ANEXA B

SECURITATEA COMUNICAȚIILOR ÎN INTERNET

Conceptele de securitate a comunicațiilor în Internet sunt ilustrate în numeroase documente RFC.

Confidențialitatea mesajelor este asigurată folosind diverse tehnici de criptare. Criptosistemele convenționale folosesc chei simetrice de criptare, transmise pe canale securizate. Criptosistemele cu chei publice utilizează seturi asimetrice de chei. Cheia unic inversabilă poate fi schimbată prin rețeaua publică.

Autenticitatea mesajelor este confirmată prin operația de autentificare a sursei, astfel încât informațiile transmise să nu fie false. Semnătura digitală reprezintă o metodă de autentificare atât a datelor, cât şi a sursei de informații.

În cadrul criptosistemelor cu chei simetrice, se disting trei tipuri de cifruri:

1. cifruri de substituție;
2. cifruri de transpoziție sau de permutare;
3. cifruri combinate.

Cifrurile de substituție înlocuiesc fiecare simbol din alfabetul de intrare cu unul sau mai multe simboluri. Se poate lucra şi cu substituția cuvintelor folosind dicționare de termeni.

Cifrurile de transpoziție modifică ordinea simbolurilor sau a grupurilor de simboluri din textul-în-clar (*plaintext*), după o anumită regulă.

Cifrurile combinate aplică atât metode de substituție, cât şi metode de transpoziție.

Metodele moderne de criptare-bloc cu chei simetrice folosesc diverse operații: substituții, transpoziții, adunări şi înmulțiri în GF, transformări liniare etc.

Dintre sistemele relativ moderne de criptare cu chei simetrice se remarcă: DES (*Data Encryption System*), 3-DES (*Triple DES*) utilizat de protocolul SSH, IDEA (*International Data Encryption Algorithm*).

Algoritmul DES, standardizat prin standardul ANSI X.392 se aplică pe blocuri de 64 de biți de date, cu o cheie de 56 de biți, repetitiv de 16 ori. Cheia de criptare corespunde unei secvențe de 8 caractere, codate ASCII pe 7 biți.

În 1991, Quisquater şi Desmedt propuneau un atac eficient împotriva algoritmului DES şi a cifrurilor asemănătoare denumit Loteria chinezească. Acesta se bazează pe capacitatea de calcul a clientului, dar şi a altor calculatoare-gazdă pentru spargerea cifrurilor.

Eficiența acestui atac a crescut considerabil prin creşterea enormă a numărului de calculatoare-gazdă din Internet, precum şi a performanțelor de calcul ale acestora. Conform Legii lui Moore performanțele echipamentelor hardware se dublează la fiecare 1,5 ani. Numărul de calculatoare din Internet se dublează la fiecare 3 ani.

RFC 3607 (*Chinese Lottery Cryptoanalysis Revisited: The Internet as a Codebreaking Tool*), apărut în septembrie 2003, analizează atacul cripanalitic masiv şi paralel denumit Loteria chinezească, prin analogii cu transmisiile criptate din Internet, şi posibilele consecințe ale acestuia.

Atacurile criptografice actuale se bazează pe activitatea viermilor de Internet.

Viermii din Internet au infectat un număr exorbitant de hosturi. În 2001, asociația CAIDA (*Cooperative Association for Internet data Analysis*) a raportat că viermele Code Red v2 că a infectat în primele 14 ore de la lansare peste 350 000 de calculatoare.

În general, un vierme de Internet poate fi folosit ca să decripteze forțat un mesaj şi astfel să determine cheia de criptare. Pentru a avea succes, viermele trebuie să acționeze pe durata a mai multor cicluri de funcționare a CPU pentru a efectua o criptanaliză completă. În plus, durata de acțiune a lui trebuie să fie suficient de mare astfel încât proprietarii săi să poată folosi cheia respectivă. Chiar şi după detectarea unui vierme de Internet, nu se poate deduce care chei au fost atacate.

Transmisia cheii către inițiatorul viermelui se va face tot prin Internet, dar prin criptare în sistem public. Cheia criptată este ascunsă chiar pe site-ul web al gazdei compromise. Fişierul care conține cheia poate fi depistat de proprietarul viermelui pe baza

unor cuvinte-cheie pe care le caută folosind un motor de căutare. Procesul este eficientizat folosind serviciile de tip « registre de cuvinte-cheie » ale motoarelor de căutare.

Controlul anonim în timp real al viruşilor şi viermilor de Internet se poate face prin intermediul serviciilor de ştiri, de chat (IRC) sau al altor servicii similare.

