

Adatbiztonság PPZH

2011. május 20.

1. *Mutassa meg*, hogy a CBC-MAC kulcsolt hashing nem teljesíti az egyirányúság követelményét egy a k kulcsot ismerő fél számára, azaz tetszőleges MAC ellenőrzőösszeghez képes csaló üzenetet előállítani. (12 p)

2. *Igazoljunk hash függvény tulajdonságokat:*

a.) az egyszerű modulo-32 ellenőrzőösszeg (32 bites szavak 32 bites összege) nem egyirányú,

b.) az $h(x)=x^2-1 \pmod p$ (p prím) leképezés nem OWHF,

c.) az $h(x)=x^2 \pmod pq$ (p és q "nagy", titkos prímekek) leképezés OWHF, de nem CRHF.

d.) az $h(x,k)=E_k(x)$ (E a DES rejtjelezés) leképezés (x,k) párban nem OWHF (12p=4*3p)

3. Egy kliens és egy szerver közötti biztonsági protokoll a következő protokollt használja:

– kölcsönös partnerhitelesítés a kapcsolat elején (C – kliens, S – szerver):

C → S: Nonce_C

S → C: $\text{Nonces}_S, \text{MAC}_K(\text{Nonces}_C)$

C → S: $\text{MAC}_K(\text{Nonces}_S)$

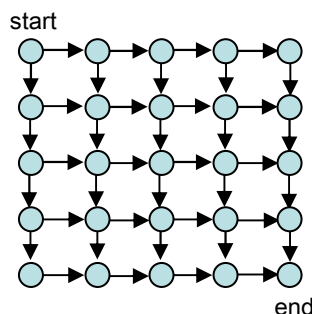
ahol Nonce_x egy 128 bites véletlen szám, K egy korábban létrehozott hosszú élettartamú közös AES kulcs C és S között, $\text{MAC}_K()$ pedig a CBC-MAC függvény az AES blokkrejtjelezővel és K kulccsal ($\text{IV} = 0$),

– kapcsolat során küldött üzenetek rejtjelezése az AES blokkrejtjelezővel CTR módban a fent említett K kulccsal,

– rejtjelezett üzenetek integritásvédelme CBC-MAC módszerrel az AES blokkrejtjelezővel és K kulccsal ($\text{IV} = 0$).

Mutasson támadást, melyben a támadó tetszőleges, a fenti módszerrel rejtjelezett üzenetet dekódolni tud! (15 p)

4. Tekintsük a következő, mobiltelefonra vagy PDA-ra tervezett grafikus felhasználó-hitelesítési módszert: A képernyőn megjelenik az alábbi ábrán látható irányított gráf. A felhasználó jelszava ebben a gráfban egy általa korábban választott útvonal mely a bal felső sarokból indul és a jobb alsó sarokba érkezik. Belépéskor ezt az útvonalat kell a felhasználónak emlékezetből újra megrajzolni. *Hány számjegyből álló PIN kód erősségével ekvivalens erősségű ez a módszer?* (10 p)



5. Bell-LaPadula modell M és f táblázatai az alábbiak:

M	F1	F2	F3
A	R	R	RWA
B	R	RA	WA
C	RWA	WA	RWA

f	Classification
F1	Unclassified
F2	Secret
F3	Top Secret

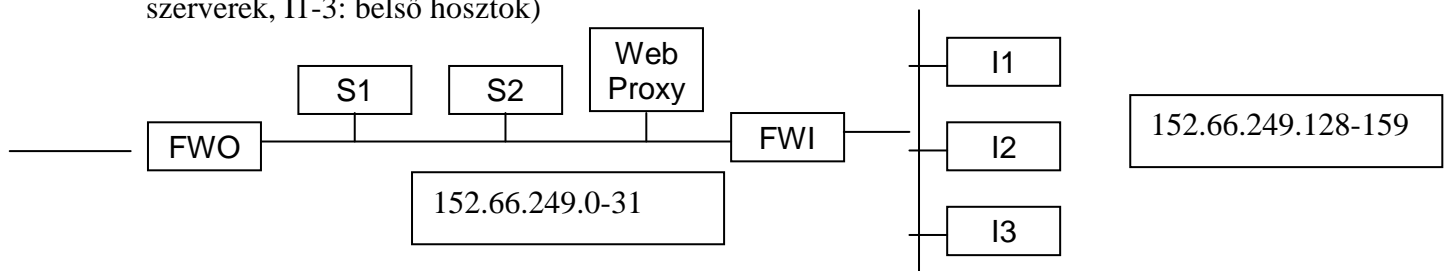
f	Clearance
A	Top secret
B	Secret
C	Unclassified

(R:Read W:Write A:Append)

A felhasználók a szabványos BLP műveleteket használják olvasás és írási hozzáférés kérésekhez (Get Access, Release Access + műveletek), a „b” tábla mindig ennek megfelelő, a H fát nem használjuk. Válaszait indokolja!

