Sisteme de Încredere
- Securitatea -

Ciprian Dobre
ciprian.dobre@cs.pub.ro

Securitate

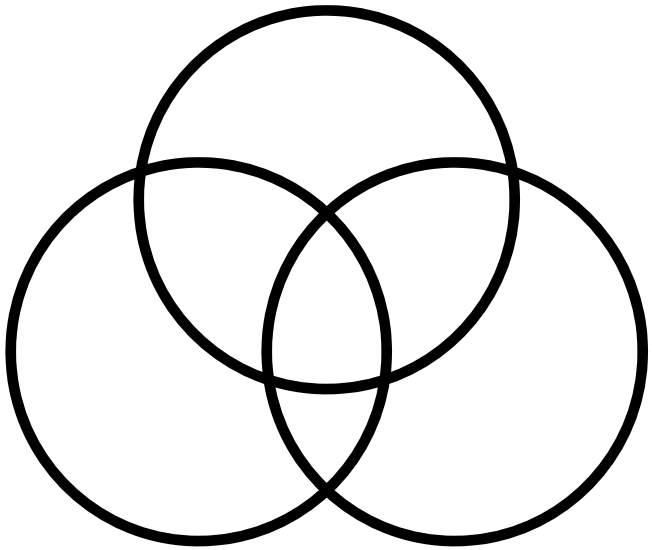
- O altă abordare specializată a fiabilității
  - Minimizarea apariției defectelor– particularizat la “atacurile ” intenționate
- Securitatea reprezintă: “protecția bunurilor”
- Tipuri de bunuri ce tb. protejate:
  - Date (e.g. stocare raw, sisteme de fișiere)
  - Informații (e.g. date confidențiale, personale)
  - Servicii
  - Resurse
  - Bani

Aspecte ale securității

- Confidențialitate
  - Anonimizare (date personal)
  - Secretizare (date organizaționale)
- Integritate
- Autentificare
  - Asigurarea că utilizatoul este cine pretinde că este
- Responsabilitate
  - Înregistrarea a ceea ce face fiecare utilizator

Obiective ale securității

SECRETIZARE
(CONFIDENȚIALITATE)



INTEGRITATE

DISPONIBILITATE
(DENIAL OF SERVICE)

Concepte de securitate

- Vulnerabilitate - problemă (c.f. fault)
- Atac – utilizarea vulnerabilității (c.f. error)
- Amenințare - vulnerabilitate+ atac
- Expunere – acces sau pierdere potențiale
- Penetrare – atac cu succes (c.f. failure)

Exemple

- Examples de:
  - Vulnerabilitate? Unlocked door
  - Atac? Burglar enters door
  - Amenințare? A break-in through door
  - Expunere? Loss of TV
  - Impact? Crime #312154

Măsurarea securității

- Securitatea este greu de cuantificat
- Depinde de ingeniozitatea atacatorului
- Securitatea este instabilă
  - Greu de prezis în viitor
  - Dispusă la modificări semnificative
  - Probleme de securitate pot apărea continuu

Asigurarea securității

- Abordări standarde pentru “fiabilitate”:
  - Evitarea vulnerabilităților
  - Tolerarea vulnerabilităților
  - Detecția compromiterilor
  - Reacția în fața compromiterilor

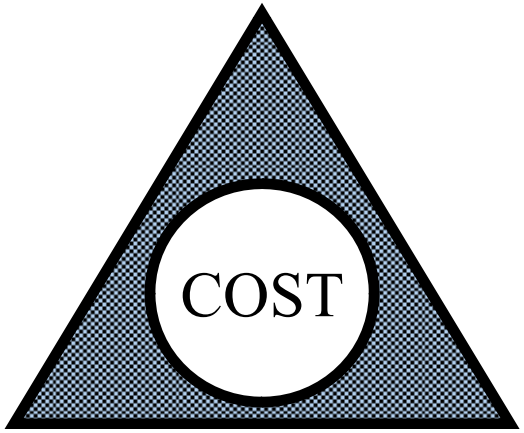
Tehnici de securitate

- **Prevenire accesului** **controlul**
- **Detecție** **auditare**
- **Toleranță** **practică**

