ALGORITMI DE CRIPTARE ŞI PROTOCOALE ÎN REŢELELE DE NOUĂ GENERAŢIE (NGN)

Autori: Dmitrii PĂDURE, Igor RUSU, Natalia PĂDURE
Conducător ştiinţific: conf. univ. dr. Lucreţia NEMERENCO

Universitatea Tehnică a Moldovei

Abstract: *Dezvoltarea sistemelor de comunicare are o viteză efemeră, astfel încît în fiecare zi apar noi tehnologii, însă în procesul de utilizare a acestora de către utilizatori, este necesară o protecţie avansată a informaţiei, astfel dezvoltarea algoritmilor de criptare şi a protocoalelor a devenit la fel o cerinţă de bază pentru producători. Fiecare folosind metodologia sa de abordare a problemei date, s-au început a evidenţia cîteva direcţii de dezvoltare: criptografia cu chei secrete, criptografia cu chei publice, ş.a., fiecare din acestea avînd la dispoziţie diverse metode de criptare, certificare şi decriptare a mesajelor.*

Cuvinte cheie: *NGN, Algoritmi, Criptografie, Protocoale, GSM, IP.*

Next Generation Network: O reţea bazată pe pachete capabilă să ofere servicii de TLC şi capabilă să folosească reţele multiple, tehnologii de transport cu QoS activat şi în care funcţiile legate de servicii sunt independente faţă de tehnologiile legate de transport. Acesta activează accesul nemijlocit al utilizatorului la reţea şi la operatorii de servicii competitivi şi/sau servicii la alegerea acestora. Aceasta suportă mobilitate generalizată care ne permite prestarea de servicii coerente şi omniprezente pentru utilizatori [1].

Criptografia este de obicei descrisă ca promovând funcţionalităţi concerte, care sunt elaborate pentru realizarea „securizată" a comunicaţiei, funcţionalităţile tipice fiind:

Confidenţialitate: Asigurarea că doar destinatorului mesajului să poată citi conţinutul acestuia.

Integritate: Permite destinatarului mesajului să verifice dacă mesajul nu a fost modificat în timpul transmisiunii.

Autenticitate: Permite destinatarului mesajului să verifice că o entitate specificată este aprobată de conţinutul mesajului.

Nonrepudierea: Previne unele entităţi specifice de la refuz întîrziat că a acceptat mesajul.

Toate aceste funcţionalităţi sunt foarte importante şi ele definesc esenţial cum criptografia este utilizată în practică, dar cu siguranţă nu defineşte toate funcţionalităţile pe care criptografia le poate propune. Pe cînd aceste funcţionalităţi sunt suficiente pentru 3G, maştabul major şi natura heterogenă a XG duce la necesitatea unor tehnici criptografice mult mai flexibile şi avansate.

Criptografia are un scop major: realizarea schemelor robuste împotriva încercărilor de a face schemele să devieze de la funcţionalităţile respective (Goldreich 1999). Criptarea şi semnăturile digitale sunt exemple bine cunoscute ale criptografie, ele ajută la realizarea robustităţii, confidenţialităţii şi autentificităţii comunicaţiilor wireless impotriva atacurilor.

În continuare se vor analiza cîteva modele de criptografie, inclusiv criptografia cu chei secrete (GSM şi 3GPP) criptografia cu cheie publică (SSL) şi cîteva propuneri diferite pentru infrastructura cu chei publice (PKI). Utilizînd criptarea cu chei publice şi semnătura digitală ca exemple v-om analiza cum criptografia defineşte forma ce înseamnă formal ce înseamnă pentru o sistemă de criptare să fie securizată.

