Protocoale pentru comerț electronic și securitate pe Internet

Prep. Carmen STANCIU,
Catedra de Informatică Economică, A.S.E. București

Extinderea utilizării comerțului electronic pe scară largă a dus la necesitatea conceperii unor protocoale speciale pentru asigurarea securității transferului datelor financiare pe Internet. Acest articol își propune să facă o trecere în revistă a principalelor protocoale de securitate existente pe Internet, precum și cele pentru comerț electronic și poștă electronică securizată.
Cuvinte cheie: *Internet, protocoale de securitate, comerț electronic, SET, SSL, S-HTTP.*

1. Clase de protocoale de securitate

Înainte de abordarea protocoalelor specifice comerțului electronic și a celor ce asigură securitatea pe Internet, vom face o scurtă trecere în revistă a claselor de protocoale de securitate ce se regăsesc în literatura de specialitate. Principalele clase de protocoale de securitate, ce asigură implemetarea securității pe niveluri în rețelele de calculatoare, sunt:

a) protocoale de identificare și autentificare, care asigură autentificarea prin semnătură digitală a entităților.

Modalitățile de autentificare utilizate de această clasă, sunt: informații prearanjate (alcătuite din parole, PIN-uri, fraze cod), cartele magentice, procesoare de identificare, chei aflate în posesia utilizatorilor, caracteristici personale ale utilizatorului (amprente, date antropometrice, voce, proprietăți biochimice etc), proceduri în timp real de identificare a îndemânării, a capacităților și obiceiurilor utilizatorului (semnături, stil de tastare, viteză de citire etc).

b) protocoale pentru protecția transferului de date, care se ocupă cu: *confidențialitatea și integritatea mesajelor, securitatea protocoalelor de comunicație.*

c) protocoale pentru gestiunea cheilor de cifrare, care asigură:

- **generarea cheilor criptografice** - care trebuie să fie un proces aleator (de exemplu, algortimul DES);
- **memorarea cheilor** -dacă cheile sunt secrete, trebuie cifrate cu alte chei de cifrare; ultima cheie din ierarhie se ține necifrată, dar protejată printr-un dispozitiv hardware separat, și se numește cheie master (principală); instalarea, verificarea și protejarea acestei chei trebuie făcute cu foarte mare grijă.
- **distribuția cheilor** - se realizează prin *centre de distribuție a cheilor* (are ca principal dezavantaj faptul că se știe ce chei au fost distribuite și cui anume) și *prin schimb direct între partenerii de comunicație.*

Una dintre problemele care se pun este verificarea faptului că mesajele pe care le schimbă protocolul nu sunt vechi. Pentru acesta există două soluții: *mecanism de tipul întrebare-răspuns* (prin care se introduce în mesaj un element impredictibil) și *mecanism bazat pe înregistrarea orei în fiecare mesaj.*

Un astfel de protocol trebuie să îndeplinească următoarele condiții:

- să nu ceară un server central unic;
- să asigure o autentificare mutuală a partenerilor;
- să poată identifica, prin mecanisme de tipul întrebare-răspuns, dacă conversația este în direct ("life");
- să schimbe un număr minim de mesaje.

2. Protocoale generale de securitate pentru Internet

Din categoria protocoalelor care asigură securitatea pe Internet, vom prezenta pe scurt cele mai importante dintre ele: S-HTTP, SSL, PCT, S/WAN.

2.1. S-HTTP

Protocolul S-HTTP (Secure Hypertext Transfer Protocol) este o extensie a protocolului HTPP, care furnizează servicii de secu-

ritate. A fost dezvoltat de **Enterprise Integration Technologies**, iar apoi proiectul a fost continuat de **Terisa System**.
HTTP este protocolul care formează baza pentru World Wide Web, permiţând schimbul de documente multimedia pe Web. S-HTTP este proiectat pentru a furniza *confidenţialitate, autenticitate, integritate şi nerespingere*, prin suportarea mai multor *mecanisme de management al cheilor* şi de *algoritmi criptografici*, cu posibilitatea de negociere între părţile implicate în fiecare tranzacţie.
Protocolul S-HTTP poate utiliza *patru metode* pentru schimbul cheilor de criptare a datelor, şi anume:
• *metoda RSA* - când cheile de criptare a datelor sunt criptate utilizând criptosistemul cu cheie publică RSA;
• *metoda out-band* - se referă la un acord extern legat de cheia de criptare;
• *metoda in-band* - se referă la transportul cheii de criptare, în mesajul protejat S-HTTP, dar într-o altă sesiune.
• *metoda Kerberos* - în care cheia de criptare este obţinută dintr-un server Kerberos.
Algoritmii criptografici suportaţi de S-HTTP includ *DES*, DES-triplu, cu două şi trei chei, *DESX, IDEA, RC2, CDMF*.