Prevenirea și detecția se bazează pe autentificare

Securitatea și celelalte aspecte ale sistemului

SECURITATE



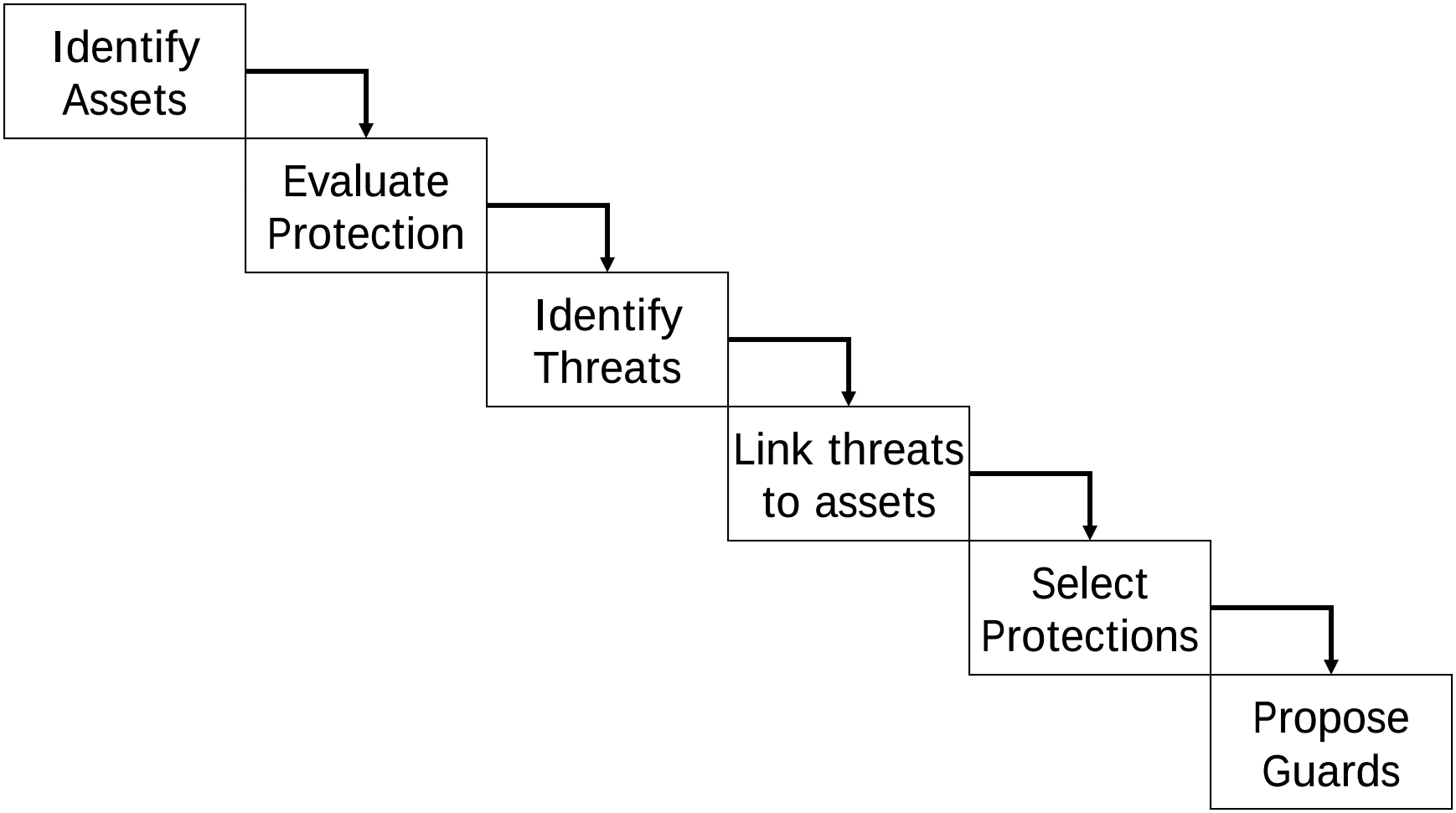
FUNCȚIONALITATE

UȘURINȚA ÎN FOLOSIRE

Cum se atinge securitatea?

- Politica — ce?
- Mecanismul — cum?
- Evaluarea — cât de bine?

Procesul de evaluare a securității



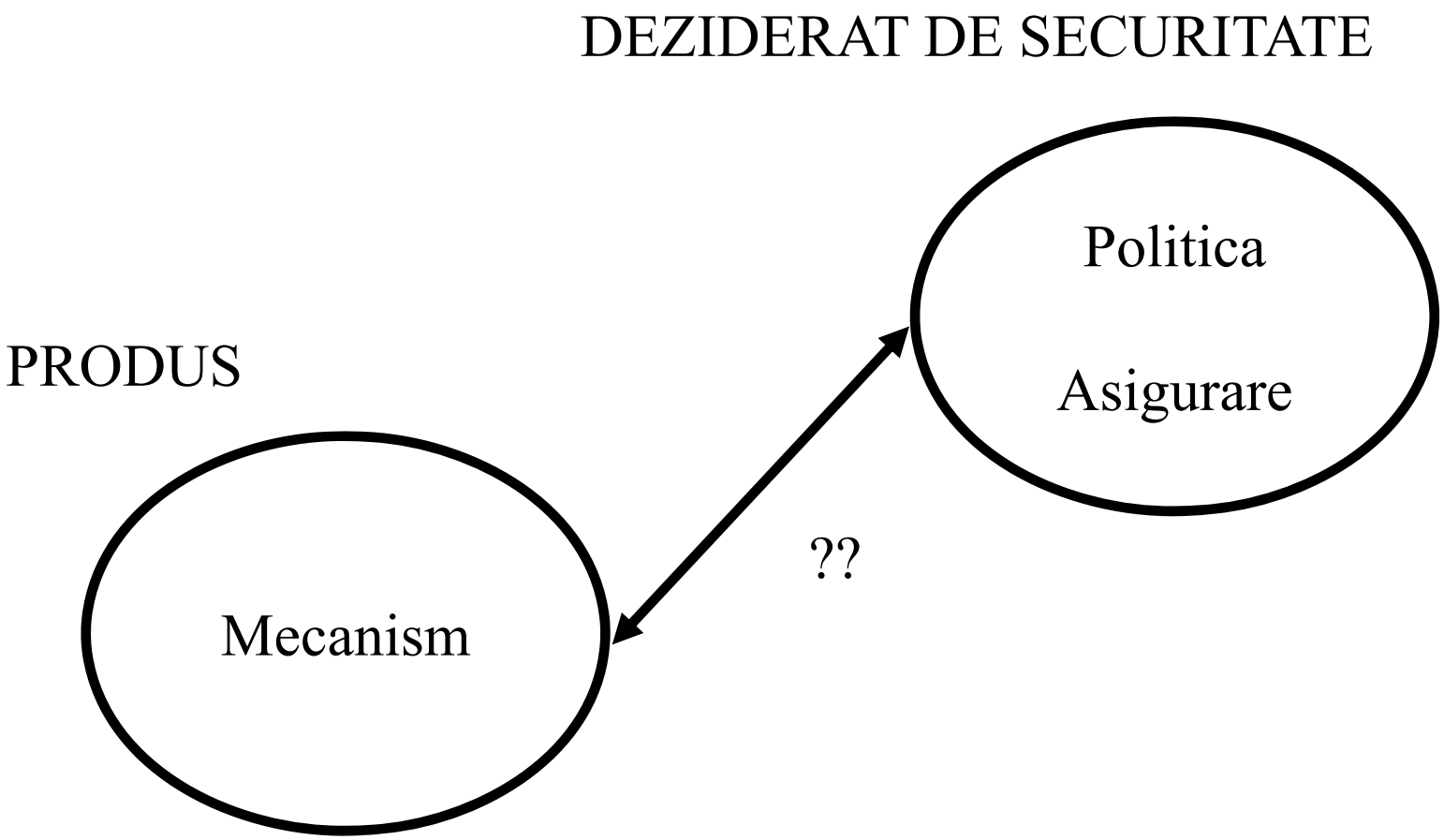
Evaluarea securității

- La fel ca în cazul altor atribute ale încrederii:
  - Putem evalua produsul sau
  - Putem evalua procesul
- Evaluarea poate fi efectuată de către:
  - Producător
  - Agenția guvernamentală
  - Compania de acreditare
  - Un organism de certificare independent

