Angela COȚOFANĂ, MAI

METODE CRIPTOGRAFICE DE PROTEJARE A INFORMATIEI

Abstract: *Communication is important to educating users on different elements of a system, and allowing them to be able to contact you in case of problems. If I take a letter, lock it in a safe, hide the safe somewhere in New York, then tell you to read the letter, that's not security. That's obscurity. On the other hand, if I take a letter and lock it in a safe, and then give you the safe along with the design specifications of the safe and a hundred identical safes with their combinations so that you and the world's best safecrackers can study the locking mechanism – and you still can't open the safe and read the letter – that's security.*

Obiectivul principal al măsurilor de protecție într-un sistem de calcul îl constituie eliminarea posibilităților de distrugere accidentală sau voită a informațiilor, precum şi de consultare nesancționată a acestora. Accesul nesancționat la informații poate provoca serioase daune prin afectarea caracterului privat al transmisiilor, introducerea unor date false sau denaturate, falsificarea identității unor calculatoare, terminale ori utilizatori. Dintre obiectivele importante, care trebuie avute în vedere la proiectarea unor mecanisme-hardware şi software pentru protecția informațiilor într-o rețea, le menționăm pe cele de prevenire a dezvăluirii conținutului clar al mesajelor, a inserării de mesaje false, a analizei traficului de mesaje, precum şi pe cele de detectare a modificării, ştergerii sau înlocuirii conținutului mesajelor, a încercărilor de conectare neautorizată la rețea.

Pentru rezolvarea problemelor asigurării securității în rețelele informațional-telecomunicaționale este necesar:

1. A proteja informația la păstrarea, prelucrarea şi transmiterea ei prin rețea;
2. A confirma veridicitatea obiectelor de date şi a utilizatorilor (autentificarea părților care fac legătura);
3. A descoperi şi a preveni încălcarea integrității obiectelor de date;
4. A proteja mijloacele tehnice şi încăperile;
5. A proteja informația confidențială de scurgere de date;
6. A proteja aplicațiile de program de viruşi;
7. A proteja resursele informaționale şi mijloacele tehnice ale rețelei de accesul nesancționat;
8. A organiza acțiunile necesare orientate spre păstrarea datelor confidențiale.

Una dintre cele mai vechi metode de protejare a informației este criptografia. ***Criptografia*** se ocupă cu cifrarea(codificarea) informației pentru a exclude accesul nesancționat de alte persoane. Ca rezultat, prin canalele de telecomunicații se transmite rezultatul modificat al informației inițiale, adică în urma aplicării unui algoritm de cifrare electronic. Ca artă a codificării şi cifrării informației, criptografia există câteva milenii.

Obiectivul de bază al unui sistem criptografic este a face extrem de dificilă decriptarea unui mesaj pentru care nu se cunosc cheile potrivite. Pentru atingerea acestui obiectiv, proiectarea este confruntată cu două cerințe contradictorii: să asigure o criptanaliză foarte dificilă şi să certifice nivelul de securitate realizabil. Securitatea este rezultatul comportamentului ipotetic al adversarului şi nu este garantată printr-un proiect care să includă măsuri specifice de contracarare a atacurilor anticipate. În prezent, se preferă criptarea care operează în mod repetat, în multe runde, asupra unui bloc de simboluri din mesajul de transmis. Aceste coduri sunt de tipul *bloc cu iterații*. Este o idee naturală, simplă şi eficientă, care împacă, cel puțin parțial, simplitatea şi complexitatea.

Strategiile de encriptare, folosite în prezent, se bazează pe presupusa complexitate a unor probleme matematice ce pot fi rezolvate pe computer. Un mesaj este encriptat bine dacă, pentru a sparge codul, un hacker are nevoie de foarte mult timp şi de resurse mari. Însă, pe măsură ce computerele devin din ce în ce mai performante, mesajele encriptate devin din ce în ce mai uşor de spart. În plus, problemele matematice pe care se bazează criptografia se dovedesc uneori a fi **mai puțin complexe decât se crezuse până atunci**.

Criptografia cuantică este cu totul altfel. Ea nu se bazează pe presupusa complexitate a unei probleme matematice, ci pe principii fizice – mai exact, pe principiul de incertitudine al lui Heisenberg. Acest principiu spune că, dacă măsori o anumită proprietate cuantică, vrei nu vrei, vei modifica într-o anumită măsură o altă proprietate cuantică. Lumea cuantică este de aşa natură, încât nu există aşa ceva precum proprietăți complet independente de orice alte proprietăți.

Ideea de baza este că, atunci când un hacker încearcă să observe ce anume a transmis cineva, el/ea va schimba în mod inevitabil mesajul transmis. Prin urmare, în condițiile în care comunicarea este bazată pe acest aspect fundamental al lumii cuantice, nici un hacker nu ar putea sa intercepteze un mesaj fără ca acest lucru să fie detectat.

„Criptografia cuantică încearcă să facă comunicarea mai sigură, ceea ce ar fi foarte util pentru sistemul bancar, de exemplu", a spus profesorul Hoi-Kwong Lo, un expert în fizică şi inginerie de la Centrul pentru Informatică Cuantică şi Control Cuantic de la Universitatea Toronto şi unul dintre autorii unui nou studiu despre aceasta tehnică. „Ideea poate fi acum implementată, pentru că noi chiar am reuşit să facem experimentul cu un aparat comercial".

Studiul descrie prima dovadă experimentală a unei tehnici de encriptare a datelor transmise prin fibre optice, bazată pe „momeli” cuantice. Mesajul a fost purtat de lumina laser prin fibra optică de-a lungul unui cablu de telecomunicații de 15 kilometri. Tehnica presupune variația intensității fotonilor şi introduce aşa-numite „momeli” fotonice. După ce semnalul a fost trimis, este expediat şi un al doilea mesaj, care spune ce fotoni conțineau mesajul şi ce fotoni erau „momeală”.

Daca un hacker încearcă să „tragă cu ochiul” la mesaj pentru a descifra codul, simplul act de „a trage cu ochiul” schimbă fotonii-momeală – un semn clar pentru computerul care primeşte mesajul că cineva neautorizat a intrat pe fir.

Rămâne să sperăm că se va găsi un geniu matematic care să rezolve problema securității datelor folosind mecanica cuantică!