2.2. SSL

Protocolul SSL (Secure Socket Layer) a fost elaborat de **Netscape Communications Corporation** pentru a furniza securitatea pe Internet, suportând autentificare atât la nivelul serverul, cât şi al clientului.
Este un protocol independent de aplicaţie, permiţând protocoalelor de pe nivelul superior, ca HTTP, FTP, Telnet, transparenţă totală. SSL este capabil de a negocia cheile de criptare, la fel de bine ca şi autentificarea serverului, înainte ca datele să fie trimise către aplicaţia de nivel înalt.
Protocolul menţine securitatea şi integritatea canalului de comunicaţie prin utilizarea de coduri de criptare, autentificare şi mesaje de autentificare.
Protocolul SSL, în procesul de "cunoaştere" (Handshake), are două faze, *autentificarea serverului şi a clientului*, a doua fiind opţională :
• serverul răspunde clientului trimiţând certificatul şi cifrul său preferat;
• clientul generează o cheie primară, pe care o criptează cu cheia publică primită de la server, şi astfel criptată o trimite serverului;
• serverul recuperează cheia primară şi autentifică clientul, trimitând un mesaj criptat cu cheia primară; datele următoare sunt criptate cu chei derivate din cheia primară;
• în faza a doua, serverul trimite o interogare clientului;
• clientul autentifică serverul, returnând interogarea, întrebarea, ce va conţine semnătura digitală şi certificatul public al cheii clientului.
Algoritmii criptografici suportaţi de SSL sunt numeroşi: în faza procesului de "cunoaştere", se utilizează *criptosistemul cu chei publice RSA*; după schimbul cheilor se utilizează o serie de cifruri, cum ar fi: *RC2, RC4, IDEA, DES, DES triplu, MD5* (algoritm de rezumat al mesajului). Sintaxa utilizată de certificatele pentru chei publice este *X.509*.
Diferenţele între SSL şi S-HTTP.O primă diferenţă vizează nivelul la care acţionează: SSL operează la nivel transport şi mimează o "bibliotecă de socket", iar S-HTTP este la nivel aplicaţie. Criptarea la nivel transport, permite protocolului SSL să fie independent de aplicaţie, în timp ce S-HTTP este limitat de implementarea unui software specific.
O altă diferenţă constă în filozofiile diferite de criptate pe care le aplică protocoalele: astfel, SSL criptează întregul canal de comunicaţie, iar S-HTTP criptează separat fiecare mesaj. S-HTTP permite utlizatorului folosirea de semnatură digitală pentru fiecare mesaj, şi nu doar pentru anumite mesaje din cadrul procesului de autentificare, ceea ce lipseşte la SSL. În prezent, cercetătorii de la **Terisa System** dezvoltă intrumente care suportă ambele protocoale.

2.3. PCT

Protocolul PCT (Private Communication Technology) este elaborat de **Microsoft** în cooperare cu **Visa International**, şi este

creat pentru asigurarea securității comunicației pe Internet. Este considerat ca o parte componentă a protocolului SSL, a lui Netscape şi intenționează să devină standard pentru Internet, la fel ca şi SSL.
Protocolul este asemănător cu SSL sub multe aspecte, iar formatul mesajului este destul de apropiat de cel al SSL-ului, încât serverul poate interacționa cu clienți care suportă SSL, la fel ca şi cu clienți care suportă PCT.
Totuşi, există deosebiri între cele două protocoale, PCT-ul venind să corecteze sau să îmbunătățească câteva lipsuri ale SSL-ului.
Principalele ***diferențe între PCT şi SSL***.
• PCT utilizează mesaje mai puține şi mai scurte între server şi client, , decât SSL;
• PCT are mai multe variante de ales în ceea ce priveşte negocierea algorimului şi formatului datelor folosit, decât SSL. Negocierea are o protecție criptografică adițională, astfel clientul şi serverul putând verifica dacă alegerile lor nu au fost modificate;
• autentificarea mesajului şi criptarea utilizează chei diferite în PCT (în SSL, ambele utilizând aceeaşi cheie), ducând la o securitate sporită; în particular, la PCT, autentificarea poate suporta chei mai lungi decât la criptare, lungimea cheii de criptare fiind dependentă doar de restricțiile de export.
• în cadrul protocolului de autentificare PCT, răspunsul clientului depinde de algoritmul de criptare negociat, pe când în SSL este dependent de algoritm. Acesta furnizează un "zid de protecție" (*firewall*), astfel că cineva care a recuperat cheia de criptare într-o sesiune în care s-a utilizat un algoritm slab, nu poate compromite o altă sesiune care a ales un alt algorim. SSL-ul nu are un astfel de *firewall*.
Pentru stabilirea cheilor, PCT utilizează: RSA, Diffie-Helmann, Fortezza.
Algortimii de criptare folosiți includ DES, DES triplu, RC2, RC4, iar semnăturile digitale suportate sunt DSA şi RSA.

