organizate automat, după diverse criterii.
- ignorare mesaje - un aspect foarte important îl reprezintă instruirea utilizatorilor în legătură cu diversele atacuri ce pot avea loc pe Internet și măsurile care se pot lua pentru a le preveni. Una din cele mai simple măsuri este ignorarea totală a mesajelor suspecte (ștergerea directă, fără a fi deschise).

### 3. Navigare

Rețeaua mondială Internet a cunoscut în ultimii ani o creștere explozivă, din păcate nu numai ca informații și servicii, ci și în domeniul amenințărilor de securitate ("security threat"). Programele malware se ascund sub diverse forme, din ce în ce mai bine disimulate. Paginile web pot conține și următoarele coduri, ce afectează, la nivel de browser sau sistem de operare, buna sa funcționare:



- **Browser exploits:** sunt secvențe de cod care se auto-instalează pe sisteme neprotejate, de obicei fără știința sau acceptul utilizatorului. Sunt programe prin care se instalează keyloggers (programe care monitorizează secvențele de taste folosite, identificând și furând astfel parole sau alte informații confidențiale) sau trojans (programe ce folosesc sistemul infectat ca inițiator al unor atacuri asupra altor calculatoare). Principalele căi folosite de aceste programe sunt:

- vulnerabilitățile în browser sau în sistemul de operare
- neatenția sau efectele necunoscute ale deciziilor utilizatorilor

- **Cookies** - fișier text stocat de un server web pe calculatorul utilizatorului în care se salvează diverse informații cum ar fi: preferințele utilizatorului, coșul de cumpărături, monitorizarea sesiunii de lucru (pentru identificarea și menținerea stării - logat, delogat). Cookies-urile nu sunt viruși sau spyware, deși sunt raportate uneori ca spyware de către programele specializate datorită faptului că pot urmări site-urile vizitate de un utilizator. Cookies-urile se pot dezactiva din browser, însă sunt mecanisme care permit buna utilizare a unor site-uri (magazine virtuale, plăți online); dezactivarea lor face imposibilă utilizarea anumitor facilități ale acestor site-uri.

- **Pop-up** - ferestrele ce apar automat la accesarea unei pagini web deschid ferestre nedorite, prezintă reclame, pot redirecta pagina curentă către diverse alte destinații, pot instala cod rău intenționat. Pentru a preveni ferestrele ce apar automat (de tip pop-up sau pop-down), la nivel de browser se poate activa opțiunea de blocare a acestor ferestre ("*pop-up blocker*").

## 1. VIRUȘI

O definiție mai academică spune că virusul reprezintă, de fapt un acronim, provenit de la Vital Information Resources Under Siege ("Informații și resurse vitale atacate").

Virușii sunt cel mai răspândit și mai cunoscut gen de programe scrise special pentru a cauza stricăciuni intenționate sistemelor de calculatoare și rețelelor. Virușii reprezintă o problemă serioasă. Chiar dacă sunt entități foarte mici (unii au numai 380 de octeți), ei pot distruge complet un calculator. Virușii sunt și mai periculoși în cazul în care se împrăștie într-o rețea (iar Internetul este și el tot o rețea).

Un virus de calculator este un program, uneori distructiv, proiectat pentru a "călători" de la o mașină la alta infectându-le pe fiecare. Infectarea presupune de obicei că virusul se autoatașează de alte fișiere (se multiplică întocmai ca un virus biologic).

Un virus prezintă două funcții de bază: se copiază pe el însuși în alte programe infectându-le și execută instrucțiunile pe care autorul le-a inclus în el. În funcție de motivele autorului, un virus poate cauza daune imediat după execuția lui sau poate aștepta până când un anumit eveniment are loc. Inițial un virus se află în interiorul unui singur program, strecurat printre instrucțiunile sale. Atât timp cât utilizatorul nu lansează în execuție acest program virusul nu poate face nimic, deoarece nu a fost activat. În schimb, atunci când pune stăpânire pe computer (la prima lansare în execuție a programului infectat), virusul are grijă în primul rând să se multiplice. Pentru aceasta el se va "infiltra" în instrucțiunile altor programe contaminând întreg sistemul.

În această perioadă de "gestație" virusul nu strică nimic în mod vizibil, programele funcționează perfect, doar că un mic procent din instrucțiuni sunt furate de virus. Viteza de lucru este diminuată imperceptibil, astfel încât utilizatorul nu are nici un motiv de îngrijorare.

Ultima fază a dezvoltării virusului o reprezintă manifestarea maladiei informatice. Această acțiune concretă (finală) pentru care a fost conceput virusul poate fi complet inocentă sau ucigătoare. De exemplu: la o anumită oră a zilei cântă o melodie, mărește dimensiunea fișierelor cu 5Kb, șterge informații aleatoare de pe discul fix, șterge toată informația de pe hard disk, "defectează" componentele calculatorului. Oricum, periculos sau nu, un virus realizează ceva nedorit, dăunător sistemului și fără a cere acordul utilizatorului.

Un virus prezintă trei caracteristici: un **mecanism de replicare**, un **mecanism de activare** și un **obiectiv**.

**Mecanismul de replicare** trebuie să îndeplinească funcțiile următoare:

- caută alte programe pentru a le infecta;
- când găsește un program determină dacă acesta a mai fost infectat anterior, verificând dacă mai prezintă semnătura acelui virus;
- inserează instrucțiunile ascunse undeva în interiorul programului;
- modifică secvența de execuție a programului infectat astfel încât codul ascuns să fie executat ori de câte ori programul este apelat;
- creează o semnătură pentru a indica faptul că programul a fost infectat.

Această semnătură e necesară pentru că fără ea programele ar putea fi în mod repetat infectate și ar crește mult în dimensiuni, fapt care ar da de gândit. Mecanismul de replicare ar mai putea îndeplini și alte funcții pentru a se ascunde faptul că fișierul a fost infectat. De exemplu, resetează data de modificare la valoarea ei inițială (data de creare a programului) sau raportează dimensiunea inițială a programului și nu cea rezultată în urma infectării.

**Mecanismul de activare** verifică dacă s-a întâmplat un anumit eveniment sau condiție. Când acesta are loc, virusul își execută obiectivul care de cele mai multe ori e unul nedorit, o acțiune dăunătoare. În cazul în care mecanismul de activare verifică dacă a fost atinsă o anumită dată pentru a executa obiectivul se spune că virusul este o **bombă de timp** sau **cu ceas** (time bomb). Dacă verifică existența unei condiții (de exemplu dacă programul a fost executat de un anumit număr de ori) se spune că virusul conține o **bombă logică** (logic bomb). Pot exista diferite mecanisme de activare sau se poate să nu fie nici unul, ci doar infectarea inițială a programului.

**Obiectivul virusului** poate îmbrăca mai multe forme: fie afișarea unor mesaje, cântarea unor melodii, ștergerea sau modificarea unor fișiere, schimbarea tabelii de partiții a harddisk-ului, etc.

## Tipuri de viruși

Cele mai importante categorii de viruși sunt:

a) După modul de infiltrare:

- **Viruși de boot**

- **MBR (Master Boot Record)** – sunt acei viruși care infectează MBR-ul de pe hard disk-uri; sectorul care conține un scurt program care încarcă sistemul de operare. În MBR sunt conținute informații cu privire la ordonarea sectoarelor și partițiilor de pe întreg hard disk-ul. Acești viruși sunt cei mai eficienți din lume, deoarece sunt destul de simplu de scris, preiau controlul asupra mașinii la nivel foarte scăzut și adesea sunt invizibili (de exemplu, un virus de acest tip care a produs multe pagube de la crearea lui este Win95.CIH);
- **BS (Boot Sector)** – sunt asemănători cu virușii MBR, singura diferență remarcabilă între aceștia fiind că virușii BS au ca țintă dischetele.

Efectul virușilor de boot poate fi devastator, distrugând întreaga informație stocată pe disc prin alterarea tabelii de partiții. Acest tip de viruși au fost larg răspândiți în anii '90, însă au dispărut odată cu apariția procesoarelor pe 32 de biți și a declinului unităților floppy-disk.

- **Viruși de fișiere** – Spre deosebire de virușii de sector de boot (care atacă doar o mică porțiune a discului), virușii de fișier se pot împrăști în întreg sistemul. În schimb efectul lor este mai puțin devastator, informația putându-se recupera (până la un anumit nivel). După modul de acțiune, acești viruși se clasifică în:

- **Viruși care infectează fișiere.** Cel mai adesea, acești viruși infectează doar o anumită categorie de fișiere – de obicei, fișiere executabile, .EXE și .COM. Totuși, virușii de fișiere nu atacă doar executabilele, unii pot infecta fișierele de sistem - overlay (OVL), librării (DLL) sau drivere (SYS, DRV). Metodele de infectare sunt: suprascriere integrală a fișierului infectat, inserare cod (la începutul, sfârșitul sau undeva în cuprinsul fișierului)
- **Viruși care duplică fișiere.** Fișierele originale sunt redenumite, locul lor fiind luat de copii infectate; în rularea proceselor vor fi astfel executate versiunile infectate ce se pot propaga mai departe. O altă variantă de astfel de viruși ("companion viruses") creează un fișier infectat cu același nume ca și executabilul .EXE, dar cu extensia .COM. Sistemul Windows va executa întâi fișierul .COM atunci când întâlnește două fișiere executabile cu același nume, dar extensii diferite (.EXE și .COM).
- **Viruși care se auto-multiplică în mai multe foldere.** Nu modifică fișiere, ci așteaptă să fie executate la un moment dat de către utilizator (poartă nume atractive gen install.exe sau startwin.bat).
- **Viruși care utilizează facilitățile sistemului de operare.** Nici aceștia nu modifică fișiere, ci structura de directoare. Intrarea directorului ce conține acel virus este redirectată spre fișierul infectat; astfel, schimbarea către acel director este echivalentă cu executarea propriu-zisă a programului ce va infecta ulterior sistemul.
- **Viruși de macro.** Programele din pachetul Office permit crearea unor macrocomenzi (liste de comenzi și funcții foarte variate, utilizate pentru automatizarea unor acțiuni repetitive. Macrocomenzile pot lua și forma unor secvențe de cod malițioase care infectează fișierele Word sau Excel.
- **Viruși de script.** Sunt scriși în diverse limbaje de scripting (JavaScript, VBScript, PHP, ...) și infectează alte scripturi (comenzi și servicii Linux sau Windows), fișiere HTML, sau fac parte dintr-un virus cu mai multe componente.

