Noi tehnologii privind securitatea Internet-lui

Prof.dr.Victor-Valeriu PATRICIU, Academia Tehnica Militara, Bucuresti
Ing. Monica ENE-PIETROSANU, Microsoft Corporation, Public Key Security Group

Lucrarea analizeaza câteva din aplicatiile criptografiei computationale cu chei publice în dimeniul comertului electronic si al distributiei sigure a documentelor si software-ului. Deoarece autenticitatea documentelor si a programelor schimbate sau distribuite prin retele reprezinta o cerinta de securitate fundamentala, articolul îsi propune sa evidentieze utilizarea noilor paradigme privind semnãturile digitale individuale ºi de grup în autentificarea tranzactiilor desfasurate în Internet.
Cuvinte cheie: *criptografie, securitate, chei publice, chei private, semnatura.*

1 Semnatura digitala

Orientarea a tot mai multe activitati u-mane catre utilizarea tehnologiilor infor-matice face ca în Internet omenirea sa se regaseasca cu *trasaturile* ei definitorii, atât dintre cele pozitive cât si negative. Ca ur-mare, oamenii sunt preocupati nu numai de folosirea eficienta si dezvoltarea continua a domeniului tehnologiei informatiei si al Internet-ului ci si de *stabilirea cadrului legal* în care sa se desfasoare interactiunile în acest domeniu, numit si *Cyberspace* sau *Global Village*. Cunoasterea diferitelor legi ce guverneaza Internet-ul si hotarârea co-munitatii internationale de a acoperi toate golurile legale ale acestei noi lumi si de a le armoniza, este una foarte actuala. Inter-net-ul este o structura si în acelasi timp o societate care, cu exceptia unor parametrii tehnici, se dezvolta liber si neîngradit în raport cu prevederile legale ale statelor pe teritoriul carora se afla server-ele retelei.

Un element esential al acestei perioade, când hârtia tinde sa devina tot mai mult un mijloc secundar de prezentare a docu-mentelor, calea de transport si arhivare fiind cea electronica, îl reprezinta înlocu-irea mijloacelor de autentificare a docu-mentelor electronice cu servicii noi, adap-tate noilor tehnologii informationale. În acest cadru, un rol esential îl are **sem-natura electronica**, mijlocul de auten-tificare a continutului unui document elec-tronic sau software si a emitentului aces-tuia. Rolul este decisiv în derularea tranzactiilor specifice comertului electro-nic.

Multa vreme **semnaturile olografe ("de mâna")** au fost folosite pentru a proba ca o anumita persoana este de acord cu un anumit document.

Cerintele generale ce se pun în fata unei semnaturi sunt urmatoarele:

1. sa fie *autentica*, adica executata de autorul documentului;
2. sa fie *nefalsificabila*, adica sa dove-deasca ca documentul a fost produs de pre-tinsul semnatar;
3. sa *fie nereutilizabila*, adica sa nu poata fi mutata, de catre o persoana rau inten-tionata, pe un alt document;
4. sa fie *nealterabila*, adica odata docu-mentul semnat, acesta sa nu poata fi modi-ficat;
5. sa fie *nerepudiabila*, adica semnatarul sa nu mai recunoasca autenticitatea ei.

Noile servicii Internet si în special comer-tul electronic, au creat necesitatea unui serviciu permanent de **semnatura electro-nica (digitala)** care, realizata prin mijloace electronice, sa garanteze tranzactiile Inter-net:

- sa permita identificarea unei persoane fara a o întâlni;

• sa creeze o proba, irefutabila în fata unei autoritati, a tranzactiei încheiate si execu-tate.

În realitate, desi a fost folosita mii de ani, semnatura olografa nu respecta întrutotul aceste deziderate. Cu atât mai mult, ata-sarea unor semnaturi scanate la documen-tele electronice face banal procesul de fal-sificare. Ca urmare, *s-a creat un* ***tip de semnatura electronica****,* numita si ***digitala****, si care se realizeaza folosind* ***metode crip-tografice cu chei publice****.* În literatura de specialitate nu se face, de cele mai multe ori, distinctia dintre termenul de semnatura electronica si cel de semnatura digitala, ti-nând cont de faptul ca tehnologia cea mai folosita în realizarea semnaturilor electro-nice o constituie azi criptografia.

