Security models and attacks on computer systems

Alin Titus Pîrcalab,
Doctorand, ASE Bucureşti

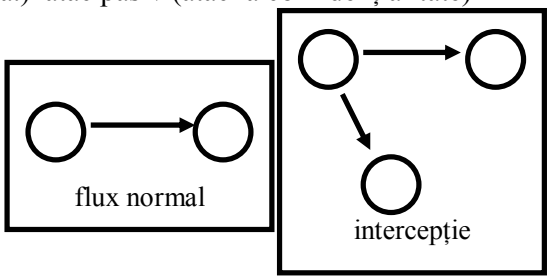
The appearing and continuous development of computer use in each and every field of activity, the existence and powerful revolution of international and national network, communication globalization are only a few of the informational premises of our society we are now stepping into. All these show a huge increase of the volume and importance of transmitted and storage data and eventually of their vulnerability (exposure). The attack over the security of a cryptographic system defines any action that compromises the security of that system.
Keywords*: cryptography, attacks, passive attacks, active attacks, cryptanalytic attacks, security.*

Atacuri asupra securităţii sistemelor criptografice

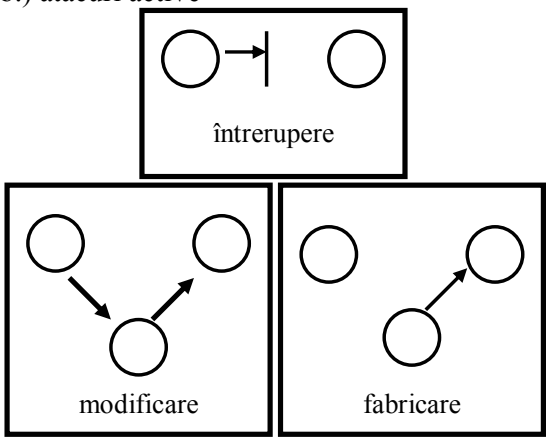
Atacul asupra securităţii unui sistem criptografic defineşte orice acţiune ce compromite securitatea acelui sistem.

O ilustrare sugestivă a principalelor tipuri de atacuri asupra unui sistem informatic este făcută in figura următoare:

a.) atac pasiv (atac la confidenţialitate)



b.) atacuri active



Atacurile criptografice pot fi îndreptate împotriva:

- algoritmilor criptografici;
- tehnicilor utilizate pentru implementarea algoritmilor şi protocoalelor;
- protocoalelor.

După modul de atacare al unui *atacator / intrus / persoană neautorizată / pirat (attacker / intruder / pirat),* aceste atacuri se pot clasifica după cum urmează:

- atacuri pasive (de intercepţie):
  - ❖ de înregistrare a conţinutului mesajelor ;
  - ❖ de analiză de trafic;
- atacuri active:
  - ❖ de întrerupere (atac la disponibilitate);
  - ❖ de modificare (atac la integritate);
  - ❖ de fabricare (atac la autenticitate).

Atacurile pasive sunt atacuri in care intrusul (persoană, calculator, program) doar ascultă, monitorizează transmisia, deci sunt *atacuri de intercepţie.* Ele pot fi de două feluri:

- *de înregistrare a conţinutului mesajelor (release of message contents),* de exemplu în convorbirile telefonice, în posta electronică, fapt pentru care dacă mesajele nu sunt criptate, se violează caracterul confidenţial al comunicaţiei;
- *de analiză a traficului (traffic analysis):* în cazul în care mesajele sunt criptate şi nu se poate face rapid criptanaliza, prin analiza traficului se pot afla o serie de date utile criptanalizei precum identitatea părţilor ce comunică între ele, frecvenţa şi lungimea mesajelor.

