Solutii de securitate pentru Internet

Asist. Razvan ZOTA,
Catedra de Informatica Economica, A.S.E. Bucuresti

Posibilitatea conectarii la o singura retea a unui numar imens de calculatoare din întreaga lume reprezinta, fara doar si poate, un lucru extraordinar, cu influente favorabile asupra educatiei în general si a setei de cunoastere; apar însa si o serie de consecinte negative ale publicizarii anumitor informatii în reteaua Internet, ce sunt legate în principal de securitatea acestor informatii. Securitatea informatiilor care circula într-o retea este un termen complex, ce presupune în principal asigurarea integritatii informatiilor, protectiei acestora si permiterea accesului la ele doar a utilizatorilor autorizati sa o faca. Cu atât mai mult cu cât este vorba de o retea internationala de retele (Internet-ul), securitatea devine greu de mentinut si apar o serie de probleme specifice care odinioara, pe vremea existentei unor simple retele locale sau chiar de arie larga, nu existau.
Cuvinte cheie: *securitate, internet, retele de calculatoare.*

Relatia Intranet - Internet

În cadrul traditional de dezvoltare a afacerilor prin retea, orientarea departamentelor de Tehnologia Informatiei (**TI**) a fost aceea de a construi adevarate ziduri de protectie în jurul sistemelor informatice ale companiilor, limitând accesul la acestea pentru foarte putine persoane fizice sau juridice. Acest lucru avea o consecinta benefica, dar, din pacate, restrângea accesul la informatiile existente în retea si excludea practic posibilitatea comunicatiei libere cu exteriorul.

În noul model global de dezvoltare a afacerilor prin retea, intram practic într-o era noua a TI, o era bazata pe notiunea de sistem deschis. Folosind Internet-ul si Intranet-ul, orientarea se schimba complet; în loc sa se restrictioneze accesul (din afara sau dinauntru) la informatii, apare o noua oportunitate: deschiderea companiei, a sistemului si a informatiilor clientilor, partenerilor, furnizorilor si, nu în ultimul rând, angajatilor.

Primul lucru necesar pentru realizarea acestui concept este construirea unui Intranet în cadrul firmei, adica a unei retele (ce foloseste tehnologiile Web existente) care sa permita accesul la informatie pentru toti angajatii dintr-o firma, indiferent de localizarea fizica a acestora. Aplicatiile Intranet revolutioneaza modul de lucru; în timp ce tot mai multe informatii pretioase sunt accesibile angajatilor, trebuie garantata o securitate adecvata pentru aceste date.

Etapa urmatoare o poate constitui necesitatea împartirii informatiilor cu parteneri cheie, prin crearea unui Extranet sigur. Extranet-ul permite companiei sa realizeze eficient schimbul de informatii cu parteneri de afaceri si poate duce la scaderea semnificativa a costurilor prin scurtarea ciclurilor procesului de încheiere a afacerilor.

În fine, urmatoarea etapa o constituie conectarea la Internet. Astazi, tot mai multe firme implementeaza sau sunt pe cale de a implementa comertul electronic pe Internet ca o modalitate de a avea un avantaj fata de firmele competitoare. Succesul comertului electronic este dat, desigur, de cele 3 posibilitati ale sale de a încheia tranzactii: **oriunde**, **oricând** si cu **oricine**. Ne vom ocupa în continuare de acest aspect al dezvoltarii afacerilor unei firme, prin conectarea sa la Internet.

Conectarea firmelor la imensele resurse disponibile pe Internet implica însa si noi pericole ce apar datorate hackerilor. În conformitate cu diverse sondaje printre managerii din domeniul TI, acest lucru este

considerat unul dintre punctele cheie pentru mentinerea securitatii retelei. Companiile iau în considerare noi modalitati de a reduce costurile prin conectarea birourilor si a angajatilor prin intermediul Internet-ului. Aceasta aplicatie este cunoscuta sub numele de **VPN** (Virtual Private Network – Retea Virtuala Privata). Folosirea unei astfel de retele implica însa doua noi aspecte legate de securitate: asigurarea confidentialitatii datelor si autentificarea utilizatorilor. Sa vedem cum se poate securiza conexiunea Internet si reteaua virtuala privata.

Solutia de securitate pentru Internet este aceea de a oferi posibilitatea angajatilor sa acceseze resursele Internet, în acelasi timp prevenindu-se traficul neautorizat de informatii. Cea mai folosita modalitate de protectie a retelei interne este cea de folosire a unui **firewall** (zid de protectie) între Intranet si Internet (vezi figura 1).

Necesitatile de baza ale unui firewall Internet sunt:

– Un firewall trebuie sa fie capabil sa analizeze tot traficul ce trece în ambele directii între utilizatorii interni si reteaua externa. În acest mod se poate asigura numai fluxul autorizat de trafic, definit de politica de securitate a sistemului. Se poate asigura, totodata, si filtrarea traficului potential daunator retelei interne.

– Un zid de protectie trebuie conceput asa încât sa reziste atacurilor, deoarece, daca un hacker reuseste sa preia controlul zidului de protectie, întrega retea interna poate fi compromisa.

– Un firewall trebuie sa aiba capacitatea de a ascunde adresele retelei interne de lumea exterioara, facând viata unui potential hacker mai dificila.

Acestea sunt necesitatile de baza ale unui firewall; de asemenea, el trebuie sa asigure cresterea constanta a vitezelor de conexiune si a traficului Internet, pentru a se evita eventualele blocarile de trafic.

