Process Models for Security Architectures

Prof.dr. Floarea NĂSTASE, asist. Radu CONSTANTINESCU
Catedra de Informatică Economică, ASE Bucureşti

This paper presents a model for an integrated security system, which can be implemented in any organization. It is based on security-specific standards and taxonomies as ISO 7498-2 and Common Criteria. The functionalities are derived from the classes proposed in the Common Criteria document. In the paper we present the process model for each functionality and also we focus on the specific components.
Keywords: *security architecture, process model, security functionality, Common Criteria.*

Introducere

Sarcina dezvoltării unor soluţii IT caracterizate de o implementare consistentă şi eficientă a principiilor de securitate prezintă o multitudine de provocări. Dintre acestea amintim: complexitatea integrării funcţiilor specifice de securitate în cadrul unor arhitecturi deja existente în sistemele de calcul, dificultatea dezvoltării unui set comprehensiv de cerinţe de bază pentru securitate şi lipsa unor metodologii de design cu largă acceptabilitate. Una dintre barierele în calea unei abordări unitare pentru dezvoltarea unor arhitecturi de securitate a fost redusă odată cu formalizarea criteriilor de evaluare a securităţii într-un standard internaţional cunoscut sub numele de Criteriile Comune (Common Criteria).

Necesitatea unei metodologii de proiectare a unor soluţii sigure este dată de:

- existenţa nevoii de a dezvolta comunitatea arhitecţilor pentru soluţii de securitate în auspiciile unor perspective comune;
- nevoia sinergiei între disciplinele tehnice aferente specializării de arhitect de securitate;
- nevoia dezvoltării unor proiecte consistente care să poată fi utilizate într-o sumedenie de domenii ale afacerilor ţinând cont că majoritatea cerinţelor sunt comune şi în ideea armonizării proiectelor.

Taxonomii, modele şi metode specifice securităţii

Standardul 7498-2 este un document des asociat cu proiectarea soluţiilor pentru securitatea IT. Scopul său este de a extinde aplicativitatea modelului OSI pentru a asigura comunicaţia sigură între sisteme. Secţiunea 5 din document descrie un set de servicii se securitate şi de mecanisme ce pot fi folosite la nivelurile OSI pentru a satisface cerinţele politicilor de securitate. Secţiunea 8 documentează nevoia pentru managementul serviciilor de securitate OSI şi mecanismele ce includ managementul funcţiilor criptografice, controlul traficului în reţea şi administrarea evenimentelor.

Mulţi dintre specialiştii în securitate utilizează modelul serviciilor de securitate OSI (autentificare, controlul accesului, confidenţialitatea datelor, integritatea datelor şi nonrepudierea) ca şi o taxonomie completă pentru cerinţele de securitate ale soluţiilor informatice. Totuşi, în preambulul standardului ISO 7498-2 se precizează în mod clar că "modelul OSI de securitate nu se preocupă de măsurile de securitate necesare în sistemele finale, instalări sau organizaţii, exceptând cazul când acestea au implicaţii asupra alegerii serviciilor de securitate vizibile în OSI"

Criteriile Comune asigură o taxonomie pentru evaluarea funcţionalităţilor de securitate printr-un set de cerinţe asiguratorii şi funcţionale. Criteriile Comune includ 11 clase funcţionale de cerinţe:

- Auditul de securitate
- Comunicaţiile
- Suportul criptografic
- Protecţia datelor utilizatorului
- Identificarea şi autentificare
- Managementul funcţiilor de securitate
- Intimitatea
- Protecţia funcţiilor de securitate
- Utilizarea resurselor
- Accesul la componente

- Căi şi canale de încredere

Aceste 11 clase funcţionale sunt împărţite la rândul lor în 66 de subclase, fiecare conţinând un număr de criterii componente. La momentul curent există documentate aproximativ 130 de criterii componente. Există un proces formalizat pentru adoptarea unor noi criterii.

Model de sistem pentru securitate

În cazul modelului curent, soluţia IT propusă este conformă cu un model de sistem informatic în reţea (NIS). Etapele pentru crearea modelului sunt: agregarea funcţiunilor apropiate; partiţionarea pe blocuri constitutive; integrarea componentelor şi subsistemelor într-un sistem funcţional.

