Security in Internet

Asist. Felician ALECU
Catedra de Informatică Economică, A.S.E. Bucureşti

A very good method that can be used to protect a private network is the implementation of a firewall between Internet and Intranet. This firewall will filter the packets that transit the network according with the security policy defined at the system level. The SSL protocol allows verifying the identity of a WEB server based on a digital certificate issued by a certification authority. Secure data transport over the Internet is done by using encryption methods.
Keywords: *Internet, Intranet, security, digital certificate, authentication, confidentiality, non-repudiation, integrity control, firewall, router.*

Securitatea rețelei

În ziua de astăzi, în condițiile în care milioane de oameni folosesc Internetul pentru plata taxelor, cumpărături sau operațiuni bancare, securitatea rețelei apare ca o mare problemă potențială.

Statisticile arată că majoritatea problemelor legate de securitate sunt cauzate deliberat de către persoane rău intenționate care încearcă să provoace neplăceri sau să obțină anumite avantaje şi beneficii.

Intruşii sunt de două categorii, după cum urmează:

- *intruşi pasivi* – sunt cei care se limitează la a asculta mesajele schimbate în cadrul rețelei;
- *intruşi activi* – aceştia nu numai că ascultă mesajele, dar şi intervin asupra acestora, modificându-le.

Problemele de securitate pot fi împărțite în patru mari domenii care sunt interconectate:

- *confidențialitatea* – presupune păstrarea informației departe de utilizatorii neautorizați. Este primul aspect care este luat în discuție atunci când se discută despre securitatea unei rețele.
- *autentificarea* – stabilirea identității interlocutorului înainte de a dezvălui informații importante;
- *nerepudierea* – se referă la semnături şi la modul în care se poate proba că o anumită comandă a fost făcută în condițiile înregistrate în sistem, indiferent de faptul că respectivul client susține altceva;
- *controlul integrității* – se referă la posibilitatea de a verifica dacă un mesaj a fost primit exact în forma în care a fost transmis fără să fi fost modificat pe parcursul traseului de către persoane rău intenționate.

Mecanismele de securitate pot fi implementate la mai multe niveluri, fiecare nivel având o anumită contribuție la securitatea rețelei:

- *nivelul fizic* – în cadrul sistemelor militare, ascultarea firelor este împiedicată prin includerea acestora în tuburi sigilate conținând gaz de argon la presiuni înalte. Penetrarea tubului va conduce la pierderi de gaz urmate de scăderea presiunii ceea ce va declanşa alarma;
- *nivelul legătură de date* – pachetele trimise de la o maşină la alta prin intermediul unei linii punct-la-punct pot fi codificate/decodificate de către fiecare computer în parte. Acest mecanism poartă numele de *criptarea legăturii*;
- *nivelul rețea* – se pot instala ziduri de protecție (*firewall-uri*) pentru respinge atacurile asupra rețelei şi pentru a filtra mesajele care intră sau ies din rețeaua privată;
- *nivelul transport* – se poate opta pentru criptarea unor conexiuni în întregime;
- *nivelul aplicație* – implementează de regulă soluții la problema autentificării şi la cea a nerepudierii.

Certificate digitale

Codificarea şi decodificarea informațiilor se realizează pe baza unor chei. Pentru a decodifica un mesaj este nevoie să se cunoască cheia cu care acesta a fost codificat.

Cel mai adesea sunt folosite două chei atunci când se codifică un mesaj: *cheia publică* –

este cea cunoscută în mod public; *cheia privată* – cunoscută doar de cel care codifică sau decodifică mesajul.
Arta de a sparge coduri se numeşte *criptanaliză*, crearea cifrurilor este cunoscută ca *criptografie* iar ambele operaţii sunt cunoscute sub numele generic de *criptologie*.
Revenind la Internet, cheile de criptare şi de decriptare pot fi falsificate şi din acest motiv sunt folosite metode de certificare a acestora. Una dintre aceste metode de certificare presupune folosirea unui certificate digital prin care se poate verifica că o anumită cheie publică aparţine într-adevăr unei anumite persoane sau companii. Certificatele digitale sunt eliberate de instituţii specializate denumite autorităţi de certificare.
Un certificate digital este compus din următoarele elemente:

- numărul serial al certificatului;
- detalii despre algoritmul de criptare folosit;
- informaţii legate de identitate;
- cheia publică a expeditorului;
- semnătura digitală a autorităţii de certificare emitente.