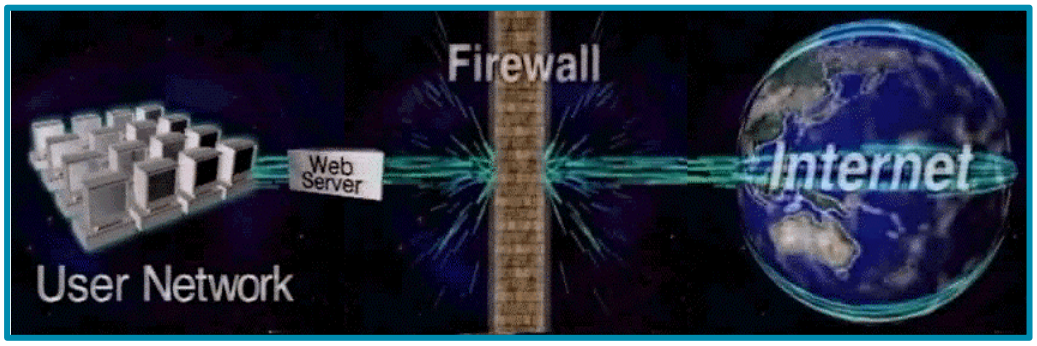

Fig.1. Protectia unei retele Intranet de conexiunea la Internet prin intermediul unui zid de protectie (firewall)

Retele private virtuale

Preocuparea continua a managerilor de retele de a asigura conexiuni la costuri reduse oriunde în lume este în continua crestere, iar preturile atractive ale serviciilor Internet ofera aceasta posibilitate: reducerea costurilor din domeniul tehnologiei informatiei. Conexiunea unui sediu al firmei aflat la distanta prin intermediul Internet-ului am spus ca tine de crearea unei retele private virtuale; conexiunea unui utilizator mobil prin Internet se face de regula prin intermediul asa numitei **VPDN** (Virtual Private Dialup Network – Retea Virtuala Privata prin Dialup).

Constructia unei retele virtuale private (vezi figura 2) înseamna, de fapt, folosirea Internet-ului ca pe o retea **WAN** (Wide

Area Network – Retea de Arie Larga) pentru a forma o retea de întreprindere extinsa; reducerea costurilor în acest caz ajunge pâna la 60%.
Pentru ca reteaua virtuala privata bazata pe Internet sa constituie o înlocuire viabila a liniilor închiriate sau a serviciilor Frame Relay, trebuie sa ofere un nivel cel putin la fel de bun de securitate, de calitate a serviciilor si de fiabilitate.
O modalitate de implementare a unei astfel de retele este prezentata în continuare, find cea a modelului IOS Cisco (Cisco Systems reprezinta unul dintre liderii mondiali în networking – "retelistica").
Pentru asigurarea unei retele virtuale private sigure pe Internet, trebuie construit un tunel de siguranta între sediul aflat la distanta si campusul retelei interne. Un astfel de tunel de siguranta consta din încapsularea si criptarea pachetelor vehiculate, aceasta facându-se la nivelul retea (vezi figura 3).