b) După modalitatea de funcționare și de tehnicile folosite la crearea lor:

- **Viruși invizibili ("stealth")** – folosesc tehnici de mascare care ascund faptul că discul a fost infectat. De exemplu, atunci când sistemul de operare cere anumite informații, virusul stealth răspunde cu informațiile originale, existente înainte de a infecta sistemul. Cu alte cuvinte, atunci când apare pentru prima dată infecția, virusul salvează informațiile necesare pentru a "păcăli" mai târziu sistemul de operare (sau scanerul antivirus);

- **Virușii polimorfici ("polymorphic")** – reprezintă un fenomen relativ nou, deoarece sunt mult mai complecși decât echivalentul lor normal. Virușii polimorfici se pot modifica, identificarea lor devenind astfel mult mai greoaie. Au existat viruși polimorfici care foloseau tehnici de criptare avansate. În plus, își pot modifica semnătura. Acest proces de modificare se numește mutație. Prin mutație, un virus își poate schimba dimensiunea și compunerea. Deoarece

scanerile antivirus caută, de obicei, "șabloane" cunoscute (dimensiune, sumă de control, dată și așa mai departe), un virus polimorf bine construit se poate sustrage acestei detecții. Pentru a combate această tehnică, specialiștii creează scanere ce pot identifica modelele de criptare folosite;

- **Virusii TSR** ("Terminate-and-Stay-Resident") – virusii rezidenți în memorie se instalează la un nivel înalt al memoriei RAM pentru a se atașa fișierelor executabile sau documentelor Office care sunt deschise la un moment dat.

Programele antivirus trebuie alese astfel încât să aibă o bază de date cat mai mare cu definițiile virusurilor cunoscute pentru a proteja eficient sistemul, să ocupe cât mai puțină memorie atunci când monitorizează activitatea din calculator și să-și facă update pe Internet cât mai des pentru a-și completa baza de date.

În ultimul timp, dat fiind avântul pe care l-a înregistrat telefonია mobilă, o nouă specie de virusi atacă dispozitivele portabile (PDA sau telefoane mobile). Primul troian pentru Palm OS a apărut în septembrie 2000, iar primul virus pentru Pocket PC în iulie 2004. Pentru telefoanele "smartphone" ce rulează sistemul de operare Symbian, primul virus a apărut în iunie 2004. Transmiterea acestor virusi se face prin MMS (viermele Commwarrior) sau prin dispozitivul Bluetooth.

Topul virusilor 2008, conform Virus Bulletin ([www.virusbtn.com](http://www.virusbtn.com))

Time interval:

Day

Week

Month

Year

☒ Top 10 threats

☐ All detected viruses

Virus	Count	Infection Ratio (%)	Infection Ratio
01. Win32/Zafi.B worm	2 156 201	0.068 %	1/ 1.5 ths
02. Win32/Netsky.Q worm	1 410 136	0.044 %	1/ 2.3 ths
03. a variant of Win32/Stration.XW worm	380 263	0.012 %	1/ 8.4 ths
04. a variant of Win32/Injector.BZ trojan	174 178	0.005 %	1/ 18.3 ths
05. Win32/Spy.Goldun.NDO trojan	123 399	0.004 %	1/ 25.9 ths
06. Win32/Bagle.HE worm	79 354	0.002 %	1/ 40.2 ths
07. Win32/AutoRun.FakeAlert.S worm	68 625	0.002 %	1/ 46.5 ths
08. a variant of Win32/Kryptik.BD trojan	68 265	0.002 %	1/ 46.8 ths
09. Win32/Netsky.D worm	54 934	0.002 %	1/ 58.1 ths
10. Win32/Mytob.BK worm	34 101	0.001 %	1/ 93.6 ths
> OTHER VIRUSES	409 481	0.013 %	1/ 7.8 ths
> TOTAL THREATS	5.0 mil	0.155 %	1/ 643.9
Total clean messages	3188.3 mil		
Total messages	3193.3 mil		

Câteva exemple din cele cunoscute tipuri de virusi:

- Anii '80: Brain, Vienna, Jerusalem, Cascade
- 1990 - Chameleon (virus polimorfic), Frodo, Whale (virusi invizibili)
- 1991 - Tequila, Ameba
- 1992 - Michelangelo
- 1993 - Strange, Bomber, Uruguay, Cruncher
- 1994 - SrcVir, OneHalf.
- 1995 - NightFall, Nostardamus, Nutcracker, Concept.
- 1996 - Win.Tentacle, OS2.AEP, Laroux, Win95.Punch. Anul 1996 a reprezentat debutul răspândirii virusilor pentru sistemele pe 32 de biți (Windows 95, Windows NT) și aplicațiile Office.
- 1997 - ShareFun, Homer, Esperanto, mIRC Worms.
- 1998 - Win95.CIH, Win95.HPS, Win95.Marburg, Backdoor.BackOrifice, VBScript.Rabbit.
- 1999 - Melissa, Corner, Tristate, Infis, Bubbleboy
- 2000 - DDoS, ILOVEYOU, Timofonica, Liberty (pentru sisteme mobile Palm)
- 2001 - Code Red, Klez, Nimda, Winux Windows/Linux Virus
- 2003 - Sobig, Somer, Blaster
- 2004 - Sasser, Mac OS X, MyDoom

2005 - Bropia, Troj/BankAsh, Commwarrior, Chod, PSPBrick, DSTahen, MSIL/Idonus, Troj/Stinx-E  
2006 - OSX/Leap-A, OSX/Inqtana.A, Redbrowser.A, Yhoo32.explr, W32.Chamb, iAdware, JS/Quickspace.A  
2007 - Agent.BKY, iPod Linux Virus, Storm, MSN Trojan  
2008 - Conficker, MacSweeper, Torpig, MoccmeX

### 1.a. Troieni (Trojans)

Troienii sunt (dupa cum sugereaza si numele) programe care nu fac ceea ce este descris in specificatiile lor. Principala diferenta dintre programele de tip Troian si virusii reali este ca troienii nu se auto-multiplica. Prin urmare, nu se pot auto-ataşa la un program existent, cu alte cuvinte nu pot infecta un fisier: troienii infecteaza sistemul.

Troienii pot fi impartiti in urmatoarele subcategorii:

1. Remote Access ("Backdoors"): odata lansat, permite cuiva sa preia controlul asupra computerului utilizatorului, via Internet, fara stiinta acestuia.
2. Passwords stealers ("Keylogger"): sunt programe incluse in fisiere, care fura parole. Parolele sunt trimise celui care a realizat troianul, fara stiinta utilizatorului.
3. Logical bombs: de fiecare data cand sunt intrunite anumite conditii, acesti troieni efectueaza operatii distructive sau care compromit securitatea sistemului.
4. Denial of Service ("Floodor", "Nuker"): aceste programe trimit anumite secvente de date catre o tinta (de obicei un server sau un site web), cu intentia concreta de a intrerupe serviciile acelei tinte.
5. Downloader / dropper - program care instalează cod maliţios. Acest cod poate fi disimulat chiar în program sau poate fi descărcat de pe Internet
6. Disable security software - dezactivează programele de securitate (antivirus, anti-malware) instalate pe calculator
7. Server Trojan (Proxy, FTP, IRC, Email, HTTP/HTTPS, etc.) - transformă maşina victimă într-un tip de server, fără ştierea utilizatorului
8. Clicker, Startpage, Link injector - deschid pagini web fără consimţământul utilizatorului, modifică setări ale browserului, suprascriu linkurile cu linkuri predefinite (site-uri afiliate care îşi cresc astfel veniturile din trafic)
9. Dialer: formează automat anumite numere de telefon (în general cu suprataxă) prin intermediul modem-ului computerului.
10. Rootkit - troian dificil de eliminat, ascunzându-se printre procesele rulate în sistem

### KeyLogger

Un KeyLogger este un program care ruleaza in background, de cele mai multe ori nefiind sesizat de task managerul din sistemul de operare si care inregistreaza toate apasarile pe taste pe care le executam. Informatiile le va scrie intr-un fisier, de multe ori criptat care urmeaza a fi trimis unei terte parti. KeyLogger-ul, initial folosit de unii angajatori pentru a urmări activitatea propriilor angajati, a devenit in zilele noastre unealta pentru una din principalele metode de fraudă online.

1. **Simptome** - Nu exista simptome specifice, clar asociate cu aceste aplicatii. Identificarea unui KeyLogger se face de obicei prea tarziu pentru a putea vorbi de o reducere a pagubelor.
2. **Efecte** - Furt de informatii critice pentru utilizator. Un exemplu ar fi: pornim calculatorul, click pe contul bancar de pe site-ul bancii, pe iconita jocului online sau pe browser si apoi pe contul de email, click pe casuta in care se cere numele de utilizator pe care-l scriem, tab pentru salt in campul pentru parola, scriem si parola, KeyLogger-ul inregistreaza aceste date hotului, care ulterior va avea acces deplin la cont. Consecintele sunt pe cat de simple si de evidente, pe atat de grave.
3. **Eliminare** - Combinatia clasica antivirus - firewall - antispysware. Chiar daca multi antivirusi nu vor detecta KeyLogger-ele, avand in vedere ca sunt transmise informatii catre o terta parte prin internet, exista o sansa foarte mare ca firewall-ul sa blocheze transferul informatiilor. Cele mai eficiente aplicatii, din experienta mea, sunt cele antivirus, iar ca exemplu ar fi Norton Antivirus 2005.
4. **Prevenire** - Metodele principale de 'achizitie' nedorita a unui KeyLogger sunt prin email, prin mesagerie instantă (Yahoo! Messenger, MSN Messenger) sau prin internet (linkuri catre pagini care contin scripturi ce instaleaza astfel de aplicatii, rulara de ActiveX-uri ascunse sau nu in spatele altei forme de continut). In mare, feriti-va de informatia primita de la surse necunoscute.

