MECANISME ŞI PROTOCOALE DE PROTECŢIA INFORMAŢIEI ÎN REŢELE ŞI SISTEME INFORMAŢIONALE

Claudia HLOPEANICOV

Academia Militară a Forţelor Armate „Alexandru cel Bun" mun. Chişinău, Republica Moldova

***Rezumat**: Investigarea protocoalelor de securitate a informaţiilor în reţele şi sisteme informaţionale reprezintă principalele tipuri de ameninţări privind clasificarea încălcărilor ale securităţii care decurg din utilizarea reţelelor de calculatoare. Consider ca mecanismele, serviciile şi opţiunile de bază pentru implementarea sistemelor de criptare sunt tipuri pentru a asigura autentificarea, integritatea şi confidenţialitatea informaţiilor transmise. Tendinţele prospective în dezvoltarea transformărilor criptografice sunt determinate şi analizate pentru a asigura protecţia informaţiilor în reţelele şi sistemele informaţionale.*

***Cuvinte cheie:** securitatea informaţiilor, criptografie conversii, confidenţialitate, autentificare, integritate algoritmi de criptare a integrităţii datelor.*

Metodele de protecţie a informaţiilor se dezvoltă dinamic, devin mai complexe şi se dezvoltă treptat într-o industrie separată a tehnologiilor informaţionale şi comunicaţiilor. Pentru protecţia informaţiilor cu acces limitat sunt folosite diferite instrumente criptografice. Scopul articolului este de a studia protocoalele şi mecanismele de protecţie a informaţiilor în sistemele şi reţelele informaţionale, analizând direcţiile promiţătoare pentru dezvoltarea transformărilor criptografice pentru a asigura confidenţialitatea, autentificarea şi integritatea informaţiilor.

Problema protejării reţelelor de calculatoare împotriva accesului neautorizat a devenit deosebit de acută. Dezvoltarea tehnologiilor de comunicare permite construirea arhitecturii reţelelor informaţionale distribuită care unesc un număr mare de segmente situate la o distanţă considerabilă una de cealaltă. Toate acestea determină o creştere a numărului de noduri de reţele şi numărul de diferite căi de comunicare între ei, care, la rândul său, creşte riscul de conectare neautorizată la reţea şi accesul la informaţii importante. O astfel de perspectivă poate fi deosebit de nefavorabilă pentru structurile de stat sau militare care deţin informaţii secrete de stat sau de orice altă natură. În acest caz, sunt necesare instrumente speciale pentru a identifica utilizatorii din reţea, asigurând accesul la informaţii numai dacă aceştia sunt pe deplin siguri că utilizatorul are drepturi de acces la acesta. În tabelul 1 prezintă principalele tipuri de ameninţări la încălcarea securităţii care decurg din utilizarea reţelelor de calculatoare. Tabel de analiză nr. 1 arată că toate nivelurile modelului de referinţă ISO/OSI sunt supuse atacului.

Pentru a proteja informaţiile în diferite combinaţii, se utilizează controlul accesului, autorizarea şi criptarea informaţiilor, suplimentate cu redundanţă. Distribuţia serviciilor şi a mecanismelor de securitate pe niveluri ale modelului de referinţă al interacţiunii sistemelor deschise (OSI) sunt prezentate în figura 1 [1,2,4].

Tabelul 1 Caracteristicile ameninţărilor la adresa încălcării securităţii.

Indicatori	**Riscuri**	**Urmările**
Autentificarea	- falsificarea datelor - încercări ale intrusului să se implice unui utilizator legitim.	- experienţă incorectă a utilizatorului. - încrederea în date false.
Integritatea	- schimbarea datelor utilizatorului - schimbarea fluxului de mesaje prin transmiterea	- pierderea datelor informaţionale - compromiterea sistemului informaţional
Confidenţialitatea	- furtul informaţiei păstrat în servere/calculatoare - preluarea informaţiei de configurarea a reţelei	- pierderea datelor - încălcarea secretelor informaţiilor.
Refuzul serviciului	- izolarea sistemului prin atacul pe servere DNS - finisarea sesiunii de accesul utilizatorului	- consecinţele devastatoare pentru sistem - întîrzierea activităţilor de utilizator

Astfel, se iau şi, în considerare mecanismele şi serviciile de bază pentru a asigura autentificarea, integritatea şi confidenţialitatea informaţiilor transmise în reţele şi sisteme informaţionale. Autentificarea asigură faptul că mesajul a provenit efectiv din sursa dorită, precum şi protecţia faţă de modificări, întârzieri,

reluarea şi reordonarea mesajelor. Pentru a asigura autentificarea, se folosesc algoritmi de criptare, semnătură digitală, coduri de autenticitate a mesajelor (MAC) şi funcţii de hash. În permanenţă se pune punctul pe considerarea mecanismelor şi protocoalelor care oferă autentificarea mesajelor în detaliu.

