Semnaturi digitale în alb

Alin Titus PÎRCALAB

The appearing and continuous development of computer use in each and every field of activity, the existence and powerful revolution of international and national network, communication globalization are only a few of the informational premises of our society we are now stepping into. All these show a huge increase of the volume and importance of transmitted and storage data and eventually of their vulnerability (exposure). An important part in protecting these data has cryptology and special digital signatures. Out of these the blind signatures have an increasing development lately.
Keywords: *cryptography, message, signature, digital signature, blind (white) digital signature.*

Terminologie

Criptografia este stiinta crearii si mentinerii mesajelor secrete, în sensul imposibilitati citirii lor de catre neautorizati (stiinta mesajelor secrete). *Mesaj în clar* (M) este mesajul care urmeaza a fi secretizat. În criptografie M se mai numeste scriere chiar daca este un document de alta natura. *Mesaj cifrat* (criptograma) (C) este mesajul secretizat, inaccesibil neavizatilor. *Criptare/cifrare* (F) este procedeul de „ascundere" a unui mesaj în clar în mesajul secretizat: E(M)=C. *Decriptare/descifrare* (D) este procedeul de regasire a mesajului în clar M din mesajul cifrat C: D(C)= D(E(M))= M. *Criptograf* este persoana care se ocupa cu criptografia. *Algoritm criptografic/cifru* este functia sau functiile matematice utilizate pentru criptare/decriptare. În general exista doua functii: una pentru criptare (E) si alta pentru decriptare (D). *Cheia criptografica* (K) este marimea (în majoritatea cazurilor secreta) necesara realizarii criptarii si decriptarii. *Criptosistemul* este sistemul format din algoritm, toate mesajele în clar (M), toate textele cifrate (C) si toate cheile (K). *Criptanaliza* este stiinta obtinerii mesajelor în clar (M) sau a cheii (K) din mesajul cifrat (C). *Criptanalist* este persoana care se ocupa cu criptanaliza. *Atac* este încercarea/tentativa criptanalitica. *Criptologia* este stiinta care se ocupa atât de criptografie cât si de criptanaliza. *Criptologul* este persoana care se ocupa cu criptologia. *Steganografia* este tehnica ascunderii mesajelor secrete în alte mesaje, în asa fel încât existenta mesajelor secrete sa fie invizibila. *Protocolul criptografic* este un protocol în care este implicat cel putin un algoritm criptografic. *Scopul* unui protocol criptografic este de a nu permite sa se faca sau sa se învete mai mult decât este specificat în protocol.

Protocoale în care intervin probleme de securitate si încredere se aplica în viata de zi cu zi aproape pentru orice situatie: cumparaturi, vot, joc etc. Forma lor este foarte simpla pentru ca presupune prezenta oamenilor. În momentul în care activitatile de zi cu zi se transpun pe retele de calculatoare, interactiunile umane fata în fata se reduc si trebuie luate în considerare o serie de probleme noi ce complica protocolul în vederea realizarii unei anumite sarcini.

Ce este o semnatura digitala?

Semnatura olografa este o proba a calitatii de autor al unui document, sau cel putin de acord cu continutul documentului. Proprietatile unei semnaturi olografe sunt:

1) Semnatura sa fie autentica, adica sa aiba calitatea de a convinge destinatarul ca semnatarul a semnat documentul în mod deliberat.
2) Semnatura sa nu poata fi refolosita, ceea ce înseamna ca semnatura este parte a documentului.
3) Documentul semnat nu poate fi modificat.
4) Semnatura nu poate fi repudiata.

Semnaturile digitale trebuie sa pastreze cerintele 1) ÷ 4), transpuse în comunicatia din re-

tele de calculatoare.

Observatie: Exista destule situatii în care cerintele 1) ÷ 4) nu se respecta pentru o semnatura olografa, dar nerespectarile sunt mult mai greu de realizat decât în cazul calculatorului, la care *copy* si *paste* sunt comenzi atât de uzuale.

Cele patru cerinte, transpuse în mediul digital se rezuma la doua cerinte de baza pentru o semnatura:

(1) sa depinda de mesaj pentru a nu fi mutata de pe un mesaj pe altul (aceasta cerinta nu apare în cazul semnaturii olografe pentru ca nu este cazul);

(2) sa depinda de emitator pentru a nu putea fi falsificata.