### 1.b. Viermi (Worms)

Viermii sunt similari virusilor, dar nu au nevoie de un fisier-gazda pentru a se multiplica. Un vierme foloseste sistemul infectat pentru a se replica si utilizeaza comunicarea intre computere pentru a se raspandi. Viermii au o caracteristica comuna si troienilor: nu pot infecta un fisier; ei afecteaza sistemul. Viermii se pot raspandi prin mai multe căi:

- email

Programul poate fi ataşat în mesaj sau se poate transmite un link către programul (sau o pagină) stocate pe un server web. Modul de răspândire este:

- prin propriul motor SMTP, codat într-o librărie API inclusă în program;
- printr-un client de e-mail, de obicei Microsoft Outlook sau Outlook Express;
- printr-o funcție MAPI implementată în Windows

Programul caută pe mașina infectată adrese de e-mail (în address book, în fișierele Outlook, în fișiere text de pe disc) la care se auto-trimite.

- fișiere stocate pe unități fixe și mobile sau partajate ("share"), infectând întreaga rețea locală de calculatoare

- programele de mesagerie instantă (tip IRC sau IM) - se trimit linkuri către site-uri infectate, care la rândul lor pot infecta calculatoarele utilizatorilor care vizitează respectivele pagini

- prin programe peer-to-peer de partajare fișiere, copiindu-se într-un folder partajat și ajungând astfel pe calculatoarele utilizatorilor care downloadează respectivul folder.

### Mass Mailer

O clasă de viermi o constituie programele de tip **Mass Mailer**, programe care se auto-răspândesc prin sistemul de poștă electronică. Termenul "mass mailer" identifică și programe al căror rol este transmiterea în masă, legitimă, a unui mesaj (de exemplu, la liste de abonați).

## 2. SPAM

În Tehnologia Informației (*IT – Information Technology*), spam se refera la mesaje email nesolicitate trimise în bloc (junk email). Aceasta înseamnă ca un mesaj cu conținut comercial sau chiar irelevant este transmis către o multitudine de destinatari, care nu l-au solicitat.

Mesajele spam constituie un subiect controversat în Curțile de Justiție de pretutindeni, mai ales în ce privește dreptul de a trimite mesaje către adrese de email publice și private. Este mai curând o problemă de consimțământ, decât de conținut. Pe lângă mesajele de email, autorii de spam dezvoltă noi cai de atac, folosind de exemplu mesageria instantă/ instant messaging (spim), weblogs, Short Messaging Service (SMS) sau pretinzând că oferă servicii de optimizare pentru motoarele de căutare pe Internet (spamdexing).

### Scopul mesajelor spam

Scopul acestor mesaje este de a tenta persoanele neavizate, să cumpere produse și servicii mai mult sau mai puțin legitime. Dacă în trecut, principalul motiv era de a bombardă newsgroup-uri sau liste de email cu mesaje inutile sau inadecvate, în prezent spam-ul este "perfecționat", orientându-se către interese banale. Întălmim în mod curent spam comercial și uneori spam legat de anumite momente (campionate internaționale, evenimente, subiecte de interes global).

Cele mai cunoscute obiective de email spam sunt:

- Promovarea și vânzarea de produse și servicii.
- Culegerea de informații confidențiale (harvesting), cum ar fi parole, conturi bancare, etc. prin loterii online, fraude bancare sau mesaje umanitare.
- Promovarea de concepte și ideologii.
- Trimiterea de spam viral:
  - Infectarea și transformarea sistemului destinat în PC zombie, pentru a forma rețele periculoase (botnets).
  - Furt de identitate și fraudă.

### Metode de email spamming

Autorii de spam oferă de obicei serviciile lor (deseori ilegale) companiilor sau persoanelor care caută un mod "mai ieftin" de a-și promova produsele.

Spammerii fie vând bazele de date companiilor interesate, fie vând serviciul complet: colectare de date, proiectarea canalului de transmitere a mesajului, pentru a evita detectarea sursei, și trimiterea de spam.

Promotorii câștigă prin plasarea costurilor de publicitate asupra destinatarilor mesajului.

Mesajul spam este expediat către colecții de adrese de email, culese prin diverse modalități:

- Harvesting (folosirea unor programe de căutare a adreselor de email în zonele publice, pe site-uri web sau pe servere de mail neprotejate);
- Flooding sau dictionary spamming (generarea automată de conturi pe anumite domenii);
- e-pending (căutarea de adrese valide pentru anumite persoane sau criterii);
- Usenet posting (trimiterea către newsgroup-uri);
- Înscriserea în liste de email, cu scopul de a obține acces la lista tuturor adreselor disponibile;
- Accesarea agendei de contacte sau a datelor personale ale utilizatorilor, folosind programe malware;
- Spionarea traficului de rețea;
- Sustragerea bazelor de date cu informații;

- Folosirea de virusi care inregistreaza datele introduse de utilizatori in formulare online.

### Consecinte

- Diverse sisteme sunt traversate de mesajul spam pana ce acesta ajunge la destinatie, pentru a ascunde expeditorul real.
- Furnizorii de servicii de Internet (ISP) se confrunta cu probleme serioase de costuri si functionare, cum ar fi timp de procesare, viteza de procesare, costuri pentru latimea de banda.
- Companiile si utilizatorii personali trebuie sa aplice liste sau scheme de filtrare, care maresc volumul din sistem, prin procesarea si stocarea unor cantitati mai mari de date.
- Livrarea de mesaje si navigarea pe Internet sunt incetinite considerabil.
- Mesajele cu spam viral raspandesc malware si sustrag date confidentiale.
- Un mail-inbox aglomerat este un factor stresant pentru orice utilizator.

### Cum evitati mesajele spam

- Folositi solutii antivirus si antispam, actualizate in permanenta.
- Actualizati in mod regulat sistemul de operare si aplicati cele mai recente "patch"-uri.
- Verificati intotdeauna autenticitatea expeditorului si folositi semnatura digitala.
- Aplicati filtre de continut, reguli euristice, filtre baysiene, graylists.
- Nu deschideti mesajele suspecte.
- Nu raspundeti si nu trimiteti mai departe mesajele spam.
- Nu folositi instructiunile de dezabonare din astfel de mesaje.
- Ignorati mesajele care sustin ca "ati solicitat" ceva sau ca ati incercat sa trimiteti un mesaj si ati primit o "eroare de transmitere".
- Folositi conturi de email si nume diferite, cand va inscrieti in newsgroups ori chat rooms.
- Mascati adresa de email (de exemplu adaugand un sir de caractere la numele domeniului: nume@nospam.domeniu.com) sau mai bine nu va publicati adresa pe Internet.

## 3. HOAX / CHAIN LETTER

Un hoax este o incercare de a insela, de a face publicul sa creada intr-o idee neobisnuita. Are deseori un obiect material ce ar conduce catre castiguri financiare ilicite sau apeleaza la convingeri religioase sau scopuri caritabile, ori pur si simplu este o farsa.

Multe tipuri de hoax urmaresc ridicolul sau satira, ironizand credulitatea publicului. S-au propagat utilizand mass-media, inca de la aparitia acestor mijloace, insa mediul IT este cel care ofera posibilitati nelimitate de raspandire.

### 3.1. Virus hoax

Este un mesaj de avertisment trimis prin email catre diversi destinatari, care se refera de obicei la un virus nou si foarte periculos. Mesajul sfarseste prin a sugera ca cititorul ar trebui sa-si avertizeze prietenii si colegii sau chiar sa retrimita mesajul primit catre intreaga agenda. Rezultatul este o proliferare exponentiala a unor mesaje inutile, care poate duce la o supraincarcare a sistemelor.

Acest hoax poate convinge utilizatorii sa stearga anumite fisiere din sistem, sub falsul motiv al anihilarii virusului, cauzand astfel pagube reale. Uneori se intampla chiar ca un hoax sa inspire aparitia unui virus.

### 3.2. Scrisori electronice in lant (chain-letter)

Scrisorile in lant sunt mesaje nedorite, care apar sub diverse forme. Acestea contin un mesaj surprinzator sau emotionant (sau chiar un text oarecare) si solicita transmiterea sa catre cat mai multi destinatari, dupa ce au fost indeplinite anumite conditii (trimiterea unei sume de bani, o dorinta, o rugaciune etc) si chiar ameninta cu consecinte grave neindeplinirea acestora.

Trimiterea mesaje in lant este considerata hartuire, deoarece sunt mesaje nesolicitate, inutile, care ajung sa contina un sir considerabil de headere colectate de la destinatarii anteriori. NU trebuie sa raspundeti sau sa transmiteti mai departe aceste scrisori! Provoaca pierdere de timp si eventual de bani.

Cateva tipuri de scrisori electronice in lant:

- Scrisori care aduc noroc - promit sa aduca noroc celor care continua lantul (este cel mai vechi tip de scrisoare in lant, care circula de multa vreme si care profita de avantajele formei electronice inca de la aparitia computerelor);
- Schema piramidala - este un sistem fraudulos de castiguri financiare, format dintr-un lant de persoane recrutate pentru a participa cu bani si pentru a inrola noi membri;
- Scrisori de caritate;

- Scrisori de rugaciune;
- Farse;
- Hoax politic;
- Legende urbane;
- Cereri fara sens;
- Anti-chain letters.