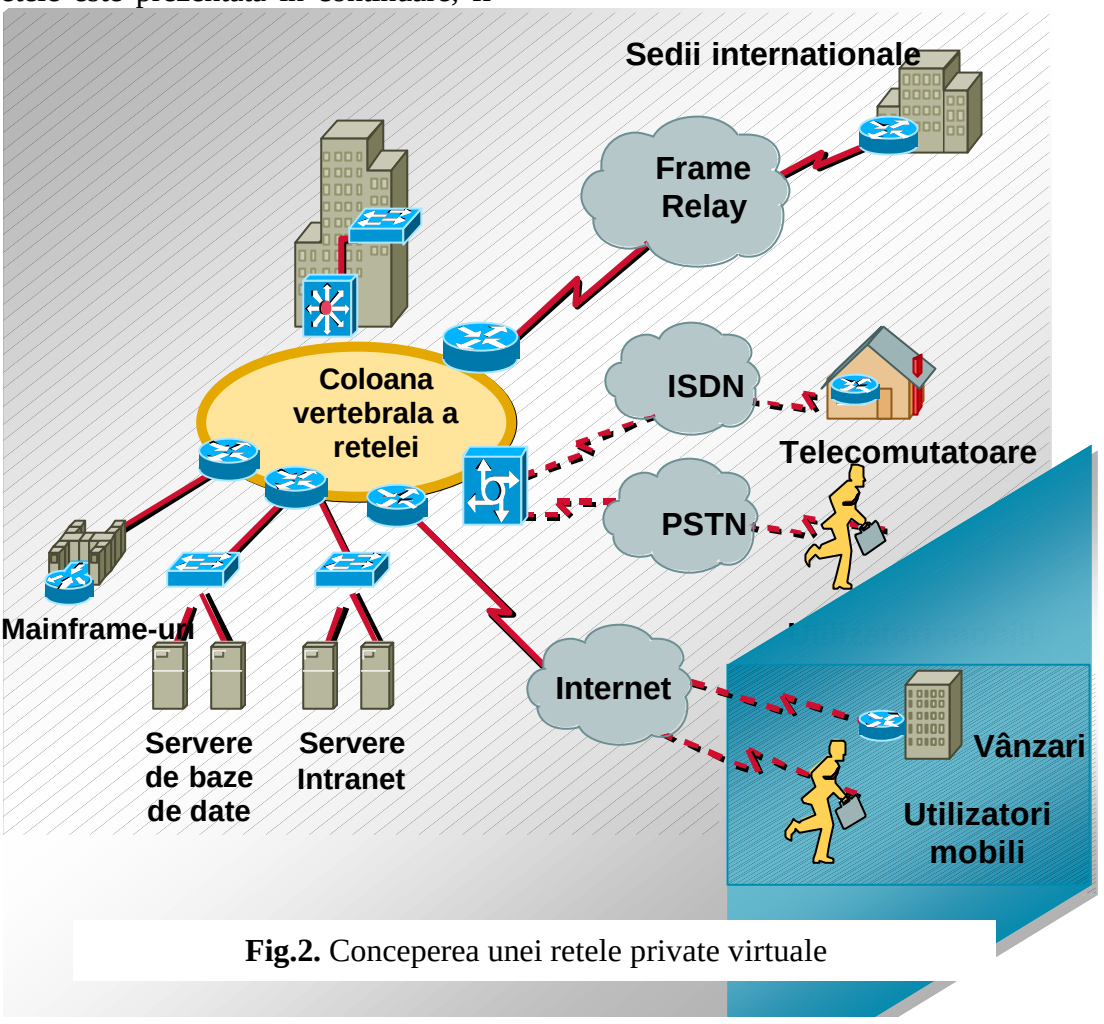

Fig.2. Conceperea unei retele private virtuale

Retele VAN

Un alt tip de retele folosit pentru comunicarea între companii si partenerii de afaceri sunt retelele **VAN**. Retelele **VAN** (Value Added Network – Retea cu Valoare Adaugata) sunt retele de comunicatie ce ofera servicii variate, printre care: functii de cutii postale, planificarea transmisiei si conversia protocolului de comunicare. Un alt avantaj al unei asemenea retele este acela ca prin intermediul ei se beneficiaza de folosirea unei singure conexiuni pentru a comunica cu un mare numar de parteneri.

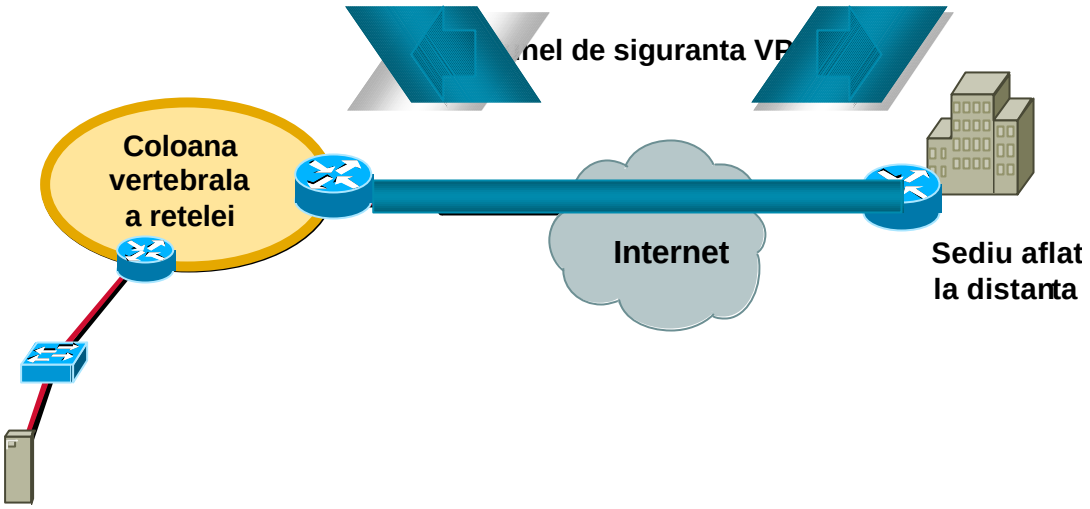

Fig.3. Tunelul de siguranta al retelei virtuale private

O companie poate trimite informatii în retea în orice moment iar reteaua VAN va trimite documentele companiei în cutia postala a partenerului caruia îi sunt adresate. Fiecare cutie postala apartine unui anumit partener si ea poate contine mesaje de la mai multi parteneri. Avantajul unei astfel de retele este ca se asigura (si se confirma) întotdeauna primirea documentelor de catre destinatar. Ca dezavantaj, comunicatia se face în modul "stocheaza si trimite mai departe", deci informatiile nu sunt schimbate în timp real. Documentele schimbate într-o retea VAN sunt în forma **EDI** (Electronic Data Interchange – Interschimb Electronic de Date), care este formatul electronic standard de documente ce poate fi usor interpretat de cealalta parte.

Securitatea este asigurata prin procedeele de autentificare si autorizare. În primul rând, un document standard, cum ar fi o factura, este creata de aplicatia respectiva a companiei. Apoi, documentul este convertit de un software de translatare EDI într-un format stabilit de comun acord. Documentul translatat este apoi plasat într-un "plic electronic" (electronic anvelope), împreuna cu un numar de identificare (pentru identificarea de catre furnizorul de servicii VAN) si trimis mai departe în retea.

Reteaua VAN citeste numarul de identificare al plicului electronic si îl trimite mai departe catre cutia postala destinatie. Partenerul respectiv foloseste propria aplicatie de comunicare si primeste continutul cutiei postale, documentul este translatat din standardul EDI în formatul necesar aplicatiei folosite. Daca este necesar un nivel sporit de securitate, aplicatia EDI poate face si criptarea datelor.