1 Criptografia cu chei secrete (CCS)

Într-o criptosistemă cu chei secrete (sau simetrică), 2 (sau mai mulţi) utilizatori utilizează aceeaşi cheie criptografică *k*. În CCS, emiţătorul utilizează *k* pentru criptarea textului în clar a mesajului nu şi generarea unui cipher *c* ($c=E_k(m)$ pentru un algoritm de criptare *E*), după care la recepţie se utilizează cheia *K* pentru a decripta *c* şi a restabili textul în clat *m* ($m=D_k(c)$ pentru algoritmul de criptare *D*). Un utilizator se poate autentifica altuia utilizînd CCS dovedind cunoaşterea K printr-un protocol cerere-răspuns.

Cunoscut ca „Principiul lui Kerckhoff", acesta spune că securitatea unui algoritm de criptare trebuie să se bazeze pe o cheie criptografică, nu pe secretizarea algoritmului. Raţionamentul principiului este că un algoritm este cu mult mai greu de a fi ţinut în secret decît o scurtă cheie criptografică.

Dea lungul timpului, proiectanţii de criptosisteme nu numai că au devenit matematic sofisticaţi, însă au început utilizarea calculatoarelor ca un mijloc de proiectare a cipherelor. La mijlocul anilor 1970, o echipă de la IBM în consultanţă cu Agenţia de Securitate a SUA au realizat DES (Data Encryption Standard). Pînă în ziua de astăzi unica metodă „practică" de atac a DES este de a încerca aleator fiecare cheie criptografică posibilă pînă la identificarea acesteia. Însă o dată cu dezvoltarea calculatoarelor, dezvăluirea acestuia a devenit foarte uşoară. Astfel a fost realizat Triple DES. Aici sunt utilizate 3 iteraţii a DES şi se utilizează 2 chei diferite în ordinea (k_1, k_2, k_1). De la cazul cu DES, SUA a început elaborarea a noi algoritmi, cel mai reuşit fiind AES (Advanced Encryption Standard).

GSM

Standartul GSM este un studiu de caz interesant în utilizarea criptografiei simetrice în criptare şi autentificare. Ca securitate, scopul GSM este de a face sistemul de telefonie mobilă atît de securizat ca şi PSTN (Public Switched Telephone Network). GSM utilizează criptografia simetrică pentru a realiza autentificarea unilaterală a staţiilor mobile faţă de staţiile de bază şi pentru a proteja confidenţialitatea datelor utilizatorului. Pentru realizarea acestui fapt, UE şi reţeaua trebuie să împartă o cheie secretă comună.

În GSM distribuirea cheii secrete este realizată după cum urmează. Staţia mobilă a unui utilizator conţine 2 elemente – aparatul însăşi şi cartela SIM (Subscriber Identity Module). Utilizatorul obţine SIM la conectarea la servicii.

Ea conţine următoarele numere:

- PIN (Personal Identification Number), care activează cartela.
- IMSI (International Mobile Subscriber Identification), corespunde unic unui număr de UE.
- O cheie de autentificare a utilizatorului – K_i, de 128 biţi, secretă, cunoscută de asemenea de AC (Authentification Center) în reţeaua sa, PIN poate fi personalizat pe cînd celelalte numere sînt fixe.

După introducerea PIN pentru activarea SIM staţia mobilă trebuie să se identifice unei staţii de bază după cum urmează. În primul rînd staţia mobilă transmite IMSI, care este transmisă centrului de autentificare. Centrul de autentificare generează atunci ciţiva tripleţi care sunt transmişi înapoi la staţia de bază, astfel încît fiecare conţine un indicator aliator RAND, un tag de autentificare XRES şi o cheie a cipherului k_c. AC derivă XRES şi k_c prin ataşarea IMSI a utilizatorului la cheia sa k_i şi atunci setînd XRES şi k_c ca fiind 2 criptări a RAND cu cheia k_i folosind algoritmi de criptare A3 şi A8, fiind,

$$XRES=A3_{ki}(RAND) \text{ şi } k_c=A8_{ki}(RAND).$$

Staţia de bază transmite indicatorul RAND staţiei mobile, ştiind că SIM a staţiei mobile conţine k_i aceasta poate trimite răspuns SRES ca fiind $A3_{ki}(RAND)$. În final staţia de bază completează autentificarea staţiei mobile prin confirmarea că XRES=SRES.