## 4. PHISHING

Phishing (derivat din termenul din limba engleza pentru "pescuit") sau "**brand spoofing**" (imitarea imaginii), este o forma elaborata de sustragere de date, care vizeaza mai ales clientii companiilor ISP, ai bancilor, ai serviciilor bancare online, agentii guvernamentale etc.

Atunci cand va publicati adresa de email pe Internet, cand completati formulare online, accesati newsgroup-uri sau site-uri web, datele dumneavoastra pot fi furate de catre aplicatii de indexare pentru Internet si apoi folosite fraudulos.

### Conceptul de phishing

Autorii de phishing creeaza pagini web contrafacute, ce imita imaginea unor corporatii furnizoare de servicii bine-cunoscute, pentru a inspira incredere. Dupa ce colecteaza sau genereaza adrese de email, infractorii "lanseaza momeala".

Este trimis un mesaj prin email sau mesagerie instant, cu un subiect credibil, prin care incearca sa va convinga sa completati informatii confidentiale, prin accesarea unei pagini web (link "click aici"; link URL; link tip imagine; text link) sau prin completarea unui formular in textul mesajului. Mesajul pare sa aiba un motiv plauzibil si chiar aduce argumente convingatoare, pentru a va determina sa actionati imediat.

Exemple de subiect pentru email:

"Update Your PayPal Account" , "Your eBay User Account has been suspended!", "Initiativa Bancii Nationale a Romaniei (BNR) - colaborare"

Informatiile cerute sunt de obicei:

- Numarul cardului de credit/ debit;
- Codul PIN pentru ATM;
- Informatii despre contul bancar;
- Codul numeric personal/ contul de asigurare;
- Parole;
- Conturi de email;
- Alte date personale.

Odata publicate, informatiile nu mai sunt confidentiale si sunt imediat folosite de catre infractori, in interesul lor. In general este foarte greu sa recuperati sumele pierdute, deoarece paginile folosite de autorii de phishing sunt online numai pentru cateva zile sau chiar ore.

### Tehnici de phishing

Principala metoda este folosirea unui mesaj email credibil, intentionat sa va directioneze catre o pagina web falsa. Unele mesaje contin un formular de inregistrare direct in textul continut. Trebuie sa tineti cont de faptul ca organizatiile oficiale nu trimit niciodata astfel de mesaje, care solicita informatii personale.

In aceste pagini web este posibil sa observati ca adresa URL nu este cea corecta. Exista totusi metode de falsificare a URL-ului:

- **"Social engineering"**: URL-ul este foarte asemanator cu cel real, lucru ce poate fi detectat la prima vedere. De exemplu, adresa <http://www.volksbank.com> poate fi inlocuita cu <http://www.v0lksbank.com> . Daca aveti impresia ca sunt identice, va inselati. Litera mica "l" este inlocuita cu majuscula literei "I".
- **Vulnerabilitatile browser-ului**: Pagina web falsa poate contine un script de exploatare a browser-ului. In acest caz, se afiseaza URL-ul real, insa pagina accesata este cea de pe serverul fals. De exemplu, in bara de adrese din browser se poate afisa o imagine. Nu puteti face "click" in campul barei, pentru a marca URL-ul. Alte tehnici de exploatare aplica un camp fals, in care veti putea chiar sa marcati un URL.
- **Pop-up**: Linkul din email este catre pagina web reala, insa o alta fereastră de navigare se afiseaza in prim-plan. Pagina reala poate fi navigata, practic, fara riscuri, insa trebuie sa va feriti de cealalta fereastră. De obicei, aceste ferestre pop-up nu au o bara de adrese, prin care sa identificati o pagina falsa.
- **Nicio bara de adrese**: Unele pagini false nu afiseaza nici o bara de adrese si, daca nu urmariti acest lucru in mod deosebit, este posibil sa nu observati ca lipseste.

În afara de exploatarea barei de adrese, se folosesc și alte tehnici, în mod individual sau suplimentar, pentru a accesa informații confidențiale:

- **Alte vulnerabilități ale browser-ului:** Se pot exploata și alte vulnerabilități ale browser-ului, pentru a descărca și a rula cod malware. Un asemenea program poate fi un troian, care înregistrează datele introduse de la tastatură și traficul Internet, mai ales când completăm și trimitem un formular online.
- **Pharming:** Numit și "domain spoofing" (falsificarea domeniului), redirectionează utilizatorul către o pagină web falsă. Deși introducem adresa corectă, suntem direcționați către o altă destinație. URL-ul corect rămâne afișat în browser, neschimbat. Pentru a realiza procesul de redirectionare, rezoluția numelui trebuie modificată. Aceasta se poate face fie prin schimbarea setărilor pentru protocolul TCP/IP, fie printr-o intrare în fișierul hosts.
- **"Man in the middle":** Probabil cea mai elaborată metodă, deoarece nu trebuie să modifice nimic pe computerul local. Autorul de phishing este situat între utilizator și serverul fals, direcționând astfel conexiunea.

### Tehnici de camuflaj

Pagina web de phishing poate folosi și trucuri precum:

- Tooltip falsificat,
- Click-dreapta inaccesibil.

Autorii de phishing folosesc tehnici de evitare a programelor antispam/ antiphishing:

- Caractere aleatoare sau citate celebre în subiectul sau textul mesajului;
- Text invizibil în email HTML;
- Conținut HTML sau Java în loc de text simplu;
- Numai imagini (fără alt text) în conținutul mesajului.

### Consecințe

Este foarte greu de stabilit când un email provine dintr-o sursă oficială sau nu, deoarece autorii de phishing folosesc foarte multe tehnici, pe care le pot chiar combina.

Care sunt consecințele publicării de informații confidențiale?

- Infractorii pot face datorii în contul dumneavoastră.
- Pot deschide noi conturi, pot semna contracte de utilități sau de împrumut în numele dumneavoastră.
- Pot comite infracțiuni sub o falsă identitate, folosind datele dumneavoastră.

Nu completați formulare prin email, cu informații confidențiale. Orice furnizor de servicii competent folosește pagini web securizate și certificate digitale.

- Nu deschideți linkuri sosite prin email, mai ales dacă mesajul este neașteptat sau nesolicitat. Contactați expeditorul, pentru a verifica dacă într-adevăr a avut intenția de a trimite mesajul (folosiți datele de contact primite direct de la furnizor, nu cele primite în acel mesaj).
- Nu răspundeți la mesaj. Stergeți mesajul și contactați presupusul expeditor (folosiți datele de contact primite direct de la furnizor, nu cele primite în acel mesaj).
- Nu deschideți linkurile din conținutul mesajului. Întotdeauna introduceți de la tastatură adresa în browser.

### Reguli de siguranță

Repararea daunelor cauzate de phishing poate fi frustrantă și laborioasă. Pe lângă reducerea productivității și consumul de resurse în rețea, sustragerea de date provoacă depunerea de eforturi considerabile din partea dumneavoastră: va trebui să vă recuperați identitatea, proprietatea și drepturile, dar și să vă demonstrați nevinovăția.

Mult mai ușor este să respectați câteva reguli de siguranță elementare:

- Actualizați sistemul de operare și aplicați cele mai recente "patch"-uri imediat ce apar.
- Alternati Internet Explorer cu alte browsere.
- Instalați soluții antivirus și firewall și mențineți-le la zi.
- Introduceți întotdeauna un URL de la tastatură, nu accesând un link.
- Asigurați-vă că folosiți o pagină web securizată (HTTPS) și verificați certificatele digitale.
- Verificați în mod regulat conturile și extrasele bancare și raportați imediat orice abuz.
- Raportați mesajele suspecte companiilor de securitate și autorităților locale.

## 5. SPYWARE SI ADWARE

**Adware** este orice aplicație software în care sunt afișate banner-e cu reclame pe tot parcursul funcționării sale. De asemenea, programul adware poate instala componente care să transmită informații despre utilizator și comportamentul său în lucrul la PC. Spre deosebire de programele spyware, utilizatorul este instiintat despre acest lucru atunci când modulul este



instalat. De fapt, o aplicatie adware este aceea care, pe langa functionalitatea ei de baza, mai are inca una - de a afisa reclame, de cele mai multe ori descarcate periodic de pe anumite servere din Internet.

**Spyware** este un program, de obicei descarcat din Internet, care trimite informatii despre calculatorul utilizatorului fara stirea acestuia, ori de cate ori se conecteaza la Internet. De obicei, pachetele transmise contin informatii de marketing si nu informatii confidentiale desi unele programe pot face si acest lucru.

Chiar daca unele aplicatii adware sunt si spyware, acesta nu este un lucru general valabil. De cele mai multe ori aplicatiile spyware s-au instalat si functioneaza fara stirea utilizatorului, spre deosebire de cele adware, unde utilizatorul este instiintat si a fost de acord cu acest lucru.

Foarte multa vreme software de calitate putea fi instalat si folosit gratuit dar odata cu cresterea complexitatii sale au crescut si costurile de implementare, iar dezvoltatorii au fost obligati sa caute metode de diminuare a lor. Una dintre cele mai la indemana a fost aceea de a livra impreuna cu programele si aplicatii de tip adware sau spyware. Pe de alta parte foarte multe programe comerciale au devenit utilizabile gratuit in mod legal prin trecerea lor in categoria adware.

De la inofensiva intentie de afisare periodica a unor reclame si pana la elemente de analiza si stocare a informatiilor despre comportamentul utilizatorului si configuratia hardware/software a calculatorului, a fost nevoie de crearea si instalarea pe calculatorul tinta a unor module suplimentare. Daca la inceput nu a fost vorba decat despre un motor ce descarca reclame si le afisa in ferestre prestabilite, industria adware a progresat foarte mult. Acum sunt folosite diverse alte instrumente, de la modificari in browser si/sau setarile acestuia si pana la diverse componente ce ruleaza ascuns in fundal si monitorizeaza activitatea la PC, transmitand informatiile unor servere din Internet.