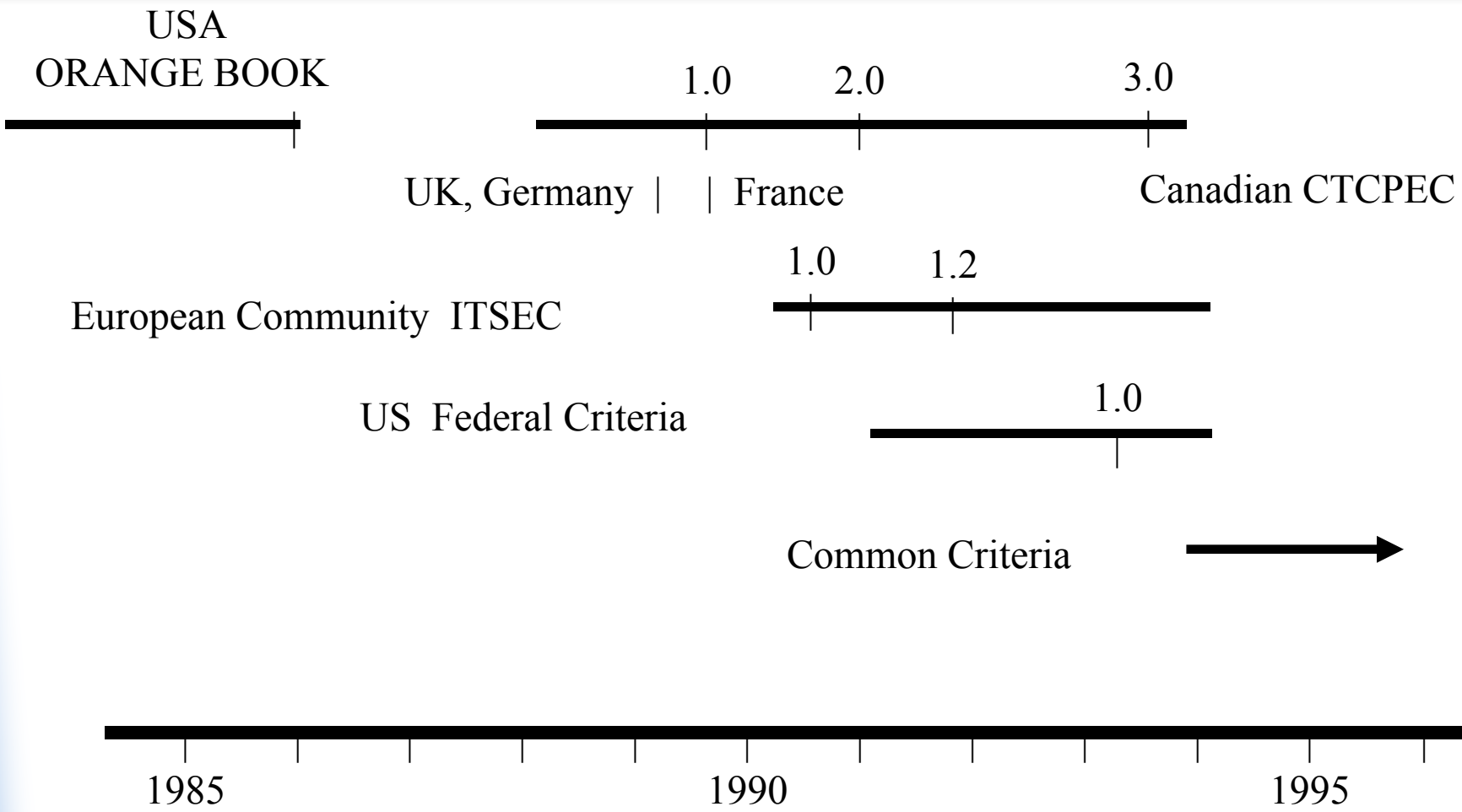
Instrumente de evaluare a securității

- Validare bazată pe experiență (bazată pe cazuri)
- Validare bazată pe instrumente (instrumente de probare)
- Tiger teams (atacatori de tip white hat)
- Verificare formală (metode formale)
- Procedura de certificare (org. specială de eval.)