Modelul sistemului de securitate va fi reprezentat ca o agregare a funcţiilor de securitate, exprimate în termeni de subsisteme şi va înfăţişa modul în care subsistemele interacţionează. Funcţiile legate de securitate din cadrul unui NIS pot fi descrise ca o mulţime coordonată de procese care sunt distribuite în soluţia informatică. Noţiunea de sistem de securitate distribuit vine în întâmpinarea aşteptărilor intuitive conform cărora securitatea în cadrul NIS trebuie să fie una penetrantă.

Pentru modelul curent, Criteriile Comune au fost utilizate pentru descrierea funcţiilor sistemului de securitate. Clasele din Criteriile Comune reprezintă agregări ale cerinţelor sistemului. Pentru a îndeplini obiectivele proiectului, criteriile funcţionale au fost reexaminate şi reagregate.

Pe baza analizei a celor 130 de cerinţe s-a ajuns la împărţirea în cinci categorii operaţionale:

- audit
- controlul accesului
- controlul fluxului
- identitate şi acreditare
- integritatea soluţiei

În tabelul 1 este prezentat modul în care sunt asociate categoriile funcţionale cu clasele din Criteriile Comune.

Tabelul 1. Asocierea dintre Criteriile Comune şi categoriile funcţionale

Categorii funcţionale	Clase funcţionale din criteriile comune
Audit	Audit, protecţia componentelor şi utilizarea resurselor
Controlul accesului	Protecţia datelor, protecţia componentelor, managementul securităţii, accesul la componente, suportul criptografic, autentificarea şi identificarea, comunicaţiile, căi de încredere
Controlul fluxului	Comunicaţiile, suportul criptografic, protecţia datelor, protecţia componentelor, canal de încredere, intimitatea.
Identitate şi credenţiale	Suport criptografic, protecţia datelor, protecţia componentelor, identificarea şi autentificarea, accesul la componente, managementul securităţii, canale de încredere
Integritatea soluţiei	Suport criptografic, protecţia datelor, protecţia componentelor, utilizarea resurselor, managementul securităţii

Cu toate că există o redundanţă aparentă la nivelul claselor, suprapunerea este redusă şi este reprezentată în principal de intersecţia funcţiunilor şi interdependenţele dintre categorii.

Subsisteme de securitate

Cele cinci categorii descrise în Tabelul 1 reprezintă o mulţime de procese interconectate. Cele cinci subsisteme sunt prezentate şi în Figura 1. Funcţionarea şi interdependenţele dintre subsistemele de securitate pot fi la rândul lor modelate. În continuare vor fi prezentate cele cinci subsisteme.

Scopul subsistemului audit de securitate în cadrul unei soluţii IT este să se ocupe de colectarea datelor, analiză şi cerinţe de arhivare conform cu standardele din mediul IT. Auditul de securitate este responsabil cu capturarea, analiza, raportarea, arhivarea şi regăsirea înregistrărilor pentru evenimentele şi condiţiile din soluţia informatică. Subsistemul poate fi constituit dintr-o mulţime finită de componente de sine stătătoare sau o dintr-o mulţime de mecanisme coordonate regăsite cadrul unor anumite componente ale sistemului. Analiza de securitate şi raportarea pot include reviewuri în timp real ca şi în cazul siste-

melor de detectare a intruziunilor sau reviewuri ulterioare folosite, de exemplu, în eventuale probleme juridice. Auditul se poate baza şi pe alte subsisteme de securitate pentru accesul la sisteme, procese sau date, pentru a controla integritatea şi fluxul informaţiei de audit şi pentru a asigura confidenţialitatea datelor de audit. Procesul este reprezentat per ansamblu în Figura 2.