Sistemele criptografice cu chei publice (a-simetrice) "inventate" de Diffie si Hell-man, de la Univeritatea Stanford, folosesc un principiu diferit de acela al cifrarii "clasice": în locul unei singure chei secrete, criptografia asimetrica foloseste doua chei diferite, una pentru cifrare, alta pentru descifrare . Una din chei-**cheia privata (PRIV)**- este tinuta secreta si este cunoscuta doar de proprietarul ei. A doua cheie (perechea ei)- numita **cheie publica (PUB)**- este facuta publica, de unde si numele de criptografie cu cheie publica. Ambele chei sunt de fapt niste siruri de biti, furnizate de un program capabil sa genereze aceste perechi. Daca cheia publica o puteti da oriunde în lume, pe cea privata trebuie sa o pastrati la loc sigur. Pentru a se asigura **confidentialitatea** unui mesaj, datele sunt cifrate la emisie cu cheia publica a receptorului. Ele pot fi descifrate doar de catre destinatarul autentic, cu cheia lui privata.

Daca însa se doreste **semnarea digitala (e-lectronica)** a datelor în vederea verificarii autenticitatii, datele sunt prelucrate astfel (vezi figura 1):

[1] Documentul *M* este cifrat cu cheia privata a emitatorului, care astfel semnea-za; în exemplul nostru este vorba de uti-lizatorul *Dan* care furnizeaza, prin interme-diul unui card, cheia sa secreta, $PRIV_{Dan}$.

[2] Documentul este trimis la receptor;

[3] Receptorul verifica semnatura prin de-criptarea documentului cu cheia publica a emitatorului.

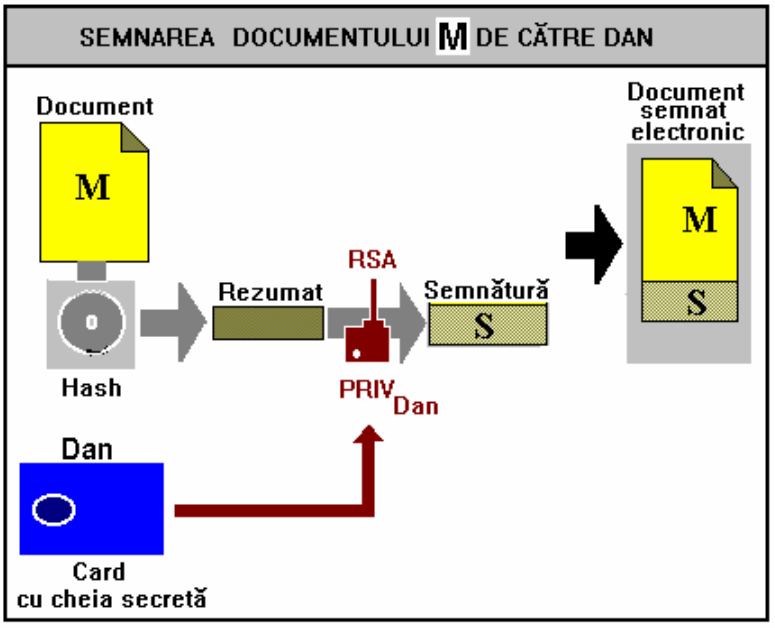

Fig. 1 - Semnarea unui document electronic sau software

Protocolul de semnatura electronica satis-face mai bine conditiile prezentate anterior:
1. semnatura este *autentica* deoarece se verifica numai cu cheia publica a emita-torului;
2. semnatura este *nefalsificabila* deoarece numai emitatorul cunoaste cheia secreta proprie;
3. semnatura este *nereutilizabila* deoarece ea este functie de continutul documentului, cel care este criptat;
4. semnatura este *nealterabila* deoarece orice alterare a continutului documentului face ca semnatura sa nu mai fie verificabila cu cheia publica a emitatorului;
5. semnatura este *nerepudiabila* deoarece receptorul documentului nu are nevoie de ajutorul emitatorului pentru verificarea semnaturii.

În concluzie, **semnatura digitala (electro-nica)** reprezinta un atribut al unei persoa-ne, fiind folosita pentru recunoasterea aces-teia. Semnatura digitala rezolva atât pro-blema *autentificarii emitatorului* cât si pe cea a *autentificarii* documentului (numita si integritate).

2. Schema de semnatura Rivest-Shamir-Adleman (RSA)

Acest sistem criptografic cu chei publice, realizat de trei cercetatori de la Massa-chusetts Institute of Technology, reprezinta standardul "de facto" în domeniul semnatu-rilor digitale si al criptarii cu chei publice. El se bucura de o foarte mare apreciere atît în mediul guvernamental cît si în cel co-mercial, fiind sustinut prin lucrari si studii de comunitatea academica. Sub diferite forme de implementare, prin programe sau dispozitive hardware speciale, RSA este astazi recunoscuta ca cea mai sigura meto-da de cifrare si autentificare disponibila co-mercial.