O dată ce autentificarea este completă, cheia cipherului k_c este utilizată pentru criptarea traficului dintre aparat şi staţia de bază utilizînd un algoritm numit A5. De cînd A5 este utilizat ca un cipher- specific, fiecare pachet este operat XOR cu o secvenţă pseudoaleatoare generată de k_c şi numărul pachetelor – o eroare de bit în textul cifrat cauzează o corespondenţă a unei erori de bit în textul în clar (fig. 1).

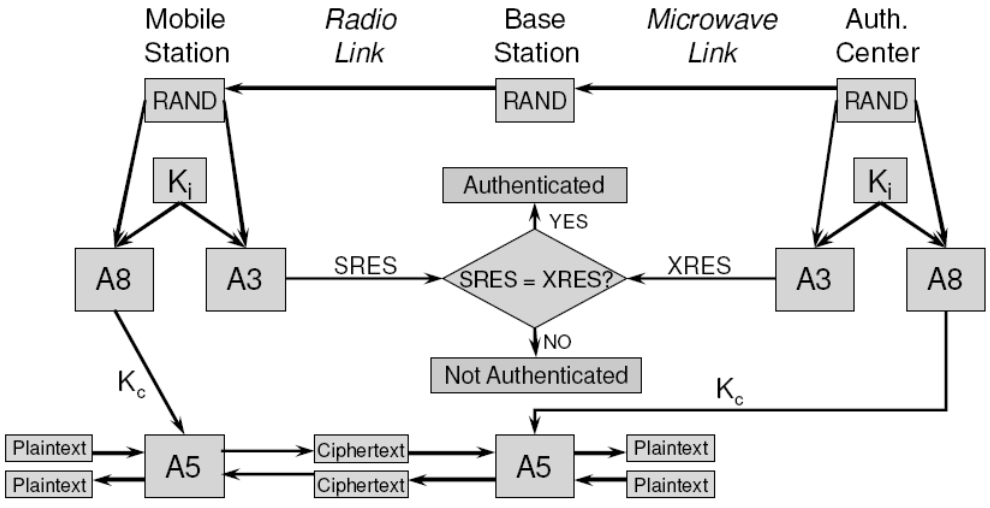

Figura 1 Autentificarea, generarea cheii şi criptarea în GSM

Pentru protecţia confidenţialităţii identităţii utilizatorului, reţeaua generează TMSI (Temporary Mobile Subscriber Identification) pentru utilizator, înregistrează asocierea între IMSE şi TNSI în baza de date şi transmise TMSI staţiei mobile criptate cu k_c. Reţeaua schimbă TMSI a staţiei mobile frecvente şi staţia mobilă poate utiliza cea mai recentă TMSI cînd apelează accesul la reţeaua.

Proiectanţii GSM nu au încercat să o facă rebustă impotriva atacurilor active asupra componentelor sistemului; existînd cîteva metode prin care se poate „distruge" securitatea GSM fără a fi necesar de a trece de criptosistemele simetrice – A3, A8 şi A5, care au neajunsuri serioase.

3GPP şi Principiul Kerckhoff

Standartul 3GPP (Third Generation Partnership Project), mai exact standartul UMTS (Universal Mobile Telecommunications System), este superior GSM prin mai multe. Spre exemplu, sistemul este mai robust prin cererea de autentificare mutuală. La fel, tot traficul utilizatorului şi datele de semnalizare sunt criptate prin aer, evitîndu-se interceptarea tripleţilor. În general, a fost realizat un efort de securizare a componentelor sistemului impotriva atacurilor active.

CCS Comp 128 şi A5 au fost înlocuite cu un bloc cipher numit Kasumi. Algoritmul Kasumi, care este public, este bazat pe blocul cipher „Misty", care este utilizat în reţeaua publică de mult timp.

