Elemente de securitate pentru Internet Banking

Asist.drd. Razvan Zota
Catedra de Infomatica Economica, A.S.E. Bucuresti

Dezvoltarea de o deosebita amploare a retelei Internet, aceasta "retea a retelelor", a determinat aparitia unor probleme aditionale legate, de regula, de securitatea informatiilor vehiculate în retea. Noua tendinta a bancilor din toata lumea este sa ofere clientilor servicii îmbunatatite si pe baza sistemelor de Internet Banking. Dar cum aceste sisteme de Internet Banking presupun conexiunea la Internet, este normal sa apara masuri cât mai stricte de securitate pentru asigurarea protectiei datelor (si conturilor) utilizatorilor. În cadrul acestui articol sunt prezentate o parte dintre elementele de securitate înglobate în astfel de sisteme.
Cuvinte cheie: *Internet Banking, sesiune electronica, securitate, SSL, firewall, browser, criptare de date*

Definirea conceptului de Internet Bank-ing

Notiunea de Internet Banking se refera la posibilitatea interactiunii, prin intermediul Internetului a unui client (sub denumirea generica de utilizator) cu banca la care acesta (de regula) poseda un cont bancar.
Mai precis, un sistem de Internet Banking ofera clientilor unei banci acces bazat pe parola la informatii referitoare la conturile acestora prin intermediul unui calculator cu acces Internet.
Accesul la informatiile referitoare la conturi se poate concretiza în:

- Vizualizarea balantelor de cont;
- Vizualizarea tranzactiilor efectuate pe o perioada de timp;
- Transferul de bani dintr-un cont în altul;
- Plata unor facturi;
- Alte operatiuni specifice, ce depind de implementare.

Nu trebuie sa confundam notiunea de *Internet Banking* cu cea de *e-banking* (uneori întâlnita sub numele de *PC Banking*); daca prima presupune o conexiune cu banca prin intermediul Internetului, cea de a doua foloseste o conexiune directa cu banca, de regula prin intermediul unui modem si a unei linii telefonice pentru oferirea unor servicii asemanatoare. Sa analizam în continuare cum se desfasoara o procedura de Internet Banking.

Desfasurarea unei sesiuni bancare electronice

O sesiune este pornita în momentul în care abonatul autorizat, prin intermediul unui browser web, trimite un mesaj securizat conform protocolului SSL serverului respectivului serviciu electronic. În acest sens, utilizatorul foloseste o parola si un identificator al sau; serverul verifica aceste date si autentifica clientul initiind sesiunea de criptare.
Odata stabilita sesiunea (securizata) electronica, calculatorul bancii ce asigura serviciul, proceseaza si directioneaza datele tranzactiei folosind protocoale interne. Acest lucru confera o siguranta împotriva accesului neautorizat a altor utilizatori Internet prin firewall-urile si ruterele de filtrare ale bancii. Programul de tranzactie electronica protejeaza tranzactionarile printr-o serie de bariere ce previn accesul neautorizat:

– Prima bariera este constituita de un sistem de rutere de filtrare si firewall-uri, ce separa Internetul de reteaua interna a bancii. Ruterul de filtrare verifica sursa si destinatia fiecarui pachet Internet si decide daca pachetul va intra în retea sau nu. Accesul este interzis daca pachetul nu este directionat catre un serviciu specific. De ase-

menea, ruterul de filtrare previne atacuri Internet obisnuite.

– În plus, firewall-ul este singurul server din reteaua bancii care comunica prin TCP/IP – protocolul de comunicatie din Internet, astfel ca nu sunt disponibile altfel de sisteme de procesare on-line a tranzactiilor prin intermediul TCP/IP. Acest lucru previne accesul utilizatorilor neautorizati la datele tranzactiilor provenite din Internet. Informatia este schimbata între calculatorul bancii si calculatorul clientului dupa ce în prealabil este criptata folosind cea mai buna metoda de criptare posibila.