Transmisia datelor prin retele VAN este o metoda preferata de marile si bogatele companii care au asigurate deja asemenea legaturi cu partenerii de afaceri; totusi, în cazul firmelor mai mici schimbul electronic de date se face mult mai ieftin si mai rapid prin intermediul Internet-ului. Costurile transmisiilor prin Internet sunt cu 60-80% mai mici decât cele ale transmisiilor printr-o retea VAN.

Internet-ul ofera noi posibilitati de dezvoltare a afacerilor prin intermediul comertului electronic. Efectuarea tranzactiilor pe Internet ofera companiilor o mai mare flexibilitate si un mediu de dezvoltare a afacerilor extins. Totusi, Internet-ul nu va înlocui complet retelele VAN sau conexiunile private; unii parteneri de afaceri de dimensiuni mari vor folosi în continuare conexiunile existente si vor folosi cone-

xiunile ieftine Internet pentru gasirea de noi parteneri mai mici.

Dupa cum am mai spus, astazi este posibila încheierea de tranzactii comerciale pe Internet; o simpla cerinta este aceea a unei politici corecte de securitate, incluzând urmatoarele nivele de securitate:

1) Primul nivel de securitate îl constituie un firewall pentru asigurarea unei conexiuni sigure la Internet.

2) Se poate folosi, de asemenea, transmisia datelor criptate printr-un tunel de securitate pe Internet prin crearea de retele private virtuale. Criptarea datelor confera un al doilea nivel de securitate. Mai mult, se pot folosi asa numitele certificate digitale pentru a se asigura comunicarea sigura cu partenerul dorit.

3) Al treilea nivel de securitate este securitatea la nivelul aplicatie.

Desigur ca uneori nu este nevoie de toate aceste masuri de securitate; în functie de importanta datelor vehiculate se poate opta fie pentru un nivel sau altul de securitate, fie pentru toate trei la un loc.

Certificate digitale

În general, în criptografie (stiinta codificarii informatiei) sunt folosite asa numitele chei pentru codificarea si decodificarea informatiilor (este evident ca pentru a decodifica un mesaj este necesar sa se stie cheia cu care a fost codificat). De regula, se folosesc doua chei pentru codificarea unui mesaj, una numindu-se cheie publica (cunoscuta public), iar cealalta cheie privata (cunoscuta doar de utilizatorul ei sau de cel care trebuie sa decodifice mesajul).

Deoarece de multe ori pe Internet se pot falsifica aceste chei de criptare/decriptare, sunt folosite metode de certificare a acestora. O metoda este aceea de a folosi un certificat digital, acesta fiind o modalitate de a verifica ca o anumita cheie publica apartine unei anumite persoane sau unei companii.

Un certificat digital contine de regula:

– Numarul serial al certificatului;
– Informatii despre algoritmul de criptare;
– Informatii referitoare la identitate;
– Cheia publica a expeditorului;
– Semnatura digitala a autoritatii de certificare emitente.

De regula, certificatele digitale sunt eliberate de institutii specializate, denumite autoritati de certificare. Mecanismul de certificare este, în principiu, urmatorul:

Autoritatea de certificare (Certificate Authority) înregistreaza cheia publica a utilizatorului într-o baza de date foarte bine protejata. Deci daca un utilizator doreste sa previna falsificarea personalitatii sale, îsi va înregistra cheia publica la o autoritate de certificare reputata. Aceasta institutie va trimite în continuare un certificat digital oricui doreste sa verifice autenticitatea cheii publice a utilizatorului. Certificatul digital este, în esenta, ca un sigiliu notarial public aplicat peste semnatura utilizatorului, el confirmând identitatea si semnatura acestuia (vezi figura 4).

Securitatea comertului electronic pe Internet

Dezvoltarea Internet-ului a condus si la proliferarea comertului în cadrul acestuia. Daca pentru început tranzactiile mari se fac între companii private sau la nivel guvernamental, treptat acestea se vor extinde si pentru persoanele particulare, odata cu cresterea securitatii comertului electronic. Se estimeaza ca la nivelul anului 2000 cifra de afaceri a comertului electronic va fi de circa 100 de miliarde de dolari, urmându-se a se tripla în 2001.

Pentru a se asigura cresterea comertului pe Internet, trebuie asigurat un nivel de securitate adecvat între cei doi parteneri ai tranzactiei, adica de la clientul web la server-ul web de la celalalt capat. Dintre elementele acestei securitati, cele mai importante pentru Internet sunt autentificarea, autorizarea si confidentialitatea.

Dar sa vedem în continuare ce înseamna aceste trei aspecte cheie legate de securitatea pe Internet.

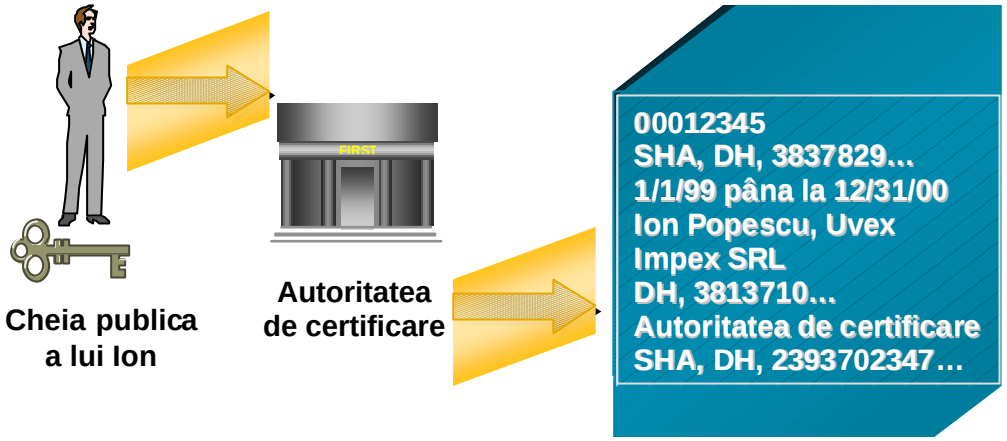

Fig.4. Continutul unui certificat digital si eliberarea acestuia de catre autoritatea de autentificare