În 1995, J. Touch a publicat o analiză detaliată a algoritmului MD5 (*Message Digest version 5*) în RFC 1810. Acest algoritm realiza echivalentul a 170000 de operații pe blocuri de date simple în fiecare secundă în timp ce, în acelaşi an, algoritmul DES lucra cu numai 50000 de operații pe secundă. La nivelul anului 2002, pentru parole de 8 caractere, algoritmul DES putea fi decriptat în circa 16 minute, iar MD5 în mai puțin de 5 minute. Pentru mesaje scurte, se poate totuşi folosi MD5 cu chei lungi, efectiv libere.

În februarie 2003, a fost lansat viermele W32/OPASERV cu sarcina de a implementa un sistem distribuit de spargere a algoritmului DES. De aceea, s-a hotărât trecerea la Triple DES sau la AES (*Advanced Encryption System*) (RFC 3268).

Algoritmul 3-DES foloseşte chei de 112 biți şi aplică DES de 3 ori, fiind considerat de două ori mai sigur.

Algoritmul AES asigură securitatea pe nivelul de transport (TLS – *Transport Layer Security*), pe baza cifrurilor simetrice RC2, RC4, IDEA, DES, 3-DES, DFE (*Diffie-Helmann Encryption*), RSA (*Rivest-Shamir-Adleman*) şi altele. Se propun noi suite de înlănțuire a blocurilor-cifru care diferă prin modul de certificare şi metoda de schimbare a cheii.

AES foloseşte chei de 128, 192 şi 256 de biți, fiind eficient la atacurile criptanalitice prelungite.

Cifrurile publice DH sunt eficiente dacă se folosesc o singură dată cheile efemere după care acestea trebuie distruse în mod securizat, iar generatorul de numere aleatoare să nu îşi arate stările trecute nici dacă este compromis.

Cifrurile DH anonime (ADH) oferă confidențialitate, dar nu şi posibilitatea de autentificare, operație care trebuie realizată prin alte metode. ADH este vulnerabil la atacul de tip « omul din mijloc » din cauza lipsei autentificării. Atacatorul poate negocia două conexiuni TLS cu fiecare parte comunicantă şi astfel deduce cifrul de transmisie.

Neajunsurile securității prin chei publice sunt evitate prin folosirea mecanismului Kerberos (RFC 3129).

Grupul de lucru IPsec a definit pe nivelul de rețea mecanismul de schimbare a cheilor IKE (RFC 2409) pentru autentificare în pereche, cu chei simetrice pre-distribuite. IKE

permite autentificarea şi schimbul cheilor în pereche, fără intervenția celei de a treia părți. Totuşi sunt multe situații în care a treia parte sigură solicită autentificarea, de exemplu prin utilizarea unui program proxy. Mecanismul Kerberos permite autentificarea unei a treia părți sigure care cere să comunice cu celelalte două entități implicate în comunicare. Autentificarea se poate face fie prin algoritmul DH, fie prin semnătură digitală, fie prin intermediul unui server KDC (*Key Distribution Center*). Kerberos specifică protocolul standard prin care un client obține de la serverul KDC un tichet de transmisie pentru fiecare sesiune deschisă şi asigură managementul centralizat al politicilor de securitate.

Pornind de la IKE, grupul KINK a propus definirea unui nou protocol de securitate cu următoarele caracteristici :

- să folosească cheile din tichetele Kerberos în arhitectura IPsec,
- să suporte mecanismul de autentificare Kerberos fie cu cheie secretă, fie cu cheie publică (PKINIT – *Public Key Initialization*),
- să permită autentificarea în pereche,
- să negocieze suitele de cifru,
- să permită recifrarea cu un cifru încă valid fără asistența KDC,
- să micşoreze şansele de atac criptografic,
- să permită modul de tunelare,
- să suporte atât Ipv4, cât şi Ipv6.

Este nevoie de un protocol care să permită cifrarea pe baza IPsec, folosind Kerberos pentru distribuția cheilor.

În prezent, se dezvoltă noi tehnici de criptare bazate fie pe metodele de extensie de spectru cu secvențe de cod pseudoaleatoare, fie pe generatoare de chei implementate cu sisteme haotice, fie pe teoria cuantică.

Metodele bazate pe teoria haosului pot fi aplicate cu succes pentru secretizarea transmisiei (de exemplu, sistemul lui Baptista, simplu sau modificat), dar pot fi proiectate şi în spații multidimensionale (ca în cazul imaginilor digitale 2D şi 3D, respectiv pentru transmisii simultane de date-voce, audio-video etc).