Rationamentul masurilor de securitate

Securitatea este obiectivul primordial al Internet banking-ului deoarece reteaua Internet este prin definitie nesecurizata. Atunci când avem de-a face cu zeci de milioane de calculatoare conectate la o retea publica, este greu, daca nu imposibil sa asiguri o securitate a tuturor datelor ce se vehiculeaza în aceasta retea, având în vedere faptul ca pot fi interceptate schimburile de informatii dintre doua calculatoare. Pe parcursul directionarii unui pachet de date în retea, acesta poate fi interceptat si de catre alt calculator decât calculatorul destinatie; chiar si calculatoare ce nu sunt implicate direct în procesul de rutare pot intercepta si accesa aceste date.

Riscurile de baza ale comunicatiilor Internet

Exista trei categorii fundamentale de riscuri în cazul comunicatiilor Internet:

– Interceptarea unei conversatii calculator-calculator de catre cineva din afara;

– Manipularea datelor – modificarea de catre terti a datelor în cadrul unei conversatii private;

– Depersonalizarea – atribuirea unei false identitati în cadrul unei conversatii.

Situatia este similara cu cazul comenzilor de bunuri prin telefon folosind carte de credit. Cumparatorii vor sa se asigure de faptul ca nu exista cineva care asculta convorbirea, ca nimeni nu poate modifica comanda facuta sau modifica adresa de destinatie sau ca la capatul firului se afla într-adevar o companie de vânzari prin telefon si ca nu este un escroc care fura numere de carti de credit.

Cum se face protejarea datelor fata de riscurile existente?

Browserele Web curente trateaza chestiunile legate de securitate prin intermediul protocolului SSL prezentat în subcapitolul anterior, care cuprinde o multime de reguli ce impun calculatoarelor pasii pe care trebuie sa-i urmeze pentru a îmbunatati securitatea comunicatiilor. Aceste reguli se refera la criptarea datelor (pentru prevenirea ascultarii de catre neaveniti), integritatea acestora (împotriva modificarii datelor reale) si la autentificarea utilizatorilor (pentru prevenirea depersonalizarii). Acest mijloc de protectie ne fereste doar pe timpul comunicatiei, aceasta însemnând ca datele nu sunt protejate ***înainte*** de trimiterea lor. Trebuie, de asemenea, sa exite încrederea în destinatarul datelor trimise on-line în sensul ca acesta nu va manipula datele în alte scopuri decât cele stabilite de comun acord.

Care este gradul de securitate al protocolului SSL?

Protocolul SSL foloseste tehnologii de autentificare si criptare dezvoltate de RSA Data Security Inc.; criptarea stabilita între client si serverul bancii ramâne valida de-a lungul a mai multor conexiuni, iar efortul depus pentru spargerea criptarii unui mesaj nu poate fi folosit pentru spargerea urmatorului mesaj. Un mesaj criptat cu o cheie RC4 pe 40 de biti necesita un timp mediu de 64 MIPS ani pentru a fi decodificat (un computer de 64 MIPS are nevoie de un an pentru a sparge codificarea mesajului). La nivel mai înalt, o protectie pe 128 de biti duce la o crestere exponentiala a timpului de spargere a codului. Autentificarea serverului foloseste criptografia bazata pe chei publice RSA în colaborare cu certificatele digitale ISO X.509.

Securitatea browser-ului

Datorita insecuritatii Internetului, este bine sa avem în vedere urmatoarele:

– Sa folosim întotdeauna ultimele versiuni ale software-ului; descoperirea unei brese de securitate este cel mai imprtant motiv pentru producatorii de software în elaborarea unei noi versiuni de software;

– Este importanta folosirea variantei celei mai sigure de software; clientii ce folosesc anumite versiuni de browsere pot încarca de pe site-ul producatorilor ultimele suplimente soft de securitate.

Protectia programelor de tranzactionare electronica

În general, programele de e-banking încearca sa asigure cel mai sigur serviciu bancar-electronic (fie prin intermediul Internetului fie prin legatura directa) astfel încât toate tranzactiile ce necesita date financiare legate de clienti sa se faca într-un mediu securizat. Fara o securitate riguroasa, informatia transmisa în Internet este susceptibila fraudelor si folosirii ilegale de catre diversi terti. Facilitati avansate de securitate înglobate în programele de Internet banking protejeaza clientii de accesul neautorizat la datele acestora. Criptarea pe 128 de biti este cea mai înalta metoda existenta, pâna nu demult restrictionata la SUA si Canada, dar disponibila si în alte state în momentul de fata. Facilitati aditionale de securitate sunt aduse de identificatorul utilizatorului si de parola ce sunt oferite de banca pentru accesarea contului bancar. Microsoft Internet Explorer sau Netscape Navigator cu criptare pe 128 de biti asigura:

– Autentificarea serverului;

– Privatizarea datelor prin folosirea criptarii;

– Integritatea datelor.