Semnatura digitala S este o succesiune de biti obtinuta din transformarea mesajului (M) si a unei informatii secrete, stiute doar de emitator. Orice semnatura digitala trebuie sa poata fi verificata, rezultatul acestei functii putând fi doar „adevarat" sau „fals". În cele ce urmeaza vom folosi notatiile:

- S_A - transformarea de semnare pentru entitatea A (ea este secreta);
- V_A - transformarea de verificare pentru entitatea A (ea este publica);
- $\{S_A, V_A\}$ - perechea de transformari care defineste schema (mecanismul) de semnatura digitala;
- v - rezultatul verificarii {adevarat, fals}.

Protocolul de semnare este:

(1) A calculeaza $S = S_A(M)$ care este semnatura mesajului M (folosind o cheie secreta);

(2) A transmite perechea {M, S}.

Protocolul de verificare este:

(1) Verificatorul (B) obtine functia de verificare a lui A: V_A, care este publica;

(2) B calculeaza. functia de verificare $v = V_A(M,S)$;

(3) B accepta ca S apartine lui A daca v = adevarat si o refuza daca v = fals.

Pentru functiile de semnare, respectiv de verificare, se cer proprietatile:

(a) S este o semnatura valida a lui A asupra mesajului M daca si numai daca: $V_A(M,S)$ = adevarat;

(b) este imposibil de determinat pentru altcineva decât A un M si S astfel încât: $V_A(M,S)$ = adevarat.

Observatie: Semnaturile trebuie sa fie verificabile pentru ca în caz de conflict sa nu poata fi repudiate sau reclamate în mod fraudulos. Un arbitru trebuie sa poata rezolva disputa fara a avea nevoie de cheia privata a lui A. Exemple de aplicatii pot fi autentificare, integritatea datelor, nonrepudiere, certificarea datelor publice în retele mari etc.

Printre realizarile în domeniu se pot aminti:

- exista numerosi algoritmi pentru semnaturi digitale, toti necesitând informatie secreta pentru semnare si informatie publica pentru verificare;
- în cazul algoritmilor cu chei publice, cheia privata folosita la criptare (D_A) poate fi folosita la semnare, iar cheia publica folosita la criptare (E_A) poate fi folosita pentru verificare (cazul algoritmului RSA) ;
- în cazul altor algoritmi, implementarile pot fi diferite ; de exemplu, pentru algoritmii bazati pe functii hash (de rezumare) si cu cerificare temporala (TS) se adauga pasi suplimentari pentru semnare si verificare;

Semnaturile în alb

O trasatura esentiala a protocoalelor cu semnaturi digitale este ca semnatarul cunoaste ceea ce a semnat. Exista situatii în care anumite persoane semneaza documente fara sa fi vazut niciodata continutul acestora. Sunt cai prin care semnatarul poate cunoaste aproximativ, dar nu exact, ceea ce semneaza. Astfel, exista doua situatii posibile:

1) Semnaturi complet în alb

Exemplu:

B - notar public;

A - doreste ca B sa semneze un document, dar nu doreste ca B sa stie continutul documentului; pe B nu-l intereseaza continutul documentului, doar certifica ca acesta a fost notarizat.

Protocolul de semnare se desfasoara astfel:

(1) A ia documentul si îl aleatorizeaza; aceasta valoare aleatoare se numeste factor de ascundere;

(2) A trimite documentul „ascuns" lui B;

(3) B semneaza documentul „ascuns";

(4) A înlatura factorul de ascundere (dezaleatorizeaza documentul), obtinând documentul original semnat de B.

Proprietatile unei semnaturi complet în alb:

1) semnatura lui B pe document este valida; semnatura este dovada ca B a semnat documentul si are toate proprietatile unei semnaturi digitale;

2) B nu poate corela documentul semnat cu actul de semnare propriu-zis; chiar daca el ar tine o copie a tuturor semnaturilor în alb acordate, el nu ar putea determina când anume a semnat un anumit document.

Un exemplu de risc al semnaturilor complet în alb poate fi: A îl poate face pe B sa semneze orice, de exemplu „B datoreaza lui A 1.000.000 $".

2) Semnaturi în alb

Pentru a evita riscul mentionat anterior se va cauta o cale în care B sa stie ce semneaza, mentinând în acelasi timp si proprietatile utile ale semnaturii în alb. Principiul folosit este *taie si alege*, ilustrat de exemplul controlului vamal. Controlul se face utilizând o solutie probabilistica, adica se controleaza o persoana din 10, celelalte noua nefiind controlate. Pedeapsa în cazul unei fraude este atât de mare încât sa descurajeze tentativa de frauda.

