

Adatbiztonság (vihim102)

2. kis zh

2010 április 13.

1. feladat

Tekintsük az alábbi `/etc/passwd` file részletet:

```
alice:x:1003:1003:,,,:/home/alice:/bin/bash
bob:x:1004:1004:,,,:/home/bob:/bin/bash
tiger:x:1005:1005:,,,:/home/tiger:/bin/bash
piglet:x:1006:1006:,,,:/home/piglet:/bin/bash
mallory:x:1007:1007:,,,:/home/mallory:/bin/bash
```

A `/etc/group` file releváns része:

```
alice:x:1003:
bob:x:1004:alice
tiger:x:1005:
piglet:x:1006:
mallory:x:1007:
winnie:x:1008:tiger,piglet
cryptoland:x:1009:alice,bob,mallory,root
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@hbgyak:/thewood# ls -la
total 16
drwxrwsr-x  4 root winnie          4096 2010-04-08 11:23 .
drwxr-xr-x 23 root root           4096 2010-04-08 11:30 ..
drwxrwx--x  2 root cryptoland     4096 2010-04-08 11:24 friends
drwxr-xr-x  2 alice winnie        4096 2010-04-08 11:25 secrets
```

```
root@hbgyak:/thewood# ls -la friends/
total 20
drwxrwx--x 2 root cryptoland     4096 2010-04-08 11:24 .
drwxrwsr-x 4 root winnie        4096 2010-04-08 11:23 ..
-rwxr--r-- 1 alice winnie        10 2010-04-08 11:26 a1
-rw-r--r-- 1 bob cryptoland      10 2010-04-08 11:26 a2
-rw----- 1 bob cryptoland      10 2010-04-08 11:26 a3
```

```
root@hbgyak:/thewood# ls -la secrets/
total 20
drwxr-xr-x 2 alice winnie        4096 2010-04-08 11:25 .
drwxrwsr-x 4 root winnie        4096 2010-04-08 11:23 ..
-rw-rw-r-- 1 alice winnie        10 2010-04-08 11:25 s1
-rw-r----- 1 tiger cryptoland   10 2010-04-08 11:26 s2
-rw-rw-r-- 1 alice winnie        10 2010-04-08 11:39 s3
```

A felhasználók (alice, bob, tiger, piglet, mallory) közül ki tudja végrehajtani sikeresen az alábbi parancsokat, miközben a `thewood` alkönyvtárban dolgozik:

- `cp friends/a1 secrets/s4`
- `cat secrets/s1`
- `ls -la friends`
- `cd friends`

[Minden alkérdés 0.5 pontot ér.]

2. feladat

- a) Milyen alprotokolljai vannak az TLS-nek, és hogyan helyezkednek ezek el a TCP/IP protokoll stack-ben? [0.3 pont] Milyen feladatokat látnak el az egyes alprotokollok? [0.7 pont]
- b) Egy webszerver és egy böngésző a TLS protokollt használja a HTTP forgalom védelmére. A handshake során RSA alapú kulcscserét használnak, ám a szervernek csak digitális aláírás ellenőrző kulcsot tartalmazó tanusítványa van. A szerver nem kéri, hogy a kliens hitelesítse magát. Adja meg, hogy ebben az esetben mely handshake üzenetek kerülnek átvitelre, és vázlatosan adja meg azok tartalmát! [1 pont]

3. feladat

Tekintsük a következő interaktív grafikus jelszó sémát:

Jelszó-választás: A felhasználó jelszava k db ikonból áll, melyeket k lépésben választ ki a következő módon: A rendszer a felhasználói névből, mint magból generál n db különböző álvéletlen egész számot az $[1, m]$ intervallumban, majd ezeket indexként használva kiválaszt n db különböző ikont egy m méretű fix ikon halmazból, és véletlen elrendezésben egyszerre megjeleníti ezeket a felhasználó számára. A megjelenített n db ikonból a felhasználó kiválasztja a jelszó első ikonját. A kiválasztott ikon a következő iterációban magként szolgál, amiből a rendszer ismét generál n db különböző álvéletlen indexet, véletlen elrendezésben megjeleníti az ezekhez tartozó különböző ikonokat, s a felhasználó ezek közül kiválasztja a jelszó második ikonját. Ez a harmadik lépés magja, és így tovább, amíg a k db ikont ki nem választotta a felhasználó.

