Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Cap. 1. Introducere în securitatea informatiei. Securitatea informației ca produs sau proces. Obiective de securitate. Tipuri de adversari si de atacuri.

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Ce este securitatea informatiei (sistemelor informatice)

- **Definitie:** Securitatea Sistemelor Informatice înseamnă protecţia sistemelor informatice împotriva accesului neautorizat sau a modificării informaţiei, fie stocată, procesată sau în tranzit, şi împotriva refuzului de servicii către utilizatorii autorizaţi sau asigurării de servicii către utilizatorii neautorizaţi, incluzând acele metode necesare detectării, documentării şi respingerii acestor ameninţări.

- **"Security is a process, not a product"**

- **Securitatea este un mod de a gandi** asupra unei probleme

A rezolva probleme inseamna a raspunde la intrebari

- Cateva intrebari fundamentale pentru a asigura securitatea unui sistem: Cum ajunge adversarul la sistem? Care sunt obiectivele de securitate care trebuie asigurate în sistem? Care este nivelul de securitate la care trebuie să răspundă sistemul? Ce trebuie protejat? Care sunt ameninţările şi vulnerabilităţile? Care sunt implicaţiile în cazul distrugerii sau pierderii echipamentului? Care este valoarea echipamentului pentru organizaţie? Ce poate fi făcut pentru a minimiza expunerea la pericole? Etc.

- Cum sa rezolvi o problema cu atatea intrebari: nicio problema nu rezista unei abordari riguroase!

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Un punct de plecare pentru o abordare riguroasa

- Ecuatie fundamentala in securitate:

$$\textit{Vulnerabilitate} + \textit{Adversar} \Rightarrow \textit{Risc de Securitate}$$

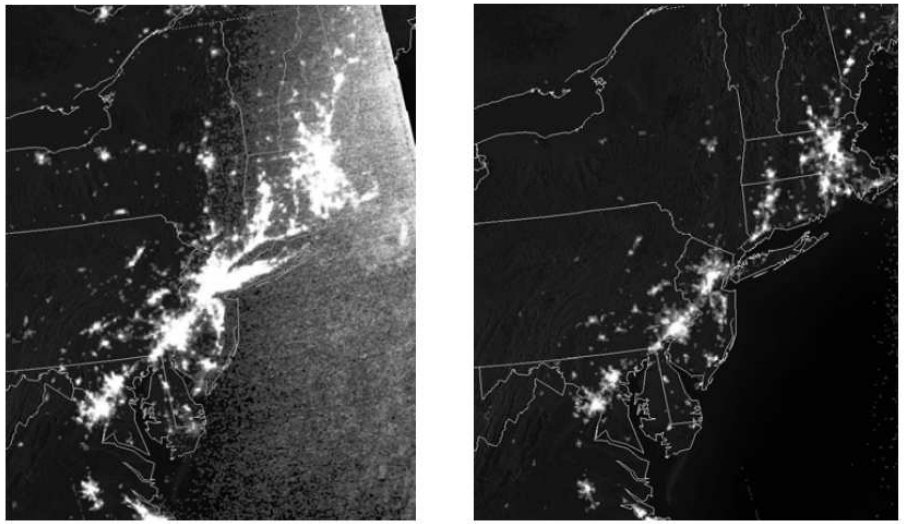
- Rezolvarea ecuatiei este in general un trade-off intre riscurile de securitate

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Cadrul de lucru

Motivatie

- Incidentul de securitate, cauzat de faptul ca exista adversari si vulnerabilitati, amploarea lui



a) b)