Printre efectele cauzate de instalarea de spyware si adware se numara:

- adaugarea de link-uri catre mari magazine
- adaugarea de noi reclame pe paginile web, uneori chiar inlocuindu-le pe cele existente
- monitorizarea comportamentului browserului in scopuri comerciale
- obtinerea de acces la parole si coduri pentru cartile de credit
- incetinirea performantelor computerului datorita utilizarii resurselor
- in unele cazuri pot apela numere telefonice cu tarif ridicat
- schimbarea paginii de start a browserului si adaugarea de bookmark-uri noi
- aparitia de icon-uri ciudate si software nou pe desktop.

## 6. Atacuri de tip IP spoofing și Denial-of-Service

Un IP spoofing attack (atac de tip spoofing pe IP) apare cand un „atacator” din afara rețelei pretinde a fi un utilizator de incredere. Realizează acest lucru folosind o adresa IP din domeniul rețelei respective, sau utilizand o adresa IP externa autorizata, si careia i se ofera acces la resursele de pe retea. Un atac de tipul IP spoofing poate da acces la conturi de utilizator si parole. In cadrul unei companii un atacator ar putea trimite mail-uri partenerilor de afaceri care ar parea ca sunt trimise din cadrul companiei. Normal, un IP spoofing attack e limitat la injectare de date sau comenzi intr-un stream existent de date care se transmit intr-o aplicatie de tip client-server sau peer to peer.

Un alt tip de atac este Denial-of-Service (DoS). Refuzul unui serviciu apare deoarece sistemul devine ocupat sa stabileasca o legatura cu cel care a initiat cererea (care ar putea sa nu foloseasca o adresa IP valida). In termeni tehnici, gazda tinta primeste TCP SYN si returneaza SYN-ACK, apoi ramane in stare de asteptare, fiecare stare de asteptare foloseste resurse pana cand gazda nu va mai putea raspunde altor cereri. Ca si Snifferele de pachete, IP spoofing si atacurile DOS nu sunt restrictionate utilizatorilor din afara rețelei. Atacurile de tipul „Denial-of-service” sunt diferite de celelalte atacuri deoarece nu urmaresc accesul la retea sau la informatia dintr-o retea, aceste atacuri sunt concentrate pe incapacitarea serviciilor.

Simptomele unui atac DoS sunt:

- încetinire neobișnuită a vitezei rețelei (prin consumarea unor resurse precum lățimea de bandă, spațiul pe disc, puterea de calcul a procesorului);
- indisponibilitatea unui site web (prin distrugerea informațiilor de routare sau resetarea nesolicitată a sesiunilor TCP)
- imposibilitatea de a accesa vreun site (prin blocarea componentelor fizice ale rețelei - placă rețea, hub)
- obstrucționarea comunicării între utilizatori
- primirea unui număr foarte mare de mesaje spam (atac de tip *e-mail bomb*)

Câteva metode de atacuri DoS:

- ICMP flood
- Teardrop attack
- Peer-to-peer attacks
- Permanent denial-of-service attacks
- Application level floods
- Nuke
- Distributed Denial-of-Service (DDoS)

- Reflected attack

## 7. HIJACK

Semnificând "a lua cu forța", "a deturna", termenul Hijack în Internet face referire la:

- furtul unor domenii web (substituirea de identitate pentru furtul unor domenii web înregistrate pe alte nume)
- utilizarea unor servere DNS care redirectează către anumite adrese IP, în special pentru phishing
- modificarea primei pagini (homepage) sau a motorului de căutare utilizate de un browser web
- preluarea ilegală a unui set de adrese IP prin coruperea tabelelor de routare IP
- crearea unui motor de căutare care redirectează către pagini ce nu au legătură cu cuvintele cheie căutate sau către site-uri cu conținut rău intenționat

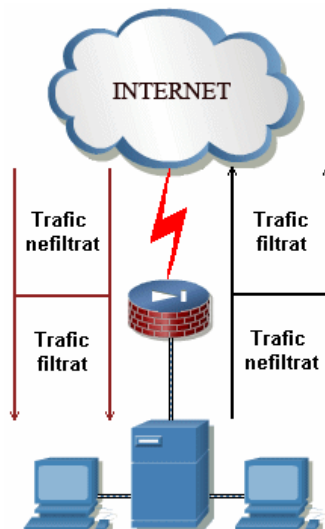
## PROBLEME DE SECURITATE ÎN 2009

- Conform unor studii, procentul spam-ului se situează în acest moment între 80-90%, datorat în principal extinderii activităților infracționale ale grupurilor de crimă organizată ce exploatează o gamă tot mai diversă de vulnerabilități, de la aplicații software până la cea mai slabă verigă, utilizatorii înșiși.
- Aplicațiile Web 2.0 care se bucură de popularitate vor fi în continuare căi de transmitere a codului malițios
- Microsoft Internet Explorer 8 sau sistemele de operare Windows 7, dar și MacOS sau Linux vor fi ținte atractive pentru malware (odată cu popularitatea *netbook*-urilor, sisteme portabile utilizate pentru navigare, e-mail și comunicare pe Internet)
- Playerele multimedia și formatul Flash vor fi căi de propagare a codurilor rău intenționate

### III. MECANISME DE PROTECȚIE

#### 1. Firewall-uri

În informatică, termenul "firewall" desemnează un ansamblu de componente hardware și software care ansamblu se interpune între două rețele pentru a regla și controla traficul dintre ele. Firewall-urile sunt folosite pentru a proteja/izola segmente ale unei rețele extinse (ex. Internet), dar mai ales pentru a proteja rețelele private (Intranet) ale unei firme/instituții/bănci/etc conectate la Internet. În cele ce urmează, prin rețea internă vom referi segmentul de rețea ce trebuie protejat, respectiv prin rețea externă vom referi segmentul de rețea de unde pot proveni amenințările și asupra căruia nu avem control (de obicei restul Internet-ului).



Prima condiție pentru ca un firewall să fie eficient este ca acesta să fie așezat în singurul punct de conexiune dintre rețeaua internă și cea externă (sau, în cazul mai multor puncte de acces către exterior, să avem firewall-uri similare în fiecare punct de acces). Dacă această primă condiție nu este îndeplinită, firewall-ul nu poate asigura controlul traficului. De exemplu dacă se neglijează anumite puncte de intrare cum ar fi modem-uri sau terminale nesupravegheate, atunci firewall-ul (sau firewall-urile) pot fi ocolite.

Un firewall oferă deci posibilitatea concentrării securității, deoarece supraveghează și controlează întregul trafic dintre rețeaua internă și cea externă. De aici derivă serviciile de securitate pe care un firewall le poate oferi:

- *Acces controlat* la și de la host-urile interne și externe. De exemplu poate fi permis accesul de la oricare stație de lucru în afară, accesul din exterior doar la serverele publice locale (eventual doar la porturile ce asigură acele servicii, nu la toată mașina), eventual, dacă s-au constatat încercări de atacuri de la o anumită adresă din Internet, se poate interzice comunicația cu subrețeaua având adresa respectivă;
- *Filtrarea protocoalelor* - interzicerea acelor protocoale sau opțiuni din protocoale (ex. comenzi SMTP) care ar reprezenta amenințări la adresa securității;
- *Autentificare centralizată* - impunerea unor protocoale avansate de autentificare pentru accesul din și în rețeaua internă;
- *Monitorizarea rețelei* - contorizarea traficului, înregistrarea în fișierele de jurnalizare (log-uri) a evenimentelor referitoare la traficul prin rețea.

Demn de remarcat este și faptul că existența unui firewall nu intră în contradicție cu aplicarea unor măsuri de securitate pe host-urile interne, acestea fiind în continuare recomandate (firewall-ul adăugând doar un nivel suplimentar de protecție ansamblului rețelei interne). Mai mult, acest lucru e chiar necesar în cazul compromiterii unuia dintre host-urile interne, altfel întreaga rețea ar fi compromisă.

De asemenea, un firewall oferă suportul ideal pentru implementarea unei rețele virtuale private (VPN - Virtual Private Network) prin criptarea automată a traficului dintre două rețele aparținând aceleiași organizații, rețele care se leagă între ele prin intermediul unei rețele publice și nesigure (ex. Internet).

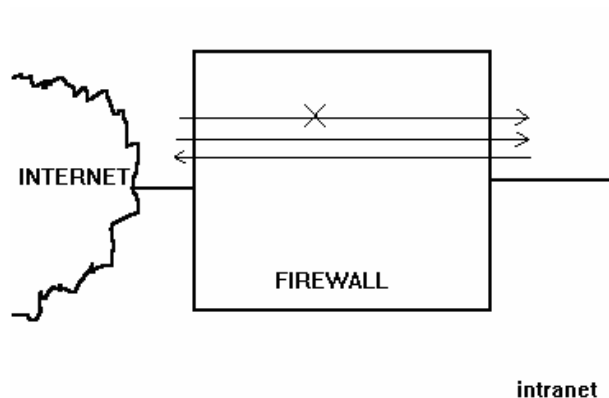
Instalarea unui firewall presupune în primul rând două acțiuni importante: analiza riscului și stabilirea politicii de securitate.

