Securitatea Informatiei

# Evaluare

* Laborator 🡪 50 pct prezenta active (1-5pct pt fiecare laborator timp de 10 lab)
* Partial🡪20pct test grila din teorie si concept importante
* Proiect🡪30pct echipa de 3 oameni
* Examen🡪1 protocol de securitate (teorie ) + 1 problema
* Proiect 1=virtualizzaree securitate ,beneficii,ce brese de securiteate include virtualizare
* 20 min de prezentare

# Curs 1

S.I.=tehnici si metode de asigurare a unor proprietati de securitate a sistemelor

Aceste prop trebuie asigurata fata de un adversary sau cauze naturale

*Proprietati de securitate a sistemelor:*

1. Integritatea
2. Disponibilitatea
3. Confidentialitatea

Fundamentale(triada CIA)

1. Autentificarea
2. Responsabilizarea

***Confidentialitatea***= o informative care circula intre 2 sau mai multe entitati si ramane cunoscuta doar de acele entitati (pe o anumita perioada de timp)

***Integritatea=***propietatea datelor ce sunt communicate intre 2 sau mai multe entitati de a fi integer (de nu a fi modificate neautorizat )

***Disponibilitatea=***capacitatea sistemului de a oferi date si servicii conf unei politici de securitate

***Autentificare***=

1)Autenticitatea datelor

2)Autenticitatea originii

***Responsabilizarea***=Actiuniile executate de o anumita entitate in system si putem sa depsistm ca aau fost facute de entitatea respective

1. *Nerecudierea*=O anumita entitate care a executat o actiune nu poate sa nege actiunea
2. *Fairness*=Schimb correct de informatii (semnarea de contracte on line)

Participantii la un system de comunicatii pot fii *onesti sau neonesti.*

Neonesti=adversari

***Amenintarea de securitate*** =orice circumstanta cu un potential effect negative asupra sitemului (politica de securitate a sistemului)

***Vulnerabilitatea***=o eroare(o omisiune ) de proiectare , implementare ,operare a sistemului

Vrem sa transmitem informatii doar de la A la B ,dar HUB ul transmite informatii catre toate capetele ,dar problema se poate rezolva cu swich-ri

HUB

D

INFO

B

INFO

C

INFO

A

INFO

***Atac=*** o metoda de exploatare a unei vulnerabilitati a sistemului

Adversar=un algortim care lucraza in O(N)

***Tipuri de adversari:***

1***.intern***=participanti la protocol care nu se comporta onest

2.***extern***

***3.pasiv=***monitorizeaza canalul de comunicatii

4.***activ=***interactioneaza cu canalul (modifica informatiile )

5.***coalitii de adversary=***grup care pun toate informatiile la un loc 🡪se trateaza ca un singur adversary

***Amenintarile de securitate :***

***Clasificare dupa efectul produs:***

1. Acces neautorizat la date
2. ***Inselatorie=***se accepta date false ca fiind valide
3. ***Perturbarea serviciilor sistemului***
4. ***Uzurpare=***adversarul a reusit sa obtina controlul/control partial asupra sitemulul

***ATACURI***

1. ***Eavesdropping,*** ***spoofing,*** ***snooping 🡪***Monitorizarea,interceptarea de date
2. ***Modificarea /alterarea de date***=active
3. Spoofing =impersonare 🡪 adrese IP,URL,ETC
4. Repudierea originii
5. Denial of recipt
6. Delay

Atacuri care se coreleaza cu *tehnici de inginerie sociala* :

1. Facute cu ajutrul Postei electronice = Phishing
2. Facute prin telefon/mesaje vocale =Vishing
3. Facute prin SMS =Smishing

*Aceste atacuri au la baza* :

1. *Autorizarea /Interceptarea de date*

*Esentiale*

1. *Modificarea /Alterarea datelor*
2. *Impersonare*
3. Perturbarea serviciilor
4. Manipularea psihologica

*1. MITM (men in the middle )*

C il impresioneaza pe B si transmite mesaj catre A si invers

Interleave= C il impresioneaza pe B si transmite mesaje gresite catre A si invers

