Miskolci Egyetem
Gépészmérnöki és Informatikai Kar
Informatikai Intézet
Általános Informatikai Intézeti Tanszék

Neptunkód: ***GEIAL30B-B, GEIAL30BB, GEIAL30B-BL, GEIAL30BBL***
Javasolt félév: 4
Kredit: 5

Kontakt órák száma / hét: 2 előadás, 2 labor gyakorlat

Biztonság és védelem a számítástechnikában

Szak: *Mérnök informatikus alapszak, gazdasági informatikus alapszak, programtervező informatikus alapszak*

Hét	Előadás	Gyakorlat
1.	Adat; információ; információ biztonság	Bot, Worm, és a behatolók detektálása
2.	Védelmi igény; veszélyforrások; kockázati osztályok besorolása; védekezési költségek	Bloatware és Crapware mobil eszközökön
3.	Az információ védelme; védelem a fizikai sérülés ellen; védelem a jogosulatlan hozzáférés ellen; behatolások	Biometrikus azonosítás mobil eszközökön
4.	Crapware; trialware; scareware; fraudware; rogueware;elterjedt azonosítási módok;birtok alapú azonosítás; tudásalapú azonosítás; biometriai azonosítások; szigorú azonosítás; multifaktoros azonosítás	Stack overflow támadások
5.	Need to know elv; védelmi tartományok; process és védelmi tartomány összerendelési lehetőségek; védelmi tartomány implementációk; Access Matrix; Access Matrix implementációk;formális módszerek	Windows, Linux hardening folyamata
6.	Biztonságpolitika; Tűzfalak; tűzfal építőelemek: Packet filtering; stateful packet filtering; deep inspection firewall; circuit level gateway; proxy firewall	Tartalomszűrő tűzfalak
7.	Védelmi struktúrák; VPN, Content filtering firewall; Web Application firewall; IPS és IDS rendszerek; personal firewall	DoS, DDoS támadások
8.	DoS és DDoS támadási módok;Web alkalmazásokon belüli támadások	DES, DESX, 3DES, Triple DES
9.	Víruskeresők; víruskereső motorok; működési elvük; titkosított vírusok; heurisztikus, ill. negatív heurisztikus keresés	Enigma, NTFS, EFS
10.	Nevezetesebb biztonsági esetek; Szteganográfia; digitális szteganográfia; robosztus és törékeny vízjelek;	Hash algoritmusok, tanúsítványok
11.	Kriptográfia; átrendezés; behelyettesítés; kulcsmegosztás problémaköre; monoalfabetikus behelyettesítés; Vigenere kódolás; homofónikus behelyettesítés; one time pad; gépesített kódolás	PKI használata
12.	Nyilvános kulcsú kriptográfia; PKI alkalmazási területek; elektronikus és digitális aláírás; tanúsítványok;SSL; TLS; Informatikai biztonsági irányítás; Közigazgatási informatikai biztonság	Operációs rendszerek biztonsága
13.	Biztonsági osztályok; TCSEC; ITSEC; Magas rendelkezésre állású rendszerek	Personal firewall-ok
14	Összefoglalás, hallgatói kiselőadások megtartása, pontozása	hallgatói kiselőadások megtartása, pontozása

Aláírás feltétele:

- A 13-ból legalább 9 gyakorlaton való aktív részvétel (a kiadott feladat elvégzése, és a megadott határidőig az oktató e-mail címére való elküldése.)
- El nem küldött feladat nem pótolható, de a nem megfelelő szinten kidolgozott feladatból kettő a félév végén javítható.
- A félév elején a hallgató által választott biztonsági témakör részletes átnézése, kb. 20 oldalas jegyzőkönyvben való kidolgozása, elektronikus formában való leadása, és …
- … a félév végén a választott félévi feladat megoldásának 10-15 percben történő előadása.