Semnatura în alb lucreaza ca în exemplul anterior. Lui B i se va da un numar mare de documente "ascunse" la semnat. El va deschide tot, exceptând ultimul document pe care îl semneaza fara a-l deschide. Documentul ascuns se afla în plic. Procesul de ascundere echivaleaza cu punerea documentului în plic. Procesul de înlaturare a factorului de ascundere poate fi comparat cu deschiderea plicului.

Un alt exemplu de utilizare de semnaturi în alb este agentia de contraspionaj. Fie un grup de agenti de contra-spionaj. Identitatea lor este secreta chiar si pentru agentie. Directorul agentiei vrea sa dea fiecarui agent un document semnat care sa-i ofere imunitate diplomatica. Fiecare agent are propria lista cu nume de acoperire si nu doreste ca agentii sa o cunoasca, de teama spargerii calculatorului agentiei. Pe de alta parte agentia nu doreste sa semneze în alb absolut orice document pentru a preîntâmpina situatii de genul: "Agentul X a fost pensionat si pensia anuala este de 1.000.000 $". Presupunem ca fiecare agent are 10 nume de acoperire cunoscute doar de el. Algoritmul are doua variabile: A – calculatorul agentiei si B – agentul sub acoperire. Protocolul de semnare în alb decurge astfel:

(1) B pregateste *n* nume, fiecare cu alt nume de acoperire, care îi confera imunitate diplomatica.

(2) B aleatorizeaza fiecare document cu un factor de ascundere diferit.

(3) B trimite cele *n* documente ascunse lui A.

(4) A alege *(n-1)* documente la întâmplare si îi solicita lui B factorii de ascundere.

(5) B trimite lui A cei *(n-i)* factori de ascundere solicitati.

(6) A deschide cele *(n-i)* plicuri, deci înlatura factorul de ascundere si se asigura de continutul acestora.

(7) A semneaza ultimul document nedeschis si-l trimite lui B.

(8) B înlatura factorul de ascundere si citeste noul nume de acoperire ce-i asigura imunitate diplomatica.

Bibliografie

1. Angheloiu, I., Gyorfi, E., Patriciu, V.V. (1986): *Securitatea si protectia informatiei în sistemele electronice de calcul*, Editura Militara, Bucuresti;
2. Angheloiu, I., *Teoria codurilor*, Editura Militara, Bucuresti (1972);
3. Borda, M., *Teoria transmiterii informatiei*, Dacia, Cluj-Napoca (1999);
4. Deavours, C.A., Kahn, D., *Selections from Cryptology*, Artech House (1998);
5. Hankerson, D. R., Hoffman, D. G., Leonard, D. A., Linder, C., *Coding Theory and Cryptography: The Essentials (Pure and Applied Mathematics*, Vol 234), Marcel Dekker, Rev&ex, 2nd edition, Sep. (2000);
6. India International Conference in Cryptology in India 2000 Calcutta (2000): *Progress in Cryptology*, Indocrypt 2000 Proceedings of the First International Conference in Cryptology Calcutta, Springer Verlag, Dec.;
7. McCurley, K. S., Ziegler, C. D. (1999):

Advances in Cryptology, 1981-1997 Electronic Proceedings and Index of the Crypto and Eurocrypt Conferences 1981 - 1997 (Lecture Notes in Computer Science), Springer Verlag, Jun.;
8. Patriciu V.V. (1998): *Securitatea informatica în UNIX si Internet*, Editura Tehnica, Bucuresti;
9. Patriciu, V. V. (1994): *Criptografia si securitatea retelelor de calculatoare*, Editura Tehnica, Bucuresti;
10. Stallings, W. (1999): *Cryptography and Network Security — Principles and Practice*, Prentice Hall, Second Edition;
11. T.I. Bajenescu, M.E. Borda – Securitatea în informatica si telecomunicatii; Ed. Dacia, Cluj-Napoca, 2001;
12. V.V. Patriciu, M. Ene-Pietrosanu – Securitatea Comertului Electronic – Ed. All, Bucuresti, 2001;
13. V.V. Patriciu, M. Ene-Pietrosanu – Securitatea în Informatica în UNIX si Internet – Ed. Tehnica, Bucuresti, 1998;