(A)

(B)

**B**

**A**

**C**

*2. Shamir*

**PAS1**: A transmite un secret (x) catre B cu propria cheie de acces

* A are o cheie kA privata
* B are o cheie kB privata

A ({x}kA)🡪 B

**PAS2:** B cripteaza mesajul pe care la trimis a cu propria cheie

A ({{x}kA}kB)🡨 B

**PAS3:**A trimite mesaj catre B cu secretul criptat cu cheia lui B,astfel B afla mesajul

A ({x}kB)🡪 B

IN CAZ DE ATAC: C afla secretul si trimite informatii false catre B

**B kA**

y\_kC

x\_kA

**C**

**kC**

**A x kA**

{x\_kA}kC

{y\_kA}kB

y\_kB

x\_kC

3*. NS cu chei publice*:A,B amundoua un secret si cand le afla creeaza o cheie

**k\_B**

**k\_A**

**B NB**

A,B{N\_A,A}k\_B

**A NA**

A,B{N\_B}k\_B

B,A{N\_A,N\_B}k\_AA

***Virtualizarea***=proccesul prin care se creeaa un obiect vitual/entitate virtuala

= abstractizarea componentelor hardware prin intermediul nivelului logic utilizant partea de software

Entitate vituala 🡪o entitate care ne existaa dar se comporta ca o entitate virtuala

🡪o entitate virtuala dar nu are realizare materiala

Componentele sistemul de virtualizare

* Host
* Sistemul ce se virtualizeaza
* Component software care face vitrtualizarea=hypervisor

2 tipuri de hypervisor(HV)

🡪Hypervizor bare-metal

🡪Hypervizorul il instalez peste sistemul de operare al gazdei

Virtualizare != emulare

Emulare=replicare comportamentului unui system informatic intr o gazda convertind comenzile sistemului emular in comnzi ale gazdei

Metasploit

# Curs 2

Tehinici si metode de asigurarea securitatii:

Elemente de criptografie pentru securitatea informatiei:

Scheme criptocrafiice: pentru criptare,hash,semnaturi digitale etc

Criptografia asigura in cadrul sec info. Confientialitate,integritate,…,…

Numai prin cryptografie nu putem sa dam un raspuns satisfacator

Criptografie:

1.Simetrica=2 entitati A,B care comunica utilizeaza o aceeiasi cheie de ultizare K,simetria provine de ls cazul ca atat criptarea, cat si decriptarea se fac cu k

2.Asimetrica=se utilezeaza perechi de chei Pk Sk o operatie relizandu-se cu pk ,iar ”inversa ei ” realizandu- se cu sk

Pk=publica,trebuiesc certificate(pt ca pot fi inlocuite de un adversar)

Sk=private ,motiv pentru care cript asimetrica se mai numeste si crypto cu chei publice

**Intrebare test sapt 8 (cate tipuri de crypto avem? )-grile multiple**

Securitate depinde de schema criptografica in cauza

1.Putem studia securitatea verificand rezistenta unei scheme la atacuri cunoscute .Daca exista un atac schema nu este sigura,daca nu depistam un atac nu stim ce concluzie sa tragem

Acesta abordare este foarte utiliazata in practica in special pt cryptografia simetrica

2.Securitate demonstrabila

2 directii: (a 2a dirctie e derivate a primei)

Securitate perfecta=sigura indiferent de adversar,apara 1949 Shannon

***Securitate perfecta*** =(in termeni decriptat)crypto textul unui mesaj nu divulga nici o informatie asupra mesajului de la care provine

Pornind de la c avem indivigibilitate pt m0 si m1

Mesaj este o secventa de date

Cheia =o secventa random de aceiasi lungime,la fiecare criptare trb generate o cheie !!(proiect Verona)

Facem exort si am criptat

(foarte greu de pus in practica)

Avantaj:”nu scurge informatii”,este rezistenta la orice adversar

***Securitatea computationala***=accepta si defectiuni ,dar intr-o limita neglijabila

\*permite scurgere de informatie in mod negllijabil si considera adversari mai slabi