Figura 2.4. Căderea de energie electrică din August, 2003: a) înainte b) după

Evolutia cauzelor in incidente de securitate

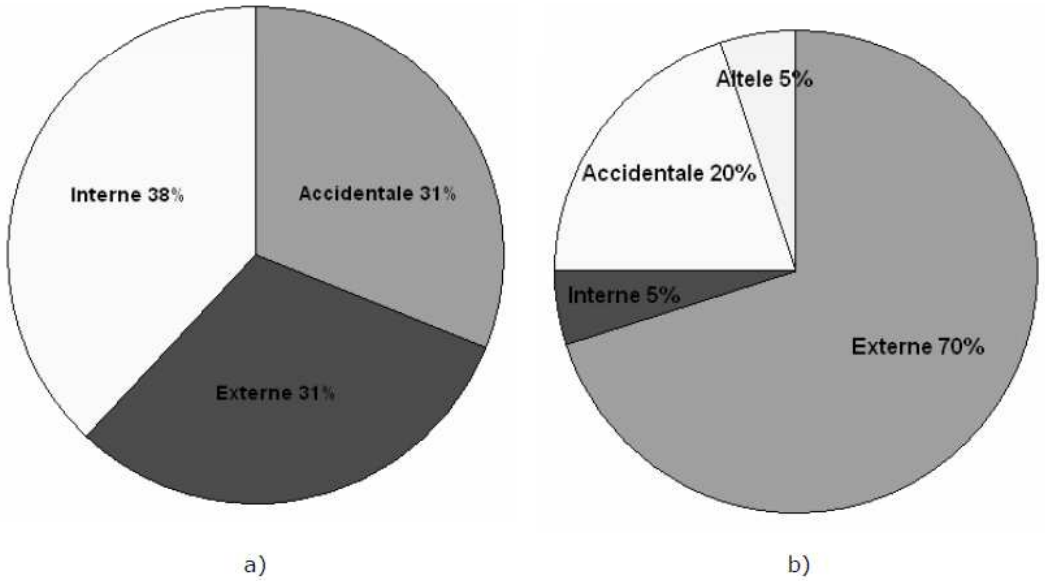


Figura 2.3. Tipuri de incidente de securitate a) în perioada 1982-2000 b) în perioada 2001-2003

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Justificare pentru evolutia cauzelor in incidente

- Evolutia de la securitate prin obscuritate la standarde (ratiuni economice)
- Evolutia de la perimetre inchise la perimetre deschise (trecerea la sisteme distribuite pe scara larga)
- Principii perimate: securitate prin obscuritate, perimetre sigure

Vulnerabilitatea se raporteaza la obiectivele de securitate

- In trecut: triada CIA (Confidentiality, Integrity, Availability), tetrada PAIN (Privacy, Availability-Authentication, Integrity, Non-repudiation)

- In prezent, in multe carti de criptografie apar ca obiective fudamentale:
  - **Confidenţialitatea -** faptul că informaţia rămâne accesibilă doar părţilor autorizate
  - **Integritatea -** informaţia nu a fost alterată
  - **Autentificarea** - două coordonate distincte: autentificarea entităţilor şi autentificarea informaţiei
  - **Non-repudierea -** previne o entitate în a nega o acţiune întreprinsă

Alte obiective

- **Actualitatea -** informaţia primită este proaspătă
- **Anonimitatea -** împiedicarea identificării identităţii unei entităţi care a solicitat un serviciu
- **Autorizarea -** controlul accesului şi la prevenirea intrării agenţilor neautorizaţi în sistem
- **Disponibilitatea -** asigurarea faptului că un serviciu este accesibil atunci când un utilizator legitim îl solicită
- **Protecţia părţilor terţe -** evitarea transmiterii pericolului asupra părţilor cu care există o legătură
- **Revocarea -** posibilitatea de a retrage un drept oferit
- **Trasabilitatea -** posibilitatea de a reconstrui istoricul funcţionării sistemului

Adversari (exemple)

- Intereseaza diverse caracteristici: putere de calcul, putere financiara, motivatie:
  - Hackerii: resurse de calcul şi financiare scăzute, motivaţi de dorinţa a brava sau pentru amuzament.
  - Clienţii unei reţele: putere de calcul limitată, motivaţi de interese economice
  - Comercianţii: putere de calcul modestă, resurse financiare apreciabile, interese financiare
  - Crima organizată: putere de calcul modestă, putere financiară ridicată, interese financiare.
  - Teroriştii: putere ridicată de calcul şi financiară fiind, motivaţi de raţiuni politico-religioase
  - Guverne: putere de calcul şi financiară ridicată, interese strategice.
  - Oamenii din sistem: motivaţi în general de interese financiare.