A HKR 50. § (5) bekezdése értelmében, előadások esetén 40%-ot, gyakorlatok esetén 30%-ot meghaladó igazolatlan hiányzás esetén a tanszék kezdeményezi az aláírás végleges megtagadását. A végleges aláírás megtagadás bejegyzése után a hallgató a mulasztását nem pótolhatja, ismételten fel kell vennie és le kell hallgatnia a tantárgyat ahhoz, hogy az aláírást megszerezze.

Vizsga:

- írásbeli és szóbeli.

Ajánlott irodalom:

- Almási János: Elektronikus aláírás és társai (ISBN 963 202 7442)
- John R. Vacca: Computer and Information Security Handbook (Elsevier, ISBN 978 0 128 03929 8)
- Bruce Schneier: Applied Cryptography (Wiley, ISBN 978 1 119 09672 6)
- Virrasztó Tamás: Titkosítás és adatrejtés (NetAcademia Kft, ISBN 963 214 253 5)
- Simon Singh: Kódkönyv (ISBN 963 530 5257)
- Alan G. Konheim: Computer Security and Cryptography (ISBN 978 0 471 94783 7)
- J. H. Allen, S. Barnum, R. J. Ellison, G. McGraw, N. R. Mead: Software Security Engineering (ISBN 978 0 321 50917 8)

Biztonság és védelem a számítástechnikában
Vizsgazárthelyi mintafeladat

1. Ismertesse az adatvesztés lehetséges okait! (2 pont)
2. Magyarázza a következőket: Bloatware, Malware, Crapware! (3 pont)
3. Ábra segítségével ismertesse az Access Matrixban használt olyan jogokat, amelyek domain-okra vonatkoznak (1 pont)
4. Hogy tudjuk biztosítani a Need to know elvet statikus védelmi tartomány esetén? (1 pont)
5. Mutassa be a Bell-La Padula modellt, térjen ki a működését meghatározó szabályokra! (2 pont)
6. Ismertesse a Deep Packet Inspection Firewall-t! (2 pont)
7. Mi a szerepe a digitális vízjeleknek? (1 pont)
8. Ismertesse a Man in the middle támadás elvét, kivitelezését kriptográfia esetén! (2 pont)
9. Mutassa be a heurisztikus elven történő víruskereséseket (Heuristic-based Generic Decryption, illetve Generic Decryption Engine) (2+2 pont)
10. Ismertesse részletesen rajz segítségével a proxy tűzfalat! (4 pont)

Kidolgozási idő: 60 perc

Max: 22 pont. (**0-11** → 1, **12-14** → 2, **15-17** → 3, **18-20** → 4, **21-22** → 5)

Biztonság és védelem a számítástechnikában
Vizsgazárthelyi mintafeladat megoldás

1. Ismertesse az adatvesztés lehetséges okait! (2 pont)
   Elemi károk, hardver vagy szoftver hibák, emberi hibák

2. Magyarázza a következőket: Bloatware, Malware, Crapware! (3 pont)
   Bloatware: felduzzasztott szoftver. Többnyire mobilokon, tableteken. Helyet és erőforrásokat foglalnak Malware: Malicious software . rosszindulatú szoftver gyűjtőfogalom Crapware: kéretlem programok. a felhasználó telepíti fel, de jellemzően nem szándékosan, leginkább tudta nélkül

3. Ábra segítségével ismertesse az Access Matrixban használt olyan jogokat, amelyek domain-okra vonatkoznak (1 pont)
   Switch jog illetve Control jog

4. Hogy tudjuk biztosítani a Need to know elvet statikus védelmi tartomány esetén? (1 pont)
   Módosíthatónak kell lennie a védelmi tartomány tartalmának

5. Mutassa be a Bell-La Padula modellt, térjen ki a működését meghatározó szabályokra! (2 pont)
   2 alapvető entitás: Objektum és szubjektum, illevte a 3 szabály