\*adversar slab=alg probilist de O(n),(PPT)🡪la sec comp

Ce intelegem prin adversar?(Test)

\*scurgere de inf =adversarul se duce pe prob mai mare

Model de securitate=avem un scop de securitate(de a sigura o prop de sec) fata de un adversary

(scop,adv)=model de securitate,trb sa se revere a o anumita clasa

Criptografie simetrica:

COMPONENTE :

1.criptare simetrica

2.functii hash

3. coduri de autentificare a msg

4.Criptare autentificare

\*Se foloseste la ***confidentialitate si integritate***

***Criptarea simetrica(SSL,TLS,..)=***utilizare pt confidentialitatea in doua var

1. Comunicare,🡪SSL,TLS

2.Datelor stocate

Schema de criptare simetrica:formata dintr un generator de chei,alg de criptare,alg de dectriptare

G(lamda=dimensiunei cheii)<--k (k generat de generator)

Generatorul este determinist!!!! DE ce?

Generatorul se utilizeaza la ambele capete ,altfel daca generatorul e nedeterminist sunt 2 chei diferite

Nu putem face comert electronic cu astel de schema ,ele trb insotite de o component cu chei publice

Securitate in criptografia simetrica:

Modele de securitate: (scop,adversar)

Scop (baza)de securitate:

1.Securitate semantica(SS)

2.Indistigibilitate(IND)

3.Nemaleabilitate(NM)=nu pot sa transform in alt formular criptat(importanta)

Adversari:

1.de tip CPA=se antreneaza cu alg de criptare a schemei inainte de a monta atacul

2.de tip CCA=antreneaza cu alg de criptare si decriptare inainte de a monta atacul

SS-CPA,SS-CCA,

IND-CPA,IND-CCA,

NM-CPA,NM-CCA

ATAC: (4 faze)

1.Antrenare:adv se antreneaza cu schema in functie de tipul lui

2.Incercare:adv formuleaza metoda dupa care sa se verifice capacitatea lui de a ataca schema

(ex:adv allege 2 msg dif si de lungime egala, le trimite laa criptre si primeste crypto textul de la unul ele )

3. antrenare=adv se antreneaza ca in prima fazza dar fara a utiliza el din faza de inncercare

4.Decizie=adv decide asupra fazei de incercare

(ex (indiscibilitate) adv decide de unde provine crypto textul:de la m0 sau m1 )

A doua faza de antrenare nu este necesara putand fii stimulta de prima faza pt CPA

CCA1(FARA ANTRENAENT IN FAZA3),CCA2(CU ANTRENAMENT IN F3)

Orice scheme ultiizate independent trb sa aiba cel putin IND-CPA

ACUM: IND—CCA2

Modele de securitate pt securiate simetrica?(Test)

Adversarul de tip COA=monteaza atacuri asupra unei scheme plecand de la un crypto text ,adv pasiv care monitorizeaza canalul de comunicatii

Adversar KPA=mai puternic decat COA,a colectat de-a-lungul mesaje crypto text si inceara sa atace sistemul folosind baza de date

COA<KPA<CPA

IND-COA,IND-KPA=scheme eficiente in practica si pot fi combinate cu alte tipuri e scheme

***Imp(trb sa stim)=scopul,structura unui system simtric,modele de securitate,cum arata structura generala a unui atac***

***Criptografie asimetrica***

1.stream

2.bloc

***Cryptografie stream:*** Generator de chei stream primate o cheie k scurta si genereaza o cheie care este o secventa de biti si aceasta merge la alg de criptare,criptarea se face de obicei prin xor bit cu bit(foarte eficient)

sau adunare modulo 256 pe octeti

Intr un system stream daca gen este PSEUDORANDOM (genereaa o sec binara care este indistingibila) acesta asigura securitate IND-COA

***Generatorul trb sa fie determinist!!!***

Unde nu trb sa utilizam astfel de sisteme?