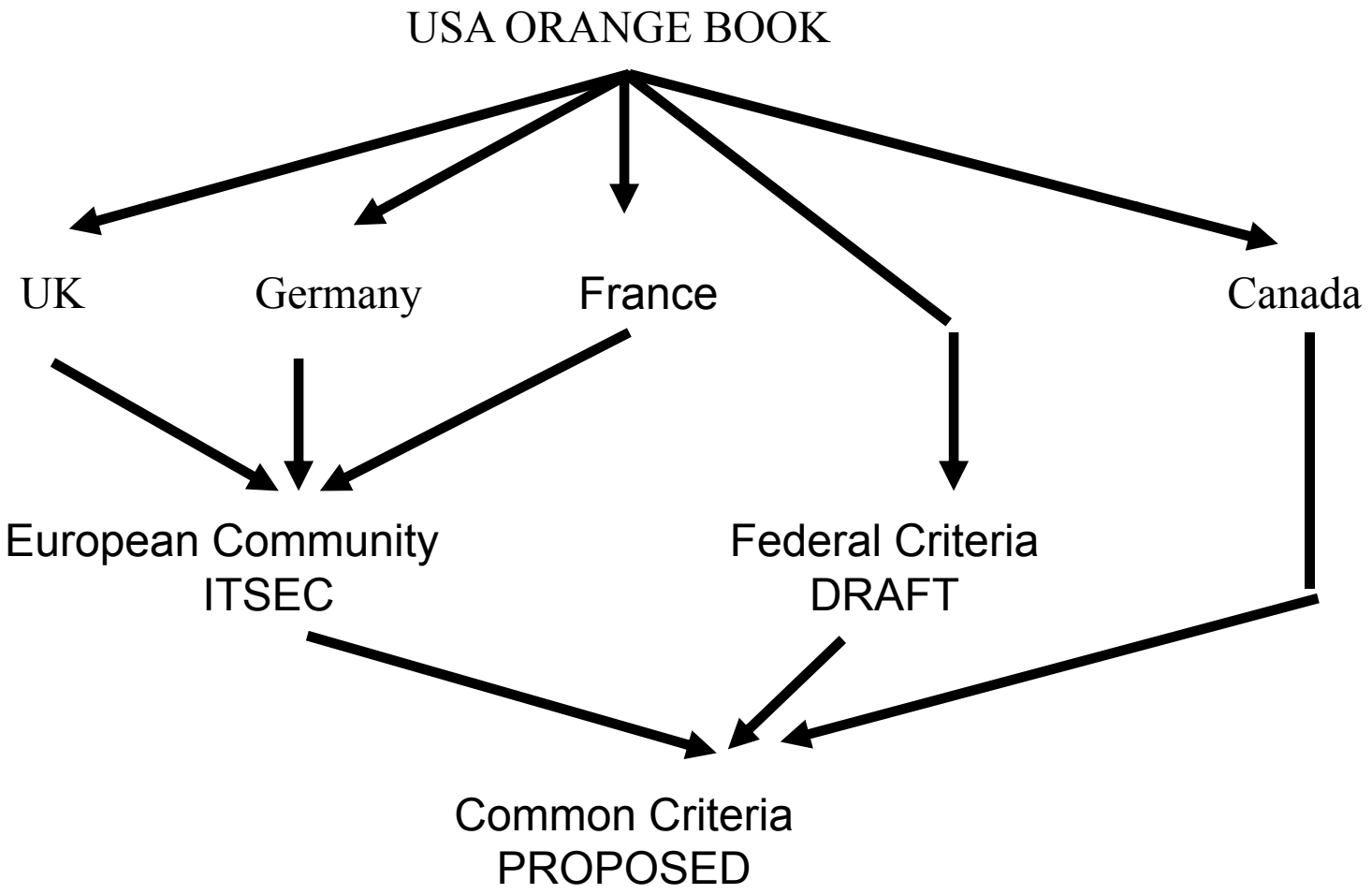
Criterii de evaluare



Diverse criterii



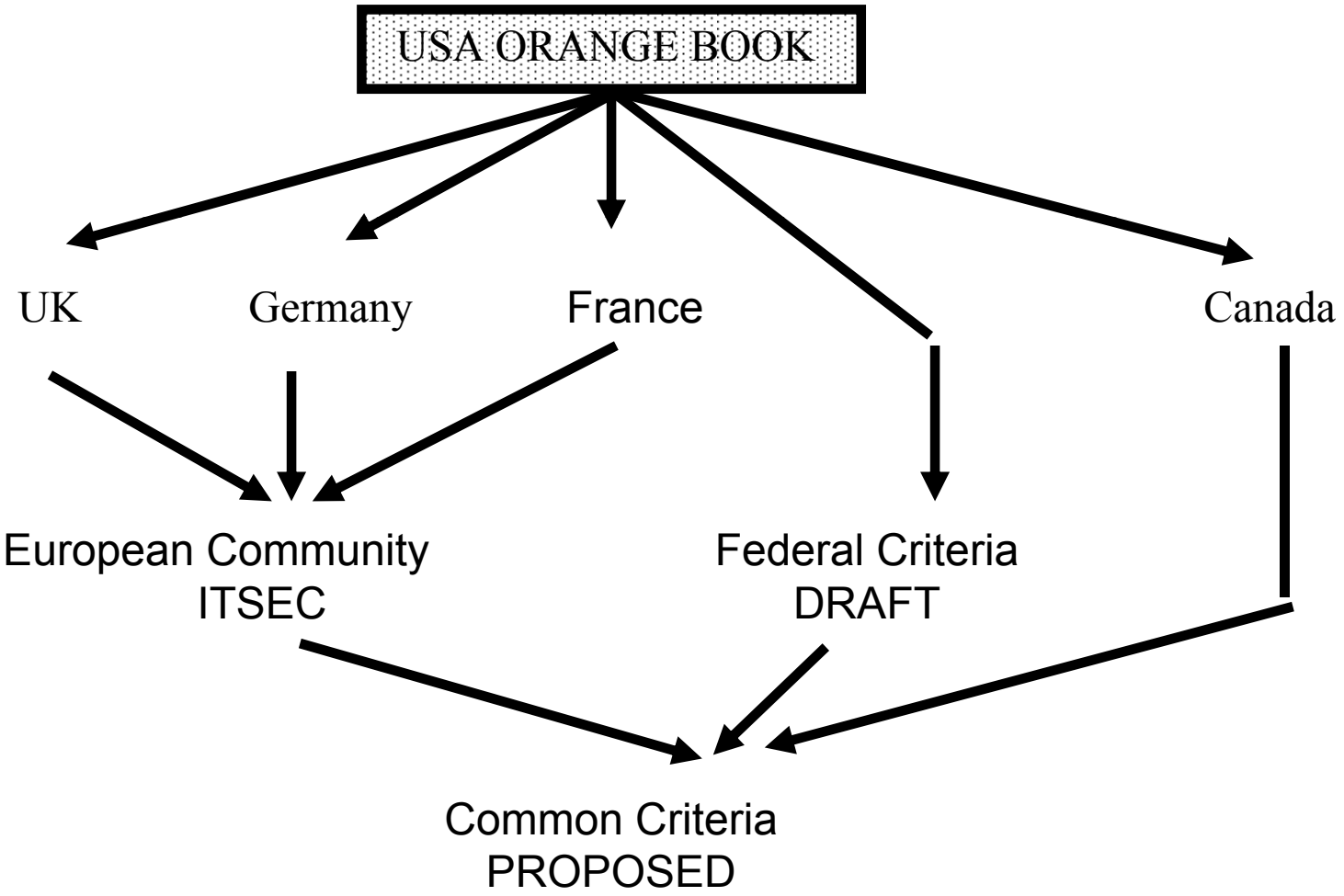
Relații între criterii



Evaluarea securității

- US Department of Defense – “Trusted Computer Security Evaluation Criteria”
  - A.K.A “The Orange Book”
  - Scop:
    - Îndrumar pentru producători (set de best practices)
    - Metodologie de comparare a securității sistemelor
    - Bază pentru specificarea necesităților de securitate

Orange Book


USA ORANGE BOOK
UK
Germany
France
Canada
European Community
ITSEC
Federal Criteria
DRAFT
Common Criteria
PROPOSED

Nivele de securitate Orange book

- D – Minimal
  - uncontrolled
- C – Discreționar
  - Protecție la nivelul obiectelor (fișier, dispozitiv, etc.) opțională
  - Oricine are același nivel de acces, aceleași permisiuni de acces
- B – Mandatoriu
  - Protecție obligatorie la nivelul obiectelor
  - Orice are permisiuni, spații izolate de adrese, administrator de securitate
- A – Verificat (rar)
  - Verificare folosind metode formale