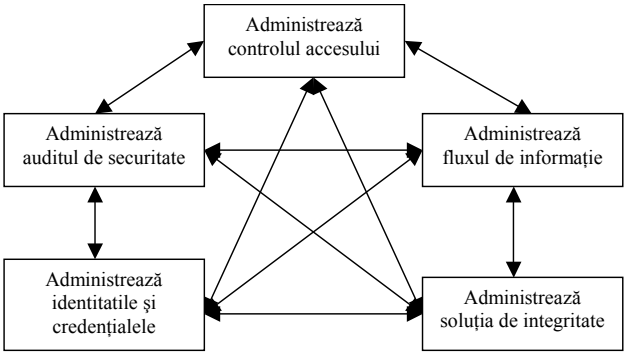

Fig.1. Procesele şi subsistemele de securitate

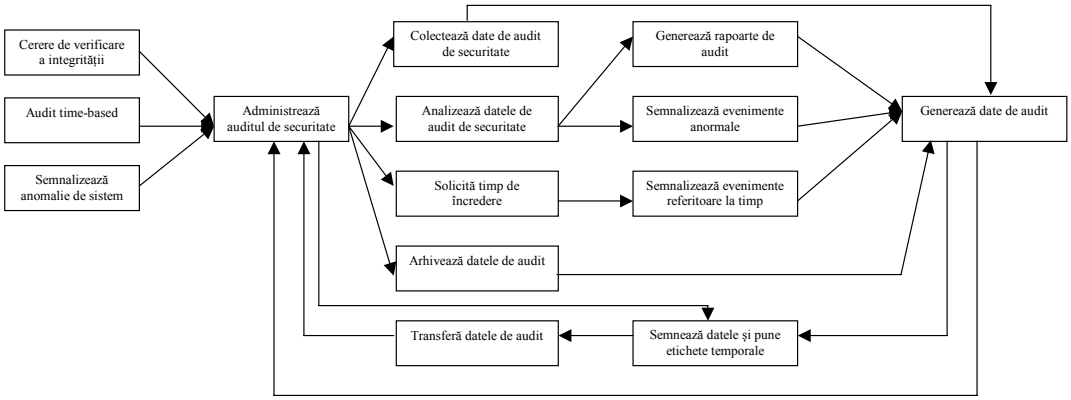

Fig.2. Procesele din subsistemului de audit

Cerinţele pentru subsistemul de audit includ:

- Colectarea de date, incluzând capturarea datelor, transferul sigur al acestora şi sincronizarea cronologiilor.
- Protecţia şi securitatea datelor de audit, incluzând utilizarea unor etichete temporale, semnalizarea evenimentelor şi asigurarea integrităţii stocării pentru a preveni pierderea datelor.
- Analiza datelor de securitate, incluzând reviewul, detecţia anomaliilor, analiza încălcării regulilor şi analiza atacurilor utilizând euristici simple sau complexe.
- Alerte pentru atingerea marjelor pentru pierderi, condiţii de atenţionare şi evenimente critice.

Obiectivul subsistemului integritatea soluţiei în cadrul unei soluţii informatice este să asigure cerinţele pentru operarea corectă şi sigură şi respectarea standardelor tehnice şi legale aferente proceselor. Subsistemul poate fi constituit dintr-o mulţime finită de componente de sine stătătoare sau o dintr-o mulţime de mecanisme coordonate regăsite cadrul unor anumite componente ale sistemului. Subsistemul se poate baza pe cel de audit pentru a beneficia de reviewuri în timp real şi de alerte în cazul unor atacuri sau a unor operaţiuni necorespunzătoare. De asemenea poate folosi raportările post-incident pentru a analiza performanţele. Procesul este reprezentat per ansamblu în Figura 3. Principalele caracteristici ale acestui subsistem sunt:

- Integritatea şi siguranţa resurselor.
- Protejarea fizică a datelor prin chei criptografice sau prin mijloace fizice, cum ar fi cablarea, hardware-ul etc.
- Operarea continuă prin toleranţa la erori, recuperarea în urma acestora şi autotestare.
- Mecanisme de stocare.

- Existența unei surse de încredere pentru furnizarea timpului exact folosit pentru măsurarea intervalelor şi pentru etichetele temporale.
- Prioritizarea serviciilor prin alocarea de resurse şi cote.
- Izolarea funcțională prin separarea domeniilor sau prin monitoare de referință.
- Alarme şi acțiuni atunci când sunt detectate atacuri fizice sau pasive.