- *analiza riscului* se refera la pericolele pe care și le asumă organizația în lipsa unui firewall și la modul în care firewall-ul elimină sau reduce aceste riscuri. Pericolele variază în funcție de natura organizației, natura datelor care circulă prin rețea, gradul în care compromiterea rețelei afectează activitatea organizației etc. . Riscurile trebuie echilibrate cu costurile (financiare și umane) de achiziționare, instalare, instruire a personalului etc. necesitate de implementare a unei soluții cu firewall. În urma acestui proces rezultă decizia de a implementa sau nu un firewall în poziția respectivă;

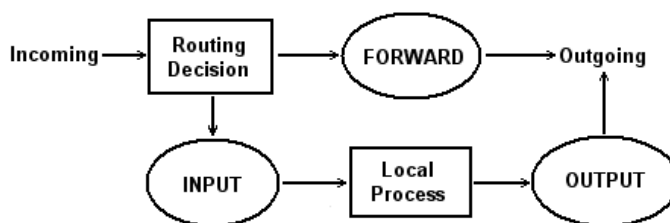
- *politica de securitate* reprezintă stabilirea drepturilor și restricțiilor legate de conectarea rețelei private la Internet. Firewall-urile reprezintă unul din mijloacele de impunere a acestei politici, fără a cărei existență scopul și modul de acțiune al firewall-urilor nu ar fi definite. Politica de securitate cuprinde elemente ca:
  - o serviciile care vor fi accesibile utilizatorilor interni (e-mail, acces full-Internet, web hosting), eventual restricțiile impuse în utilizarea acestor servicii (cota de alocare pentru dispozitivul de stocare a e-mail-urilor, contorizare de trafic,...);
  - o serviciile furnizate de către organizație în afară (către comunitatea Internet), de exemplu pagini de web prin server-ul public, FTP public, news, whois, etc;
  - o host-urile interne de la care se poate sau nu se poate ieși în Internet și în ce mod host-urile interne care pot fi accesate din exterior (de exemplu server-ele de mail, www, ftp, dns etc.);
  - o serviciile particulare ce pot fi accesate pe host-urile de mai sus (de ex. doar web pe server-ul de www, nu și ftp care ar putea fi folosit pentru utilizatorii interni ce au pagini publice de web);
  - o utilizatorii interni care au drept să acceseze Internet-ul din rețeaua internă;
  - o utilizatorii care au dreptul de a accesa date din rețeaua internă din exteriorul acesteia (de ex. persoanele aflate în deplasări care au nevoie de date din rețea, colaboratori externi, ...);
  - o politici și metode de autentificare pentru accesul din/în rețeaua internă.

Cele două tipuri principale de firewall-uri le constituie firewall-urile de filtrare și cele de tip intermediar (proxy). Deseori, pentru protecția unei rețele sunt utilizate ambele tipuri.

### Firewall-uri de filtrare



Un firewall de filtrare execută filtrarea traficului dintre rețeaua de calculatoare și Internet, blocând accesul anumitor elemente care pot reprezenta factori de risc pentru rețea. De asemenea, poate limita accesul la și dinspre Internet numai pentru anumite calculatoare din rețea. Acest firewall poate limita tipurile de comunicații, permițând sau refuzând în mod selectiv diferite servicii Internet. Pachetele IP care pătrund în sistemul firewall trec printr-un set de lanțuri care definesc operațiile ce se aplică pachetului.



Informația este transmisă în rețea sub forma unor pachete care parcurg drumul între mașinile sursă și destinație. Pachetele sunt transmise prin intermediul rutelor, care au sarcina de a găsi drumul optim dintre două host-uri (de fapt ruterele caută drumul optim de la ele către destinație, existând posibilitatea rutării asimetrice în cazul existenței legăturilor de date asimetrice). Filtrarea pachetelor este realizată prin intermediul unei componente a firewall-ului numită ruter protector (*screening router*). În momentul în care un pachet ajunge la firewall, ruterul protector determină întâi dacă acesta are dreptul de a fi trimis către destinație; dacă are acest drept, atunci ruterul protector își îndeplinește funcția de ruter și găsește o rută pe care îndrumă pachetul respectiv - dacă nu, atunci pachetul este abandonat. În acest moment, dacă firewall-ul este unul cu inspecția stării, atunci își modifică și starea internă a filtrului. Dreptul unui pachet de a traversa firewall-ul este stabilit conform politicii de securitate a organizației respective. Decizia de a trimite sau abandona un pachet este luată pe baza anumitor informații conținute în antetul pachetului respectiv (antetul IP în cazul Internet-ului), cum ar fi:

- adresa IP a sursei pachetului;
- adresa destinației;

- protocolul căruia îi aparțin datele (ICMP, UDP, TCP, ....);
- portul sursă;
- portul destinație;
- diverși indicatori din antetul TCP (ex. SYN, ACK, RST, FIN).

Filtrarea pachetelor se realizează pe baza unui set de reguli stabilite de către administratorii rețelei, reguli care implementează politica de securitate a organizației respective. La primirea unui pachet, router-ul parcurge pe rând toate regulile din memorie; la întâlnirea primei reguli aplicabile pachetului respectiv, acțiunea specificată de aceasta este aplicată pachetului. (Acțiunea poate fi eliminare, rutare sau respingere - respingerea reprezintă eliminarea cu eroare vizibilă, necesară unor anumite protocoale pentru evitarea timeout-ului generat de eliminarea silențioasă; există servicii (ex. IRC, SMTP) care depind de un răspuns (pozitiv sau negativ, dar la timp) asupra existenței serviciului ident.). Dacă unui pachet nu i se aplică nici o regulă, atunci pentru filtrarea acestuia va fi folosită regula implicită (de obicei refuzare sau eliminare).

O politică uzuală de acces care poate fi implementată prin filtrarea de pachete este de a permite utilizatorilor interni să deschidă conexiuni în exterior (de ex. să navigheze pe WorldWide Web) dar de a nu permite conexiuni din exterior către host-urile interne (eventual cu excepția server-elor publice de web, ftp, e-mail,...). De asemenea, prin filtrarea după porturi se pot selecta serviciile permise/interzise.

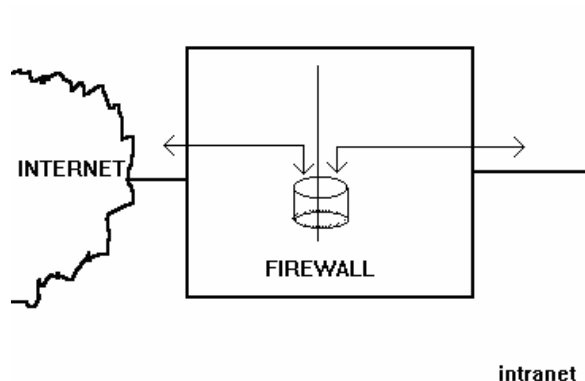
Avantajele unui firewall la nivel de pachet sunt următoarele:

- un firewall bine configurat poate proteja întreaga rețea internă aflată în spatele său;
  - firewall-ul este transparent, în sensul că utilizatorii serviciilor Internet din interiorul rețelei nu au cunoștință de existența acestuia;
  - un firewall oferă posibilitatea concentrării securității, nefiind necesară instalarea acestuia pe fiecare calculator din rețea în parte;
  - permit monitorizarea rețelei, adică înregistrarea în fișierele jurnal (*log*) a evenimentelor privind traficul în rețea.
- Dezavantajele firewall-urilor la nivel de pachet sunt:
- sistemul este vulnerabil la atacuri cu protocoale mai înalte decât nivelul de transmisie a pachetelor care sunt tratate de către firewall;
  - firewall-urile pot afecta funcționarea anumitor aplicații Internet;
  - firewall-urile nu oferă nici un fel de protecție împotriva atacurilor din interiorul rețelei.

Trebuie avut în vedere faptul că firewall-ul nu reprezintă rezolvarea tuturor problemelor dintr-o rețea ci doar un prim pas în protecția acesteia. În acest sens, existența unui firewall nu exclude necesitatea implementării de măsuri de securitate pe calculatoarele din cadrul rețelei interne. De multe ori, se acordă prea multă importanță firewall-ului și se consideră în mod eronat că acesta protejează rețeaua împotriva cracker-ilor. Există situații în care din motive de organizare a securității, accesul la diverse servicii trebuie permis în afara rețelei, necesitând astfel compromisuri în ceea ce privește securitatea acesteia; spre exemplu dacă se dorește, accesarea sistemului prin intermediul SSH dintr-o rețea externă unde nu se cunoaște adresa sistemului client (o conexiune cu alocarea dinamică a adresei, unde numărul de adrese posibile este de ordinul zecilor de mii, cum este cazul AOL sau XNET). Configurarea firewall-ului constă în principal în definirea serviciilor care vor fi „vizibile” din afara serverului; spre exemplu, vom bloca accesul utilizatorilor în sistem (telnet sau SSH), accesul la sistemele de fișiere în rețea (NFS sau *Samba*<sup>1</sup>) și vom permite accesul la sistemul Web (Apache) și la poșta electronică (Send-mail).

Politica de securitate se referă în cazul firewall-urilor la nivel de pachet la definirea serviciilor care vor fi permise, respectiv interzise și la stabilirea calculatoarelor din afara rețelei care vor avea acces la respectivele servicii. Această politică se stabilește mai întâi prin determinarea serviciilor care sunt necesare utilizatorilor. De multe ori trebuie făcute compromisuri în ceea ce privește balanța dintre serviciile care sunt necesare și cele care trebuie protejate.

### Firewall-uri proxy



Un firewall intermediar nu permite trecerea directă a nici unei categorii de trafic, ci se comportă ca un interpus între Internet și calculatoarele din rețeaua internă. Sistemul firewall execută el însuși unele dintre serviciile de rețea, în loc de a transfera altor sisteme. În acest sens este un reprezentant „intermediar” pentru sistemele care execută cererea.

<sup>1</sup> SAMBA este un sistem care oferă servicii SMB/CIFS, asigurând compatibilitatea cu sistemele Microsoft Network

Un firewall intermediar „ascunde” existența calculatorului față de Internet. De asemenea, un firewall intermediar va îndeplini, în mod obișnuit, toate solicitările de conexiune sosite din Internet (trafic Web, descărcări FTP, livrări de mesaje e-mail). Acesta are ca scop reducerea la minimum a vizibilității rețelei interne în exterior.

Un astfel de program rulează pe o mașină - componentă a firewall-ului - numită în literatura de specialitate "bastion host". De obicei bastionul este o poartă (gateway) - o mașină conectată între cele două rețele (internă și externă). Din această cauză, un server proxy mai este întâlnit și sub denumirea de "application gateway" (gateway la nivel de aplicație). Gateway-urile nu sunt specifice firewall-urilor, ci sunt folosite în general pentru conectarea la nivel de servicii a două rețele (acolo unde nu se pot folosi ruterele, de ex. gateway de mail pt. SMTP->UUCP sau SMTP->FidoNet).