6. Ismertesse az IDS rendszerek szerepét, működési elvét, sorolja fel változatait egy-egy mondat kíséretében! (3 pont)
   Intrusion Detection System: viselkedése alapján passzív. Komponensei: érzékelők, konzol a riasztások megjelenítésére illetve értékelő-naplózó rendszer. Van HIDS: host-based, NIDS: network-based, valamint PIDS illetve APIDS: ezek ügynökre épülnek, amely a szerveren fut és figyeli a szerver és a hozzá csatlakozott eszközök közti kommunikációs protokollt

7. Mi a szerepe a digitális vízjeleknek? (Térjen ki a robosztus illetve törékeny fogalmakra)(1 pont)
   Szerzői jogvédelem, Másolás védelem, Nyomon követés, Eredetiség (törékeny vízjel)

8. Ismertesse a digitális aláírás elvét, kivitelezését! (2 pont)
   A digitális aláírás előállítása

   A digitális aláírás során nem az a cél, hogy a dokumentum titkosításra kerüljön, és jogosulatlanok számára olvashatatlan legyen, Ellenkezőleg. Az elvárás az, hogy a dokumentum olvasható legyen, de:

   - *egyértelműen azonosítható legyen, hogy ki írta alá (más ne írhassa alá)*
   - *az aláíró ne tagadhassa le az aláírását*
   - *ne legyen áthelyezhető egy másik dokumentumra*

- *egyértelműen megállapítható legyen, hogy a dokumentumot megváltoztatták-e az aláírás óta*

Kivitelezése a következőképpen működik:

- *Az üzenetből készítünk hash algoritmussal egy egyedi ujjlenyomatot.*
- *Ezt a küldő (aláíró) titkos kulcsával eltitkosítjuk*
- *az üzenetet a titkosított hash-sel együtt elküldjük*
- *A címzett ketté választja az üzenetet és a titkosított hash-t*
- *A címzett a hozzá megérkezett üzenetnek elkészíti a hash-ét*
- *A hozzá érkezett titkosított hash-t megfejti a küldő nyilvános kulcsával*
- *Összehasonlítja a két hash-t.*

Ha a két hash megegyezik, akkor:

- *A dokumentum tartalma nem változott meg*
- *Mivel a küldő nyilvános kulcsával meg tudta fejteni, ezért biztos, hogy a küldő az, akinek vallja magát.*

9. Mutassa be a heurisztikus elven történő víruskereséseket (Heuristic-based Generic Decryption, illetve Generic Decryption Engine) (2+2 pont)
HGD: feltételezi minden esetben, hogy az vírus. Ennek valószínűsége 10%. Ezek után vizsgálja a program utasításait: NOP +5%; regiszter megsemmisül használat nélkül +1,2%; interrupt használat -15%; nincs memória írás 100 egymást követő utasításon belül -5%.

GDE: a motor analizálja a vírus kódszegmensben levő kódoló-dekódoló utasításait. Ez alapján visszafejti a titkosított utasításokat, majd beazonosítja a vírust.

10. Ismertesse részletesen rajz segítségével a proxy elvű tűzfalat! (3 pont)

Másik, szokásos elnevezése: proxy firewall. Nevét onnan kapta, hogy a benne levő (általában két) hálózati kártya közti forgalmat kis jogosultság ellenőrző programok valósítják meg a letárolt szabályoknak megfelelően. Jellemzően egy-egy protokollra készült egy-egy proxy. Így beszélünk ftp proxy-ról, http proxy-tól, pop3 proxy-ról, stb.

A csomagszűrő tűzfalnál jóval több lehetőséget biztosít, mivel:

- *szétválaszthatók a user-ek*
- *szétválaszthatók az alkalmazások*
- *alkalmazás szinten szűr, így nem csak a csomag tartalma, hanem az egész információfolyam vizsgálható*
- *kérhető teljes részletességű logfile*

Egy középkori vár védelméhez hasonlítva megfelel a vasrácsnak. Ha egy behatoló elvágja annak kötélzetét, a vasrács leszalad, és nem csak befelé nem tud senki

bemenni, de ki sem tud senki jönni. (Egy behatoló a szabályrendszer kiiktatásával nem megnyitja a tűzfalat, hanem teljesen leállítja a forgalmat.)