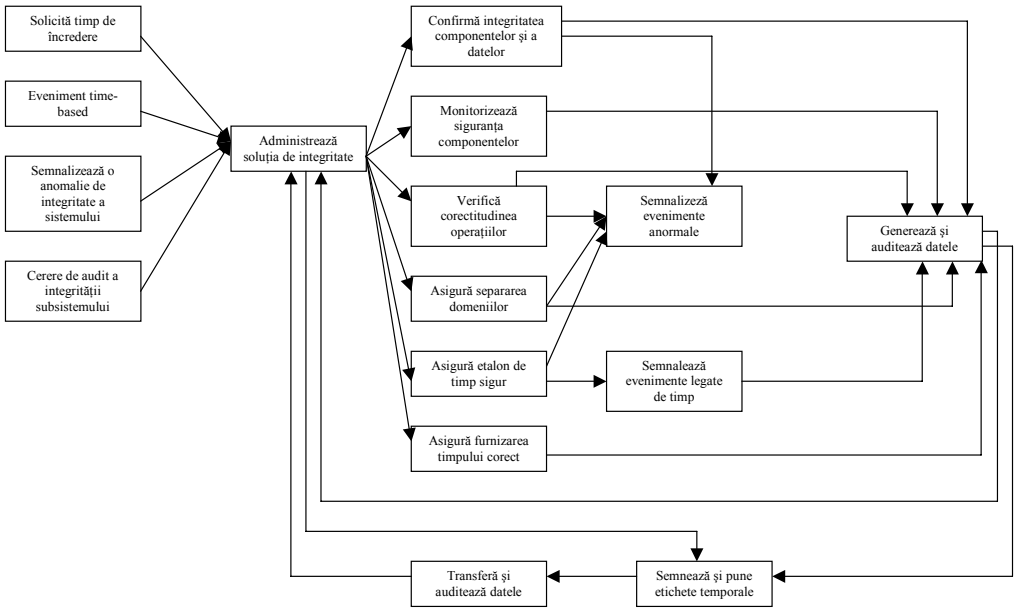

Fig.3. Procesele din subsistemului de integritate

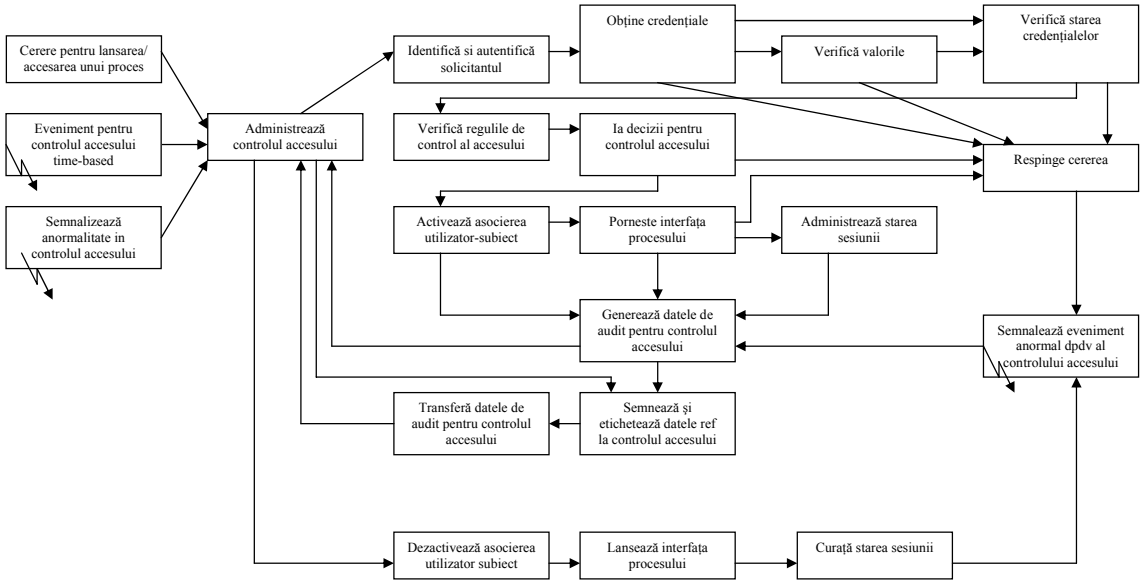

Fig.4. Procesele din subsistemului de control al accesului

Scopul unui subsistem de control al accesului în cadrul unei soluții informatice este să pună în aplicare politicile de securitate prin filtrarea accesului pentru execuția proceselor şi serviciilor prin identificarea, autentificarea şi autorizarea proceselor şi cu ajutorul mecanismelor de securitate care utilizează atribute şi credențiale.

Credențialele şi atributele utilizate de subsistemul de control al accesului împreună cu mecanismele de identificare şi autentificare sunt definite printr-un subsistem corespunzător. Subsistemul de control al accesului poate furniza informații referitoare la evenimentele înregistrate către subsistemul de auditare. De asemenea, poate lua măsuri corective pe baza unor notificări din partea auditului. Procesul este reprezentat per ansamblu în Figura 4.

Cerinţele funcţionale includ:

- Activarea controlului accesului.
- Monitorizarea şi implementarea controlului accesului.
- Mecanisme de autentificare, incluzând verificarea secretelor.
- Mecanisme de autorizare ce includ atribute, privilegii şi permisiuni.
- Mecanisme de control al accesului, incluzând controlul subiectelor şi a obiectelor pe baza atributelor şi asigurarea asocierii între subiecte şi utilizatori.
- Mecanisme de punere în aplicare, incluzând managementul erorilor, prevenirea bypasului, modalităţi de interdicţie, cronometrare şi timeout, capturarea evenimentelor şi deciziilor sau logarea componentelor.

