Caracteristici ale securitatii unui sistem informatic pentru managementul resurselor si plasamentelor bancare

Ec. Lucian Claudiu ANGHEL
Banca Comerciala Româna

The security of the informatics system, which is used within banking sector, represents one of the central key elements of the informational architecture existing in any institution. The isolated analysis of the informatics security system is no longer valid in our days, and it is not the best solution, which one institution can find. Having in view this new approach the architecture of the informatics system must take a part of the functions managed previously by an ordinary old type security system.
***Keywords**: architecture of informatics system; access control; audit trail; levels of security; hierarchy of security components; encryption Front-End and Back-End.*

Arhitectura sistemului informatic pentru managementul resurselor si plasamentelor unei banci comerciale trebuie sa asigure atât aplicatiile cât si datele de accesul neautorizat sau rauvoitor. Arhitectura este astfel înzestrata cu algoritmi de criptare, securizarea rutarilor, smart carduri, fire-walls, autentificarea utilizatorilor la nivel de mesaje si la nivel de aplicatie si controlul accesului atât la aplicatii cât si la nivelul retelei, toate acestea genereaza împreuna un nivel de securitate ridicat pentru fiecare tranzactie bancara.

Functiile de securitate

Encriptarea este procesul de codificare a datelor astfel încât originalul sa nu poata fi extras din fisiere fara utilizarea codurilor secrete. Aceasta necesita un algoritm de codificare pentru criptarea si decriptarea datelor. De asemenea, este necesar un mecanism care sa înmagazineze în siguranta codurile secrete pentru codificare. În plus, transferul codurilor secrete trebuie realizat în conditii de maxima siguranta.

Instrumentele de autentificare valideaza sursele de informatie. Câteva dintre tipurile de semnaturi sunt utilizate pentru o identificare unica a sursei. Semnatura poate sa derive de la un cod secret, sau poate pur si simplu sa fie ca o combinatie a identificatorului de utilizator si o parola secreta.

Controlul accesului stabileste care functii sau ce date pot fi accesate de o persoana sau de catre un proces.

Audit trail reprezinta o înregistrare a încercarilor sau a acceselor la functii sau date, reprezentând o secventa a unei înregistrari care permite reconstruirea unor evenimente.

Componentele sistemului de securitate

Asigurarea unui sistem cu mai multe *niveluri de securitate* creste probabilitatea mentinerii integritatii acestuia. Arhitectura sistemului de securitate poate fi împartita în: nivel retea, nivel interfata si nivel aplicatie.

Nu toate elementele pot fi prezente într-un anumit sistem, aceasta depinzând de performantele solicitate de fiecare institutie, de bugetul alocat acestui proiect sau de alte caracteristici specifice. Securitatea poate fi doar o parte a functionalitatii asigurate de anumite componente.

Componentele de securitate pot fi *ierarhizate* în functie de nivelul la care se aplica conform tabelului 1.

Firewall este un sistem destinat pentru monitorizarea si restrângerea dreptului de acces la un set de servicii utilizate de un anumit grup de utilizatori.

Ruterele de retea pot filtra mesaje la un nivel redus si, de asemenea, pot sa le codifice.

Smart cardurile se introduc într-un cititor al unui PC al utilizatorului, care vor genera o parola, ce este autentificata înaintea intrarii în baza de date.
Interfata cu rol de rutare permite o facilitate de tip gateway pentru construirea unui firewall. Aceasta are urmatoarele functii legate de securitate:

- comunicatii sigure, permitând sesiuni între grupuri de utilizatori aflati de o parte si alta a firewall-ului;
- filtrare, specificându-se care mesaje pot fi importate si care exportate;
- login, care poate fi analizat si care poate fi testat în scopul generarii alertelor de încercari potentiale de fortare a sistemului.

Tabel 1 – Ierarhizarea componentelor de securitate

Nivel	***Componenta***	***Functii de securitate***
Retea	Firewall	Controlul accesului
	Ruter	Controlul accesului si encriptare
	Protocol comunicatie	Autentificare
Interfata	Interfata	Encriptare, Autentificare, Controlul accesului, Audit trail
Aplicatie	Smart card User Login Permitere acces Baza de date Login	Encriptare, Autentificare Autentificare Controlul accesului Audit Trail Audit Trail

Procesul de login autentifica utilizatorii prin intermediul identificatorului si al parolei (si un cod PIN când este utilizat un smart card). Identificatorul utilizatorului si parola sunt memorate în baza de date. Administrarea acestei portiuni din baza de date este controlata utilizând *drepturile de acces*.
Fiecare utilizator are definite o serie de drepturi de acces pentru o anumita sesiune. Aceasta informatie este o parte importanta a profilului utilizatorului care este extras din baza de date când un utilizator efectueaza procesul de login si care este utilizat de interfata front-end a sistemului si de alte componente pentru managementul controlului accesului.
Informatia de audit trail este încarcata în baza de date si în plus în anumite situatii si pe o masina pe care se ruleaza o anumita componenta. Multe înregistrari din baza de date contin câmpuri ce retin ora crearii sau modificarii si de catre cine. În plus, anumite tabele sunt create special pentru audit trail.