Pentru protejarea datelor bancare din calculatorul central sunt folosite dispozitive firewall si doar persoane autorizate au acces la aceste date din sistem. Protocolul SSL permite autentificarea serverului, criptarea datelor si integritatea mesajelor. Acest protocol se afla sub stratul protocoalelor nivelului aplicatie precum HTTP, SMTP, Telnet, FTP, Gopher sau NNTP si deasupra nivelului transport pe care se afla protocolul TCP/IP. Aceasta strategie permite SSL sa opereze independent de protocoalele aplicatiilor Internet. Implementarea SSL se face atât la nivel server cât si la nivel client, astfel ca transmisiile Internet se fac criptat si informatiile trimise se considera ca ajung în siguranta la serverul specificat (si doar la acesta).

Cookies

Cookie-urile sunt mici structuri de date emise de un site web catre hard discul unui calculator. În unele cazuri – în functie de datele continute în cookie – web site-ul necesita reîntoarcerea acestuia. Aceste mici structuri de date permit web site-urilor sa stocheze o serie de informatii pe parcursul vizitei utilizatorului pe acest site; ele nu pot prelua informatii de pe hard disk, adresa de e-mail sau alte informatii private. Majoritatea site-urilor securizate vor trimite temporar astfel de cookies PC-ului client. Datorita tot unor ratiuni legate de securitate, în timpul folosirii unui program bancar de plata electronica, de exemplu, daca browser-ul client este setat sa avertizeze înainte de primirea unui cookie, trebuie sa se selecteze optiunea de acceptare a tuturor cookie-urilor. În momentul refuzului unui cookie, sesiunea programului respectiv se termina, acest lucru facându-se pentru asigurarea protectiei utilizatorilor.

Transmiterea unor informatii confidentiale precum numarul unei carti de credit

Informatiile confidentiale de genul numarului unei carti de credit pot fi trimise în siguranta folosindu-se un formular securizat aflat la o adresa de tipul **https://**, fara a exista pericolul de interceptie a informatiilor de catre terte persoane. Desigur, comunicatiile securizate nu elimina în totalitate grijile utilizatorilor; spre exemplu, trebuie sa avem încredere în adminis-

tratorul serverului înainte de a începe o tranzactie cu o carte de credit. Tehnologia sigura ne protejeaza pe parcursul drumului informatiilor în Internet, dar nu ne poate proteja împotriva unor oameni necinstiti si fara scrupule cu care poate ca am ales sa facem afaceri în nestiinta de cauza.

Situatia este similara cu cea în care spunem cuiva numarul cartii de credit prin telefon. Daca putem fi siguri în privinta faptului ca nimeni nu a ascultat convorbirea noastra privata si ca persoana de la capatul firului lucreaza într-adevar pentru firma de la care vrem sa facem achizitia, nu putem fi siguri pe deplin de persoana respectiva sau de firma respectiva.

Notiuni de criptare a datelor

Criptarea reprezinta modalitatea de codificare a informatiilor în scopul transmiterii acestora de-a lungul unui canal de comunicatie. Browserul de Web foloseste un sir de numere, caractere si chei speciale facând din procedeul de codificare si decodificare a datelor ceva extrem de complicat. Calculatorul utilizatorului ce trimite datele si cel ce primeste datele trebuie sa cada de acord asupra cheilor folosite în procedeul de codificare. Aceste chei sunt bazate pe o serie de formule matematice sau, mai bine spus, pe niste algoritmi. Atunci când se face criptarea datelor în calculator, exista miliarde de combinatii posibile pentru a se face decriptarea, din care, evident, doar una singura este cea corecta. Doar cele doua calculatoare ce comunica între ele cunosc aceasta combinatie pe parcursul sesiunii de comunicatie. Cele doua calculatoare folosesc combinatii diferite pentru fiecare sesiune în parte, acestea fiind cunoscute doar de cele doua calculatoare. Criptarea este foarte folositoare într-o serie de tranzactii ce implica lucruri delicate cum ar fi tranzactiile financiare sau chestiuni legate de securitatea statului. Criptarea se foloseste pentru trimiterea mesajelor e-mail, a unor documente importante, precum si în comertul electronic la tranzactiile prin carti de credit si e-banking.