Scopul subsistemului de control al fluxului de informaţie este de a pune în aplicare politicile de securitate prin filtrarea fluxului de informaţii din soluţia informatică, influenţând vizibilitatea informaţiei în cadrul soluţiei şi asigurând integritatea acesteia.

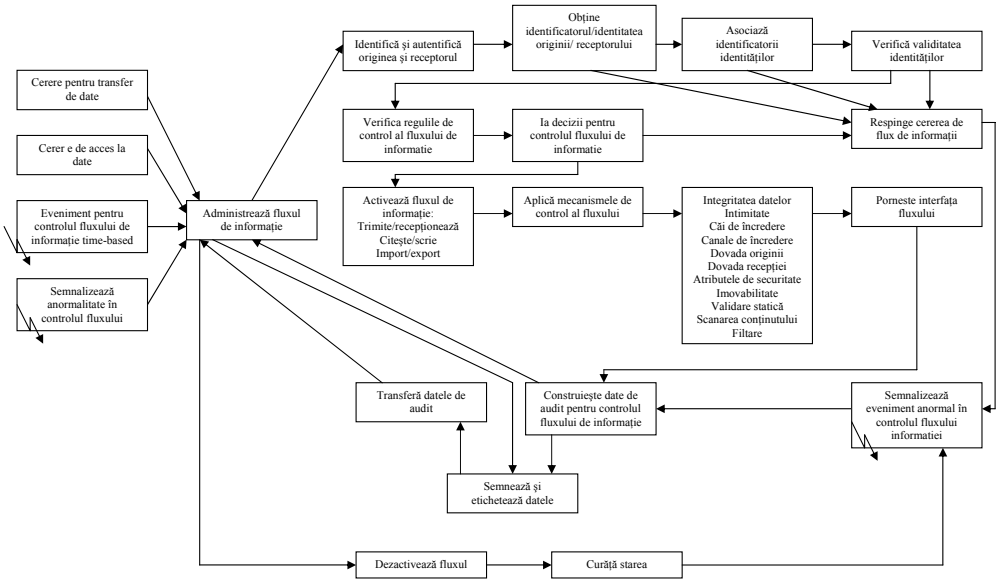

Fig.5. Procesele din subsistemului de control al fluxului de informaţie

Subsistemul este dependent de credenţiale şi de mecanismele de control al accesului. Subsistemul poate furniza informaţii către audit în scopul unor analize în timp real sau pentru analize în scop juridic. Subsistemul poate întreprinde acţiuni corective pe baza notificărilor primite de la subsistemul de auditare. Procesul este reprezentat per ansamblu în Figura 5. Următoarele cerinţe pot fi cuprinse în subsistem:

- Prevenirea sau aprobarea fluxului.
- Monitorizarea sau impunerea fluxului.
- Servicii de transfer şi medii: canale deschise sau sigure, căi deschise sau sigure, conversii media, transfer manual, import şi export între domenii.
- Observabilitatea mecanismelor.
- Mecanisme de stocare.
- Mecanisme de implementare: asocierea activelor şi atributelor, capturarea evenimentelor, logarea deciziilor şi a componentelor, monitorizarea datelor stocate, restaurarea, protejarea şi distrugerea informaţiilor reziduale

Scopul subsistemului de credenţiale este să genereze, să distribuie, şi să administreze datele care transmit identităţi şi permisiuni în cadrul reţelelor şi platformelor, a proceselor şi a subsitemelor de securitate dintr-o soluţie informatică. În unele cazuri, aceste criterii trebuie să fie conforme cu prevederile legale pentru crearea şi mentenanţa identităţilor de încredere utilizate pentru tranzacţii conforme. Subsistemul se poate baza pe alte subsisteme pentru a administra distribuirea, integritatea şi acurateţea credenţialelor. Faţă de celelalte subsisteme, un sistem credenţial are potenţial o legătură directă către activităţile operaţionale de business. Acest lucru se datorează faptului că suportul aferent utilizatorilor este

parte integrantă a procesului de control pe care îl conţine. Procesul este reprezentat per ansamblu în Figura 6.