Aparent secretizarea proiectului unei criptosisteme conferă „securitatea majoră", însă este dificil în practică de a evita repetarea inginerească. Cel mai eficient, conform principiului este sacrificarea secretizării proiectului algoritmului pentru obţinerea în loc a unui algoritm respectat de critica publică.

2. Criptografia cu chei publice (CCP)

Într-o criptosistemă cu cheie publică (sau asimetrică) un utilizator generează o pereche de chei publică/locală (k_{pu}, k_{pr}). Utilizatorul declară cheia publică k_{pu}, făcînd-o disponibilă pentru fiecare, dar păstraază cheia sa privată. Cu toate că aceste chei sunt legate printr-o relaţie matematică complicată, ar trebui să fie foarte greu pentru partea terţă de a obţine cheia privată din cea publică; altfel, oricine ar putea obţine cheia privată a utilizatorului şi CCP ar deveni nesecurizat.

Într-o schemă de criptare cu cheie publică, emiţătorul utilizează k_{pu} pentru criptarea textului în clar a mesajului m şi generarea unui text criptat c ($c=E_{kpu}(m)$, pentru algoritmul de criptare E dat) după care destinatorul utilizează k_p pentru decriptarea c şi restabilirea textului în clar m ($m=D_{kpr}(c)$, pentru algoritmul de decriptare D). Cu alte cuvinte pentru algoritmii fixaţi E şi D şi pentru toate mesajele m, trebuie să fie cazul $D_{kpr}(E_{kpr}(m))=m$. Părţile terţe nu ar trebui să fie apte să decripteze c utilizînd k_{pu}; numai deţinătorul cheii private ar fi apt să decripteze .

În schema unei semnături cu cheie publică, semnătorul utilizează k_{pr} pentru generarea semnăturii s pe un mesaj m($s=S_{kpr}(m)$, pentru un algoritm de semnare S). Pentru verificarea unei semnături , un verificator utilizează un algoritm de verificară a semnăturii ce răspunde cu „1" sau „0", în dependenţă dacă semnătura este validă sau nu. Pentru toate mesajele m, $V(m, k_{pu}, S_{cpr}(m))=1$ pentru algoritmul de verificare V, ce înseamnă că toate semnăturile produse legitim trebuie să fie valide. Părţile terţe trebui să aibă o probabilitate nesemnificativă de producere a unui exemplu ce ar trece testul de verificare; doar semnătarul legitim ar trebui să producă semnături valide.

Prima criptare cu cheie publică practică şi semnătura a fost realizată de Rivest, Shamir şi Adelman. Schema lor, cunoscută RSA este una dintre cele mai răspîndite criptosisteme din utilizare astăzi. De fapt, este tehnologia criptografică după SSL, care permite tranzacţii securizate pe internet de pe credit-card.

SSL

Secure Socket Layer este o sistemă de criptare utilizate de majoritatea paginilor web pentru securizarea tranzacţiilor on-line; conectările utilizează SSL încep cu https://. Protejează cererile şi răspunsurile http împotriva modificărilor prin utilizaera CCP.

Fiecare server web are o cheie publică care trebuie certificată de una dintre CA de bază, cheile publice ale cărora sunt stocate în browserul utilizatorului.

Totuşi detaliile pot varia, SSL funcţionează în modul următor:

1. Clientul transmite un mesaj CLIENT–HELLO spre server, conţinînd numele său C, specificaţiile cipherului SP_c şi un indicator aleator R_c.
2. Serverul transmite înapoi un mesaj SERVER-HELLO conţinînd numărul acestuia S, unele specificaţii ale cipherului SP_s, o conexiune ID aleatoare R_s şi cheia publică K_s şi certificatul cheii publice C_s.