RSA este bazat pe cvasi-imposibilitatea a-ctuala de a factoriza numere (întregi) ma-ri; fuctiile de criptare/decriptare sunt de tip exponential, unde exponentul este cheia iar calculele se fac în inelul claselor de resturi modulo n.

Parametrii sistemului

-**p** si **q** sunt doua numere prime foarte mari secrete (de exemplu de 100 de cifre zeci-male).

-**modulul n,** facut public, este obtinut prin produsul (secret) al celor doua numere pri-me mari:

$$n = p * q$$

Securitatea metodei depinde de dificultatea factorizarii lui n în p si q. Rivest, Shamir si Adleman sugereaza utilizarea unor numere prime p si q de 100 cifre zecimale, adica a unui n de 200 de cifre zecimale, ceea ce cere pentru factorizare mai multe milioane de ani calculator.

-**indicatorul lui Euler** j **(n)=(p-1)*(q-1);** imposibil de determinat de un atacator, întrucât nu se cunosc factorii primi ai lui n, p si q;

-**cheia secreta**, ***PRIV,*** aleasa ca un întreg relativ prim cu *j (n),* preferabil în intervalul [max(p,q)+1, n-1];

-**cheia publica,** ***PUB,*** un întreg calculat printr-o versiune a algoritmului lui Euclid, ca invers multiplicativ modulo φ(n) :

PUB = inv (PRIV, j **(n))**

-**M, documentul electronic,**

-**H(M), rezumatul documentului,** calculat cu o **funtie de hash, H.**

Recente progrese facute în factorizarea întregilor si în procesarea paralela au dat nastere la necesitatea unor chei din ce în ce mai mari pentru sistemele de criptare cu chei publice. Însa cresterea dimensiuni cheilor va face aceste sisteme cu chei pu-blice mai lente decât sunt la momentul ac-tual. Pentru a pune în evidenta acest aspect, iata care sunt ultimele recomandari facute pentru alegerea dimensiunii cheilor RSA:

- Securitate pe termen scurt (ex.: chei ale utilizatorilor): 768 biti, suficienta în apli-catii pentru utilizatori individuali;

- Securitate pe termen mediu (ex.: cheile unei organizatii): 1024 biti, suficienta în aplicatii comerciale;
- Securitate pe termen lung (ex.:cheile administratorului): 2048 biti, considerata suficienta pentru aplicatii cu cerinte de securitate sporita, la nivel militar.

Criptarea si semnarea unui document

Spre deosebire de metodele DSS sau El Gamal, care pot fi folosite doar pentru semnatura digitala, RSA este un sistem criptografic ce poate fi folosit atât la crip-tare cât si la semnare. De aceea vom expli-ca substratul matematic al ambelor servicii.

Baza teoretica a lui RSA este *generaliza-rea lui Euler a Teoremei Fermat* care sta-bileste ca:

$$M^{j(n)} = 1 \bmod n$$

Aceasta proprietate implica necesitatea ca cele 2 chei, PUB si PRIV sa fie inverse multiplicativ modulo φ(n):

$$PUB*PRIV = 1 \bmod j(n)$$

Fiecare utilizator, de exemplu Dan, obtine de la un administrator modulul n_{Dan} si exponentii PUB_{Dan} si $PRIV_{Dan}$. Apoi user-ul Dan va înregistra într-un fisier public, cheia publica (n_{Dan}, PUB_{Dan}), ti-nînd secreta pe $PRIV_{Dan}$.

-functia de criptare cu RSA

Un alt utilizator, Ana, va putea emite un **document M criptat** utilizînd cheia publi-ca a lui Dan, adica ridicarea la puterea PUB_{Dan}, modulo n_{Dan}, a documentului electronic, interpretat ca un întreg:

$$C = M^{PUB_{Dan}} \bmod n_{Dan}$$

La receptie, utilizatorul destinatar Dan va obtine documentul în clar, tot prin ridicare la putere, cu cheia sa secreta $PRIV_{Dan}$:

$$M = C^{PRIV_{Dan}} \bmod n_{Dan}$$

$$= (M^{PUB_{Dan}})^{PRIV_{Dan}} \bmod n_{Dan}.$$

-functia de semnatura digitala cu RSDan

Utilizatorul Dan va putea semna un rezu-matul H(M) al unui document M calcu-lând, cu cheia sa secreta $PRIV_{Dan}$:

$$S = (H(M))^{PRIV_{Dan}} \bmod n_{Dan},$$

Orice alt user, de exemplu Ana, va putea autentifica acest document, utilizînd cheia publica PUB_{Dan} a lui Dan si calculând, tot prin exponentiere, rezmatul H(M), din semnatura S receptionata:

$$H(M) = S^{PUB_{Dan}} \bmod n_{Dan} .$$

Daca rezumatul astfel calculat coincide cu cel calculat direct din documentul electro-nic, semnatura se considera a fi valida.

