ALEXANDRU TĂBUŞCĂ

ÎMBUNĂTĂŢIREA SECURITĂŢII TRANSMISIILOR DE DATE ÎN CADRUL REŢELELOR DE CALCULATOARE

ALEXANDRU TĂBUŞCĂ

ÎMBUNĂTĂŢIREA SECURITĂŢII TRANSMISIILOR DE DATE ÎN CADRUL REŢELELOR DE CALCULATOARE

PRO UNIVERSITARIA
2014
BUCUREŞTI

Descrierea CIP a Bibliotecii Naționale a României
TĂBUŞCĂ, ALEXANDRU
Îmbunătățirea securității transmisiilor de date în cadrul rețelelor de calculatoare / Alexandru Tăbuşcă. - Bucureşti : Pro Universitaria, 2014
Bibliogr.
ISBN 978-606-26-0169-0

004

ACTUALITATEA ŞI GRADUL DE STUDIERE ACTUAL AL PROBLEMEI ADUSE ÎN DEZBATERE

... Aproape că nu mai este cazul să detaliez „actualitatea" temei, aceasta fiind deja oarecum subînțeleasă de toți cei cu preocupări în domeniul it sau orice alt domeniu cât de cât conex... adică practic orice domeniu din viață cotidiană a secolului XXI.

Pentru a începe cu dreptul și în cunoștință de cauză citirea acestei teze de doctorat trebui să aduc întâi în prim plan însăși termenul de bază din cadrul titlului "**securitatea**".

Conform unei definiții academice aceasta poate fi astfel definită:

Securitatea informațiilor reprezintă protejarea informațiilor şi a sistemelor informaționale împotriva accesului, utilizării, divulgării, întreruperii funcționării, modificării sau distrugerii neautorizate a acestora, cu scopul de a se asigura:

• Integritatea informațiilor - adică protecția împotriva modificării sau distrugerii neautorizate a informațiilor, incluzând aici și asigurarea non-repudierii şi autenticității informațiilor;

• Confidențialitatea informațiilor - adică prezervarea restricțiilor autorizate de acces şi divulgare, inclusiv mijloacele pentru protecția datelor personale şi a informațiilor proprietare și/sau confidențiale;

• Disponibilitatea informațiilor – adică asigurarea accesului şi a utilizării informațiilor într-un interval de timp rezonabil.

În general, în conjuncție cu termenul de "securitate" în sens informatic, al asigurării securității datelor, sunt întâlniți mai mulți termeni: autorizare, control, virtualizare, proceduri și criptare. Autorizarea se referă la "cine" are voie să manipuleze anumite date; controlul se referă la modalitățile de a avea permanent cunoștință despre operațiile realizate cu datele respective; virtualizarea se referă la prezentarea datelor unor anumiți utilizatori numai în "copie" pentru a se evita posibila lor deteriorare; procedurile speciale se referă la diverse seturi de acțiuni sau programe care conlucrează în vederea introducerii sau menținerii unui climat de siguranță; criptarea se referă la "cifrarea" datelor astfel încât acestea sa nu fie inteligibile decât pentru cei cărora le sunt destinate.

In cadrul tezei mele de doctorat mă voi axa practic pe ultima componentă a acestui concept de securitate informatică a datelor: **criptarea**. Acest concept asigură în mare parte posibilitatea transmiterii datelor dintr-o locație în alta în siguranță, fără ca o eventuală parte neautorizată să aibă acces la respectivele date.

Securitatea transmisiilor de date a fost o problemă apărută cu mii de ani în urmă! Încă din primele stagii ale unor societăți umane cât de cât organizate un grup a avut secrete față de alt grup. Între mărturiile documentate privind primele metode și sisteme de criptare a informației astfel încât cineva neautorizat să nu aibă acces la ea găsim elemente din perioada Egiptului antic, a Feniciei, a celebrilor spartani sau a persanilor.

Avansând de-a lungul istoriei omenirii ajungem la cifrul lui Cezar, probabil primul sistem de codificare compatibil și comparabil chiar cu cele din zilele noastre, la o distanța în timp de peste 2000 de ani.

Dacă până în secolul XIX securitatea datelor prin criptare înseamnă în general cifrarea unui mesaj text astfel încât doar destinatarul să îl poată înțelege, din momentul descoperirii electricității și telegrafului problema a început să devină mai complexă.