– **Autentificarea**. Cum stim ca persoana care pretinde ca are o anumita identitate are într-adevar acea identitate? Apare astfel problema autentificarii, care presupune cunoasterea exacta a persoanei (sau firmei) cu care efectuam tranzactia.

– **Autorizarea**. Ne întrebam apoi daca informatiile pe care le trimitem ajung într-adevar la persoanele autorizate. Autorizarea este de asemenea importanta pentru tranzactii financiare precum cele cu cartile de credit.

– **Confidentialitatea** implica faptul ca trebuie sa fim asigurati ca atunci când purtam "dialogul de tranzactie" cu interlocutorul, nimeni altcineva nu "asculta la usa".

– Securitatea comertului electronic pe Internet se poate implementa la nivele diferite de retea, precum nivelele retea, sesiune, aplicatie si gazda.

– Securitatea la nivelul retea reprezinta baza securitatii si este necesara pentru a asigura securitatea echipamentului si a serviciilor de retea de-a lungul drumului parcurs, indiferent de aplicatiile folosite.

– Securitatea la nivelul sesiune ofera securitate web-client si web-server asigurând integritatea informatiei transferatede-a lungul retelei.

– Datorita diverselor aplicatii ce ruleaza pe Internet, sunt necesare si protocoale de securitate la nivelul aplicatie deoarece acestea permit interoperabilitatea aplicatiilor între comercianti, clienti si institutiile financiare.

– Securitatea la nivelul gazdei apare necesara pentru protejarea serverelor de comert electronic de intruziuni din afara. Aceasta securitate este importanta deoarece serverul gazda poate foarte usor sa devina, daca nu suntem atenti, cea mai slaba veriga din întreg lantul de securitate creat.

Exemple de aplicatii din lumea comerciala a Internet-ului:

1) Aplicatia de comert electronic dezvoltata de Charles Schwab, denumita **SchwabNow!** este cea mai de succes aplicatie on-line de comert electronic, oferind securitate participantilor la comertul pe web prin priotocolul **SSL**;

2) Magazinul electronic **Wal-Mart On-line** foloseste protocolul **SET** (Secure Electronic Transaction – Tranzactie Electronica Securizata), pentru tranzactiile cu carti de credit pe Internet;

3) Aplicatiile comerciale Cisco Connection Online ofera posibilitatea de efectuare a vânzarilor pe Internet si diverse ins-

trumente pentru comertul electronic pentru clientii si partenerii firmei Cisco de pretutindeni în lume.

Primul exemplu, **SchwabNow!** ofera un mediu comercial bazat pe Web care este privat si securizat. Schwab eate în prezent liderul afacerilor de brokeraj online detinând 50% din piata si peste un milion de conturi. Numarul de conturi adaugate saptamânal se cifreaza undeva între 12000 si 15000. Pentru a oferi deplina securitate clientilor, acestia folosesc un **SSL**-browser (capabil sa foloseasca protocolul **SSL**) pentru accesarea sitului SchwabNow! de pe Internet, sesiunea deschisa fiind codificata prin protocolul **SSL**. Odata cu codificarea sesiunii, utilizatorii pot introduce numele contului si parola, sa vizualizeze informatiile referitoare la bursa si sa faca tranzactii on-line cu siguranta ca acestea sunt protejate.

Sa vedem în continuare cum este implementata securitatea la un sit de acest fel. Clientul se conecteaza la severul Schwab de pe Internet folosind un browser standard ce suporta protocolul **SSL**, protocol care ofera o securitate la nivelul sesiune de la clientul web la serverul web. Un firewall protejeaza serverele si mainframe-urile de tranzactionare Schwab de patrunderi ilegale, oferind securitatea la nivelul retea.

Doar dupa ce clientul a introdus numele contului si parola poate accesa informatia referitoare la contul respectiv si sa faca tranzactii online. Acesta este un bun exemplu pentru modul cum actioneaza împreuna securitatea comertului electronic la cele 3 nivele: sesiune, retea si aplicatie.

Protocolul SSL

De regula, schimbul securizat de documente de afaceri pe Web se face prin stabilirea unei conexiuni de tipul Secure Socket Layer. **SSL** foloseste certificate digitale pentru a verifica identitatea serverului web al companiei, si metode de criptare pentru transmisia securizata a datelor pe Internet.

Pasul urmator este acela de identificare a furnizorului fata de client; acest lucru poate fi facut prin intermediul unui cont de genul utilizator/parola pe web server-ul clientului. Conexiunea **SSL** realizeaza, de asemenea, si criptarea parolei pentru asigurarea confidentialitatii. Odata ce furnizorul a fost autentificat, i se atribuie un nivel de autorizare de catre client. Spre exemplu, nivelul de autorizare îi poate permite furnizorului accesul la anumite date de productie si restrictia accesului la altele. Furnizorul poate prelua informatiile în mod securizat.