Caracteristicile atacurilor pasive:

- sunt greu de detectat pentru că datele nu sunt alterate;
- măsurile ce pot fi luate pentru evitarea acestor atacuri sunt acelea care fac criptana-

liza extrem de grea dacă nu imposibilă;
• este necesară prevenirea şi nu detecţia lor.
Atacurile active sunt atacuri în care intrusul are o intervenţie activă atat în desfăşurarea normală a traficului, cât şi în configuraţia datelor (modificarea datelor, creearea unor date false). Dintre atacurile active amintim :
• *întreruperea / refuzul serviciului (denial of service)*: un bloc funcţional este distrus, sau se inhibă funcţionarea normală sau managementul facilităţilor de comunicaţie; acest tip de atac este un *atac Ia disponibilitate (attack on availability) ;*
• *modificarea:* mesajul iniţial este întârziat, alterat, reordonat pentru a produce efecte neautorizate ca de exemplu:
  ▪ schimbare de valori in fişiere de date;
  ▪ modificări în program astfel încât acesta va lucra diferit;
  ▪ modificarea conţinutului mesajelor transmise în reţea.
• *fabricarea:* un neavizat inserează informaţii false în sistem; acest atac este un atac *la autenticitate.* Din această categorie fac parte şi:
  ▪ *mascarea (masquerade):* o entitate pretinde a fi altă entitate. Exemplu: secvenţele de autentificare pot fi capturate şi după validarea unei autentificări se înlocuiesc, permiţând astfel unei entităţi să obţină privilegii pe care nu le are de drept.
  ▪ *reluarea (replay)* constă în capturarea prin atac pasiv a unei cantităţi de informaţie şi transmiterea sa ulterioară pentru a produce efecte neautorizate.
Caracteristicile atacurilor active:
• deşi pot fi detectate, prevenirea lor este foarte grea, deoarece ar însemna protecţie fizică permanentă a întregului sistem.

Atacuri criptanalitice
Atacurile criptanalitice sunt atacuri asupra textelor cifrate în vederea obţinerii textului în clar sau a cheilor folosite pentru decriptare.
Există mai multe tipuri de asemenea atacuri dintre care amintim:
1) *Atac asupra textului cifrat (cipher text-only attack):* criptanalistul are criptograma $C_1 = Ek (M_1)$ şi trebuie să obţină mesajul în clar (Mi*)* sau cheia k.
2) *Atac asupra unui text cunoscut (known plain-text attack):* criptanalistul are criptogramele Ci*,* şi mesajele în clar Mi*,* corespunzatoare şi trebuie să determine cheia k sau algoritmul de determinarea lui M_{i+1} din $C_{i+1} = Ek (M_{i+1})$;
3) *Atac cu text în clar ales (chosen plain-text attack):* se pot alege o serie de mesaje M*,* după dorinţă şi se cunosc criptogramele corespondente:$Ci = Ek (M_i)$. Criptanalistul trebuie să determine cheia k sau algoritmul de determinare al lui M_{i+1} din $C_{i+1} = Ek (M_{i+1})$.
4) Atac cu text în clar ales adaptiv (adaptive chosen plain-text attack): mesajele în clar Mi se pot alege după dorinţă şi sunt adaptabile în funcţie de rezultatele criptanalizelor anterioare, iar criptogramele Ci = Ek (Mi) se cunosc. Se cere cheia k sau algoritmul de determinare al lui M_{i+1} din $C_{i+1} = E_k (M_{i+1})$
Aceste patru atacuri constituie atacurile criptanalitice de bază. În afara acestora mai putem aminti:
5) Atac cu text cifrat Ia alegere (chosen cipher-text attack) în care se aleg Ci*,* şi Mi = Dk (Ci)*,* sarcina criptanalistului fiind determinarea cheii k. Acest atac se aplică mai ales algoritmilor cu chei publice.
6) *Atacul de "cumpărare" a cheii (rubber-hose cryptanalysis / purchase-key attack)*, în care aflarea cheii se face fără mijloace criptanalitice (se apelează la şantaj, furt, etc.) şi este unul dintre cele mai puternice atacuri.
Observaţie: Atacurile 3) si 5) se numesc atacuri cu text ales (chosen text attack) şi au fost folosite cu succes în cel de-al doilea război mondial pentru spargerea codurilor german şi japonez .

Securitatea algoritmilor
În secolul at XIX-lea, olandezul A. Kerckhoff a enunţat conceptul fundamental al criptanalizei: secretul se rezumă în întregime la cheie, algoritmul criptografic şi implementarea considerându-se cunoscute.
Diferiţii algoritmi pot asigura diferite grade de securitate, funcţie de dificultatea cu care pot fi sparţi :
• dacă costul spargerii unui algoritm este mai mare decât valoarea datelor criptate, algorit-

mul este *probabil sigur (PS);*

- dacă timpul necesar spargerii este mai mare decât valabilitatea datelor criptate, algoritmul este *PS*;
- dacă mulţimea datelor necesare spargerii este mai mare decât mulţimea datelor criptate la un moment dat de o cheie, algoritmul este *PS*.