Pentru un gateway se mai folosește și termenul de "dual-homed host" (host conectat în două locuri).

În mod normal, o sesiune de comunicație în Internet se desfășoară după modelul Client-Server: clientul emite o cerere către server (de exemplu transferul unei pagini de web) iar acesta răspunde cererii. În cazul implementării serviciilor proxy, comunicația se desfășoară în următorii pași:

- clientul emite cererea nu către server-ul real, ci către server-ul proxy, comunicându-i acestuia destinația dorită (server-ul real care va răspunde cererii);
- server-ul proxy analizează cererea și, dacă aceasta respectă politica de securitate a organizației, este trimisă server-ului real (destinație) ca și cum ar proveni de la un program-client de pe acea mașină (dual-homed host);
- server-ul real răspunde cererii către server-ul proxy (care e client pentru server-ul real);
- server-ul proxy analizează răspunsul și, dacă acesta respectă politica de securitate a organizației, este trimis clientului din rețeaua internă.

Ca urmare, nu mai este creată o singura conexiune client - server, ci două: client - proxy și proxy - server real. Server-ul real nu este conștient de existența clientului; el comunică doar cu server-ul proxy. Clientul nici el nu comunică direct cu server-ul real, ci doar cu proxy-ul. Pentru ca această schemă să funcționeze, trebuie ca între client și server să nu existe conectivitate directă (la nivel IP) - în caz contrar, clientul poate trimite cererea direct către server-ul real, eludând astfel sistemul de protecție prin server proxy. Din acest motiv, pe gateway, opțiunea de rutare (transfer automat și îndrumarea pachetelor dintr-o rețea în cealaltă) va trebui să fie dezactivată.

Fiecare server proxy va avea un set de reguli (analoage celor de la routerele filtrante) care implementează politica de securitate a organizației relativ la protocolul respectiv.

Avantajul serverelor proxy este că ele înțeleg protocolul pentru care au fost proiectate, făcând astfel posibil controlul la nivel de aplicație, constând din:

- autentificare - aceasta permite selectarea utilizatorilor (interni sau externi) care au dreptul să acceseze un anumit serviciu;
- filtrarea individuală a operațiilor protocolului - de exemplu cu ajutorul unui server proxy pentru FTP poate fi implementată o politică de securitate care permite aducerea (*downloading*) dar interzice exportarea (*uploading*) de fișiere;
- monitorizare - jurnalizarea (în fișierele de *log*) a sesiunilor de rețea.

Principalul dezavantaj al serverelor proxy îl constituie faptul că, prin existența a două conexiuni logice în loc de una, se modifică procedura de utilizare a serviciilor Internet. Acest lucru impune modificarea fie a programelor client, fie a modalității de apel al acestora de către utilizatori. Rezultă astfel două abordări posibile:

- utilizarea de programe-client normale împreună cu modificarea comportamentului utilizatorilor: aceștia nu se mai pot conecta direct la server-ele dorite ci trebuie să se conecteze întâi la firewall (pe care rulează serviciul de proxy respectiv) și să-i "ceară" acestuia destinația dorită, într-un limbaj specific fiecărui server proxy. Această metodă impune un mod de lucru mai greoi utilizatorilor, diferit de cel cu care erau, probabil, obișnuiți. În particular, utilizatorii trebuie să folosească proceduri diferite pentru accesarea server-elor din rețeaua internă a organizației (pentru acestea nu trebuie să treacă prin firewall) față de cele externe (din Internet, via firewall);
- utilizarea de programe-client modificate sau configurate corespunzător pentru conlucrarea cu server-ul proxy. În acest caz, utilizatorul nu va sesiza prezența server-ului proxy (exceptând cazul când este necesară autentificarea la firewall): programul-client va efectua automat toate procedurile privind conectarea prin firewall. Astfel de programe-client există în prezent pentru o serie de protocoale printre care FTP, Gopher, HTTP. De exemplu programe ca Netscape Navigator / Communicator, lynx, mosaic,... pot fi configurate să se conecteze prin intermediul unui server proxy.

## Ruter filtrant

Sistemul de operare LINUX are, printre multele calități care îl fac preferat în mediul academic precum și, mai ales, în Internet, posibilitatea de a funcționa și ca ruter cu filtrare de pachete. Astfel se poate implementa foarte ușor un firewall bazat pe principiul cu ruterul filtrant.

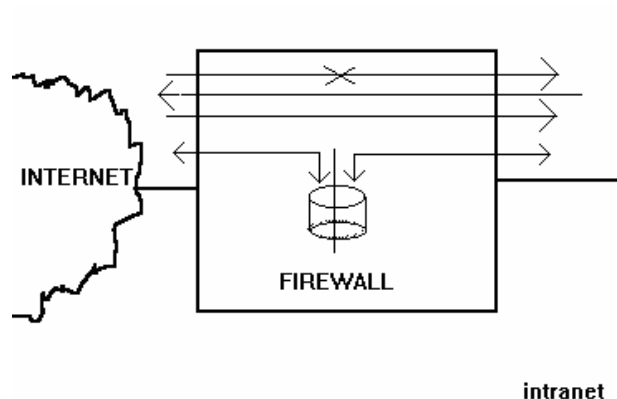
Dat fiind că sistemul LINUX permite (ca orice alt sistem de operare pentru servere de rețea) și rularea de servicii pe aceeași mașină cu ruter-ul, se pot implementa și combinații de server proxy și ruter filtrant (de ex. se poate face proxy cu

caching pentru www, ftp; gateway de e-mail respectiv filtrare de pachete pentru protocoalele ce nu pot folosi proxy - cum ar fi cele ce presupun sesiuni interactive de login sau conferință electronică).

Sistemul de filtrare poate fi folosit și pentru host-uri ce nu sunt rutere (adică au o singură interfață fizică de rețea) pentru protecția mai eficientă a diverselor servicii de pe mașina respectivă (acele servicii ce nu pot fi protejate prin alte metode, sau care pot fi protejate mult mai greu).

În plus, acest sistem de operare permite și folosirea metodelor numite NAT *network address translation* (cunoscută și sub numele de *IP masquerading*), respectiv PAT - *port address translation* folosite pentru accesul unui Intranet întreg la Internet având o singură adresă de Internet atribuită firewall-ului. (Protocoalele ce pot funcționa prin proxy se folosesc cu proxy, pentru celelalte se folosește translatarea de adrese și eventual de port).

Un ruter filtrant nu oferă prea multă informație asupra activității în rețea. În plus, există posibilitatea ca pe anumite porturi cunoscute, pe anumite mașini - fie ostile, fie compromise - să se afle cu totul alt serviciu decât cel a cărui utilizare se dorea permisă.



În sistemul de operare Linux, a fost implementat un firewall la nivel de nucleu, sistem numit – în versiunea 2.4.x a acestuia – *iptables*. Acest sistem oferă posibilitatea de a filtra sau redirectiona pachetele de date, precum și de a modifica informațiile despre sursa și informația pachetelor, procedură denumită NAT (Network Address Translation). Una dintre aplicațiile sistemului NAT este posibilitatea „deghezării” pachetelor (masquerading). Deghizarea înseamnă ca pachetele trimise de către sistemele aflate în rețea, care au stabilit ca gateway o anumită mașină, să pară transmise de mașina respectivă, și nu de cea originală. Cu alte cuvinte mașina configurată ca firewall retrimite pachetele venite dinspre rețea către exterior, făcând să pară că provin tot de la ea. Acest mecanism este foarte util atunci când există o mașină care realizează legătura la Internet, o singură adresă IP alocată și mai multe calculatoare în rețea care au definită mașina respectivă ca gateway. Situația este des întâlnită în cadrul companiilor mici și mijlocii dotate cu o legătură Internet permanentă, mai ales ca urmare a crizei de adrese IP manifestată în ultimii ani. Nucleul Linux definește două tabele de reguli, prima numită *filter*, utilizată pentru filtrul de pachete, și a doua numită *nat*, utilizată pentru sistemul NAT. Există 5 lanțuri (chains) predefinite, adică o succesiune de reguli utilizate pentru verificarea pachetelor de date care tranzitează sistemul. Lanțurile INPUT și FORWARD sunt disponibile doar pentru tabela filter, lanțurile PREROUTING și POSTROUTING sunt doar pentru tabela nat, iar lanțul OUTPUT, pentru ambele tabele. Atunci când un pachet intră în sistem printr-o interfață de rețea, nucleul decide dacă pachetul este destinat mașinii locale (lanțul INPUT) sau altui calculator (lanțul FORWARD). Într-un mod similar, pachetele care pleacă dinspre mașina locală trec prin lanțul OUTPUT. Fiecare lanț conține mai multe „reguli” ce vor fi aplicate pachetelor de date care le tranzitează. În general, regulile identifică adresele sursă și destinație a pachetelor, însoțite de porturile sursă și destinație, precum și protocolul (serviciul) asociat. Atunci când un pachet corespunde unei reguli, adică parametrii menționați mai sus coincid, asupra acestuia se va aplica o anumită acțiune, care înseamnă direcționarea către o așa zisă „țintă” (target). În acest sens, dacă o regulă specifică acțiunea ACCEPT, pachetul nu mai este verificat folosind celelalte reguli ci este direcționat către destinație. Dacă regula specifică acțiunea DROP, pachetul este „aruncat” – cu alte cuvinte, nu i se permite să ajungă la destinație –, netrimțând nimic calculatorului care l-a expediat. Dacă regula specifică acțiunea REJECT, pachetului nu i se permite să ajungă la destinație, însă este trimis un mesaj de eroare expeditorului. Este important ca fiecărui lanț să îi fie atribuită o acțiune implicită, care va reprezenta destinația pachetului dacă nici una dintre regulile stabilite nu corespunde. Astfel, lanțul INPUT trebuie să aibă drop sau reject ca acțiune implicită pentru orice pachet care se dorește a fi filtrat. Pentru a include sistemul iptables în nucleu, acesta trebuie compilat cel puțin cu următoarele opțiuni activate:

- Networking options
- Network packet filtering (replaces ipchains)
- IP: Netfilter Configuration
- Connection tracking (required for mask/NAT)
- IP tables support
- Packet filtering
- Full NAT
- Packet mangling
- LOG target support
- De asemenea, trebuie instalat pachetul iptables. Programul iptables servește la manipularea lanțurilor și regulilor.