Exemplu numeric

Sa consideram un mic *exemplu* care sa ilustreze folosirea algoritmului RSA pentru semnatura digitala.

-fie p=53 si q=61 cele doua numere prime (tinute secrete);

-fie n=53*61=3233 produsul acestor doua numere;

-indicatorul lui Euler calculat este φ(n)=(p-1)*(q-1)=52*60=3120.

-se alege o cheie secreta $PRIV_{Dan}$=71;

-se calcueaza cheia publica PUB_{Dan}=791 ca invers multiplicativ mod 3120 a lui PRIV:

$$71*791 = 1 \bmod 3120$$

Sa consideram un document al carei rezu-mat H(M) este 13021426. Cum valoarea sa depaseste marimea modulului n=3233, vom sparge acest rezmat în 2 blocuri (1302 si 1426), pe care Dan le va semna separat, folosind cheia sa secreta $PRIV_{Dan}$=71:

$$1302^{71} \bmod 3233 = 1984$$

$$1426^{71} \bmod 3233 = 2927$$

Semnatura electronica obtinuta este:

$$S = 1984\ 2927.$$

La receptia documentului M si al semnaturii sale S, Ana va calcula H(M) prin ridicare la putere cu cheia publica PUB_{Dan}=791 a pretinsului semnatar:

$$1984^{791} \bmod 3233 = 1302$$

$$2927^{791} \bmod 3233 = 1426$$

Aceste numere, identice cu valoarea în clar a documentului, confirma validitatea semnaturii. pentru cele de *semnatura digitala*.

3. Certificatele digitale si infrastructuri cu chei publice

În functionarea sistemelor de semnatura digitala este necesar un sistem de generare, circulatie si autentificare a cheilor folosite de utilizatori. Sa ne imaginam situatia când o persoana, sa zicem Vlad, doreste sa se dea drept altcineva, Dan, si vrea sa semneze în fals în numele lui Dan; falsificatorul (Vlad) poate face acest lucru usor, generându-si propria sa pereche de chei si punând-o pe cea publica în fisierul public, în locul celei autentice a lui Dan. Documente semnate de Vlad cu cheia sa secreta vor fi verificate cu cheia publica ce pare a fi a lui Dan si orice persoana se va însela de autenticitatea documentelor semnate în numele lui Dan.

Problema fundamentala este deci accea a *încrederii absolute în cheile publice*, cele cu care se face verificarea semnaturlor digitale. Acestea trebuie sa fie disponibile în retea, astfel ca orice client sa poata obtine cheia publica a unui emitent de document semnat. În acest context, solutia tehnica exista: crearea unei infrastructuri internationale, bazat pe **Autoritati de Certificare -AC (Certification Authority)**, care sa permita obtinerea cu usurinta si într-o maniera sigura a cheilor publice ale persoanelor cu care se doreste sa se comunice prin Internet. Aceste autoritati urmeaza sa distribuie, la cerere, certificate de chei autentificate.

Cel mai larg recunoscut si utilizat **format pentru certificatele de chei publice** este acela definit în standardul X.509 de catre ISO/IEC/ITU. Formatul X.509 pentru certificate a evoluat de-a lungul a trei versiuni. Versiunea 3 (care a fost adoptata în 1996) a introdus câteva caracteristici noi. În timp ce versiunile anterioare asigurau suport numai pentru sistemul de nume X.500, versiunea 3 suporta o mare varietate de forme pentru nume, incluzând adrese de email si URL-uri. Versiunea 3 introduce niste extensii pentru certificate incluzând în acestea extensiile standard, private sau cele definite la nivel de comunitat.

Infrastructurile de chei publice (***PKI – Public Key Infrastructure***) constau in multimea serviciilor necesare a fi asigurate atunci când tehnologiile de criptare cu chei publice sunt folosite pe o scara larga. Aceste servicii sunt atât de natura tehnologica cât si legislativa iar existenta lor este necesara pentru a permite exploatarea tehnologiilor de chei publice la întreaga lor capacitate în vederea asigurarii suportului pentru comertul electronic. Elementele cheie ale infrastructurilor de chei publice sunt:

- certificatele digitale,
- Autoritatile de Certificare (AC),
- facilitatile de management al certificatelor.