*Intr un system stream nu trb sa utilizam cheile de 2 ori*

*Cryptostemele stream* ***sunt maleabile***

***Ex:***RC4=are generator prost,RCP efficient ca e cu XOR

Ex:CSS=generator prost

Ex:A5/1,A5/2,A5/3 ,generator prost

EX: E0 analog

Ex:Salsa ,CHACHA sunt bune deocamdata

***De stiut: structura,tipul de securitate,cand nu se foloseste!,exemple***

## Curs 3(nu am fost)

Protocol de autentificare

Client A

Serviciu B

Server S (entitate de incredere)

Protocolul ARP=

# Curs 4

Funtii Hash= instrument de baza in integritatea mesajelor

Th. de constructive pt fct hash:

PAS1:Se porneste de la o fct hash h (fct de compresiee),pe domenii mici

PAS2: Iteram h pe mesaje arbitrare mari

***Tehnica MD:***

l=dimensiune rez hash 🡪formula curs silde 35

Iterarea=pt itereare vom imprti mesajul n in blocuri m1,m2,m3..,mn-1,mn

m1,m2,m3..,mn-1=lunggime =k

|mn|<=k

Pad(n)

Padam mesajul m(cruciala)

Propritati:

1.m este trb sa fie prefix in pad(m)(nu trb sa taimee chestii)

2.daca |m1|=|m2| 🡪 pad(m1)=pad(m2)

3.m1!= m2 attunci ultimul bloc din pad(m1) este diferit de ultimul bloc din pad(m2)

Iterarea slide 36

Pad(m)=m1,m2….mn

IV 🡪h\*(m)=h padat pe m

LUNGIME IV=l

Daca h este reziistenta la coleziuni atunci tehnic MD produce o functie care este rezistenta la coleziuni

Cum arata o functie rez la coliziuni?

Nimeni nu cunoaste o fct rez la coliziuni care sa nu se baze pe o presupuere de dificultate .

***Teh. SPONGE***

Def fcr slide 39

l=r+c(rata=dimensiunea blocului absorbit din mesajul pt care calculam hash ul)

c= padare pt a aduce blocul absorbit la dimensiunea l

*Iterarea:*

Pas1: m1….mn-1 mn

|m1|=…=|mn-1|=r

|mn|<=r

pad(m)=mesaul padat

Th

Daca permutarea pi este random iar l,c sunt sufficient de mar(2^l,2^c) atunci constructia sponge produce o functie rez la coleziune,este la baza lui SHA3

SHA3 – azi=la baza orice fct hash

Ce trb sa stim=

Ce este o fct hash?

Care este conceptual de securitate?=rez la coleziune

MD,SPONGE

REZULTAT REFERITOR LA DIM REZ HASH

Coduri de autentificare a mesajelor =

Securitaeta=dificultatea generarii de msaje valide fara a cunoaste cheia

O schema mac este valida daca prob cu care adv creeaza cheia este negllijabila

Cum construim schema de MAC

Shema CM=bazata pe funcii psudo-random

Fk0 in CBC si retinem doar ul

Daca F este pseudorandom atunci CMAC este sigur

HMAC slide 44

H sufficient de buna ar trb sa se coomporte pseudorandom atunci formula mare este pdeuorandom

Frecvent utilizata cu SHA1

Proprietartea ,daca se utilizeaza cu functi hash mai slabe atunci se imbuntateste securitatea

Mac=

Def

Concept de securitate

Cmac

Hmac

CRIPTARE AUTENTIFICARE(AF)=trb sa am integritate a criptotext ului

Criptarea fara autentificre are val foarte mica in speciat atunci cand utilizam chei publice sai atunci cand o chei private este partajata in mai multe parti.In esenta criptarea aut inseamna garantarea integritatatii criptari criptotextului

criptari criptotextului=daca un adversary vede un crypto text pe canalul de comunicatie ele nu poate sa produca un crypto text care sa pacaleasca chestiile

AF alcatuita din

1. o schema de criptare sigura (ind-cpa)

2. o metoda de asigurare a integritatii

🡪 ind-cca (creste securittea daca adaugam integritatea)

Tehnici pt obtinerea AF:

1.EtM=cripteaa intai si dupa fa un mac (cea mai buna metoda)