Clase cf. Orange Book

HIGH SECURITY

NO SECURITY

A1: Verified Design

B3: Security Domains

B2: Structured Protection

B1: Labeled Security Protection

C2: Controlled Access Protection

C1: Discretionary Security Protection

D: Minimal Protection

Criterii pentru Orange Book

- POLITICA DE SECURITATE
- RESPONSABILIZAREA (ACCOUNTABILITY)
- ASIGURAREA (ASSURANCE)
- DOCUMENTAREA

Politica de Securitate

	C1	C2	B1	B2	B3	A1
Discretionary Access Control	+	+			+	
Object Reuse		+				
Labels			+	+		
Label Integrity			+			
Exportation of Labeled Information			+			
Labeling Human-Readable Output			+			
Mandatory Access Control			+	+		
Subject Sensitivity Labels				+		
Device Labels				+		

+ added requirement

Responsabilizarea

	C1	C2	B1	B2	B3	A1
Identification and Authentication	+	+	+			
Audit		+	+	+	+	
Trusted Path				+	+	

+ added requirement

Asigurarea

	C1	C2	B1	B2	B3	A1
System Architecture	+	+	+	+	+	
System Integrity	+					
Security Testing	+	+	+	+	+	+
Design Specification and Verification			+	+	+	+
Covert Channel Analysis				+	+	+
Trusted Facility Management				+	+	
Configuration Management				+		+
Trusted Recovery					+	
Trusted Distribution						+

+ added requirement

Documentarea

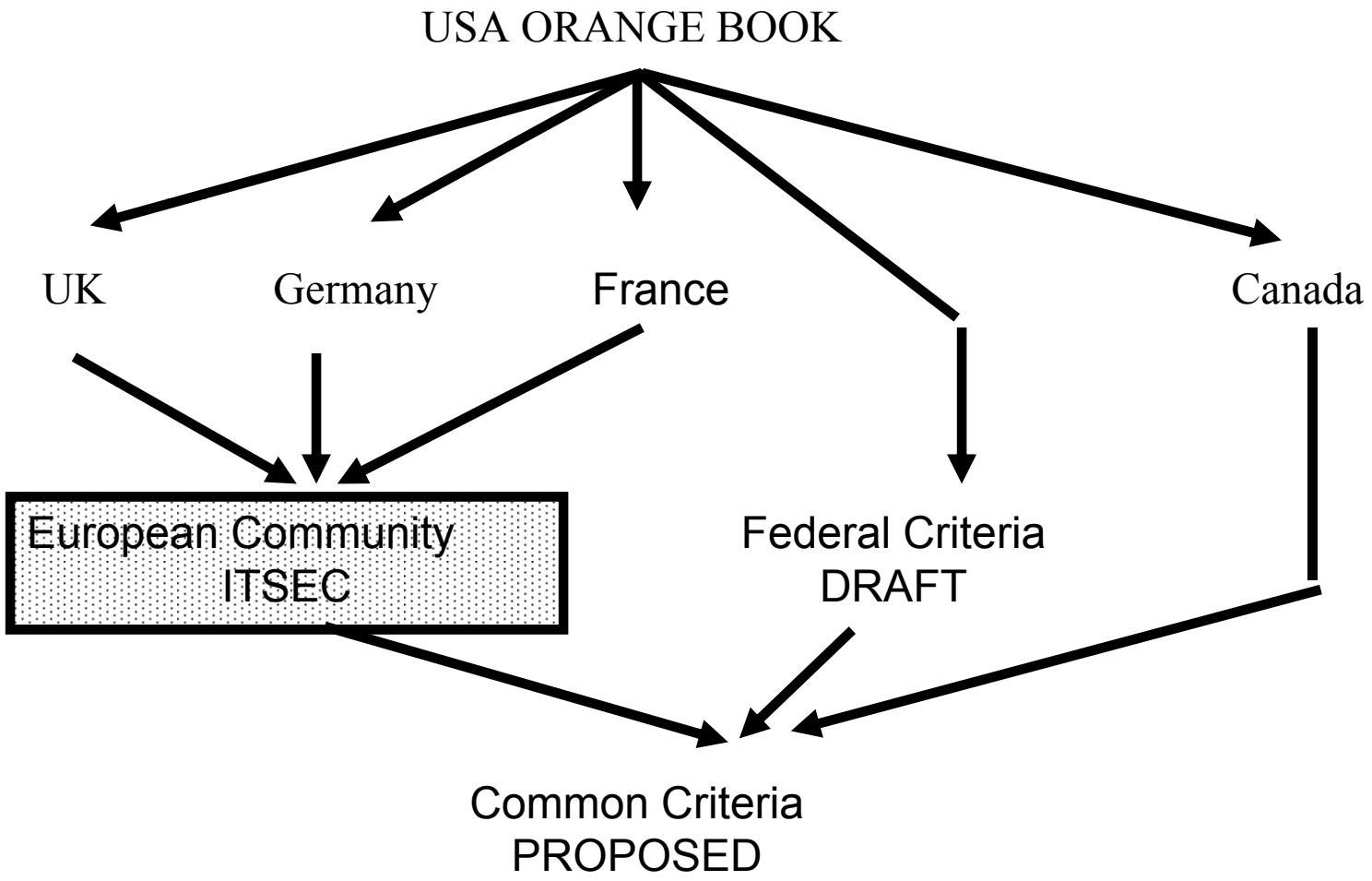
	C1	C2	B1	B2	B3	A1
Security Features User's Guide	+					
Trusted Facility Manual	+	+	+	+	+	
Test Documentation	+			+		+
DesignDocumentation	+		+	+	+	

+	added requirement

ITSEC

- Info Technology Security Evaluation Criteria
- Standard EU mai nou
- Accent pe:
  - Eficacitate – cât de bine un sistem tratează amenințările (potrivire, rezistență, ușurință)
  - Corectitudine – cât de bine un sistem aderă la specificațiile sale de siguranță

ITSEC


USA ORANGE BOOK
UK
Germany
France
Canada
European Community
ITSEC
Federal Criteria
DRAFT
Common Criteria
PROPOSED

Recomandări ITSEC

- Obiective de Securitate (politica de securitate)
- Obiective la nivel de Mediu (descriere)
- Presupuneri la nivel de Mediu (presupuneri)
- Funcții de Securitate (security reqs)
- Logica de Funcționare (rationale for reqs)
- Mecanisme de Securitate (implementare)
- Nivele de Evaluare (ce nivel se dorește a se atinge)
- Evaluarea de Securitate Minimală (nivelul obținut)