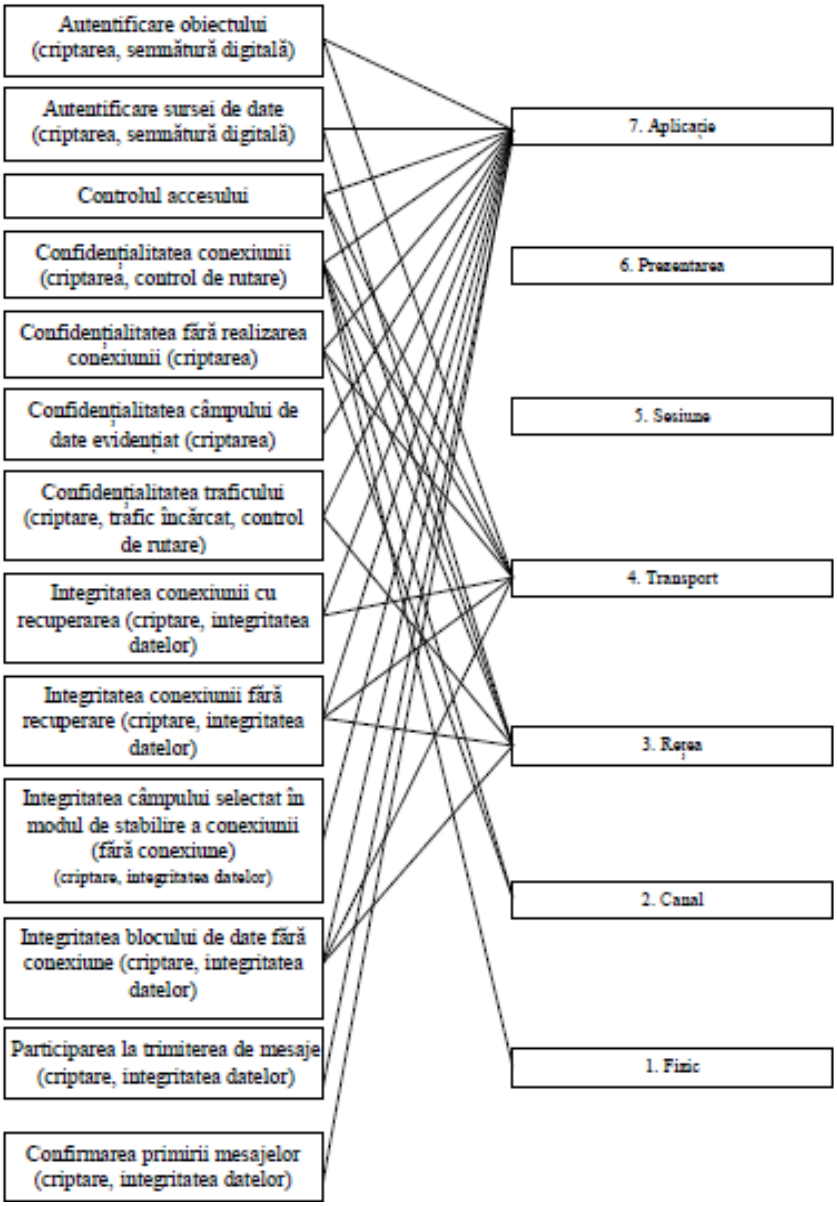

Figura 1 Distribuţia serviciilor şi a mecanismelor de securitate prin nivelurile modelului de referinţă ISO/OSI.

Atunci când se utilizează un algoritmi de criptare simetric, se asigură confidenţialitatea şi un anumit nivel de autentificare. Metodele de criptare asimetrice oferă atât confidenţialitatea, cât şi autentificarea mesajelor transmise.

Putem vorbi despre trei opţiuni pentru protejarea mesajelor utilizând criptarea asimetrică. Prima opţiune - transferul mesajelor cu cheia publică a unui abonat. Acest lucru asigură confidenţialitatea mesajului (numai un abonatul poate avea cheia privată), dezavantajul schemei fiind imposibilitatea de a furniza autentificare (orice abonat poate folosi cheia publică a sistemului pentru a se declara sub nume altuia abonat).

A doua opţiune - utilizarea de către un abonat la trimiterea unui mesaj al cheii sale secrete. În acest caz, sunt furnizate autentificarea şi semnătura digitală (numai primul abonat are cheia secretă). Dezavantajul schemei este capacitatea oricărui utilizator de a utiliza cheia publică pentru a verifica semnătura.

A treia opţiune este utilizarea de către cel puţin doi abonaţi a cheilor lor pentru schimbul de mesaje. Acest lucru asigură confidenţialitatea, semnătura digitală (deoarece se foloseşte cheia publică) şi autentificarea (deoarece se foloseşte cheia privată).