Teorema Daca crypto sist este IND-CPA produce criptarea autentificata

Greseli==se folosesc aeleasi chei pt cypher si MAC

2.MtE=facem intai un tag si dupa criptam

!!!!!cheile trbuie alese random independent

Atacuri poodle

AF

-Def

-Mte,Etm

# Criptografia cu chei publice

Exista 2 cerinte fundamentale:

1.Distributia cheilor : (metode:transportul cheii,agreement al cheii,protocoale de distribuie al cheii=STS,etc) nu rezolva niciunul problema satisfacator

2.Autentificare

Criptografia cu chei publice determinista nu asigura sec IND-CPA

Criptografia cu chei publice nu poate asigura securitate perfecta

## CURS 7

Controlul accesului

Implementarea practica a acestei matrici se poate face in 2 metode:

Liste de control al accesului ACL🡪 centrate pe obiecte

DEZVANTAJ MAJOR cand doresc o anumita statistica in system bazata pe subiect.de ce?ca matricea e centrata pe obiect

IN UNIX: avem in mod usual 3 drepturi standard R={r,w,x}

Proprietar ,grupul din care face proprietarul si others

Max 3 dr max 3dr max 3dr

Obiectele pot fi fisiere sau foldere

Pentru un fisier lista de control al accesului arata: (primul pozitie e goala )-rw \_rw \_r \_ \_

Pt foldere: d(prima pozitie specifica folderul )

Permisiuni special de tipul setuserID(SUID) ,set group id(SGID),Stiky Bit

*SUID*=o permisiune ce se aplica numai fisierelor ,

* se specifica prin S sau s in poz a 3a a zonei proprietarului,
* specificatia s o=orice utilizator/subiect care are acces la obiectul(fisierul) ,marcat SUID s poate executa fisierul ,
* specifictia S fisierul nu poate fi executat nici de proprietar
* U are acces la fiserul marcat SUID cu s,atunci daca U pune fisierul inntr un folder la care are acces U’ atunci U’poate accesa fis cu dr lui U .
* EX: passwd🡪comada chage mod

*SGID*= pt fisiere si foldere

Se specifica prin s ssau S in pozz a 3a a zonei grup

specificatia s =orice membru al grupuilui caRE ARE ACCES LA FISIER poate executa fisierul

specificatia s =orice fiser din folder primeste aceasta permisiune

specificatia S fisiere= orice membru ai acces la el dar nu ai voie sa l executi

specificatia S=

*Sticky bit*=numai la foldere

Se specifica prin t in poz a 3 din zona others

Ssemantica specificatiei consta in faptul ca fiserele din acest folder nu pot fi sterse cu exceptia owner sau root

In Windows:

6 drepuri (macar)

Utilizatorii se impart in user si grup

ACL (forma): (user/grup, drepturi )

*Liste de permisiuni/capacitate:*

=implementare listei de control al accesului pe linii ,not=Cs: ( o1,r1)…(ok,rk)🡪 sare deptul r asupra lui o

(o.r)=numit si tichet

Ex:IBM …

Probleme=

1.Cum sunt reprezentate tichetele?

2.Cum fac asocierea tichetului unui obiiect/cum se autentifica subiectul cu ticketul lui cand vrea sa accesee obiectul?

3.Prevenirea falsificarii tichetelor

In general se ultilezeaza criptografia🡪 (MAC(k,(o,r),s))

Autentificare =cum stabilim ca un utilizator are acces la o lista de control al accesului /lista de tichete

ACL: s se auth ACLo

Trb verificata integritatea listei sa nu contina dr suplimentare

Cs: (o,r)

Integritatea tichetului

Modul in care se auth subiectul cu tichetul

Propagara controlului=sa nu poate fi dat mai departe unui al subiect !!!

Analiza a dr de accces in system

ACL: ob

C: subiect

Revocarea drepturilor;

ACL :ob

C: sub

Principiu Privilegiu minim

ACL: complexa de ce ,trb sa trec prin listele orientate obiect

C: ( este BUNA )pemite o gradare destul de fina a privilegiilor pe care le au subiectii in sys

IN practica majoritatea sys folosesc ACL

DAC🡪 model central 🡪 AMC

Exista modele mai bune?