Nivele ITSEC

- E0 – asigurare neadecvată
- E1 – descriere de securitate informală
- E2 – descriere informală extinsă
- E3 – descriere detaliată, trasabilitate la nivel de cod
- E4 – descriere de model formal
- E5 – trasabilitate de la model la cod
- E6 – model formal și al politicii de securitate

Fiecare nivel are la bază mecanisme pentru analiză, testarea, verificare și validare

Mecanisme de Asigurare a Politicii de Securitate

EVALUARE

POLITICA
sau
FUNCȚIONALITATE

ASIGURARE

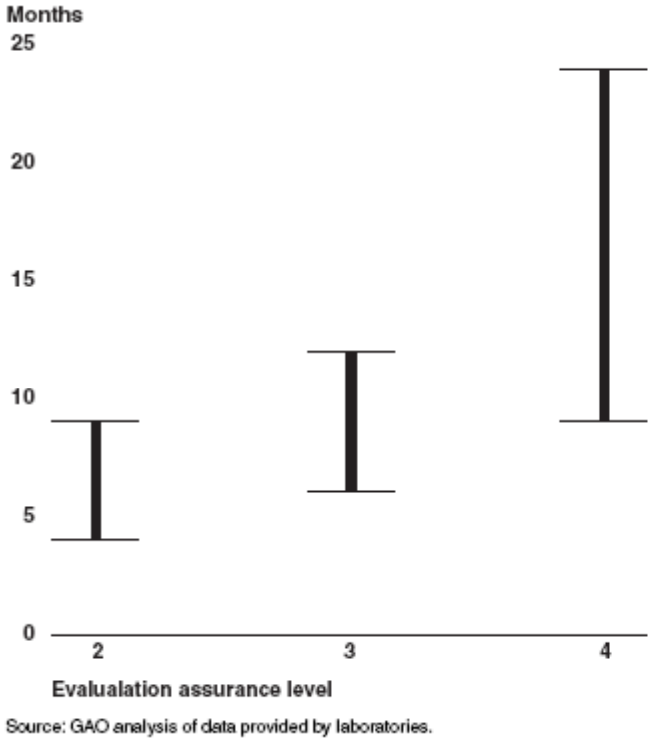
EFICACITATE

CORECTITUDINE

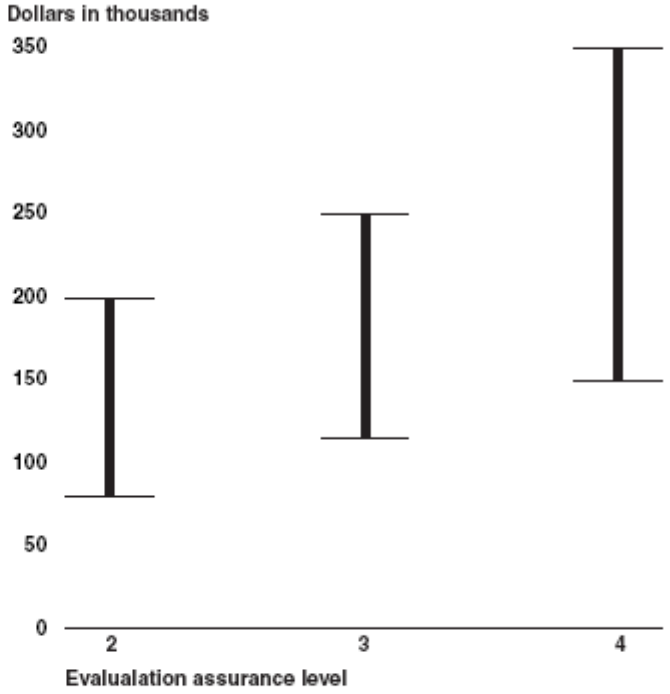
Common Criteria (ISO/IEC 15408)

- Unificarea a ITSEC + TCSEC + CTCPEC
- Nivele
  - EAL1: Functionally Tested
  - EAL2: Structurally Tested
  - EAL3: Methodically Tested and Checked
  - EAL4: Methodically Designed, Tested, Reviewed
  - EAL5: Semiformally Designed & Tested
  - EAL6: Semiformally Verified Design & Tested
  - EAL7: Formally Verified Design & Tested

Costul crește cu fiecare nivel



Source: GAO analysis of data provided by laboratories.



Source: GAO analysis of data provided by laboratories.

*US Government Accountability Office, 2006

Exemple

- EAL4 (or 4+) este nivelul atins de majoritatea produselor comerciale
  - Windows XP + Service Pack 2
  - Windows 2007 + Service Pack 1
  - SuSE Linux Enterprise Server
- Problema?
  - Update-uri (patch-uri) de securitate sunt necesare la intervale de timp pentru fiecare dintre aceste produse

Probleme cu evaluarea

- Poate fi costisitoare
- Adesea influențată de politicile guvernamentale
- Include multe probleme sociale
- Diverse interpretări ale criteriilor
- Procesul de evaluare este *secret* (ascunde posibile probleme/breșe de securitate)

Alte standarde

- DITSCAP/DIACAP
  - US Defence… din nou proces + produs
- FIPS 140
  - Serie de standarde de securitate ale US Government
- ISO 17799
  - Mai mult decât hardware/software
    - Set de standarde pentru politici de securitate
      - Include aspecte de personal, planificare continuă, etc.