2.4. S/WAN

Protocolul S/WAN (Secure Wide Area Network) se ocupă cu proiectarea specificațiilor pentru implementarea protocolului IPSec, arhitectura de securitate pentru Internet Protocol. Aceasta îşi propune să asigure interoperabilitatea printre produsele TCP/IP şi firewall-uri.
Scopul S/WAN este de a utiliza IPSec pentru a permite companiilor de a mixa şi comuta între cele mai bune firewall-uri şi aplicații pentru TCP/IP, în vederea construirii **VPN**-urilor (Virtual Private Networks), rețelelor private virtuale bazate pe Internet.
În prezent, utilizatorii şi administratorii sunt deseori blocați într-o singură soluție de platformă pentru rețea larg răspândită geografic, deoarece producătorii nu sunt capabili să cadă de acord în legătură cu detaliile implementării lui IPSec. Astfel cu S/WAN se reduce cel mai mare obstacol în implementarea pe scară largă a securității VPN-urilor. S/WAN suportă criptare la nivel IP, care furnizează o securitate la nivele joase mai puternică decât protocoalele de nivele superioare, cum ar fi SSL şi HTTP. Se aşteaptă ca specificațiile de securitate de la nivelele înalte, SSL şi S-HTTP, să fie suportate de către implementarea S/WAN, şi să lucreze împreună sinergetic.
Pentru a asigura interoperabilitatea lui IPSec, S/WAN defineşte un set comun de algoritmi, moduri şi opțiuni. S/WAN utilizează *RC5* cu chei între 40 şi 128 biți, precum şi **DES**.

3. Protocoale pentru comerț electronic

Comerțul electronic pe Internet este asigurat prin intermediul unor protocoale specifice, dintre care amintim iKP, SET şi Secure Courier.

3.1. iKP

iKP - Internet Keyed Payments Protocol - este un protocol bazat pe cheie publică pentru efectuarea plăților pe Internet, în care sunt implicate cel puțin trei parteneri.
Elaborat de IBM, şi anume de Centrul de Cercetare T.J.Watson în colaborare cu Laboratorul de Cercetare Zurich, protocolul defineşte tranzacțiile de tipul "cărților de credit", în care cumpărătorul şi vânzătorul

interacţionează cu o a treia parte, cum ar fi banca sau sistemul de cărţi de credit, pentru autentificarea tranzacţiilor.
Tranzacţia tipică iKP implică şase fluxuri, cu următoarele descrieri simplificate:
• INITIATE - iniţierea, în care cumpărătorul trimite vânzătorului începerea tranzacţiei;
• INVOICE - factura, în care vânzătorul răspunde, iar opţional poate conţine semnătura sa în cadrul tranzactiei;
• PAYMENT - plata, conţine răspunsul cumpărătorului, şi include fişa de plată, cu numărul de cont al cumpărătorului, eventual PIN-ul (Personal Identification Number), ambele criptate cu cheia publică a băncii sau sistemului de cărţi de credit; opţional se poate adăuga şi semnatura sa;
• AUTH-REQUEST- cerere de autentificare, în care vânzătorul trimite băncii, părţii a treia, fişa de plată criptată;
• AUTH-RESPONSE - răspunsul de autentificare, adică răspunsul băncii către vânzător, ce conţine şi semnătura băncii pentru tranzacţia de date;
• CONFIRM - confirmarea vânzătorului către cumpărător asupra autorizării tranzacţiei.
Mesajele dintre cumpărător şi vânzător sunt transmise prin Internet, iar cele dintre vânzător şi bancă sunt trimise fie prin Internet, fie printr-o reţea financiară privată.
Principala protecţie criptografică se referă la criptarea fişei de plată cu cheia publică a băncii şi cu semnătura sa pe autorizaţie. Contul cumpărătorului este ţinut secret, nici vânzătorul şi nici altcineva neputând obţine fişa de plată; aceasta reprezintă o îmbunătăţire semnificativă adusă faţă de sistemele de cărţi de credit convenţionale.
Semnăturile vânzătorului şi cumpărătorului sunt opţionale, furnizând o protecţie suplimentară împotriva respingerii (repudiation).
Ca şi în cazul cărţilor de credit convenţionale, partea a treia (acquirer) reconciliază separat tranzacţiile cu contul bancar al cumpărătorului, dar aceasta nu face parte din scopul iKP. Protocolul iKP poate fi adaptat unor medii variate, incluzând tranzacţiile pe WWW sub HTTP. Foloseşte algoritmul de semnătură şi de criptare cu cheie publică, iar tehnica de criptare se numeşte "criptare RSA cu integritate", bazată pe criptarea asimetrică optimală a lui Bellare şi Rogaway.

