

## Security in Internet

Asist. Felician ALECU

Catedra de Informatică Economică, A.S.E. București

*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 și beneficii.

Intrușii sunt de două categorii, după cum urmează:

- *intruși pasivi* – sunt cei care se limitează la a asculta mesajele schimbate în cadrul rețelei;
- *intruși activi* – aceștia nu numai că ascultă mesajele, dar și 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 și 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 pri-

mit 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 declanșa alarma;
- *nivelul legătură de date* – pachetele trimise de la o mașină 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 și 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 și la cea a nerepudiării.

### Certificate digitale

Codificarea și 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 numește *criptanaliză*, crearea cifrurilor este cunoscută ca *criptografie* iar ambele operații sunt cunoscute sub numele generic de *criptologie*.

Revenind la Internet, cheile de criptare și de decriptare pot fi falsificate și 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 aparține într-adevăr unei anumite persoane sau companii. Certificatele digitale

sunt eliberate de instituții specializate denumite autorități de certificare.

Un certificate digital este compus din următoarele elemente:

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

Certificatul digital confirmă identitatea utilizatorului și 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 dorește 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*) folosește 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 față acesta este o componentă standard pentru majoritatea browser-elor și a serverelor WEB.

Utilizatorul se identifică prin furnizarea pe WEB server a unui nume de utilizator însoțit de o parolă. Conexiunea *SSL* realizează și criptarea parolei pentru asigurarea confidențialității.

Printre caracteristicile protocolului *SSL* putem enumera:

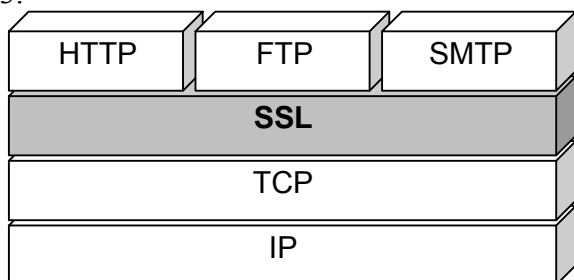
- *SSL* permite autentificarea serverului (oferă clientului certitudinea identității serverului) și a clientului. În plus, datorită codificării acestora, *SSL* asigură confidențialitatea datelor. Autentificarea se realizează prin utilizarea certificatelor și semnăturilor digitale;
- *SSL* folosește algoritmi diferiți pentru criptare, autentificare și pentru asigurarea integrității datelor;
- Stratul *SSL* se află între protocolul *TCP/IP* și cele ale nivelului aplicație (Fig. 2).

Stabilirea unei conexiuni sigure între navigatorul WEB și server se realizează într-un număr de patru pași:

1. *Inițierea 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 tranzacția 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 și *chei de sesiune*. Când sesiunea se încheie, cheile respective sunt șterse;

3.



**Fig. 2.** Poziționarea SSL între TCP/IP și protocoalele nivelului aplicație

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 și tranzacția poate să înceapă;

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

### Internet și Intranet

Pentru reducerea riscurilor privind securitatea informațiilor (menținerea confidențialității)

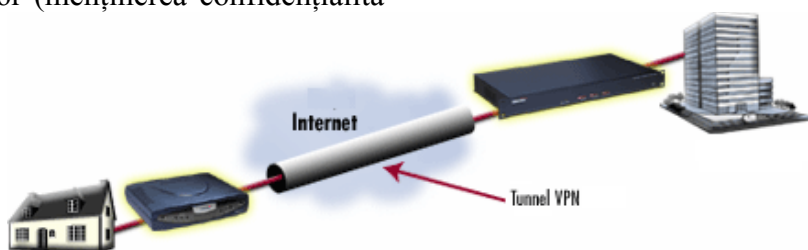
și prevenirea accesului neautorizat, conectarea diverselor sedii și birouri ale unei companii prin intermediul Internetului se realizează prin folosirea unei rețele virtuale private (*VPN – Virtual Private Network*). Construcția unei astfel de rețele virtuale private înseamnă folosirea Internet-ului ca pe o rețea *WAN (Wide Area Network – rețea de arie largă)* care atrage după sine reducerea semnificativă a costurilor.

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

*Firewall*-ul trebuie să reziste atacurilor malițioase din exterior și interior deoarece întreaga rețea poate fi compromisă dacă o persoană rău intenționată preia controlul zidului de protecție.

Mai mult decât atât, *firewall*-ul trebuie să fie în măsură să ascundă de rețeaua externă adresele reale ale stațiilor din Intranet. Toate aceste servicii trebuie să fie puse la dispoziția utilizatorilor rețelei fără ca traficul să fie perturbat sau ștrangulat din cauza existenței zidului de securitate.

Pentru a conecta două sedii ale unei companii se poate utiliza un tunel de siguranță la nivelul rețelei virtuale private (Fig. 3).



**Fig. 3.** Tunel de siguranță în cadrul unei rețele virtuale private

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

- existența unui zid de securitate (*firewall*) pentru asigurarea unei conexiuni sigure la Internet;

- criptarea datelor și transmiterea acestora printr-un tunel de securitate pe Internet prin crearea unei rețele virtuale private;
- implementarea unor mecanisme de securitate al nivelului aplicațiilor.

În funcție de specificul datelor vehiculate și 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., Mârșanu R., Pocatilu P., Reveiu A., Bologa R., Alecu F. *Tehnologii WEB și baze de date*, Editura Tribuna Economică, 2005
- [4] Surcel T., Mârșanu 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