Normál használat: A felhasználó hitelesítése a jelszó-választáshoz hasonlóan k lépésben történik. A rendszer a felhasználói névből mint magból legenerálja ugyanazt az n db különböző álvéletlen egész számot, mint a jelszó-választás első lépésében, véletlen elrendezésben (ami lehet más mint a jelszó-választáskor) megjeleníti az ezekhez tartozó ikonokat, s a felhasználónak ezek közül ki kell választania a jelszava első ikonját. A kiválasztott ikonból, mint magból, a rendszer generálja a második kör különböző álvéletlen számaikat, és megjeleníti az ezekhez tartozó ikonokat, melyek közül a felhasználónak ki kell választani a jelszó második ikonját, és így tovább.

- a) Ez a séma felismerés (recognition) vagy emlékezet (recall) alapú? [0.2 pont]
- b) Mekkora egy adott felhasználó potenciális jelszavai halmazának mérete? [0.4 pont]
- c) Mekkora jelszó-erősséget jelent ez bitekben mérve? [0.4 pont]
- d) Tekintsük az alábbi két variánst:
- (i) Hitelesítéskor, ha egy adott körben a felhasználó hibásan választ, a rendszer azonnal megszakítja a hitelesítést és "Failed login attempt." üzenetet küld.
- (ii) Hitelesítéskor, ha egy adott körben a felhasználó hibásan választ, a rendszer nem szakítja meg a hitelesítést, hanem legenerálja a hibás választáshoz tartozó következő kört. Az így megjelenő ikonok természetesen különbözhetnek a helyes válasz esetén megjelenő ikonoktól. A hitelesítés így mindig pontosan k lépésből áll, s ha közben valahol nem jól választott a felhasználó, arról csak a k . kör végén értesül egy "Failed login attempt." üzenet által.

Melyik variáns nyújt nagyobb biztonságot, és miért? [1 pont]

Érdemjegy: pontszám $\geq 5 \rightarrow 5$; $4 \leq$ pontszám $< 5 \rightarrow 4$; $3 \leq$ pontszám $< 4 \rightarrow 3$; $2 \leq$ pontszám $< 3 \rightarrow 2$; pontszám $< 2 \rightarrow 1$;

1. feladat

- a) alice
- b) mindenki: alice, bob, mallory, tiger, piglet
- c) alice, bob, mallory
- d) mindenki: alice, bob, mallory, tiger, piglet

2. feladat

a) Alprotokollok:

- TLS Record: fragmentáció, tömörítés, rejtjelezés, üzenet-hitelesítés és integritásvédelem, visszajátzás elleni védelem
- TLS Handshake: algoritmusok egyeztetése, kulcscsere, partner-hitelesítés
- TLS Alert: hibüzenetek
- TLS Change Cipher Spec: Handshake végének jelzése, állapotváltás

Elhelyezkedés a protokoll stack-ben:

- TLS Record: TCP felett
- TLS Handshake, Alert, Change Cipher Spec, és alkalmazások (pl. HTTP): TLS Record felett

a) A következő handshake üzenetek kerülnek átvitelre:

$C \rightarrow S$:	client-hello	: kliens véletlenszáma, javasolt algoritmus-csokrok listája
$S \rightarrow C$:	server-hello	: szerver véletlenszáma, választott algoritmus-csokor, session ID
$S \rightarrow C$:	server-certificate	: szerver azonosító, szerver aláírás-ellenőrző kulcsa, CA aláírása
$S \rightarrow C$:	server-key-exchange	: szerver RSA rejtjelező kulcsa, szerver aláírása
$S \rightarrow C$:	server-hello-done	
$C \rightarrow S$:	client-key-exchange	: pre-master secret a szerver RSA kulcsával rejtjelezve
$C \rightarrow S$:	(change-cipher-spec)	
$C \rightarrow S$:	client-finished	: eddigi handshake üzeneteken és a mester titkon számolt MAC
$S \rightarrow C$:	(change-cipher-spec)	
$S \rightarrow C$:	server-finished	: eddigi handshake üzeneteken és a mester titkon számolt MAC

3. feladat

a) felismerés (recognition)

b) n^k

c) $k \cdot \log n$

d) A (ii) variáns biztonságosabb, mert annál a találgatásos támadás komplexitása n^k , míg az (i) variáns esetében ez a komplexitás csak nk : a támadó az i . ikont átlagosan $n/2$ próbálgatásból tudja megfejteni, miután az $i - 1$. ikont már megfejtette.