Securitatea criptarii

Securitatea oferita de criptare se masoara în functie de lungimea cheii de codificare folosita de calculator pentru codificarea datelor. Nivelul de criptare poate fi astfel de 40 de biti sau de 128 de biti. Se spune în aceste cazuri ca se foloseste o criptare pe 40 de biti sau pe 128 de biti. Cu ajutorul criptarii pe 40 de biti, numarul total de combinatii posibile este de 2^{40}, pe când în cazul criptarii pe 128 de biti exista 2^{128} diverse combinatii posibile. Criptarea pe 40 de biti foloseste una dintre cele 2^{40} combinatii posibile(ordinul de marime este de un 1 urmat de 12 zerouri) pe când criptarea pe 128 de biti foloseste una dintre cele 2^{128} combinatii posibile. Conform Netscape, criptarea pe 128 de biti este de 309.485.009.821.345.068.724.781.056 (309 de milioane de miliarde de miliarde) ori mai puternica decât criptarea pe 40 de biti. Browserele Netscape si Internet Explorer folosesc procedeele de criptare, pe 40 sau pe 128 de biti.

Elaborarea unui plan de securitate pentru un sistem de Internet Banking

Dupa cum mai subliniat, tranzactiile bancare pe Internet au ca cerinta fundamentala securitatea. De aceea, orice sistem de tranzactionare de acest tip trebuie sa ia în considerare masuri de precautie corespunzatoare astfel încât informatiile vehiculate sa fie protejate si securizate. Ultimele metode de securitate folosite în domeniul tranzactiilor bancare pe Internet sunt menite sa mareasca securitatea si sa monitorizeze integritatea aplicatiei bancare on-line.

Securitatea unui model de tranzactionare pe Internet trebuie sa cuprinda trei nivele (vezi figura 1). Primul nivel este legat de asigurarea securitatii informatiilor provenite de la clienti în momentul în care acestea sunt transmise de la calculatorul clientului catre serverul Web. Al doilea domeniul sau nivel de securitate se refera la securitatea mediului în care activeaza serverul de

Internet banking si baza de date ce contine informatii confidentiale despre clienti. În sfârsit, cel de-al treilea nivel de securitate implica masurile care trebuie luate pentru a preveni accesul neautorizat al anumitor persoane la sistemul de tranzactionare on-line al site-ului Web respectiv.

Securitatea datelor transmise de programul browser (navigator) al clientului catre serverul Web al bancii este asigurata, precum am mai spus, prin intermediul protocolului de securitate SSL (Secure Sockets Layer), care ofera criptarea datelor, autentificarea serverului si integritatea mesajelor transmise prin conexiunea Internet. De asemenea, SSL asigura existenta unui schimb de informatii între client si server de tip "handshake" care este folosit pentru a initia conexiunea.