Când se încearca transpunerea acestor concepte în lumea reala (în special în medii implicând organizatii si comunitati foarte diverse, care necesita sa interopereze în moduri complexe) apar o serie de aspecte greu de solutionat. Infrastructurile de chei publice trebuie sa asigure suport atât pentru functii de *criptare* cât si pentru cele de *semnatura digitala*.

4. Semnaturi digitale de grup

Semnaturile digitale de grup extind conceptul de semnatura digitala obisnuita prin aceea ca implica participarea mai multor entitati: membrilor unui anumit grup le este permis sa semneze în numele întregului grup. Aceste semnaturi pot fi verificate folosind o **singura** cheie, numita *cheie publica de grup*. De asemenea, odata ce un document a fost semnat, nimeni, cu excep-tia unui membru special al grupului (numit *manager de grup*), nu poate determina ce membru al grupului a semnat acel document. Semnaturile de grup trebuie proiectate în asa fel încât nici un

membru al grupului sa nu poata falsifica semnatura al-tui membru din grup pe un anumit docu-ment.

Ca exemplu sa presupunem ca patronul unei companii dezvoltatoare de software doreste ca anumti angajati ai sai sa vali-deze liste de preturi, sa semneze contracte digitale sau pachete software în numele companiei. El poate pune în practica o schema de semnatura de grup în care el sa fie managerul de grup. Angajatii pot semna si valida diverse documente sau pachete software în numele companiei. Prin aceasta abordare patronul poate masca structura interna a companiei sale. Mai mult, clientii vor avea nevoie de o singura cheie publica (cea a companiei) pentru a verifica semna-turile de pe documente. Pe de alta parte, în caz de frauda, doar patronul va putea deter-mina ce angajat a semnat un anumit docu-ment.

Semnaturile digitale astfel produse satisfac o serie de cerinte de securitate, cum ar fi:

1. sunt imposibil de falsificat;
2. este imposibil pentru un angajat sa re-produca semnatura altuia;
3. este imposibil pentru patron sa falsifice semnaturile angajatilor.

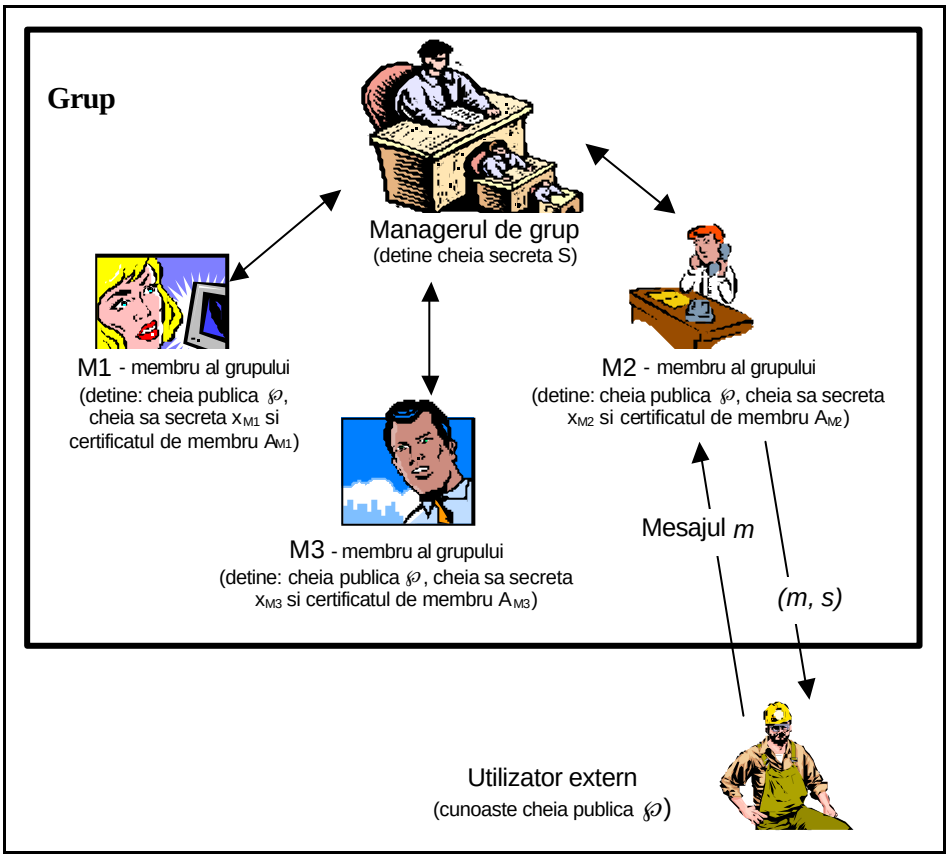

Fig. 2 - Schema de semnatura de grup

Protocolul

O schema de semnatura digitala de grup consta din 5 proceduri:

1. Initializare – un algoritm probabilistic care genereaza cheia publica a grupului ℘ si o cheie de administrare secreta *S* pentru managerul de grup.

2. Aderare – un protocol interactiv între managerul de grup si un nou membru al grupului, Dan, care rezulta în producerea cheii secrete a lui Dan, notata cu *x*, si a certificatului sau de membru, notat cu *A*.

3. Semnare – un protocol interactiv între un membrul al grupului, Dan, si un

utilizator extern, Alin, care preia ca intrare un mesaj *m* de la Alin si cheia secreta *x* a lui Dan producând o semnatura *s* pentru mesajul *m*.

4. Verificare – un algoritm care preia ca parametrii de intrare (m, s, $\wp$) si verifica daca *s* este o semnatura valida pentru mesajul *m* relativ la cheia publica a grupului $\wp$.

5. Dezvaluire - un algoritm care preia ca parametrii de intrare (*m*, *s*, *S*) si determina identitatea membrului grupului care a emis semnatura *s* pentru mesajul *m*.

În protocolul de mai sus se presupune existenta unei ***infrastructuri cu chei publice (PKI)*** si oricine doreste sa adere la grup trebuie sa faca anterior parte din aceasta PKI. Toti membrii PKI au perechi de chei publica/privata asociate cu aceasta infrastructura.

Cerinte de securitate

Semnaturile digitale de grup trebuie sa satisfaca urmatoarele cerinte de securitate:

1. Imposibilitate de falsificare: doar membrii grupului pot emite semnaturi valide în numele grupului (***verificabile*** folosind cheia publica a grupului $\wp$).

2. Anonimitatea conditionala a semnatarului mesajului: oricine poate verifica cu usurinta ca o pereche (*mesaj*, *semnatura*) a fost semnata de catre un membru al grupului însa numai managerul de grup poate determina ce membru al grupului a emis semnatura.

3. Imposibilitatea negarii identitatii semnatarului: managerul de grup poate determina întotdeauna identitatea unui membru al grupului care a emis o semnatura valida. Mai mult, el poate dovedi unei alte entitati (cum ar fi un judecator) ce membru a semnat un anumit document fara a compromite anonimitatea acelui membru al grupului în mesajele ***anterioare*** sau ***viitoare*** pe care le poate semna.

4. Lipsa de relatie între doua semnaturi: pentru oricine, cu exceptia managerului de grup, este imposibil din punct de vedere computational sa determine daca doua semnaturi au fost produse de acelasi membru al grupului.

5. Securitatea la atacurile prin înscenare: nici un subgrup format din membrii ai grupului (incluzând si managerul de grup) nu poate semna în numele unui alt membru al grupului.

6. Rezistenta la comploturi: nici un sub-grup al membrilor grupului (incluzând chiar si managerul de grup) nu trebuie sa se poata coaliza si sa genereze semnaturi de grup valide, a caror origine sa nu poata fi identificata.

Eficienta semnaturilor de grup

Urmatorii parametrii sunt deosebit de importanti atunci când se evalueaza eficienta unei anumite scheme de semnatura de grup:

1. Dimensiunea cheii publice de grup $\wp$
2. Dimensiunea semnaturii de grup pentru un mesaj
3. Eficienta protocoalelor de ***Semnare***, ***Verificare***,
4. Eficienta protocoalelor de ***Initializare***, ***Dezvaluire*** si ***Aderare***.

În continuare vom prezenta un exemplu concret de scheme de sematuri de grup si una dintre cele mai folosite în practica la ora actuala. Aceasta a fost propusa de Carmenisch si Stadler in 1997. În prealabil vom introduce trei constructii elementare, numite *semnaturi cu cunostinte suplimentare*, folosite ulterior în constructia schemei de semnatura de grup CS.