Tot odată se pune accentul pe mecanismele de protecţie utilizând protocolul de Internet (Internet Protocol), care oferă autentificare, confidenţialitate şi gestionarea cheilor.

Pentru a proteja schimbul de date în reţelele locale (LAN), reţelele corporative şi publice (WAN) şi Internetul, se utilizează protocolul IPSec.

Obiectul cheie în mecanismele de autentificare şi confidenţialitate pentru IP este asociaţia de securitate, care asigură protecţia unilaterală a fluxului de date la nivel de transport şi utilizează diferite portocoale: fie protocolul AH (Authentication Header), fie ESP (Encapsulating Security Payload header) antetul de protecţie a încărcăturii). Autentificarea în protocoalele AH şi ESP se bazează pe utilizarea unui cod de autentificare MAC cu o lungime prestabilită de 96 de biţi, iar serviciul de criptare a protocoalelor ESP utilizează algoritmi de criptare : "Triple" DES cu trei chei, RC5, IDEA, "Triple" IDEA cu trei taste, SAST, Blowfish. Protocoalele AH şi ESP susţin două moduri de utilizare: transport şi tunel. Modul de transport este proiectat pentru a proteja protocoalele de nivel înalt şi asigură comunicarea între două noduri informaţionale principale (un utilizator şi un server sau două staţii de lucru). Avantajul modului de transport este acela de a asigura confidenţialitatea pentru orice aplicaţie care utilizează acest mod, ceea ce evită necesitatea implementării funcţiilor de confidenţialitate, în fiecare aplicaţie individuală. Dezavantajul este că utilizarea acestuia nu exclude posibilitatea de a analiza traficul de pachete transmise.

Modul tunel protejează întregul pachet IP şi este util în configurarea reţelei, care necesită o metodă de protecţie, ca de exemplu un firewall sau un gateway de securitate. Avantajul acestui mod este de a descărca nodurile informaţionale reţelei interne de la necesitatea de a cripta datele şi de a simplifica procedura de distribuţie a cheilor. Dezavantajul este complexitatea analizei fluxului de date către o anumită destinaţie.

Analiza protocoalelor şi a mecanismelor de protecţie a arătat că metodele criptografice bazate pe utilizarea algoritmilor de conversie a informaţiilor simetrice şi asimetrice sunt utilizate pentru a asigura autentificarea, integritatea şi confidenţialitatea transmisiei de date în reţelele şi sisteme informaţionale. În acelaşi timp, sporirea în continuare a ameninţărilor/riscuri indică necesitatea unei abordări integrate pentru a asigura protecţia informaţiilor transmise.

Metodele criptografice sunt utilizate în mod tradiţional pentru a construi mecanisme de securitate. Metodele de criptare simetrice se bazează pe blocuri simple şi uşor implementate de permutare a datelor. Metodele de criptografie a cheilor publice se bazează pe utilizarea problemei teoretice şi complexe corespunzătoare (factorizare, logaritmă discretă etc.).

Astfel, studiile au arătat că, pentru a asigura protecţia datelor transmise în reţele de calculatoare, se folosesc seturi de protocoale de securitate care nu asigură pe deplin confidenţialitatea, autentificarea şi integritatea datelor.

O direcţie promiţătoare a soluţionării integrate a problemelor de asigurare a indicatorilor necesari este utilizarea protocoalelor şi a mecanismelor de protecţie a schemelor teoretice şi codurilor pe codurile de bloc algebrice.

Bibilografie

1. Горбенко И.Д., Потий А.В., Терещенко П.И. Ре-комендации международных стандартов по оценке без-опасности информационных технологий // Мат-лы тре-тьей международн. научно-практич. конф. "Безопас-ность информации в информационно-телекоммуника-ционных системах" – К., 2000.-pag. 150-160.
2. Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А. Методологические основы концеп-ции и политики безопасности информационных техноло-гий // Радиотехника. – 2001. – Вып.119. – pag. 5-17.
3. Горбенко И.Д., Потий А.В., Терещенко П.И. Критерии и методология оценки безопасности информа-ционных технологий // Радиотехника.
4. Стасєв Ю.В., Кузнецов О.О., Корольов Р.В. Аналіз існуючих послуг і механізмів захисту інформації // Системи озброєння і військова техніка. – Х.: ХУ ПС. – 2006.– 4(8) – pag. 81-87.
5. Garfinkel,S., and Spafford, G. Web Security & Commerce. Camridge, MA: CTReilly fnd Associates, 1997.
6. Кузнецов А.А., Евсеев С.П. Разработка теоре-тико-кодовых схем с использованием эллиптических ко-дов // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 5. – pag. 127-132.