Apoi au apărut, pe la mijlocul secolului XX, echipamentele electronice de stocare și manipulare a datelor iar următorul pas logic a fost interconectarea lor pentru a face schimb de astfel de date.

Principalii utilizatori și promotori ai sistemelor de securitate au fost pentru mult timp în principal organizațiile și instituțiile naționale precum și cei din domeniul militar. Odată cu adevărata explozie a utilizării pe scară largă, nu doar industrială ci și casnică, a echipamentelor și dispozitivelor electronice de calcul, comunicații și divertisment asigurarea securității datelor a devenit un element primordial însă și pentru majoritatea companiilor principale ce acționează pe piața economică de zi cu zi.

Interconectarea calculatoarelor în rețeaua globală INTERNET din zilele noastre a adus încă un plus în ceea ce privește necesitatea asigurării unui grad sporit de securitate metodelor de transmisie și stocare a datelor în format electronic. Este ușor de imaginat ce probleme ar putea crea alterarea datelor prelucrate de calculatoare nu numai în domenii ca sănătatea sau activitățile financiar-bancare, dar chiar și în cazuri mai puțin spectaculoase, ca de exemplu alterarea poștei electronice a unui utilizator, în contextul în care astăzi sistemul de comunicare prin e-mail este un element cvasi-prezent în viața noastră cotidiană.

În ceea ce privește gradul de studiere al problemei în literatura de specialitate practic este imposibil să menționez măcar un număr aproximativ de lucrări de referință în domeniu. Problematica a fost practic studiata continuu în ultimele... mii de ani din istoria actuală a omenirii. Mai mult, în zilele noastre miliarde de oameni se bazează zilnic, la orice banală utilizare a calculatorului personal, pe rezultatele cercetărilor și teoriilor unor nume celebre în domeniu: Rivest, Shamir, Adleman, Zimmerman, Diffie, Hellman, Rijmen sau Daemen.

Aproape an de an apar teorii și algoritmi noi și deși, într-adevăr, nu toate aceste soluții devin celebre și de neînlocuit ele arată totuși constanta preocupare a unora dintre cele mai strălucite minți ale secolelor XX și XXI pentru îmbunătățirea acestor aspecte privind securitatea transmisiilor de date.

Mai mult, alături de teoriile pur matematice în domeniu se îngemănează utilizarea mai multor ramuri științifice distincte: electronica, optica și mai nou cuantica joacă un rol de prim rang în aceste procese de asigurare a securității.

I - ALGORITMI DE CRIPTARE – PIATRA DE TEMELIE A SECURITĂŢII INFORMATICE

În universul complex și plin de potențiale pericole din ziua de azi este practic imposibil de imaginat existența omului fără acces la calculator. Chiar fără să ne dăm seama în mod direct multe acțiuni sunt dictate și controlate de fapt de utilizarea unor calculatoare! Astăzi apa menajeră, circuitele telefonice, centralele termice care asigură încălzirea, programul de creștere și producție al fermelor animale, asistența socială, asistența medicală și în general orice serviciu este asistat sau coordonat măcar parțial de un set de calculatoare.

În întâmpinarea nevoilor tot mai stringente de securitate sporită a venit **criptografia** - o ramura științifică bazată pe matematică și algoritmi din ce în ce mai puternici. “Adversarul” criptografiei este și el bazat pe teorii matematice, fiind cunoscut sub denumirea de **criptanaliză**. Ambele ramuri ale științelor aplicate au mers destul de aproape una de cealaltă și este de presupus ca aceeași tendință se va menține, cel puțin pentru viitorul apropiat. Metodelor noi de criptare le-a fost descoperită destul de repede o metodă oponentă în domeniul criptanalizei iar în momentul în care criptanaliza „amenință” serios securitatea s-au descoperit și implementat noi metode de criptare.

Până acum, diferența principală între cele două științe este făcută în principal de echipamentele hardware care nu reușesc, deocamdată cel puțin, să susțină operațiile extrem de complexe și numeroase impuse de criptanaliză pentru a reuși să descifreze rezultatele criptografiei de vârf într-o perioadă de timp foarte scurtă. Practic orice metodă criptografică poate fi atacată prin metoda atacului cu „forță brută” – “brute-force attack”, detaliat și exemplificat mai târziu și în cadrul tezei mele; acest atac este însă astăzi aproape imposibil de utilizat în majoritatea cazurilor de algoritmi de criptare moderni, necesitând resurse de timp și hardware uneori imposibil chiar de imaginat și în imensă majoritate a cazurilor ar aduce rezultate mult prea târziu pentru a mai fi viabile.