Semnaturi cu cunostinte suplimentare

O semnatura cu cunostinte suplimentare este o constructie în care semnatarul se poate folosi de cunoasterea unei anumite informatii secrete (cum ar fi logaritmul discret al lui *y* în baza *g*, unde $G=\langle g \rangle$) pentru a genera semnatura digitala a mesajului. Într-o semnatura cu cunostinte suplimentare semnatarul leaga cunoasterea informatiei secrete de mesajul ce este semnat.

Semnatura SC1: Un (l+1)-tuplu (c, s_1,…s_l) $\in \{0,1\}^l \times \mathbf{Z}_n^l$ care satisface relatia:

$c = H\ (m, y, g, g^{s_1} y^{c[1]}, g^{s_2} y^{c[2]}, ..., g^{s_l} y^{c[l]})$

unde $c[i]$ este al i -lea bit din stânga al lui c, este o *semnatura cu cunostinta suplimentara a logaritmului lui y Î G* în baza g, pentru mesajul m, relativa la parametrul de securitate l si se noteaza cu $SCSLOG_l [\ a \mid y = g^{\alpha}\ ] (m)$

Semnatura SC2: *O semnatura cu cunostinta suplimentara a dublului logaritm discret al lui y* în bazele g si a, pentru mesajul m, cu parametrul de securitate l, notata cu $SCSLOGLOG_l [\ \alpha \mid y = g^{(a^a)}\ ] (m)$ este un (l +1)-tuplu (c, s_1,…s_l) $\in \{0,1\}^l \times \mathbf{Z}_n^l$ care satisface relatia $c = H\ (m, y, g, a, t_1, ..., t_l)$ unde

$$t_i = \begin{cases} g^{(a^{s_i})} & \text{daca c[i] = 0} \\ y^{(a^{s_i})} & \text{in caz contrar} \end{cases}$$

Semnatura SC3: *O semnatura cu cunostinta suplimentara a radacinii de ordinul e a logaritmului discret al lui y* în baza g, pentru mesajul m, cu parametrul de securitate l, notata cu $SCSRADLOG_l [\ \alpha \mid y = g^{(a^e)}\ ] (m)$ este un (l +1)-tuplu (c, s_1,…s_l) $\in \{0,1\}^l \times \mathbf{Z}_n^l$ care satisface relatia:

$c = H\ (m, y, g, e, t_1, ..., t_l)$ unde

$$t_i = \begin{cases} g^{(s_i^e)} & \text{daca c[i] = 0} \\ y^{(s_i^e)} & \text{in caz contrar} \end{cases}$$

Odata introduse modulele de baza, putem prezenta în continuare constructia schemei de semnatura de grup Camenisch-Stadler.

5. Schema de semnatura Camenisch-Stadler

Initializare

Pentru initializarea schemei Camenisch-Stadler managerul de grup alege un parametrul de securitate l si calculeaza urmatoarele valori:

1. Cheia publica RSA (n, e), unde lungimea lui n este de cel putin 2l biti (n=p q, cu p si q numere prime mari).
2. Se presupune existenta unei infrastructuri cu chei publice (PKI) si oricine doreste sa adere la grup trebuie sa faca anterior parte din aceasta PKI. Toti membrii PKI au perechi de chei publica/privata asociate cu aceasta infrastructura
3. Un grup ciclic G=<g> de ordinul n, în care calculul logaritmilor discreti este nefezabil
4. Un element a Î $\mathbf{Z}_n^*$
5. O limita superioara l pentru lungimea cheilor secrete si o constanta e >1. Cu cât e este mai mare cu atât sistemul este mai sigur.

Cheia publica a grupului este Ã = (n, e, G, g, a, l **,** e **).**

Aderarea la grup

Generarea cheilor pentru membrii grupului si a certificatelor se face astfel:

Atunci când un utilizator doreste sa adere la grup, el îsi alege cheia secreta $x \in \{0, \ldots, 2^l - 1\}$ si calculeaza valoarea $y = a^x \pmod n$ si cheia lui de membru $z = g^y$. Utilizatorul îsi leaga identitatea sa de va-loarea y (de exemplu o semneaza, folosind cheia sa secreta asociata prin PKI) apoi trimite (y, z) managerului de grup pentru a-i demonstra acestuia ca are cunostinta de logaritmul discret al lui y în baza a. Când managerul de grup este convins ca noul utilizator cunoaste acest logaritm, el va trimite utilizatorului **certificatul de mem-bru**:

$v \equiv (y+1)^{1/e} \pmod n$

Semnarea

Pentru a semna un mesaj m $\in \{0, 1\}^*$, utilizatorul calculeaza urmatoarele valori:

1. $\bar{g} = g^r$ pentru r$\in \mathbf{Z}_n$
2. $\bar{z} = \bar{g}^y \quad (= (g^r)^y = z^y)$
3. $V_1 = SCSLOGLOG[a \mid \bar{z} = \bar{g}^{a^a}](m)$
4. $V_2 = SCSRADLOG[b \mid \bar{z}\bar{g} = \bar{g}^{b^e}](m)$

Semnatura pe mesajul m este $(\bar{g}, \bar{z}, V_1, V_2)$.