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013.
"Investește în oameni!"

Cel mai periculos adversar

- Combinaţii ale variantelor anterioare

Tipuri de atac asupra canalului de comunicare

- **Atacuri pasive**: citirea mesajelor şi analiza de trafic
- **Atacuri active**: modificarea informaţiei, impostura, retransmisie, întreruperea legăturii

Ce este criptografia

- "Criptografia înseamnă comunicare în prezența adversarilor" - Ron Rivest
- Intr-un sens mai strict, domeniul se numeste criptologie si inseamna criptografie (constructia codurilor) si criptanaliza (spargerea codurilor)

Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. "Investește în oameni!"

Context istoric

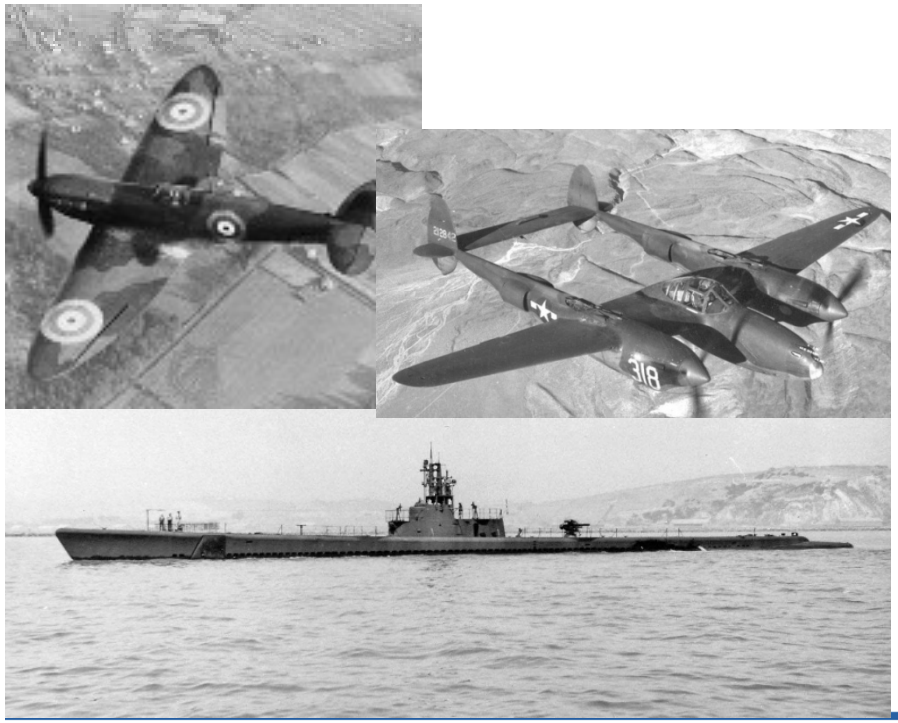
- Evolutie in 4 etape relevante:
  i. Preistoria: utilizata inca de acum mii de ani (greu de spus ca atunci s-a nascut criptografia pentru ca sistemele folosite era rudimentare)
  ii. Renasterea: Inregistreaza o usoara crestere in perioada renasterii (de ex. Sistemul Vigenere)

iii. Al 2-lea razboi mondial: Crestere relevanta (de ex. Enigma), dar si in deceniile premergatoare (Kerckhoff). Lucrari fundamentale ale lui Shannon si Turing