Probleme de securitate

- Intenționate:
  - Hacking
  - Viruși
  - Sabotaj
  - Spionaj
- Neintenționate:
  - Accidente (e.g. rm -rf *)
  - Defecte la nivelul componentelor

Viruși

- Publicitate și interes public de nivel ridicat
- Media și filmele le-au acordat un rol ridicat
- Totuși nu sunt atât de semnificativi ca alte probleme de securitate
- Pot fi deranjanți de cele mai multe ori…

Definiții - Virus

- Payload – biți ce declanșează o problemă
- Parazit - infectează fișiere .com sau .exe
- Aplicație gazdă – gazda parazitului
- Tranzient – activ doar când gazda rulează
- Rezident – activ tot timpul

Tipuri de Virusi

- Bombe Logice – declanșate de un eveniment particular
- Viermi – fără payload, doar replicare
- Troiani – arată ca o app, folosit pentru obținerea accesului
- Zombii – activare întârziată
- Virusi Macro – construiți folosind limbaje macro

Convenția CARO

- CARO - Computer Antivirus Research Org.
- Reduce confuzia și ambiguitatea
- Numele de viruși derivă din:
  - Familie – Clasificarea celor mai comuni viruși
  - Etichete pentru familie - R C E P B
  - Grup – colecție de subfamilii
  - Variant Major – instanța clasei de viruși
  - Variant Minor – versiune patch
  - Modificator - ex. mecanismul de ascundere
- Exemplu: GotchaR.Pogue:MtE.0_90:PK

Mecanisme Anti virus

- Controlul fizic
- Gateway-ul la nivel organizațional - firewall, sheepdip
- Sume de control – pentru toate fișierele
- Scanere – caută amprente de viruși
- Scanere de memorie – monitorizare constantă
- Scanere semantice – comportament “virus like”

Sheepdip

- Sheepdip = mecanism de verificare la nivel media, de obicei a mediilor CD-ROM, pentru posibila existență a unui viruși înainte ca acestea să fie folosite în cadrul unui calculator sau rețea.
- Sheepdip computer → folosit pentru verificarea existenței virușilor.
  - Computerul folosește unul sau mai multe programe antivirus actualizate.

Hacking

- Acces neautorizat la date sau servicii
- Adesea o activitate meticuloasă și bine instrumentată
- Securitate apare ca o specializare a fiabilității, însă
  - Defectele sunt căutate explicit
  - Hackerii fac ca toate lucrurile improbabile să se întâmple
  - Rata de defecte pe ora de obicei maximizată

Tipuri de atacatori

- Black hat (a.k.a. cracker):
  - Subminează, produc daune, anarhie, activități ilegale
- White hat:
  - Învață, ajută, crează, îmbunătățesc, activități legale
- Grey hat:
  - Hibrid, fac ceea ce e “corect”, unele ilegalități produse
- Script kiddies:
  - Împuterniciți, neinformați, daune accidentale

Motivațiile Hackerilor

- Rar au la bază motivații financiare
- Curiozitate (tehnologii)
- Spionaj (asupra unor persoane)
- Prestigiu (acoperire media)
- Provocare (cu cât mai greu cu atât mai bine)
- Anarhie (politică, anti-globalizare)
- Grey hat în mod neoficial se mai numesc și “tiger team”

Colectarea (Furtul) de informație

- Colectarea la distanță
  - Monitorizare rețea
  - Scanare porturi
  - Packet sniffing
- Colectare directă
  - Trashing (manuale, diskuri, memo-uri, rapoarte)
  - Jobbing (temp, vânzătorul de sandwich, omul de serviciu)
  - Inginerie socială (colectare “confidence trick”)

Exemple de atacuri

- Coruperea datelor
- Acces neautorizat la informație
- Furtul unui serviciu
- Denial of service (atac la *disponibilitate*!!!)

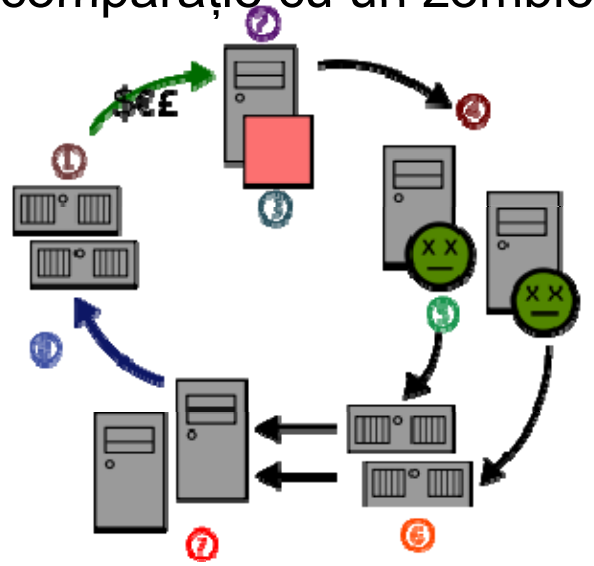
Crearea unui atac

- Scripturi CGI
- Applicații defectuoase (ex. sendmail, DNS, FTP)
- Protocoale de comunicație (ex. TCP)
- Sisteme de operare “*defectuoase*” (ex. Windows :o)
- Configurații defectuoase ale unor aplicații
- Troiani/zombii (snooping sau invocation)
- Address spoofing
- Privilege escalation

Zombies

- Un zombie reprezintă un computer conectat la Internet compromis de un cracker, virus sau trojan, și care poate fi folosit pentru alte task-uri maliționale mai departe.
- Pe calculatorul zombie se instalează botnets pentru trimiterea unor spam-uri sau lansarea unor atacuri denial-of-service.
- Majoritatea utilizatorilor unor computere zombie nu știu că sistemul este folosit remote în felul acesta. (de unde și comparație cu un zombie).

(1) Spammer's web site (2) Spammer
(3) Spamware (4) Infected computers
(5) Virus or trojan (6) Mail servers
(7) Users (8) Web traffic



Abordări pentru atacarea parolelor

- Vizualizarea introducerii parolelor
  - Atenție la persoanele din jur când introduceți parole
  - Instrumente de colectare automată…
- Sindromul “Post-it note in draw”
- Furtul fișierelor cu parole
- Atacuri prin re-play
  - Key-loggere
- Spargerea parolelor
  - Atacuri la nivel de dicționar – oamenii folosesc cel mai adesea parole ce pot fi memorate
- O serie de parole implicite bine cunoscute !!!
  - Multe programe folosesc parole de început pe care oamenii uită să le modifice
  - Câți aveți codul PIN = 0000 ???

Îmbunătățirea securității

- Controlul fizic al securității
- Identificare și Autentificare
- Limitarea ariei de acțiune (permisiuni de acces)
- Detecția intruziunilor
- Mecanisme automate de răspuns la intruziuni
- Audit și responsabilizare

Autentificare

- Identificarea corectă și verificarea utilizatorului
- Abordări posibile:
  - Username și password
  - Carduri ID
  - Smart card/smart buttons
  - Scanar de retină
  - Detector de amprente
  - Profiling al comportamentului la nivel HCI

Detecția intruziunilor

- Nu se poate asigura o securizare completă a unui sistem
- Când apar breșe de securitate…
- încercăm să le detectăm
- Dacă putem detecta intruziunea, putem:
  1. Opri servicii înainte de compromiterea acestora
  2. Repara orice eventuală defecțiune cauzată de atacator
  3. Îmbunătăți securitatea pe viitor
  4. Acționa împotriva atacatorilor (căi legale, etc.)