Lars Knudsen - în teza de doctorat susţinută în 1994 - a clasificat diferitele categorii de spargere a unui algoritm în ordine descrescătoare a securităţii:

1) *Spargere totală (total break) / securitate zero*: un criptanalist găseşte cheia, deci orice criptogramă va fi decriptată: Dk(C) = M;

2) *Deducţie globală (global deduction)*: criptanalistul găseşte un algoritm alternativ echivalent cu Dk (C) fără a cunoaşte cheia k;

3) *Deducţie locală (local deduction)*: un criptanalist găseşte textul în clar al unui text cifrat interceptat;

4) *Deducţia informaţională (information deduction)*: criptanalistul capătă unele informaţii privitor la cheie sau la textul în clar (de exemplu câţiva biţi ai cheii, anumite informaţii privitoare la M, etc.) ;

5) *Algoritm computaţional puternic (computational strong)* este algoritmul care nu poate fi spart cu resursele existente, atât la momentul curent, cât şi într-un viitor predictibil ;

6) *Algoritm necondiţionat sigur (unconditional secure)* este algoritmul pentru care indiferent cât text cifrat are criptanalistul, informaţia nu este suficientă pentru a deduce textul în clar. Privitor la aceşti din urmă termeni trebuie atenţionat că sunt extrem de expuşi interpretărilor.

Observaţii:

- Doar *cheia de unică folosinţă (one time pad),* inventată în 1917 de Major J. Maubergue si Gilbert Vernon, având aceeaşi lungime cu a textului în clar, este *de nespart*.
- Toţi ceilalţi algoritmi pot fi sparţi cu ajutorul unui atac cu text cifrat, prin încercarea tuturor cheilor, până când textul descifrat are sens. Acest atac se numeşte *atac prin forţă brută (brute force attack).*

Complexitatea unui atac (complexity) se manifestă în mai multe feluri:

a) *Complexitatea datelor (data complexity)* este volumul de date necesar pentru atac;

b) *Complexitatea procesării / factorul de lucru (processing complexity / work factor)* este timpul necesar realizării atacului;

c) *Complexitatea stocării (storage complexity)* este cantitatea de memorie necesară atacului.

Regula: *complexitatea unui atac=max{a, b, c}.*

Bibliografie:

1) Angheloiu, I., Gyorfi, E., Patriciu, V.V. (1986): *Securitatea şi protecţia informaţiei în sistemele electronice de calcul,* Editura Militara, Bucureşti;

2) Angheloiu, I.(1972): *Teoria codurilor,* Editura Militară, Bucureşti;

3) Borda, M. (1999): *Teoria transmiterii informaţiei,* Dacia, Cluj-Napoca;

4) Deavours, C.A., Kahn, D. (1998): *Selections from Cryptologia,* Artech House;

5) Hankerson, D. R., Hoffman, D. G., Leonard, D. A., Linder, C.(2000): *Coding Theory and Cryptographv: The Essentials (Pure and Applied Mathematics,* Vol 234), Marcel Dekker, Rev&ex, 2nd edition, Sep.;

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 informatică în UNIX şi Internet,* Editura Tehnică, Bucureşti;

9) Patriciu, V. V. (1994): *Criptografia şi securitatea reţelelor de calculatoare,* Editura Tehnică, Bucureşti;

10) Stallings, W. (1999): *Cryptography and Network Security — Principles and Practice,* Prentice Hall, Second Edition;

11) T.I.Băjenescu, M.E.Borda – Securitatea în informatică şi telecomunicaţii; Ed. Dacia, Cluj Napoca, 2001;

12) V.V.Patriciu, M.Ene-Pietroşanu – Securitatea Comerţului Electronic – Ed.All, Bucureşti, 2001;

13) V.V.Patriciu, M.Ene-Pietroşanu – Securitatea în Informatica în UNIX şi Internet – Ed.Tehnică, Bucureşti, 1998;