Certificatul digital confirmă identitatea utilizatorului şi semnătura acestuia (Fig. 1). Pentru certificare, cheia publică a unui utilizator este înregistrată de către autoritatea de certificare într-o bază de date foarte bine protejată.

Fig. 1. Eliberarea unui certificat de către autoritatea de certificare

După înregistrare, autoritatea de certificare va transmite un certificat digital oricui doreşte să verifice autenticitatea cheii publice a utilizatorului.

Protocolul SSL

De multe ori schimbul securizat de documente pe WEB se face prin stabilirea unei conexiuni de tip *SSL*. Protocolul *SSL* (*Secure Socket Layer*) foloseşte certificate digitale pentru a verifica identitatea serverului WEB al companiei. Transmiterea securizată a datelor pe Internet este realizată cu ajutorul metodelor de criptare.
Protocolul *SSL* a fost dezvoltat de către compania *Netscape* iar în momentul de faţă aceasta este o componentă standard pentru majoritatea browser-elor şi a serverelor WEB.
Utilizatorul se identifică prin furnizarea pe WEB server a unui nume de utilizator însoţit de o parolă. Conexiunea *SSL* realizează şi criptarea parolei pentru asigurarea confidenţialităţii.

Printre caracteristicile protocolului *SSL* putem enumera:

- *SSL* permite autentificarea serverului (oferă clientului certitudinea identităţii serverului) şi a clientului. În plus, datorită codificării acestora, *SSL* asigură confidenţialitatea datelor. Autentificarea se realizează prin utilizarea certificatelor şi semnăturilor digitale;
- *SSL* foloseşte algoritmi diferiţi pentru criptare, autentificare şi pentru asigurarea integrităţii datelor;
- Stratul *SSL* se află între protocolul *TCP/IP* şi cele ale nivelului aplicaţie (Fig. 2).

Stabilirea unei conexiuni sigure între navigatorul WEB şi server se realizează într-un număr de patru paşi:
1. *Iniţierea protocolului SSL* – clientul trimite un mesaj serverului iar acesta răspunde prin furnizarea certificatului digital pe care clientul îl poate folosi pentru a stabili identitatea serverului;
2. *Acceptarea clientului* – navigatorul (browser-ul), după ce a identificat serverul cu care comunică, va genera două chei private

care vor fi folosite pentru tranzacţia ce urmează. Aceste chei private vor fi criptate folosind cheia publică primită de la server. Acesta din urmă va decripta cele două chei, fiecare parte având în acest moment respectivele chei. Valabilitatea acestora este la nivel de sesiune, din acest motiv ele se mai numesc şi *chei de sesiune*. Când sesiunea se încheie, cheile respective sunt şterse;

3.

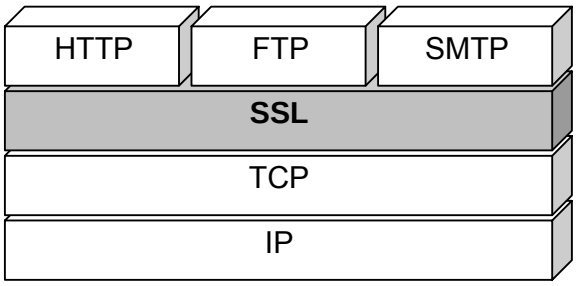

Fig. 2. Poziţionarea *SSL* între *TCP/IP* şi protocoalele nivelului aplicaţie

4. *Verificarea* – presupune trimiterea unui mesaj securizat către server. Criptarea mesajului este realizată folosind una din cheile de sesiune. Serverul răspunde tot printr-un mesaj criptat, folosind cea de-a doua cheie de sesiune. Dacă tot acest mecanism se derulează corect, atunci putem afirma că legătura sigură este stabilită şi tranzacţia poate să înceapă;

5. *Schimbul de date* – protocolul *SSL* este optimizat astfel încât criptarea şi decriptarea cheii publice este necesară o singură dată pe sesiune.