3. Clientul verifică certificatul servirului C_s pentru a se asigura că K_s aparţine lui *S*. Atunci, clientul generează PMSK (Pre-Master-Secret-Key). Din PMSK, clientul derivează alte trei chei simetrice, inclusive MSK (Master-Secret-Key), CWK (Client-Write-Key) şi SWK (Server-Write-Key). La server se transmite PMSK (criptat cu k_s), la fel ca un mesaj FINISHED inclusive codul mesajului de autentificare (MAC) sau MSK (keyed hash) şi toate transmisinile precedente (criptate cu CWK).
4. Serverul trimite înapoi mesajul FINISHED cu MAC a MSK şi toate transmisiunile precedente (criptate cu SWC). Atunci serverul începe transmiterea datelor actuale.

Infrastructura cheilor publice

Un certificat trebuie să includă ceva de genu unei date de expirare, însă CA poate revoca certificatul apriori acestiu timp din cîteva motive.

CRL (Certificate Revocation List), care este o listă semnată si fixată in timp de către CA specificînd care certificate au fost revocate în acord cu unii identificatori. Aceste CRL trebuie distribuite periodic chiar dacă nu există scimbări pentru a preveni reutilizarea ilegală a certificatelor. (CRL este similar cu listele negre a companiilor de carduri credit, cardurile cărora nu mai sunt valide). Un aspect important este simplitatea. Managementul CRL trebuie realizat cu luare în consideratie a preturilor comunicatiei: scanării şi verificării. Prin criptare listei ca şi frunzele arborelui Merkle putem obţine îmbunătaţiri a performanţei. Această idee a fost întrodusă de Kochev in 1998.

Se poate de omis utilizarea listelor prin oferirea autorizării certificatului abilitatea de a răspunde on-line validitatea cererilor despre certificatele respective.

OCSP (On-line Certificate Status Protocol) – Myers in 1999. Acest model are un dezavantaj major. În particular răspunsul CA trbuie transmisă securizat, care necesită ca fiecare răspuns să fie semnat digital. Acest proces este scump, luînd în consideraţie că CA trebuie să răspundă la numeroase cereri. Semnăturiile prin sine sunt lungi, astfel costurile comunicaţiei prin OCSP sunt majore .

Certificarea bazată pe Hash

Schema NOVOMODO (1996) lui Micali realizează multe din aceste probleme prin utilizarea lanţurilor hash în conjunctură cu o semnătură digitală singulară pentru amortizarea costului semnăturii digitale pentru multe intervale. La fel, lanţurile hash, diminuează semnificativ costurile comunicaţiei.

Criptarea bazată pe certificate

Schema Gentry (2003) descrie cum este utilizată structura ierarhică pentru îmbunătăţirea eficientă şi scalabilităţii. Avantajele acestei metode cu respect a infrastructurii nu sunt la fel de importante în afara contextului de criptare.

Criptografia bazată pe identitate

Ca şi schemele anterioare, aceasta poate fi sonsiderată similară cu managementul certificatului şi totuşi este într-atit de diferit încît merită o analiză separată. Algoritmul dat se dezice atît de certificate cît şi de cheile publice. Totuşi sunt multe din avantajele criptografiei cu cheie publică şi de asemenea posedă avantaje semnificative. Dezavantajele majore sunt centralizarea excesivă şi utilizarea generatorului de chei publice, care ar permite decriptaera mesajelor şi falsificarea semnăturilor oricăruia [2].

Concluzii

Este destul de clar că securizarea în NGN este un obiect demuncă continuă. Cu toate că există o mulţime de instrumente excelente, heterogenitatea XG a introdus mult mai multe probleme. Totuşi, aceste probleme reprezintă oportunitpţi pentru cercetări ulterioare. Cu atît mai mult, cu cît se avansează în arta criptografică, cu atît mai tentantă devine spargerea algoritmilor şi sistemelor de criptare şi cu atît mai multe posibilităţi de dezvoltare apar.

Bibliografie

1. ITU-T Recommendation Y.2001, *General overview of NGN*. 2004, p.1-7.
2. Minoru Etoh, *Next Generation Mobile Systems 3G and Beyond*. John Wiley & Sons, New York, 2005, p.285-314.