Encriptarea
Arhitectura trebuie sa permita realizarea encriptarii datelor transferate între interfetele Front-End si Back-End ale sistemului informatic al unei institutii financiar-bancare, adica între datele schimbate cu un sistem informatic exterior dar si în cadrul propriului sistem între diverse componente interne. Software-uri specifice procesului de encriptare se pot utiliza pentru datele transferate între interfata Front-End si serverul de aplicatii sau Front-End Proxy.
Comunicatia între interfata de tip HTML Front-End si HTTP Server poate fi encriptata utilizând standarde de protocoale. Comunicatia între componentele back-end nu este encriptata, constituind o comunicare de informatii si date în interiorul sistemului. În figura 1 este prezentata modalitatea de encriptare a datelor în cadrul unui sistem informatic utilizat în cadrul managementului resurselor si plasamentelor unei banci comerciale.
Aceste caracteristici ale sistemului de securitate sunt generale, fiind adaptate conditiilor concrete fiecarei institutii în parte. Din practica reiese însa dualitatea cost-per-

formanta care de multe ori poate reduce performantele unui sistem de securitate ca urmare a costurilor superioare solicitate. Institutiile financiare ce doresc sa îsi construiasca un sistem informational performant care sa îsi aduca activ aportul la amplificarea pozitiva a rezultatelor economice nu trebuie sa accepte un compromis în sensul alegerii unei securitati inadecvate domeniului în care activeaza. Orice compromis în prezent poate genera în viitor costuri extrem de ridicate – putând conduce chiar la faliment – în urma unei eventuale spargeri a bazelor de date financiare, ceea ce în domeniul bancar echivaleaza cu un colaps financiar, ca urmare a neîncrederii clientilor în siguranta conferita de acea institutie.

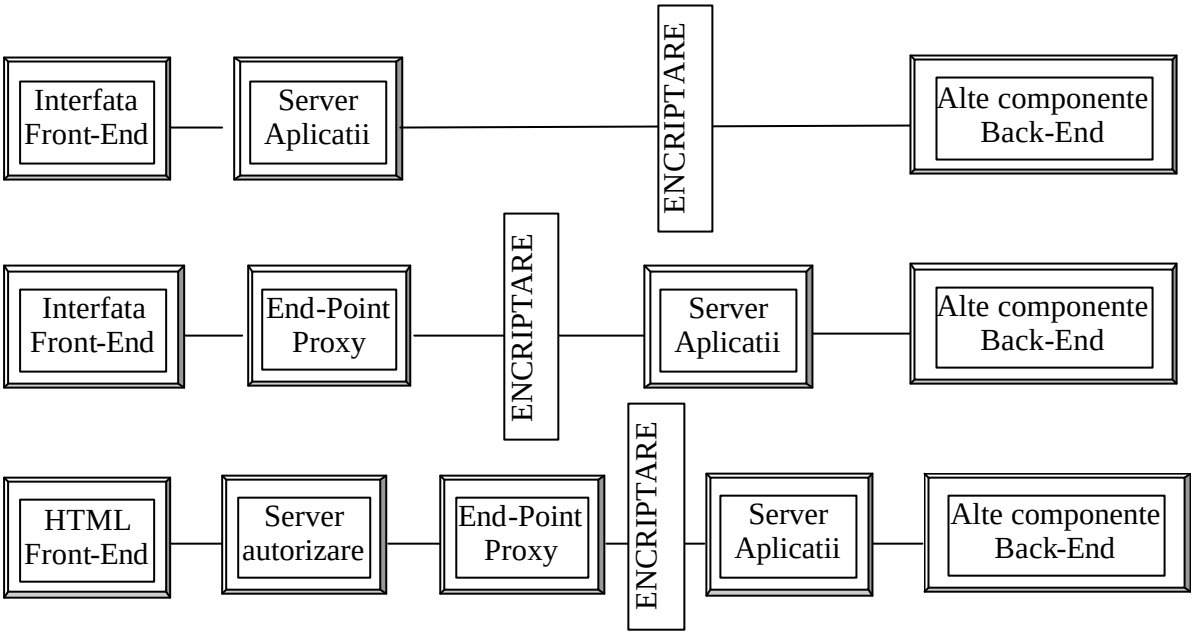

Fig.1. Modalitatea de encriptare a datelor

Bibliografie

1. Anghel L.C., Arhitectura sistemului informatic pentru managementul activelor si pasivelor bancare, Inforec, Bucuresti 1999

2. TIBCO Ltd, Branch and Corporate Foreign Exchange Trading System, TIBCO, London, 2001.