Vitalie SEMENCIUC, ASEM

ASPECTE DE SECURITATE ÎN REȚELE DE CALCULATOARE

Abstract: *This text point out the problem of computers network's security and give some mens of solving this problem.*

Importanța aspectelor de securitate în rețelele de calculatoare a crescut odată cu extinderea prelucrărilor electronice de date şi a transmiterii acestora prin intermediul rețelelor. În cazul operării asupra unor informații confidențiale, este important ca avantajele de partajare şi comunicare aduse de rețelele de calculatoare să fie susținute de facilități de securitate substanțiale. Acest aspect este esențial în condițiile în care rețelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea de operațiuni bancare, cumpărături sau plata unor taxe.

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) şi se va împiedica falsificarea informațiilor transmise sau utilizarea clandestină a anumitor servicii destinate unor categorii specifice de utilizatori ai rețelelor.

Persoanele care atentează la securitatea rețelelor pot aparține unor categorii diverse, comițând delicte mai mult sau mai puțin grave: studenți care se amuză încercând să fure poşta electronică a celorlalți, hackeri care testează securitatea sistemelor sau urmăresc să obțină în mod clandestin anumite informații, angajați care pretind că au atribuții mai largi decât în realitate, accesând servicii care în mod normal le-ar fi interzise, sau foşti angajați care urmăresc să distrugă informații ca o formă de răzbunare, 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 terorişti care fură secrete strategice.

În condițiile în care pot exista interese atât de numeroase de spargere a unei rețele, este evident că proiectanții resurselor hard şi soft ale acesteia trebuie să ia măsuri de protecție serioase împotriva unor tentative rău intenționate. Metodele de protecție care pot stopa „inamicii" accidentali se pot dovedi inutile sau cu un impact foarte redus asupra unor adversari redutabili cu posibilități materiale considerabile.

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

- *confidențialiatea* se referă la asigurarea accesului la informație doar pentru utilizatorii autorizați şi 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 transmițătorului este esențială);
- *nerepudierea* 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).

Aspectele de securitate enumerate anterior se regăsesc, într-o oarecare măsură, şi în sistemele tradiționale de comunicații: de exemplu, poşta trebuie să asigure integritatea şi confidențialitatea scrisorilor pe care le transportă. În cele mai multe situații, se cere un document original şi nu o fotocopie. Acest lucru este evident în serviciile bancare. În mesajele electronice, însă, distincția dintre un original şi o copie nu este deloc evidentă.

Procedeele de autentificare sunt foarte răspândite şi ele: recunoaşterea fețelor, vocilor sau a scrisului sau semnăturilor unor persoane pot fi încadrate în această categorie. Semnăturile şi sigiliile sunt metode de autentificare folosite extrem de frecvent. Falsurile pot fi detectate de către experți în grafologie prin analiza scrisului şi chiar a hârtiei folosite. Evident, aceste metode nu sunt disponibile electronic şi trebuie găsite alte soluții valabile.

Dintr-un punct de vedere mai pragmatic, implementarea unor mecanisme de securitate în rețelele de calculatoare de arie largă, în particular – *Internetul, priveşte rezolvarea următoarele aspecte:*

- bombardarea cu mesaje – aşa-numitul spam – trimiterea de mesaje nedorite, de obicei cu un conținut comercial;
- rularea unui cod (program) dăunător, adesea de tip virus – acesta poate fi un program Java sau ActiveX, respectiv un script JavaScript, VBScript etc.;
- infectarea cu viruşi specifici anumitor aplicatii – se previne prin instalarea unor programe antivirus care detectează viruşii, devirusează fişierele infectate şi pot bloca accesul la fişierele care nu pot fi „dezinfectate”. În acest sens, este importantă devirusarea fişierelor transferate de pe rețea sau ataşate mesajelor de mail, mai ales dacă conțin cod-sursă sau executabil, înainte de a le deschide / executa;

- accesarea prin rețea a calculatorului unui anumit utilizator şi „atacul” asupra acestuia. La nivelul protocoalelor de rețea, protejarea accesului la un calculator sau la o rețea de calculatoare se realizează prin mecanisme de tip fire-wall, prin comenzi specifice; acestea pot fi utilizate şi în sens invers, pentru a bloca accesul unui calculator sau a unei rețele de calculatoare la anumite facilități din Internet;
- interceptarea datelor în tranzit şi eventual modificarea acestora – snooping. Datele se consideră interceptate atunci când altcineva decât destinatarul lor le primeşte;
- expedierea de mesaje cu o identitate falsă, expeditorul impersonând pe altcineva (pretinde că mesajul a fost trimis de la o altă adresă de poştă electronică) – spoofing.

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 (fire-wall) 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.

Împiedicarea interceptării fizice este în general costisitoare şi 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.

Bibliografie:

1. Lars Klander, Anti-hacker. Ghidul securității rețelelor de calculatoare, 679 p., ALL Educațional, Bucureşti 1998.
2. Andrew S. Tanenbaum, Rețele de calculatoare, Ed. Computer Press Agora, 1997.