3.2. SET

Colaborarea dintre Visa şi MasterCard a dus la elaborarea şi dezvoltarea protocolului numit SET - Secure Electronic Transaction - tranzacţii electronice securizate, ca o metodă pentru securizarea tranzacţiilor bazate pe carduri bancare prin reţele.
SET include mesaje pentru achiziţii de bunuri şi servicii electronice, necesitând autorizaţii de plată şi "credentials" , cum ar fi certificate, pentru legarea cheilor publice cu entităţile. SET suportă:
- DES, pentru criptarea datelor majoritare;
- RSA, pentru semnături;
- criptări cu chei publice, pentru cheile datelor criptate şi numerele cărţilor bancare.
Criptarea cu chei publice RSA utilizează criptarea optimală asimetrică (Optimal Asymetric Encryption Padding).
Planurile de viitor ale celor de la RSA sunt de a suporta complet specificaţiile SET în linia lor de produse RSA. SET se află în prezent ca o specificaţie deschisă pentru industrie, ce poate fi folosit de producătorii de software pentru dezvoltarea de aplicaţii.

3.3. Secure Courier

Secure Courier este protocolul propus de Netscape pentru realizarea unui comerţ electronic securizat pe Internet. Se doreşte să fie un protocol pentru nivelul următor lui SSL.
La fel ca şi iKP, Secure Courier se bazează pe modelul cărţii de credit ce implică o a treia parte, banca de achiziţie. Mesajele sunt trimise între vânzător şi cumpărător, precum şi între vânzător şi bancă (acquirer gateway).
Comparativ cu alte protocoale pentru plată, Secure Courier lasă o parte din serviciul de integritate şi confidenţialitate a mesajului protocolului SSL sau altora din nivelele inferioare. De exemplu, pentru câmpul "ID transaction" din mesaj, este suficient de a realiza o legătură spre răspunsul tranzacţiei, deoarece nivelele inferioare asigură că acel câmp nu a fost modificat. În alte protocoale, ID-ul tranzacţiei trebuie să fie în mod expli-

cit protejat criptografic. Acest protocol suportă criptare cu cheie-publică RSA, semnături digitale, DES. Fişele de plată dintre client şi bancă pot fi trimise în mesaje cu format PKCS #7.

4. Protocoale pentru poştă electronică securizată: PEM, S/MIME, MOSS

4.1. PEM

Standardul, încă neoficial pentru Internet, legat de securitatea mesajelor poştale este PEM (Privacy-Enhanced Mail). Acesta a fost proiectat şi propus de Internet Activities Board pentru asigurarea seurităţii mesajelor electronice pe Internet.
A fost proiectat să lucreze cu formatul e-mail din RFC 822, şi include criptare, autentificare şi management de chei, permiţând utilizarea criptosistemelor cu chei *publice şi cu chei secrete*, precum intrumente criptografice multiple.
Fiecare mesaj din e-mail are specificat în header-ul său algortimul de criptare folosit, algoritmul de semnătură digitală şi funcţia de dispersie.
PEM suportă în mod explicit doar câţiva algoritmi criptografici, restul urmând să fie adăugaţi ulterior. Algoritmul criptografic implementat este DES în modul CBC; pentru managementul cheilor se foloseşte DES şi RSA, iar certificatul cheilor publice se face în conformitate cu standardului X.509.
Timp de doi ani PEM s-a aflat pe post de "draft", iar acum se pare că tinde să fie înlocuit cu S/MINE şi PEM-MIME. În prezent a fost elaborată o implementare noncomercială a lui PEM de către Trusted Infromation System, împreună cu alte protocoale, sub denumirea de RIPEM. Detalii despre PEM se găsesc în RFC 1421, 1424.