Enumeram în continuare câteva dintre caracteristicile protocolului **SSL**:

– Stratul **SSL** se afla între protocolul TCP/IP si protocoalele nivelului aplicatie (vezi figura 5) si a fost dezvoltat de Netscape, fiind acum o componenta standard pentru majoritatea browserelor si a serverelor Web.

– **SSL** ofera câteva elemente de securitate printre care autentificarea clientului si a serverului. Autentificarea serverului este lucrul cel mai uzual folosit si ofera clientului certitudinea identitatii serverului. Prin intermediul protocolului **SSL** se asigura confidentialitatea datelor datorita codificarii acestora.

– **SSL** foloseste algoritmi diferiti pentru criptare, pentru autentificare si pentru asigurarea integritatii datelor. Aceasta permite **SSL** sa fie exportat oriunde în lume.

– **SSL** permite autentificarea prin folosirea certificatelor digitale si a semnaturilor digitale.

– **SSL** foloseste certificatele digitale X.509 v3 pentru autentificare.

*Cum functioneaza protocolului **SSL**:*

În esenta exista 4 pasi necesari pentru transmiterea unei sesiuni sigure între browserul web si serverul de comert.

Primul pas îl constituie initierea ("handshake" - schimbul initial de mesaje) protocolului **SSL**. Atunci când un web browser client se conecteaza la un server este

necesar sa trimita ca prim mesaj mesajul "client hello". Serverul raspunde cu un "server hello" ce include Certificatul Digital folosit de browserul client pentru a identifica serverul.
Al doilea pas consta în acceptarea clientului. Odata ce browserul este convins ca serverul este autentic, el genereaza doua chei private ce urmeaza a fi folosite pentru tranzactia ce urmeaza. Browserul cripteaza cheile private folosind cheia publica a comerciantului si le trimite serverului. Serverul le decripteaza si în acest moment fiecare dintre parti are chei private. Acestea se mai numesc si chei de sesiune, deoarece sunt valabile doar pentru sesiunea respectiva si dupa aceea sunt sterse.
Al treilea pas este verificarea. Browserul trimite un mesaj securizat serverului, folosind una dintre cheile de sesiune pentru criptarea mesajului. Serverul raspunde prin trimiterea unui raspuns criptat cu cealalta cheie de sesiune. Daca tot mecanismul se deruleaza corect, înseamna ca s-a stabilit o legatura sigura si tranzactia poate începe fara teama.
Ultimul stadiu îl reprezinta schimbul de date; protocolul **SSL** este optimizat astfel încât criptarea si decriptarea cheii publice sunt necesare o singura data pe sesiune.

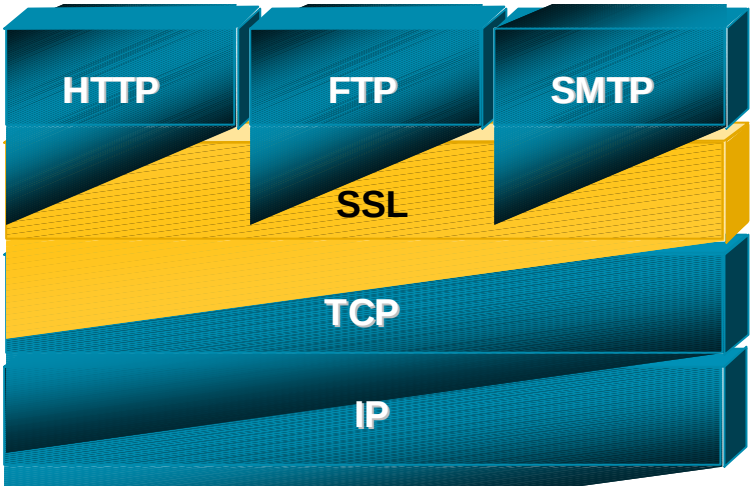

Fig.5. "Locul" protocolului SSL între TCP/IP si protocoalele nivelului aplicatie

Cel de-al doilea exemplu, **Wal-Mart**, reprezinta unul dintre cei mai mari comercianti en-detail de bunuri de consum care foloseste Internet-ul pentru a gasi noi clienti si piete de desfacere fara a investi în deschiderea de noi magazine. Exista deja la Wal-Mart peste 400.000 de produse online, cu precadere din domeniul muzicii, cartilor, calculatoarelor si jocurilor, domenii alese si dorite cel mai mult de cumparatorii de pe Internet.
Wal-Mart este cladit pe o impresionanta fundatie de retea ce trebuie sa suporte întreaga afacere; securitatea este una dintre problemele cheie iar ei implementeaza tehnologii de ultima ora în domeniu. Preluarea sefiei în domeniul tranzactiilor cu carti de credit pe Internet s-a facut folosind sistemul **SET** (Secure Electronic Transactions – Tranzactii Electronice Securizate). Versiunea de încercare a protocolului **SET** a fost lansat în Statele Unite pe Wal-Mart Online. Folosind metode avansate de criptare si tehnologii de semnaturi digitale oferite de **SET**, un posesor al unei carti de credit American Express a facut prima tranzactie electronica, aceasta prima tranzactie fiind cea care a atestat practic versiunea 1.0 a protocolului **SET**. Deoarece MasterCard si Visa au

publicat specificatiile versiunii **SET** 1.0, s-a format o noua organizatie, denumita **SETco** pentru a superviza implementarea, testarea si elaborarea noilor versiuni de **SET**. SETco cuprinde companiile Mastercard, VISA, American Express si JCB (Japonia).
Infrastructura menita sa asigure tranzactiile **SET**, care necesita software specific si numere de identificare pentru consumatori, comercianti web si banci este înca în curs de elaborare si perfectionare.

