INFORMATIKAI KAR DOKTORI PROGRAM
SZIGORLATI TEMATIKA

Informatikai biztonság (főtárgy)

I. Logikai és fizikai biztonság

1. Bevezetés az informatikai biztonságba
2. Informatikai biztonság tervezése, rendszertervezési modell
3. Védelmi igény feltárása
    - Informatikai elemek feltérképezése
    - Informatikai elemek értékeinek meghatározása
4. Fenyegetettség-elemezés
    - Alapfenyegetettségek
    - Sebezhetőség
5. Kockázat-elemzés
    - Kvalitatív kockázatelemzés
    - Kvantitatív kockázatelemzés
6. Kockázat-menedzselés
    - Kockázat-menedzsment stratégiák
    - Intézkedés kiválasztása
    - Költség/haszon elemzés
7. Fizikai Biztonság
8. Biztonság és személyzet
    - Jogosultsági szintek
    - Monitorozás
    - Szervezet
9. Biztonsági rendszer nyomon követése
    - Új fenyegetések megjelenése
    - Új elemek, kockázatok frissítése
    - Külső, belső monitorozás
10. Informatikai biztonsági szabványok
    - CoBIT
    - Common Criteria
    - BS7799-ISO 17799
    - ITIL
    - Hazai szabványos eljárások (ITB ajánlások, ITKTB ajánlások)

Ajánlott irodalom:

- Michael S. Whitman, Herbert J. Mattord: Principles of Information Security, Thomson Course Technology, 2003.
- David Vose: Risk Analysis: A Quantitative Guide (Wiley, John&Sons, 2000)
- Horváth László, Dr Lukács György, Dr Tuzson Tibor, Vasvári György: Informatikai biztonsági rendszerek (BMF Kandó Kálmán Villamosmérnöki Főiskolai Kar és az Ernst&Young együttműködésében, 2001)
- Információmenedzsment (szerk.: Gábor András, Budapest, 2002)
- Infostrázsa (4. kiadás), KÜRT Computer Rendszerház Rt., Budapest, 2004

II. Kriptográfia

1 .A rejtjelzés információelméleti vonatkozásai:

Klasszikus rejtjelzési módszerek, monoalfabetikus helyettesítés; homofonikus rejtjelezés. A monoalfabetikus helyettesítés fejtése.
Polialfabetikus helyettesítés, a kulcshossz meghatározása; önkulcsolás; véletlen átkulcsolás.
A rejtjelezés információelméleti alapjai; egyértelműségi pont, kulcstér.
2. Blokkos rejtjelzések
Helyettesítés és keverés; a transzpozíciós rejtjel egy lehetséges fejtése.
Példák; a DES algoritmus, az AES algoritmus szerkezete, a blokkos rejtjelzési elvek érvényesülése.
Visszacsatolási módok.
A differenciál és lineáris kriptoanalízis alapelvei.
4. Nyilvános kulcsú rejtjelzés
Alapelv, a bonyolultság és a kriptográfia; tipikus használat.
Az alapelvből következő támadási lehetőségek.
A diszkrét logaritmuson alapuló nyilvános kulcsú rejtjelezési rendszerek.
A hátizsák-algoritmuson alapuló nyilvános kulcsú rejtjelezési rendszerek és a felmerülő problémák.
A hibakorlátozó kódolás és a rejtjelezés kapcsolata.
5. Az RSA algoritmus
Az algoritmus felépítése, működése.
Támadási módszerek; iterációs fejtés.
Biztonságos működéshez szükséges kulcsméret; paraméter-választás.
Protokollhibák.
Rabin RSA, gyökvonás Zm-ben.
6. Azonosítás, hitelesítés
Jelszavak, erős hitelesítés.
Shamir három lépéses protokoll.
Kérdés-válasz hitelesítés.
Zero knowledge protokoll fogalma.
Fiat-Shamir, Feige-Fiat-Shamir protokoll működése.
7. Integritásvédelem
Hash függvények, példák
Hash-függvények kulcs alapján és anélkül.
MAC számítási algoritmusok, ezek szerepe.
8. Digitális aláírás
Elvi alapok, szerepe, gyakorlati jelentősége.
RSA digitális aláírás.
AlGamal és általánosított AlGamal séma.
DSA.
PKI alapstruktúrák.
9. Bitsoros rejtjelzés (stream cipher)
Pszeudorandom generátorok.
Shiftregiszterek (LFSR).
Shiftregiszterek nemlineáris összekapcsolása (Geffe, Clock-controlled, Shrinking generátorok).
Példák bitsoros algoritmusokra.
10. Kulcscsere protokollok
Kulcscsere szimmetrikus kriptográfia használatával.
Shamir háromlépéses protokollja; a Massey-Omura és a Diffie-Hellmann kulcscsere-protokoll.
Biztonsági meggondolások gyakorlati használat során, kulcsmenedzsment.

11. A rejtjelezés egyéb kérdései
Titokmegosztás.
Digitális pénz, bankjegy digitális másolásvédelme.
Kriptográfiai számítások.
12. Szteganográfia

Ajánlott irodalom:

- Beutelspacher, A.: Cryptology: The Mathematical Association of America, 1994
- Brassard, G.: Modern cryptology, Springer Verlag, 1988
- Buttyán, L.-Vajda, I.: Kriptográfia és alkalmazásai Typotex 2004
- Ködmön, J.: Kriptográfia, Computerbooks 1999
- Menezes, A. - van Oorshot, P. - Vanstone, S.: Handbook of Applied Cryprography, CRC Press, 1996
- Nemetz, T. - Vajda, I.: Algoritmikus adatvédelem, Akadémiai Kiadó, 1991
- Salomaa, A.: Public-key cryptography, Springer Verlag, 1990
- Schneier, B.: Applied Cryptography Wiley, 1996
- van Tilborg: An introduction to cryptology, Kluiver Academic Publisher, 1988