4.2. S/MIME

Protocolul S/MIME (Secure/ Multipurpose Internet Mail Extensions) adaugă criptare şi semnătură digitală mesajelor trimise cu formatul Internet MIME. Acesta este descris în RFC 1521.

MIME este standardul oficial propus pentru formatul poştei electronice extinse pe Internet. Mesajele e-mail au două părţi, antetul şi corpul scrisorii. Antetul conţine o colecţie de perechi de câmpuri şi valori structurate în conformitate cu RFC 822, ce furnizează informaţia necesară trasmiterii mesajului. În mod normal, corpul mesajului este nestructurat, mai puţin mesajele trimise în format MIME. Acesta defineşte cum să fie structurat corpul mesajului, pentru includerea de texte, grafice, audio etc.
MIME în sine nu furnizează nici un mecanism de securitate. Scopul S/MIME este de a defini servicii de securitate, urmând sintaxa PKCS#7, pentru criptare şi semnătură digitală. Astfel corpul scrisorii MIME conţine un mesaj PKCS#7, care este rezultatul procesului de criptare a altei părţi MIME.
Recent S/MIME a fost sprijinit de un număr de leaderi din cadrul producătorilor de instrumente pentru reţea şi transferul datelor şi mesajelor, cum ar fi ConnectSoft, Frontier, FTP Software, Qualcomm, Microsoft, Wollongong, Banyan, NCD, SecureWare, VeriSign, Netscape şi Novell.

4.3. PEM-MIME sau MOSS

PEM-MIME, cunoscut şi sub numele de MOSS (MIME Object Security Standard) este un draft propus pe Internet şi proiectat ca un succesor al lui PEM.
El propune adăugarea mesajelor MIME de servicii de securitate bazate pe PEM, la fel ca şi la S/MIME. Datorită naturii lui MIME, se pot adăuga servicii de securitate diferite fiecărei părţi a corpului mesajului. De exemplu, corpul MIME poate conţine două copii ale mesajului, dintre care una semnată digital. Astfel va permite receptorului să citească mesajul, chiar dacă nu are un mailer compatibil MIME. Dacă receptorul are un mailer compatibil PEM, atunci va fi verificată semnătura digitală. O altă posibiltate este de a cripta blocuri diferite ale corpului mesajului utilizând algoritmi şi chei diferite.
Standardul MOSS se doreşte să fie între PEM şi S/MIME, de unde îi şi vine numele de PEM-MIME, mailer-ele compatibile cu

PEM-MIME fiind foarte flexibile. Această flexibilitate provine din două mailer-e: unul care produce mesaje PEM-MIME, iar celălalt fiind incapabil de a le citi. Flexiblitatea este în parte o reacţie la rigiditatea din structura PEM, care nu este prea populară în rândul utilizatorilor. S/MIME este o cale de mijloc între rigiditatea PEM şi flexibilitatea PEM-MIME.

Bibliografie

1. /ELGA95/, ELGAMAL.,T., Commerce on the Internet, http://home.netscape.com, july 14, 1995;
2. /FEDE97/, Data Encryption Standard, Federal Information Processing Standards Publication, nr. 46, 1997;
3. /HULM90/, HULME,M., ş.a, Security in the Financial Service Sector, Electronic Banking&Finance, Elsevier Publishers, U.K., 1990;
4. /IBMZ97/, IBM Zurich Research Lab, Secure Electronic Commerce, sept 29, 1997;
5. /MATY96/, MATYAS, M, ş.a., Asymmetric Encryption: Evolution and Enhancements, CryptoBytes, nr.1, Spring, 1996;
6. /MOIS97/, MOISA,T., Securitatea datelor în Internet, Planeta Internet, octombrie,1997;
7. /PATR94/, PATRICIU, V., Criptografia şi securitatea reţelelor de calculatoare, Ed. Tehnică, Bucureşti, 1994;
8. /RSAD96/, RSA Data Security, Answers to FAQ About Cryptography Version 3.0, http://www.rsa.com, 1996;
9. /STAL92/, STALLING,W., Computer Communications: Architecture, Protocols and Standards, 3rd ed., LosAlaminos, 1992;
10. /TANE97/, TANENBAUM, A.,Reţele de calculatoare, ediţia a treia, Ed. Computer Press Agora, Bucureşti, 1997;