Modul de functionare al protocolului SET

Cartile de credit reprezinta metoda cea mai folosita în tranzactiile comerciale, dar ele reprezinta noi amenintari ale securitatii atunci când sunt folosite pe Internet. Numerele cartilor de credit reprezinta practic parole care nu se schimba ce pot fi folosite în mod repetat pentru efectuarea de plati din contul cumparatorului.
Pe Internet, numerele cartilor de credit ale consumatorilor trebuie protejate de aceesul persoanelor neautorizate. Cu toate ca **SSL** poate fi folosit pentru a transmite în mod securizat informatii despre cartile de credit pe Internet, exista anumite limitari. De exemplu, cu ajutorului protocolului **SSL**, informatia referitoare la cartea de credit trebuie procesata de comerciant, ceea ce poate conduce la erori sau chiar fraude din partea acestuia. Folosind protocolul **SET**, informatiile referitoare la cartile de credit nu sunt disponibile comerciantului ci sunt trimise direct institutiei financiare (bancii) pentru autorizare. Protocolul **SET** se adreseaza în mod specific acestei limitari, tocmai pentru a asigura tranzactii sigure cu carti de credit pe Internet. Figura 6 ilustreaza folosirea protocolului de securitate **SET**.

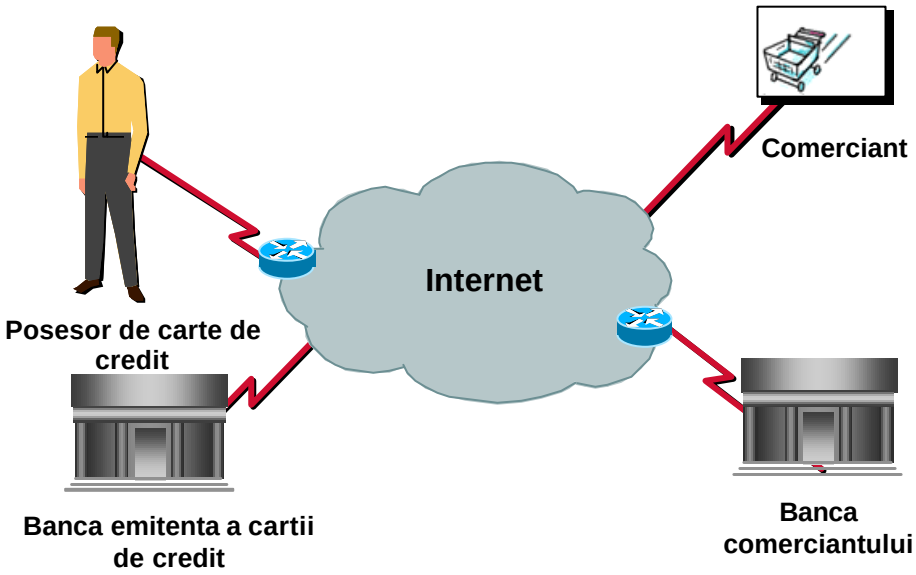

Fig.6. Functionarea tranzactiilor folosind protocolul SET

Protocolul **SET** face parte din nivelul aplicatie al securitatii (vezi figura 7) si a fost conceput în mod special pentru a asigura comertul electronic pe Internet cu ajutorul cartilor de credit. MasterCard, Visa si alte companii coopereaza pentru a defini o specificatie deschisa care sa se adreseze necesitatilor unor tranzactii se-

curizate cu carti de credit pe Internet. **SET** permite interoperabilitatea dintre aplicatii, astfel încât software-ul de pe calculatorul unui client sa functioneze cu software-ul comerciantului si al bancii, indiferent de tipul calculatorului. Protocolul **SET** se asteapta a servi ca baza de securitate si pentru alte modalitati de plata folosite pe Internet, precum ar fi cecurile electronice.
Protocolul a fost conceput doar pentru codificarea informatiilor referitoare la platile prin cartile de credit, deci algoritmii si modalitatile de criptare nu pot fi folosite pentru alte aplicatii.