Metode de detecție a intruziunilor

- Identificarea se bazează pe auditarea datelor din logurile corespunzătoare acțiunilor utilizatorilor
- Majoritatea activităților se loghează la nivelul OS
- Se crează o mare cantitate de date
  - Care se analizează ulterior
- Analiza are la bază identificarea unor tipare de comportament suspicios
  - Adesea un proces prea complex pentru a putea fi făcut manual
  - Mecanisme pentru automatizare
  - Analiza se poate efectua chiar în timp real

Tipuri de atacatori

- Interni - “inside job”, acces neintenționat
- Externi – atacator neautorizat
- Masquerader – pretinde a fi un utilizator valid
- Clandestin – putere de ascundere a datelor de audit trail

Tipuri de mecanisme de intrusion detection

- Detecția anomaliilor (cum)
  - Identificarea unor comenzi sau comportament anormale
- Detecția folosirii incorecte (de)
  - Identificarea unor scenarii de atac bine-cunoscute
- Biometrie (cine)
  - Verificarea unor proprietăți de comportament pentru persoanele ce folosesc sistemul

Detecția anomaliilor (cum)

- Identificarea activităților sau comportamentului anormale
- Se bazează pe efectele observabile ale intruziunii
  - CPU, folosire I/O, comenzi, acces la rețea
- Fiecare persoană are un “profil normal de activitate”
- Sistemul marchează deviațiile de la acest profil comportamental
- Profilele pot evolua odată cu utilizatorul în timp
- Dar atacatorii pot “antrena” sistemul în timp

Detecția activităților anormale (ce)

- Scenarii de atac bine-cunoscute – bazate pe cazuri anterioare
- Variante ale aceluiași atac pot fi detectate
- Scenariile trebuie să fie diferite de ceea ce înseamnă activitate normală a sistemului
- Nu putem identifica atacuri despre care nu știm nimic
- Metodele de detecție sunt dependente de cât de buni sunt dezvoltatorii/programatorii din spatele lor.

Biometrie (cine)

- Distingerea între diverse persoane
- Se pot detecta masqueraderi
- Monitorizarea modului de apăsare a tastelor, mișcarea cursorului mouse, etc.
- Se bazează pe metrici inexacte
- Oamenii pot să sufere modificări la nivelul comportamentului (ex., rănirea unei mâini)

Probleme cu mecanismele de Intrusion Detection

- Securitatea mecanismului de detecție/auditare
- False negatives
- False positives
- Selecția unor nivele de threshold este esențială
- Detecția este un proces computațional
- Utilizatorii stresați au tendința să se comporte bizar

Computer forensics

- Folosirea legală a datelor derivate dintr-un calculator
- Identificare, extragere, interpretare
- Datele sunt folosite ca mărturie pentru:
  - Urmăriri penale
  - Procese juridice
  - Delapidare
  - Utilizarea incorectă a resurselor
  - Furtul unor secrete
  - Găsirea unor testamente pierdute
  - Divorțuri

Computer forensic

http://www.computerforensicsassociates.com/forensic_investigations/computer_fore

Computer Forensics: Divorc...

Convert Select

Computer Forensics Associates

- Forensic Services
- Evidence Analysis
- Data Acquisition
- Forensic Investigation
- Forensic Imaging
- Nationwide Locations

Computer Forensic Services:

Find Out If Your Spouse Is Cheating - Prove Marital Infidelity

Computer Forensics for Divorce Cases

The obvious signals that your spouse is up to something could range from spending a lot of time 'at work' or perhaps more time than normal 'out with friends'. The more subtle indicators that you are being lied to are conveniently hidden from your view, especially if you are not familiar with computers, e-mail or the Internet.

In situations such as this, a Computer Forensics Investigation can help uncover what exactly is going on. Computer Forensic Investigators can identify the truth by examining the computer's hard drive and see what websites, e-mails, chat logs and other pieces of useful information are available to help you. Once the

Aplicațiile securității

- Abordări ale analizelor de securitate post-atac
- Focus pe:
  - Fișiere de date
  - Fișiere log
  - Fișiere program
  - Fișiere cache pentru proxy
  - Fișiere șterse

Honeypot

- Sistem introdus explicit pentru atragerea atacatorilor
  - Monitorizarea folosirii neașteptate
- Hackerii au devin din ce în ce mai conștienți de această tehnică
  - Ascunderea faptului că sistemului este un honey pot
    - Folosirea de SO virtuale, ex. VMWare
- Folosite și ca instrumente de cercetare

Criptologie

- Criptografie - știința scrierii secrete
- Criptanaliză – citirea scrisului secret
- Criptologie = Criptografie + Criptanaliză
- Cifru – algoritm de criptare
- Cheie – folosită de cifru pentru criptarea/descriptarea unui text

Aplicații ale Criptologiei

- Prevenirea accesului neautorizat la date
- Prevenirea modificării neautorizate a datelor
- Prevenirea creării nedetectate de date
- Permite autentificarea
- Verificare la nivelul integrității datelor

Tipuri de criptări

- Simetrice:
  - O aceeași cheie e folosite pentru criptare și decriptare
  - Cheile trebuie să fie ținute secrete
- Asimetrice:
  - Chei diferite pentru criptare/decriptare
  - Cheia de criptare “publică” poate fi distribuită
  - Cheia “privată trebuie să fie ținută secretă

“Spargerea” criptării

- Majoritatea algoritmilor de criptare pot fi forțați
  - Operație consumatoare de timpâ
  - Limitare datorată puterii computaționale curente
- Abordări pentru atacarea criptării:
  - Forța brută – căutarea în întreg spațiul de chei
  - Statistica – abordări matematice, lingvistice sau sintactice
  - Snooping și sniffing – încercarea de a obține cheile folosite
  - Eludarea criptării

Integritatea Datelor

- Nu putem garanta securitatea
- Dar putem lua măsuri de ridicare a gradului de securitate:
  - Sume de control
  - Semnături ale criptării
  - Back-up de execuție
  - Sisteme RAID

Q&A