Verificare

Semnatura de mai sus poate fi verificata prin testarea semnaturilor cu cunostinte suplimentare V_1 si V_2. Semnatura V_1 dovedeste ca utilizatorul apartine grupului deoarece valoarea $\overline{\overline{zg}}$ trebuie sa fie de forma $\overline{\overline{zg}} = \overline{g}^{a^a+1}$ pentru un întreg a pe care utilizatorul îl cunoaste. V_2 dovedeste ca utilizatorul cunoaste radacina de ordinul e a lui $a^a + 1$, ceea ce înseamna ca utilizatorul cunoaste certificatul de membru.

În concluzie, verificarea cu succes a lui V_1 si V_2 demonstreaza ca utilizatorul cunoaste cheia secreta si certificatul de membru corespunzator acelei chei secrete.

Dezvaluirea

Data fiind semnatura $(\overline{g}, \overline{z}, V_1, V_2)$ pentru mesajul m, managerul de grup poate determina semnatarul testând relatia $\overline{g}^{y_P} = \overline{z}$ pentru fiecare membru P al grupului (unde cu y_P se noteaza logaritmul discret a cheii de membru z_P a lui P în baza g). Aceasta metoda are însa un timp de rulare linear dependent de numarul membrilor grupului.

Consideratii de eficienta

Pentru urmatoarele valori ale parametrilor sistemului: k =160, l = 64, l = 170, e =4/3, $|n|$=600 si e = 3 dimensiunea semnaturii este mai mica de 7Kbytes si operatiile pentru semnarea mesajelor si verificarea semnaturilor necesita aproximativ 140000 înmultiri modulare cu un modul de 600 de biti, ceea ce este echivalent cu aproximativ 155 exponentieri folosind exponenti de 600 de biti.

1. Concluzii

Internet-ul furnizeaza corporatiilor dar si micilor firme oportunitati pentru dezvoltarea unui nou tip de afaceri de mare eficienta, cuprinse generic în paradigmele de e-commerce sau e-business. În acest context, securitatea informatica devine o provocare majora, care trebuie sa confere încredere în noua lume electronica. Autentificarea entitatiilor implicate în desfasurarea tranzactiilor, autentificarea continutului pieselor de informatie schimbate sau distribuite prin Internet, non-repudierea unor documente sau programe ce au facut obiectul unor afaceri on-line, reprezinta cerinte de securitate ce sunt abordate prin intermediul semnaturilor digitale individuale sau de grup. Existenta unor entitati emitente de certificate digitale si a unor infrastructuri care sa permita distributia sigura a acestor certificate reprezinta noi cerinte tehnologice, în curs de implementare pentru securizarea spatiului cibernetic al Internet-ului.

Bibliografie

1. Denning D.E.,"*Encryption Policy and Market Trends*", RSA Data Security Conference, 1997;
2. Holbrook P., Reznolds J., "*Site Security Handbook*", RFC 1244;
3. Jennifer S, Pieprzyk J, "*Cryptography: An Introduction to Computer Security*", Prent. Hall, 1989;
4. Karila Arto, "*Open Systems Security-an Architectural Framework*", Helsinki, 1991
5. Muftic S., "*Security Mechanisms For Computer Networks*", Proj. Rep. CEC COST-11,1990;
6. .RSA Data Security, Inc., "*The Keys to Privacy and Authentication" , Products Catalog, Redwood City, USA, 1996;*
7. Schneier B., "*Applied Crypography*", John Wiley & Sons, 1996.
8. Patriciu,V.V., "*Criptografia si securitatea retelelor de calculatoare*", Ed Tehnica, Bucuresti,1993;
9. Patriciu V., Pietrosanu M., Bica I., Cristea C., "*Securitatea informatica în UNIX si Internet*", Ed.Tehnica, 1998.
10. Patriciu V., Vasiu I., Patriciu S., "*Internet-ul si dreptul*", Ed. All-Back, 1999.
11. Patriciu V., Pietrosanu M., "Securitatea comertului electronic*l*", Ed.All, 2000, sub tipar.