iv. O crestere spectaculoasa in ultimii 30-40 de ani

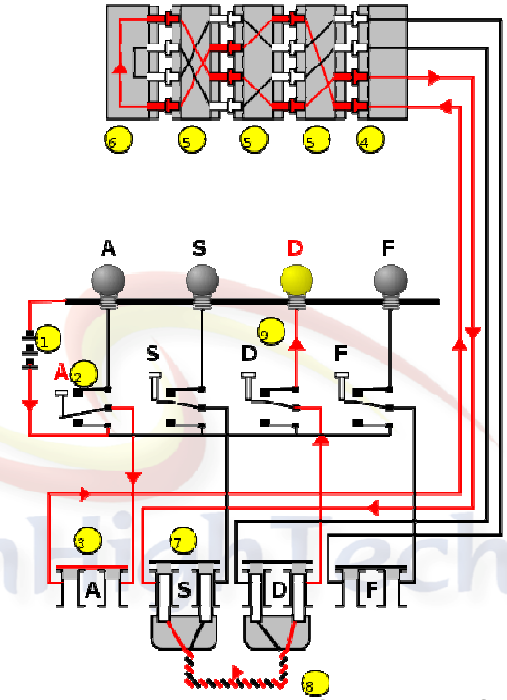
iii) si iv) au ca vector comunicatiile wireless

Ieri



Azi

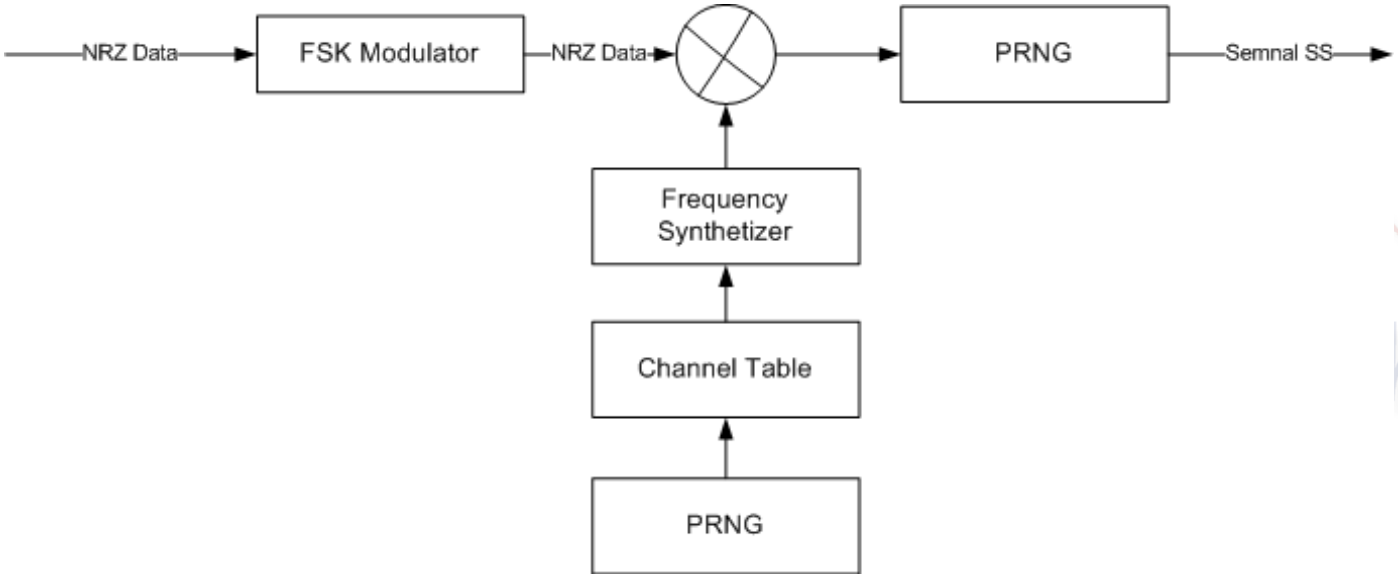
Masina Enigma (studiu de caz clasic)



- Circuit din wiki

Un alt exemplu din WW2

- Frequency hopping spread spectrum
- Diversi inventatori, intre titulari un nume mai interesant Hedy Lamarr



Directia curenta in criptografie

- Concepte gresite
  - Exista doua comunitati: a celor care construic functii si a celor care le sparg (intr-o vesnica lupta)
  - Criptografia urmareste constructia unor functii de criptare care nu pot fi sparte

- Intentii reale:
  - Constructia unei functii cat mai sigure cu o cheie de cat mai mica si cat mai eficienta computational