Model TG 🡪 chestii ,scrie de la madalina

Avantaj:scurgerea de dr se poate verifica in O (N^2),N=nr de noduri din gff initial

Dezavantaj: puterea de exppresivitate este redusa 🡪nu poate fi utilizat pt sys complexe

Se poate utiliza pt a verif daca exista vulnerabilitati in retele de calculatoare

Exista model intermediar? 🡪 s a propus modelul schematic care poate fi ajusta intre cele 2 modele,gradul de implementare este mic

*Exemplu de abordari:*

* Drepturi negative
* Drepturi slabe/tari
* Drepturi implicite sau explicite
* Drepturi bazate pe contex
* Drepturi dependente de continut

DAC(discretionar) nu poate rezolva atacul de cal troian

DAC 🡪 se bazeaza pe identitatea celui care solicita accesul

Nu face diferenta intre utilizzator si subiect

Nu ofera protectia asupra atacului de cal troian 🡨 pt ca nu putem controla modul in care se scurge inf si Nu face diferenta intre utilizzator si subiect

Test fara controlul accesului

Vreo 60 intrebari 🡪A si Fals

1.Triada CiA !! toate prop

2.Amenintte de sec,vulnerabilite, atac def

3.adverersa def +classificare

4.clasificare a amenitarilor de securitate!!! Da niste scenarii si dupa zice sa clasificam

5.atacuri practice eveasdropping etc

6.atac de inginerie sociale def

7.atac man in the middle si interleave

Crypto

8.prop care pot fi reolvate cu ajutorul crypto (fara nerepudiere )

9.clasificare cryptografie si in ce consta (probleme)

10.diferenta dintre sec perfecta si computationala

11.model de seuritate (def)!!!

12.cripto system simetric def

13.Scop de securitate simetrica

14.6 modele de atac(cpa cca)coa si KPA

15.fazele modelului de atac

16.stream crypto def ,securitatea maxima=ind-coa care e securitate maxima :

17.generator pshudo random def

18.cele 2 situatii critice pt sistemul stream (maleabil!!)

19.exemple de crypto stream slasa ,cha-cha ce fac ?

20.cryopto sys block dif fundamentale dintre block is stream

21.diagrama generala pt cryptosisteme block 🡪intreabri pe diagrama DES AES

22.fct pseudo random 🡪 def !!!!!!!!!!!!!!!!!!!!!!!

23.existena fct pseudo random? Raspuns negativ nu exista

24.moduri de criptare ECB(prost), CBC vector de init random !!!!

25.IND-CPA =MIN DE SEC PE CARE IL DORIM

26.DCTR det si nedeterminist !! fara ofb

27.functii hash rol!!!!

28.modeld sec pt functiii hash ,rez la coleziune!!!

29.merkle-damgard cum arata ,sa inytelegem procedeul

30.sponge cum artata sic a e baza pt SHA3

31.Integritatea msg sistemul

32.veficarea tag se face cu aceiasi cheie cu acare se face si …

33.constuctia de mac CDC!!!!!, Hmac !!

34.criptarea autentificata !!!!ind-cpa si integritatea crypto textului🡪 nivel de sc IND-CCA=MAX DE SEC IN CRYPTO

35.CLASIFICARE 2 FORME

36.criptare cu key publice def

37.problem distributiei cheii ,semnaturi digitale

38.key publice det nici un sys cu chei publice fara ind-cpa ,nu poate oferi sec perfecta

39.Rsa ,LGAMAL DOAR CA EX

40. crypto Hybrid !!!!!!!!! neaparat ,ind-coa si public ind-cpa 🡪annsamblu ind-cpa(stream cel mai eff la ora actuala)

41.sem digitala !!!!!!!

42. sem digitala din ce e formata

43.dif fundamental dintr mac s idem digitala

44.se realizeaza peste ceva hash

45.rsa lgamal.rss

46 crypto pe curbe eliptice se caracterizeaza key mici dar fara a diminua sec sys

47.certificare ,scopul in crypto cu keey publice, autoritate de certifiaccare ,lant de incredere,