Acest prim capitol al tezei mele prezintă, din punct de vedere principial, mai multe metode de criptare pe baza de algoritmi diferiți, însoțite de caracterizări și considerații personale privind eventualele atacuri la care acestea pot fi supuse.

Aparatul matematic folosit citează lucrări recunoscute în domeniu neavând decât rol de suport în ceea ce privește înțelegerea de ansamblu a modelelor, în vederea unei reușite depline a implementării lor în cadrul unor aplicații software funcționale. Calculele matematice complexe au fost ocolite, fiind menținute doar acele explicații care sunt vitale pentru perceperea mecanismului descris, ele nefăcând de fapt obiectul acestei teze.

1. ELEMENTE DE BAZĂ ÎN UNIVERSUL CRIPTOGRAFIC

1.1 TERMINOLOGIE

Adresant și Receptor

Adresantul este cel care trimite mesajul către Receptor. Acest adresant dorește să trimită mesajul către Receptor în condiții de securitate.

Mesaj și Criptare

Un mesaj este, în general, un text în clar. Procedeul de deghizare a mesajului în așa fel încât acesta să nu poată fi înțeles decât de Receptorul căruia îi este destinat se numește Criptare. Un mesaj criptat este denumit și mesaj cifrat. Procedeul de transformare a unui mesaj cifrat în mesaj în clar se numește Decriptare. Știința care se ocupă cu securitatea mesajelor se numește criptografie iar cercetătorii respectivii criptografi. De asemenea, există o ramură a matematicii care se ocupă cu studiul criptografiei și criptanalizei și care se numește generic criptologie.

Pe scurt, matematic, criptarea poate fi redată folosind următoarele simboluri:

M - pentru mesaj
P – pentru text plan
C – pentru textul cifrat
E – funcția de criptare
D – funcția de decriptare

$E(M) = C$ și $D(C) = M$

Cum întreaga logică a criptării și decriptării consta în recuperarea mesajului original rezultă normal și următoarea formula:

$D(E(M)) = M$

Autentificare, Integritate și NonRepudiere

Pe lângă asigurarea confidențialității, criptografia trebuie să asigure și cel puțin alte trei lucruri de bază:

1. Autentificarea – trebuie să existe posibilitatea Receptorului de a cunoaște Adresantul; un intrus nu trebuie să aibă posibilitatea de a lua locul legitim al unui eventual Adresant;
2. Integritatea – trebuie să existe posibilitatea Receptorului de a verifica faptul ca mesajul a ajuns complet; un intrus nu trebuie să aibă posibilitatea de a substitui o parte a mesajului fără a fii detectat;
3. Non-repudierea – un Adresant nu trebuie să aibă posibilitatea de a nega trimiterea reala a unui mesaj.

Autorizarea

Reprezintă determinarea faptului că un utilizator sau un calculator are dreptul de a efectua o anumita operațiune, cum ar fi de exemplu accesarea unui fișier sau execuția unei aplicații.

Algoritmi și chei

Un algoritm criptografic, denumit și cifru, este o funcție matematica folosită pentru criptare și respectiv decriptare. Dacă securitatea oferită de algoritm se bazează pe păstrarea secretului modului său de funcționare atunci algoritmul se numește algoritm restrictiv. Acest tip de algoritmi au fost îndelung folosiți dar în momentul actual sunt depășiți, utilizarea lor în continuare fiind bazată doar pe diverse elemente conjuncturale.

Criptografia modernă rezolvă problemele algoritmilor restrictivi cu ajutorul utilizării unor elemente denumite chei, notate simbolic în general cu simbolul K. Spectrul valorilor posibile pentru o cheie se numește spațiul cheii. Atât criptarea cât și decriptarea folosesc aceeași cheie. Există însă și algoritmi care folosesc cheii diferite pentru criptare și respectiv decriptare:

$Ek_1 (M) = C$
$Dk_2 (C) = M$
$Dk_2 (Ek1(M)) = M$

Întreaga responsabilitate a asigurării securității bazate pe criptarea datelor se bazează pe chei. Acest lucru asigură o mare flexibilitate metodelor de criptare și dă posibilitatea publicării deschise a algoritmilor, analizării lor amănunțite de orice persoană interesată.