Internet şi Intranet

Pentru reducerea riscurilor privind securitatea informaţiilor (menţinerea confidenţialităţii) şi prevenirea accesului neautorizat, conectarea diverselor sedii şi birouri ale unei companii prin intermediul Internetului se realizează prin folosirea unei reţele virtuale private (*VPN – Virtual Private Network*). Construcţia unei astfel de reţele virtuale private înseamnă folosirea Internet-ului ca pe o reţea *WAN* (*Wide Area Network – reţea de arie largă*) care atrage după sine reducerea semnificativă a costurilor.

Cea mai utilizată modalitate de protejare a reţelei interne o constituie folosirea unui *zid de protecţie* (*firewall*) între Intranet şi Internet. Un zid de protecţie trebuie să analizeze tot traficul ce se desfăşoară între reţeaua externă şi utilizatorii interni, în ambele direcţii. În felul acesta se realizează filtrarea pachetelor pe baza politicii de securitate care este definită la nivelul sistemului.

Firewall-ul trebuie să reziste atacurilor malitioase din exterior şi interior deoarece întreaga reţea poate fi compromisă dacă o persoana rău intenţionată preia controlul zidului de protecţie.

Mai mult decât atât, *firewall*-ul trebuie să fie în măsură să ascundă de reţeaua externă adresele reale ale staţiilor din Intranet. Toate aceste servicii trebuie să fie puse la dispoziţia utilizatorilor reţelei fără ca traficul să fie perturbat sau strangulat din cauza existenţei zidului de securitate.

Pentru a conecta două sedii ale undei companii se poate utiliza un tunel de siguranţă la nivelul reţelei virtuale private (

Fig. 3).

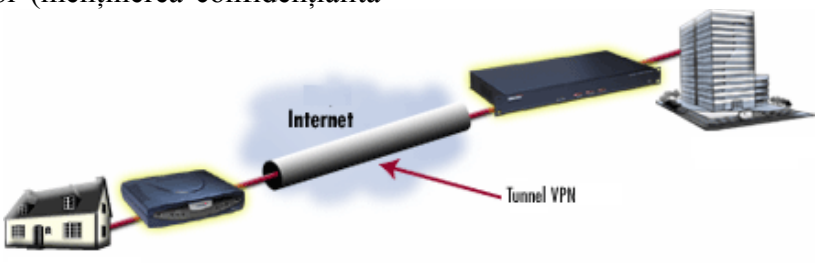

Fig. 3. Tunel de siguranţă în cadrul unei reţele virtuale private

O politică de securitate la nivelul unei companii include următoarele niveluri:

- existenţa unui zid de securitate (*firewall*) pentru asigurarea unei conexiuni sigure la Internet;
- criptarea datelor si transmiterea acestora printr-un tunel de securitate pe Internet prin crearea unei reţele virtuale private;
- implementarea unor mecanisme de securitate al nivelul aplicaţiilor.

În funcție de specificul datelor vehiculate şi de importanța acestora, o companie poate decide să implementeze numai anumite niveluri de securitate sau chiar pe toate.

Bibliografie

[1] Tanenbaum A. S. *Rețele de Calculatoare*, Computer Press Agora, 1998
[2] Tanenbaum A. S. *Computer Networks*, Prentice Hall, 1996
[3] Surcel T., Mârşanu R., Pocatilu P., Reveiu A., Bologa R., Alecu F. *Tehnologii WEB şi baze de date*, Editura Tribuna Economică, 2005
[4] Surcel T., Mârşanu R., Pocatilu P., Reveiu A., Bologa R., Alecu F. *Informatică Economică*, Editura Tribuna Economică, 2005
[5] Cheswick R., Bellovin S. *Firewalls and Internet Security,* Addison-Wesley Professional, 2004
[6] Noonan W., Dubrawsky I. *Firewall Fundamentals,* Cisco Press, 2006