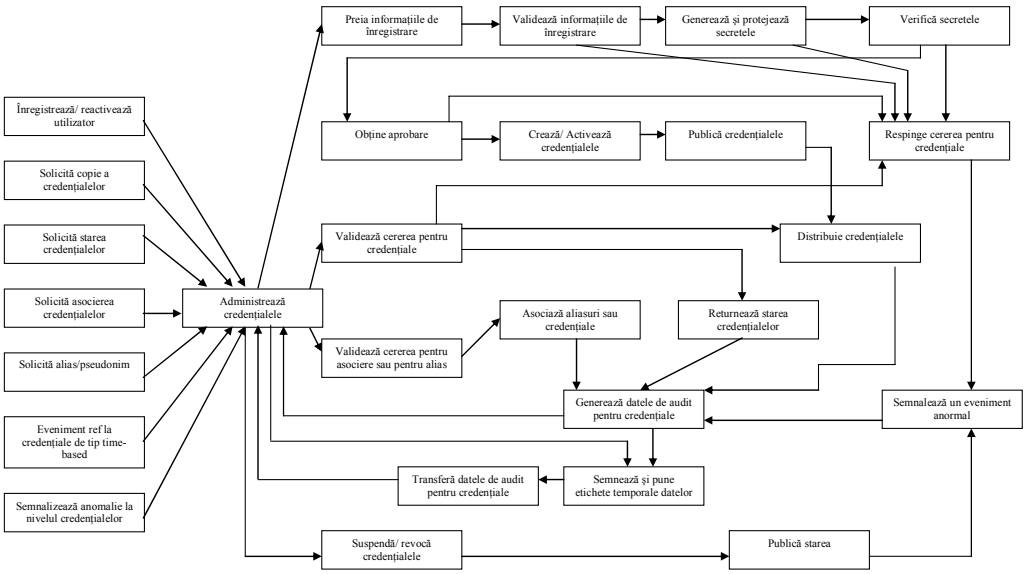

Fig. 6. Procesele din subsistemului pentru autentificare şi credenţiale

Un sistem de credenţiale conţine:

- Generarea şi verificarea secretelor.
- Identităţi şi credenţiale folosite pentru a proteja fluxurile de securitate sau ale proceselor de business.
- Identităţi şi credenţiale folosite pentru a proteja activele: integritate şi non-observabilitate.
- Identităţi şi credenţiale folosite pentru controlul accesului: identificare, autentificare, controlul accesului în scopul asocierii utilizatorilor cu subiectele.
- Credenţiale folosite conform cerinţelor legale pentru identificarea în tranzacţii.
- Cronometrare şi durată pentru identificare şi autentificare.
- Ciclul de viaţă pentru credenţiale.
- Mecanisme de păstrare a anonimităţii.

Cele cinci subsisteme de securitate descrise există la nivel conceptual în cadrul fiecărei soluţii informatice, iar designul, integrarea şi interconectarea serviciilor şi a mecanismelor asociate reprezintă funcţionalitatea de securitate a soluţiei. Modelul trebuie să fie utilizat împreună cu metode de dezvoltare în detaliu a arhitecturii soluţiei.

Concluzii

Referitor la modelele şi procesele propuse pot fi făcute următoarele observaţii:

- Securitatea este o responsabilitate împărţită între toate disciplinele IT.
- În plus faţă de necesitatea protecţiei faţă de atacuri, designul securităţii este legat de obiectivele de business.
- O mare parte a punctelor de control pentru securitate se regăsesc în segmente ale soluţiei IT care nu sunt considerate ca fiind componente de securitate.

Operarea corectă şi sigură a soluţiei folosind protocoale securizate cum ar fi IPSec sau SSL se regăseşte prin funcţii din cadrul tuturor celor cinci subsisteme de securitate definite în modelul propus. Aceste protocoale se bazează pe identităţi de încredere ce utilizează chei criptografice şi presupun integritatea stocării, protocoale sigure pentru schimbul de chei şi rapoarte de audit de încredere. Modelul oferă o nouă perspectivă cu privire la profilele de protecţie în contextul securităţii subsistemelor.

Bibliografie

[Bish03] Bishop, M. - *Computer Security Art and Science*, Ed. Addison-Wesley, 2003

[TiKr02] Tipton, H., Krause, M. - *Information Security Management - Handbook 4th edition*, Ed. Auerbach, 2002;

[BuDe06] Buecker, A., Destro, J., "Enterprise Security Architecture", IBM Redbooks, 2006

[ISO7498] ISO 7498-2 Standard

[CommC] Common Criteria, www.commoncriteriaportal.org