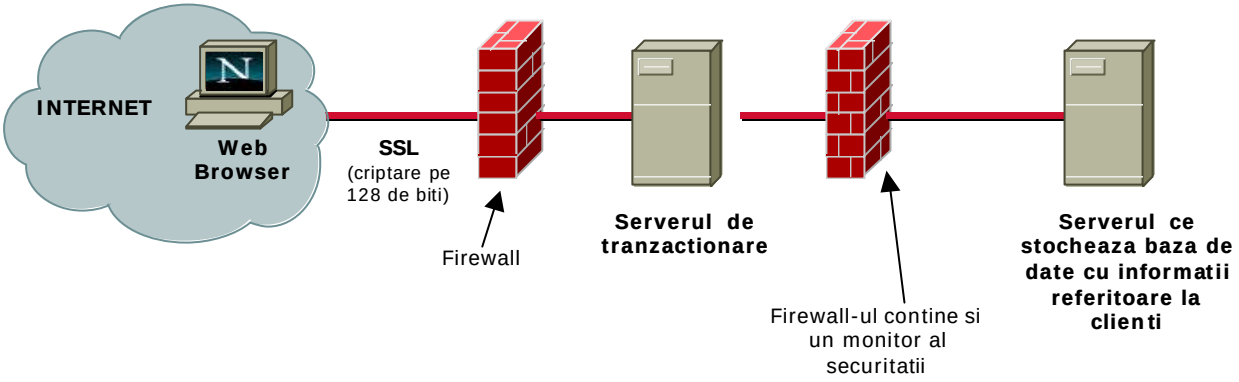

Fig.1. Structura unui sistem de securitate al unei tranzactii bancare în Internet

Cererile legate de date necesare unei tranzactii on-line sunt directionate de la serverul Web catre serverul de tranzactionare bancara. Aplicatia de tranzactionare pe Internet este conceputa pe baza unei arhitecturi arborescente pe trei niveluri, care contine doua firewall-uri ce izoleaza complet serverul Web de informatiile despre clienti aflate în baza de date.

Interfata World Wide Web primeste datele provenite prin intermediul protocolului SSL si trimite cererile respective prin intermediul unui firewall de-a lungul unei retele private dedicate catre serverul de tranzactionare Internet. Aceasta interfata reprezinta unicul proces ce poate comunica prin intermediul firewall-ului cu serverul de tranzactionare Internet, în acest fel asigurându-se faptul ca doar cererile autentificate pot comunica cu serverul de tranzactionare. Baza de date ce contine informatii referitoare la clienti este gazduita de un server ce implementeaza securitatea sistemului de operare folosit (spre exemplu, poate fi folosit ca server de baze de date Microsoft SQL Server si sistemul de operare Windows NT) împreuna cu tehnologia firewall. Baza de date a clientilor trebuie sa fie stocata pe un disc cu sistem avansat de protectie (spre exemplu RAID-5) care sa permita accesul neîntrerupt la date chiar si în cazul unei caderi a hard discului.

În acelasi mod în care interfata World Wide Web este singura ce poate comunica cu serverul de tranzactionare, serverul de tranzactionare este singurul ce poate trimite cereri bazei de date. În acest mod, lumea exterioara este izolata de baza de date cu informatii referitoare la clienti prin intermediul a doua retele private dedicate. Exista, de asemenea, de regula, un monitor al securitatii analizeaza în mod constant încercarile de login si recunoaste esecurile ce pot reprezenta încercari de acces neautorizat la un anumit cont. Atunci când se observa un astfel de incident, se iau masuri corespunzatoare pentru a preveni accesul la acel cont.

Concluzii

Sistemele de Internet Banking ce ofera posibilitatea clientilor unei banci sa acceseze on-line informatii cu privire la situatia conturilor lor sau care le permit sa efectueze plati sau transferuri bancare on-line vor fi, cu siguranta, din ce în ce mai utilizate in lume si la noi în tara. De aceea, sporirea masurilor de securitate privind aceste sisteme este un lucru esential pentru succesul în continuare a acestui tip de servicii bancare oferite de catre o banca clientilor sai.

Împreuna cu toate celelate aplicatii de afaceri pe Internet, printre care comertul electronic, e-banking, e-cash, s.a., sistemele de Internet Banking vor continua sa se dezvolte (la ora actuala la noi în tara exista un singur produs de acest tip oferit de banca BTR), urmând sa apara, desigur, noi plusuri legate de functionalitatea si securitatea acestora.

Bibliografie

- Busschbach Peter – *The Internet Protocol and other things of interest*, Lucent Technologies, 1999
- Leiner M. Barry, Cerf G. Vinton, Clark D. David and others – *A brief History of the Internet*, Internet Society, bleiner@computer.org, 1997
- Medvinsky G., Neuman B. Clifford – *NetCash: A design for practical electronic currency on the Internet*, Proceedings of the first ACM Conference on Computer and Communications Security, USA, 1993
- Prologic Corporation – *i-WealthView Internet Banking*, www.PrologicCorp.com, 2000
- Neuman B. Clifford, Medvinsky Gennady – *Requirements for Network Payment: The NetCheque™ Perspective*, Proceedings of IEEE Compcon '95 San Francisco, USA, 1995