Autor: Ruxandra F. Olimid
Departamentul de Informatică, Universitatea din București

- Laboratorul 2 -

Introducere în criptologie

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători**!

1. *Noțiuni generale*

Atribuiți fiecărui termen definiția corespunzătoare. Definițiile au fost preluate din glosarul de termeni *NIST – Computer Security Resource Center* [1].

(A) Criptologie	(1) Asigurarea că informațiile nu sunt dezvăluite entităților neautorizate.
(B) Criptografie	(2) Disciplina care studiază principiile, mijloacele și metodele de transformare a datelor pentru a ascunde conținutul lor semantic, a preveni utilizarea lor neautorizată sau a preveni modificarea lor nedetectată.
(C) Criptanaliză	(3) Asigurarea accesului și utilizării informațiilor în timp util și fiabil.
(D) Confdențialitate	(4) Știința care se ocupă de criptanaliză și criptografie.
(E) Integritate	(5) Încercarea de a înfrânge protecția criptografice fără o cunoaștere inițială a cheii utilizate în furnizarea protecției.
(F) Disponibilitate	(6) Protejarea împotriva modificării sau distrugerii necorespunzătoare a informațiilor.

2. *Triada Confidentiality, Integrity, Availability (CIA)*

Puteți citi mai multe despre *confidențialitate*, *integritate* și *disponibilitate* în [2].

Pentru fiecare dintre afirmațiile de mai jos, indicați proprietatea (proprietățile) CIA la care se face referire:

1. Salariile angajaților nu trebuie făcute publice.
2. Biroul casierie trebuie să aibă acces la salariile angajaților (pentru a realiza plățile).
3. Un angajat nu își poate modifica singur suma primită ca salariu pe luna în curs.
4. Un angajat nu ar trebui să afle cât câștiga un coleg fără acordul acestuia (ex. să îi spună direct).
5. Biroul casierie trebuie să aibă certitudinea că suma pe care o înmânează angajatului de plată este cea corectă.

Dați exemplu de *primitive criptografice* care se folosesc pentru a satisfacere o proprietate criptografică. Spre exemplu, ce primitivă criptografică oferă *confidențialitate*? Dar *integritate*?

3. Adversar Probabilistic Polinomial în Timp (PPT)

Citiți mai multe despre ce înseamnă un adversar *Probabilistic Polinomial în Timp* (PPT).

Răspundeți cu adevărat sau fals:

1. Un adversar care are la dispoziție un timp infinit pentru criptanaliza unui sistem este un adversar PPT.
2. Un adversar PPT are dreptul de a „ghici” cheia.
3. Un adversar PPT are la dispoziție algoritmi exponențiali în timp.

4. Funcții neglijabile

Înțelegeți ce înseamnă o funcție *neglijabilă* vs. *ne-neglijabilă* (într-un parametru de securitate, dpdv al unui adversar PPT, etc.).

Care dintre următoarele funcții sunt neglijabile în parametrul de securitate n, având în vedere un adversar PPT?

1. $f(x) = 2$
2. $f(x) = 1/2000$

3. $f(x) = 1/n^{2000}$
4. $f(x) = 1/2^n$
5. $f(x) = f1(x) + f2(x)$, unde $f1(x)$ și $f2(x)$ sunt neglijabile
6. $f(x) = f1(x) + f2(x)$, unde $f1(x)$ este neglijabilă și $f2(x)$ este ne-neglijabilă

5. Securitate computațională

Dați câteva argumente pentru care preferăm să utilizăm *securitatea computațională* în practică. De ce nu avem ca scop *securitatea perfectă* (i.e., indiferent de resursele adversarului un sistem să nu poată fi spart)? Discuție.

6. Atac prin forță brută/căutare exhaustivă

Se consideră un sistem criptografic care folosește o cheie de criptare pe 512 biți.

- Câte chei posibile distincte există?
- Cât timp îi va lua unui adversar găsirea cheii corecte (cazul cel mai nefavorabil) dacă are la dispoziție un calculator care testează 2^{30}chei pe secundă?
- Considerați că este un atac eficient?

Referințe bibliografice

1. National Institute of Standards and Technolohy (NIST) – Computer Security Resource Center (CSRC), *Glossary*. Accesibil la: https://csrc.nist.gov/glossary/ Ultima accesare: septembrie 2021.
2. Kryszczuk, K., & Richiardi, J. (2014). *Springer Encyclopedia of Cryptography and Security*. Accesibil la: https://www.researchgate.net/publication/230674947_Springer_Encyclopedia_of_Cryptography_and_Security Ultima accesare: septembrie 2021.