

2. Kis ZH VIHIM183 Adatbiztonság – 2010. 11. 16.

Név:

Neptun kód:

1. Feladat 15p

Milyen alprotokolljai vannak az TLS-nek, és hogyan helyezkednek ezek el a TCP/IP protokoll stackben? [10 pont] Milyen feladatokat látnak el az egyes alprotokollok? [5 pont]

2. Feladat 20p

a) Milyen tulajdonságokkal kell rendelkeznie egy emberi fiziológiai vagy viselkedési jellemzőnek ahhoz, hogy alkalmas legyen biometriai azonosításra? (7 p)

b) Milyen típusú ujjlenyomat minutiák léteznek (2 db.) és milyen paraméterekkel reprezentálják ezeket? (6 p)

c) Milyen típusú hibákkal kell számolni a matching során? Mit jelentenek ezek a hiba fogalmak? (7 p)

3. Feladat 20p

Adja meg a jelszó alapú felhasználó hitelesítés általános modelljét (segítség: U, V, f) ! Mik a jelszó alapú felhasználó hitelesítés előnyei és hátrányai? Soroljon fel néhány ökölszabályt és módszert erős jelszó választásra! (csak korlátos terjedelemben, bónusz pont nincs.)

4. Feladat 15p

Adja meg a (PKI) tanúsítvány életciklusát! Írja le a tanúsítvány-visszavonás két fő módszerét, adja meg azok előnyeit és hátrányait!

5. Feladat 10p

Milyen típusú sérülékenységellenőrzést végeznek: flawfinder, splint, valgrind, nessus ? (hol, miben keresnek sérülékenységet, milyen sérülékenységet, milyen kategóriába sorolható (statikus, dinamikus?)

6. Feladat 10p

Unix hozzáférésvédelem környezetben mi a umask lényege, hogyan működik amikor egy alkalmazás fájl akar létrehozni?

7. Feladat 10p

Mi a letagadhatatlanság (non-repudiation) 2 fő típusa, definiálja őket 1 mondatban.