- Ki tudja elvégezni F2 olvasását?(3p)
- Ki tudja elvégezni F3 írását (W)? (2p)
- Ki tud hozzáférni (append) F2 fájlhoz? (3p)
- Adja meg a *-property formális definícióját. (3p)

6. Egy tűzfal topológiát az alábbi ábra mutat be (FWO: külső tűzfal az internet felé, FWI: belső tűzfal, Web proxy: egyfajta bástya hoszt webes lekérdezésekhez, S1,S2: szerverek, I1-3: belső hosztok)



Az FWO kifele minden kapcsolatkezdeményezést megenged, visszafelé csak az S1,S2 szerverekre enged SSH (TCP/22) kapcsolódást, illetve átengedi a már létrejött kapcsolatokat. A Web proxyt a belső hálózathoz bárki elérheti és rajta keresztül application level tűzfalként kezdeményezhet webes kéréseket korlátlanul. AZ FWI az internetre minden kapcsolódást engedélyez (és a rá jövő válaszcsoomagokat is), továbbá S1, S2 felé SSH-t, illetve a Web proxy elérését engedi, befele semmit, minden más is tiltva van.

- Új féreg terjed az interneten, a 445-ös portra csatlakozást használva mindenkit feltör. Mi fog történni a DMZ-nkben és a belső hálózatunkban? (2p)
- I3 gépen egy támadó program fut. S2 web szerverén futó alkalmazás ellen akar SQL injection támadást intézni, van rá lehetősége? (4p)
- I3 gépen futó támadó program az interneten levő szerverek felé spam üzeneteket próbál továbbítani. Meg tudja ezt tenni? (2p)
- S1-et feltörik kívülről, mert rossz SSH jelszava van. I1-en is fut egy SSH szerver, de a rossz jelszó nem azonos. Mekkora az esélye a támadónak I1 SSH jelszavainak feltörésére? (2p)

Pontozás: 1: 0-27, 2: 28-38, 3:39-48, 4: 49-58, 5: 59-70

Adatbiztonság PPZH megoldások
2011. május 20.

Név:
Neptun kód:

1.

2.

a.)

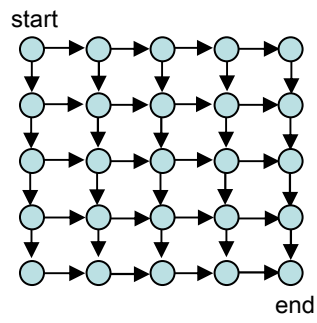
b.)

c.)

d.)

3.

4.



5.

a.)

b.)

c.)

d.)

6.

a.)

b.)

c.)

d.)

Adatbiztonság PPZH megoldások

2011. május 20

1. Tk. 6.5 feladat

2. Előadás slide

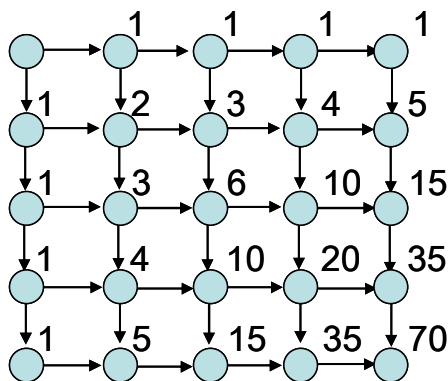
3. Bármely fél rejtjelező-orákulumként használható a partnerhitelesítés protokollt felhasználva:

$A \rightarrow S: X$

$S \rightarrow A: Y, \text{MAC}_K(X) = \text{AES}_K(X+0) = \text{AES}_K(X)$

A rejtjelezett üzenet i . blokkja így áll elő: $M_i \text{ XOR } \text{AES}_K(C_i)$ ahol M_i az i . nyílt blokk, C_i az i . számláló érték. Tehát tetszőleges rejtjeles blokk dekódolható úgy hogy megszerezzük $\text{AES}_K(C_i)$ -t az orákulumtól.

4. A bal felső sarokból az egyes csúcsokba vezető lehetséges útvonalak számát rekurzíven tudjuk kiszámolni: adott csúcsba vezető utak száma egyenlő a csúcsba mutató élek kezdőpontjába vezető utak számának összegével. Ez alapján a jelszótér mérete 70. Ezzel ekvivalens erősségű PIN kód hossza: $\log_{10} 70 = 1 + \log_{10} 7 / \log_{10} 10 < 2$



5.

- M miatt csak A és B jön szóba, az ss-property miatt A és B jöhet szóba: A és B
- M miatt csak A, B, C mind szóba jön, a *-property miatt csak A
- M miatt csak B,C jön szóba, a *-property miatt mind B és C jó, tehát B és C.
- for all $(S_i, O_j, \text{append})$ in b , $fc(S_i) \leq fo(O_j)$ and for all (S_i, O_j, write) in b , $fc(S_i) = fo(O_j)$

6.

- Az égvilágon semmi, a 445-ös portra nem lehet csatlakozni egyik hálózatunkban sem
- U3 csatlakozni tud a web proxyra, az pedig az S2-re, ha a web szerver tényleg hibás, feltörhető valóban.
- Természetesen képes rá, FWI engedi, FWO mindent enged kifelé.
- Hiába törték fel S1-et, befele FWI nem enged SSH kapcsolódást így nem lehet kísérletezni, így a támadás esélye 0 a feltételek mellett.