Criptosistemele bazate pe haos utilizează sisteme dinamice haotice deterministe, fie continui, fie discrete, sensibile la condițiile inițiale. Prin legea lor de mişcare, aceste sisteme dinamice determină în mod unic evoluția stărilor criptosistemului şi permite decodarea necatastrofică a secvenței codate. Aceste sisteme dinamice sunt descrise de ecuații

funcționale de stare în care se utilizează o funcție ***f*** de 'dinamică a sistemului', liniară sau neliniară:

$$x^{+}(t) = f(x(t), t) \tag{B.1}$$

Prin ***x*** se înțelege vectorul variabilelor de stare dependent de variabila continuă de timp ***t*** iar **+** reprezintă operatorul de schimbare a stării sistemului.

Similar, în cazul sistemelor discrete, ecuația de stare se scrie în funcție de variabila discretă de timp ***n*** sub forma:

$$x[n+1] = f(x[n], n) \tag{B.2}$$

De exemplu, se poate utiliza un sistem dinamic descris de ecuația discretă neliniară :

$x_{n+1} = Rx_n \cdot (1 - x_n),\ R \in (1, 4),\ x_n \in (0, 1),\ x_0 \neq 0.$

Se preferă utilizarea sistemelor dinamice neliniare care pot avea în regim permanent mai multe mulțimi limită, cu bazine de atracție diferite, dependente într-un mod foarte senzitiv de condiția inițială, astfel încât devine imposibilă predicția pe termen lung a stării acestora.

În cazul criptosistemelor haotice discrete mixte, procedura de criptare şi de decriptare se realizează prin iterații multiple, inverse şi directe, iar secvența codată corespunde numărului de iterații efectuat. Aceste sisteme se dovedesc a fi deosebit de robuste față de atacurile statistice.

Principiul criptografiei bazate pe teoria haosului este dat de difuzia şi confuzia parametrilor traiectoriilor generate pe baza cheii de criptare şi a mesajului transmis. La mici variații ale cheii de transmisie trebuie să apară modificări extreme ale traiectoriei din spațiul fazelor pentru sistemul dinamic utilizat. Astfel se asigură rezistența criptosistemului față de atacurile brute bazate pe încercarea tuturor cheilor posibile de transmisie.

Traiectoriile haotice nu sunt nici periodice, nici cvasiperiodice, şi au un aspect aleator, cu un spectru de putere de tip 'zgomot alb' (de bandă largă).

Nici un calculator şi nici un program software nu poate prezice traiectoria unui sistem dinamic haotic deoarece complexitatea algoritmică a traiectoriilor este pozitivă, fiind dată de entropia K-S (Kotulski-Szczepanski) a sistemului. Pe acest fapt se bazează ideea proiectării unor tehnici eficiente de criptare a datelor pe baza teoriei haosului astfel încât entropia sistemului să crească prin codare şi să depăşească limitele capacității computaționale a criptanalistului.

Optimizarea algoritmilor de criptare vizează reducerea timpului de procesare a datelor, reducerea capacității de memorie necesară, diversificarea cheilor posibile de transmisie, respectiv scăderea eficienței atacurilor criptografice. Aplicarea unei precodări de compresie a sursei informaționale pentru scăderea redundanței acesteia reduce riscul de intercepție a cheii de transmisie şi eficiența oricărui atac.

Valoarea unui criptosistem se apreciază pe baza mai multor factori:grad de secretizare, mărimea spațiului cheilor de criptare, propagarea erorilor, distanța de unicitate.

Elaborarea unui criptosistem performant presupune maximalizarea volumului de muncă necesar criptanalizei prin orice metodă. Când se realizează criptanaliza unui algoritm de criptare, presupunerea generală care se face este că şi criptanalistul cunoaşte exact modul de funcționare a criptosistemului. Sunt date mai jos, tipurile de atacuri criptografice, ordonate de la cel mai puternic la cel mai uşor:

1. atac cu text cifrat: criptanalistul posedă un şir din mesajul criptat;
2. atac cu text în clar cunoscut: criptanalistul posedă un şir din textul în clar, *p*, şi textul cifrat corespunzător, *c*;
3. atac cu textul în clar ales: criptanalistul a obținut temporar accesul la algoritmul sau sistemul de criptare. Astfel, el poate alege un şir *p* din textul în clar şi să construiască textul criptat corespunzător *c*;
4. atac cu text criptat ales: criptanalistul a obținut temporar accesul la sistemul de decriptare. Astfel, el poate alege un şir din textul criptat pe baza căruia construieşte textul în clar corespunzător.

În fiecare din aceste patru atacuri, obiectivul este construcția cheii utilizate. Ultimele două tipuri de atac pot pare nerezonabile la prima vedere, dar ele sunt foarte utilizate când algoritmul criptografic, a cărui cheie este fixată de producător şi necunoscută de atacator, este implementat într-un dispozitiv pe care atacatorul poate să-l manipuleze uşor (carduri smart, carduri electronice, cartele SIM ale telefoanelor GSM, maşini POST sau sesiuni ale aplicațiilor web.