## 2. PROGRAME ANTIVIRUS

Programele antivirus sunt programe create special pentru a efectua următoarele operațiuni:

- sa detecteze viruși prin verificarea conținutului fișierelor si semnalarea prezentei semnăturii unui virus cunoscut sau a unor secvențe suspecte in interiorul lor
- sa dezinfecteze sau sa stearga fișierele infestate de viruși cunoscuți
- sa prevină infectarea prin supravegherea acțiunilor din memorie si semnalarea întâlnirii unor anumite acțiuni ca ar putea fi generate de existenta in memorie a unui virus

Exista doua feluri de antivirusi după modul in care actioneaza:

1. Programe care după ce au fost lansate ce raman in memoria calculatorului si supraveghează fiecare aplicație lansata in execuție.
2. Programe care sunt lansate de către utilizator numai atunci când el dorește sa verifice calculatorul

In următoarele conditii are loc devirusarea:

- Scanarea = citirea fișierelor si a memoriei si identificarea virușilor cunoscuți de programul antivirus respective
- Devirusare = extragerea virusului sau ștergerea fișierului infectat
- Monitorizare = este operația prin care un antivirus existent in memorie verifica si semnalează sistematic eventuala apariție a unui virus

10 reguli de baza pentru a evita virusii:

1. Folositi un program antivirus.
2. Instalati un firewall.
3. Asigurati-va ca sistemul dumneavoastra este la zi continand toate update-urile existente.
4. Pastrati setarile referitoare la securitatea browserului la nivel mediu sau ridicat.
5. Niciodata nu dati 'Yes' cand browserul va intreaba daca vreti sa instalati/rulati continut provenit de la o organizatie pe care nu o cunoasteti sau in care nu aveti incredere.
6. Instalati un program anti-spyware pentru a spori protectia antivirus.
7. Nu instalati nici o bara de cautare ajutatoare pentru browser decat daca provine de la o sursa de incredere.
8. Verificati in care certificate ale companiilor software puteti avea incredere.
9. Folositi o carte de credit numai pentru cumparaturi on-line.
10. Nu executati attachment-urile de la email-uri chiar daca aparent au fost trimise de prieteni.

### Antivirusi, scurtă istorie

1993 - Microsoft lansează **MSAV** - Microsoft Antivirus

1994 - **Symantec** achiziționează mai multe companii profilate pe programe anti-virus: Central Point (care a stat la baza MSAV), Peter Norton Computing, Cetus International, Fifth Generation Systems

1995 - Două companii de renume, ESaSS (autoare a antivirusului **ThunderBYTE** - TBAV) și Norman Data Defense (Norman Virus Control), se aliază.

1997 - Apar compania **Kaspersky Labs** și produsul **F-Secure Anti-Virus** al companiei DataFellows (autoarea antivirusului **F-PROT**). Alte companii existente la acea vreme: McAfee și Dr. Solomon

1998 - Symantec și IBM își unesc forțele în Norton Anti-Virus

Top AntiVirus 2008, conform [toptenreviews.com](http://toptenreviews.com)

Rank	1	2	3	4	5	6	7	8	9	10
<div> <div>■ ■ ■ ■</div> Excellent         </div> <div> <div>■ ■ ■ □</div> Very Good         </div> <div> <div>■ ■ □ □</div> Good         </div> <div> <div>■ □ □ □</div> Fair         </div> <div> <div>□ □ □ □</div> Poor         </div>	BitDefender Antivirus	Kaspersky Anti-Virus	Webroot Antivirus	G DATA Antivirus	ESET Nod32	ParetoLogic Anti-Virus PLUS	AVG Anti- Virus	Vipre Antivirus + Antispyware	F- Secure Anti- Virus	Trend Micro
Overall Rating	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■
Ease of Use	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■
Effectiveness	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■
Updates	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■
Feature Set	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■
Ease of Installation	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■
Help/Support	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■	■ ■ ■ ■



### 3. PROGRAME ANTI-MALWARE

Există aplicații scrise individualizat, nerezidente, destinate eliminării unui singur program malware din sistemul infectat, sau aplicații complexe destinate recunoașterii și eliminării unui număr foarte mare de programe nedorite. Ca și antivirusii, aceste programe anti-malware pot funcționa rezident în memoria sistemului și monitorizează toate evenimentele nedorite ce au loc în timpul navigării pe Internet, citirii e-mailului sau în alte situații. Funcțiile avansate ale acestor programe permit scanarea regiștrilor, a librăriilor, plugin-urilor, cookies-urilor, imunizarea setărilor, backup-ul și restaurarea datelor, actualizarea online a bazei de date cu programele detectate și/sau eliminate.

Printre aplicațiile anti-malware gratuite sunt:

- [AdAware](#)
- [GIANT AntiSpyware](#)
- [SpywareBlaster](#) - ofera protectie pentru Internet Explorer/Mozilla/Firefox, dar opreste si controalele ActiveX si alte elemente daunatoare inainte de a fi instalate pe calculator.
- [Spybot - Search and Destroy](#) - poate detecta elemente pe care alte programe de eliminare adware nu le recunosc drept amenintari.
- [HouseCall](#) - on-line scan, poate inlatura cei mai multi troieni care vin impreuna cu produsele spyware/adware.
- [Zone Alarm Firewall](#) - limiteaza accesul la calculator si previne instalarea troienilor.
- [HijackThis](#)

Deși variantele comerciale pot dispune de unele avantaje în plus față de cele gratuite, acestea sunt suficiente pentru a vă proteja computerul cu condiția să nu uitați să le faceți update săptămânal pentru a fi mereu la curent cu noile apariții de potențiale pericole.

### 4. CREAREA COPIILOR DE SIGURANȚĂ

#### 4.1. BACKUP & RESTORE

**Informația este una din cele mai importante resurse**

Clienți, contracte, date contabile, planuri de afaceri, toate aceste informații sunt în general stocate în calculatoare care sunt expuse riscului de defectiune, furt sau calamitate naturală. Importanța pe care o au aceste informații stocate în format digital este din ce în ce mai mare pentru bunul mers al unei afaceri sau chiar pentru existența ei. Salvarile pe suport extern se fac în general săptămânal, în funcție de volumul de date și specificul activității firmei.

**Backup-ul de date** reprezintă procesul de copiere al datelor cu scopul de a putea fi restaurate în eventualitatea în care datele originale se pierd. Procesul de backup reprezintă o succesiune de operații complexe: **arhivare, compresie, criptare, salvare, verificare, restaurare.**

Copiile de siguranță ("*backup*") sunt necesare pentru a permite recuperarea datelor și aplicațiilor în cazul unor evenimente cum ar fi: dezastre naturale, defectiuni ale discurilor de sistem, spionaj, erori de introducere a datelor, erori de funcționare a sistemului, etc.

**Motive pentru backup:**

##### 1. Ștergerea din greșală a unor date

##### 2. Erori ale hard-disk-ului

Deși rata de erori a hard-disk-urilor a scăzut considerabil în ultimii ani, datorită capacităților din ce în ce mai mari ale acestor discuri, în cazul unor erori, cantitatea de date pierdute este mai mare decât în trecut.

##### 3. Virușii și programele de tip malware

##### 4. Mai mult spațiu pe hard disk

DVD-urile și alte medii de stocare de mari capacități permit salvarea informației multimedia (muzică, filme) care ar putea ocupa (inutil) hard-disk-ul.

##### 5. Cazuri de forță majoră

Dezastrele, fie ele naturale sau provocate de om, pot afecta orice program care se bazează pe cantități importante de date stocate. Recomandabil este ca, în plus față de backup-ul uzual, să se facă un backup care să fie stocat într-o altă locație.

##### 6. Transferul de fișiere

Transferul de fișiere, în special când este vorba de volume mari, poate să dureze foarte mult. Unitățile cu bandă magnetică sau hard-disk-rile portabile au o capacitate mare de stocare și o rată de transfer care le recomandă pentru acest tip de operațiune. Față de hard discuri, casetele sunt mai mici, mai ieftine și au o durată de viață mai mare. Hard discurile portabile sunt însă mai ușor de folosit. Și DVD-urile pot reprezenta o soluție, însă doar aici, în cazul backup-ului pentru transport, nu și a celui care presupune o stocare îndelungată (de exemplu, câțiva ani).

#### **7. Stocarea în siguranță a copiilor backup**

Pe lângă realizarea acestor copii de siguranță, un rol important îl are stocarea acestora, în condiții climatice adecvate (umiditate, temperatură), ferite de influențe ale undelor electromagnetice, bine împachetate, etichetate și securizate față de accesul neautorizat.

#### **4.2. DISK MIRRORING**

"*Disk mirroring*" (sau RAID 1) reprezintă o tehnică de replicare (multiplicare) a datelor, sistemul menținând una sau mai multe copii ale unui disc logic pe mai multe discuri fizice diferite, în timp real. În cazul defectării unuia dintre discuri, datele vor fi găsite pe celelalte copii (versiuni identice). Se asigură astfel disponibilitatea permanentă a datelor.

Replicarea se poate realiza local (prin matrici de discuri - "disk arrays") sau la distanță (asigurându-se siguranța datelor în caz de calamități naturale).

RAID - acronimul de la *Redundant Array of Inexpensive Disks*