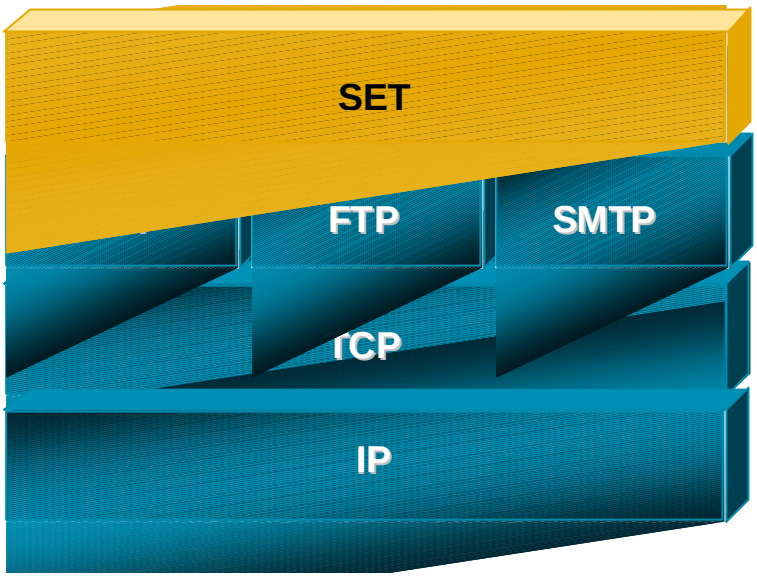

Fig.7. Locul protocolului SET la nivelul aplicatie al securitatii

Protocolul **SET** împreuna cu specificatiile sale au aparut în special pentru a asigura o solutie completa pentru comertul electronic pe Internet, ajutând la asigurarea confidentialitatii si integritatii informatiilor prin autentificarea partilor implicate în tranzactii. Specificatiile protocolului cer autentificarea tuturor partilor implicate în tranzactiile cu carti de credit prin folosirea semnaturilor si a certificatelor digitale. Certificatul digital al detinatorului de card nu autentifica doar persoana, ci face si legatura între respectiva persoana si o anumita carte de credit.
SET asigura integritatea si confidentialitatea datelor prin folosirea semnaturilor digitale si criptarea numerele cartilor de credit folosind algoritmul RSA. Prin folosirea tehnicilor de criptare, **SET** apeleaza la o etapa separata (de criptare) între partile implicate în tranzactia prin cartea de credit, ajutând la garantarea confidentialitatii si integritatii datelor în fiecare moment. Deoarece informatia continuta de cartea de credit este codificata, aceasta este greu de folosit de alte persoane.
Protocolul **SET** este înglobat în software-ul destinat detinatorilor de carti de credit, comercianti si banci. Detinatorii de carti de credit folosesc asa numitele "portofele electronice" (electronic wallets) care pot fi încarcate (prin download) sau sunt deja înglobate în browsere.

*Etapele unei tranzactii electronice bazate pe **SET** sunt:*
Pentru început se introduce numarul unei carti de credit într-un portofel electronic de pe PC sau smartcard. Atunci când consumatorul ajunge la situl comerciantului, el poate selecta optiunea de plata prin **SET** de pe un sit web pentru a activa portofelul electronic. Software-ul necesar pentru folosirea portofelului va genera cheia publica

si cea privata pentru codificarea informatiilor, le va memora si va fi gata sa înregistreze toate tranzactiile facute.
Protocolul **SET** codifica ordinul de achizitie si informatiile referitoare la cartea de credit si le trimite serverului comerciantului. Software-ul comerciantului foloseste un asa numit "registru de casa electronic" (electronic cash register) care verifica toate certificatele digitale si tine evidenta tuturor vânzarilor – înlocuind operatiunile care înainte erau facute manual de catre comerciant. Certificatele digitale sunt oferite comerciantilor, bancilor si consumatorilor de Autoritatile de Certificare, despre care am vorbit anterior.
Dupa ce cheile publica si privata sunt folosite pentru asigurarea unei conexiuni securizate, software-ul comerciantului revede comanda, semneaza digital mesajul de plata si trimite mai departe informatiile bancii care proceseaza tranzactia. Serverul de plati al bancii decodifica toate informatiile si încheie operatia (extrage banii) cu cartea de credit, apoi se trimit chitante de confirmare a operatiunii atât comerciantului cât si cumparatorului.

Cel de-al treilea exemplu, Cisco Connection Online (**CCO**), ofera prin intermediul Internetului o interfata interactiva în timp real între firma Cisco si resellerii si clientii sai. Avantajele **CCO** sunt, printre altele, comenzi si livrari mai rapide, de unde se asigura cresterea satisfactiei consumatorilor. De asemenea, **CCO** duce la îmbunatatirea productivitatii, ceea ce conduce la niste economii anuale de costuri de peste 250 de milioane de dolari.
Comenzile facute prin **CCO** reprezinta acum aproximativ 40% din totalul vânzarilor Cisco, adica aproximativ 3 miliarde de dolari anual. Comertul electronic se face prin intermediul asa numitilor Commerce Agents (Agenti de Comert) care reprezinta baza sistemului **CCO** si care permit clientilor si partenerilor sa aiba usor acces la configuratie, preturi si starea informatiilor de oriunde si în orice moment pe Internet.
Spre exemplu, Configuration Agent (Agentul de Configurare) permite clientilor sa vada catalogul produselor, sa caute anumite articole si sa verifice automat informatiile înainte de a pregati formularul final de comanda. În mod asemanator, Agentul de Preturi simplifica modalitatea de comandare a produselor si reduce erorile de stabilire a preturilor iar Agentul de Stare ofera acces imediat la informatii referitoare la facturi sau alte documente fiscale. Se pot furniza informatii si despre eventuala expeditie a marfii prin intermediul unor sisteme Web (vezi firmele FedEx, DHL, sau UPS).

Concluzie

Aparitia comertului electronic securizat pe Internet duce, în mod evident, la transformarea lumii afacerilor si la crearea unui comert global de retea.
Mai exista unele probleme legate de taxe, drepturi de autor si de dezvoltarea cu adevarat a unei retele modiale de comert, dar avantajele legate de încheierea mai rapida a tranzactiilor, gasirea mai rapida si cu costuri mai mici de noi parteneri si rezolvarea onorabila a chestiunilor legate de securitate face ca viitorul sa surâda comertului electronic.

Bibliografie

http://www.cisco.com
http://www.networkcomputing.com
http://www.peapod.co.uk
http://www.fnbinternet.com