A TANTÁRGY ADATLAPJA

1. A képzési program adatai

1.1 Felsőoktatási intézmény	Babeş-Bolyai Tudományegyetem
1.2 Kar	Matematika és Informatika Kar
1.3 Intézet	Magyar Matematika és Informatika Intézet
1.4 Szakterület	Informatika
1.5 Képzési szint	Mesteri
1.6 Szak / Képesítés	Informatikai modellek optimalizálása

2. A tantárgy adatai

2.1 A tantárgy neve	Számítási rendszerek biztonsága Securitatea sistemelor de calcul						
2.2 Az előadásért felelős tanár neve	ROBU Judit,						
2.3 A szemináriumért felelős tanár neve	ROBU Judit,						
2.4 Tanulmányi év	2.	2.5 Félév	3.	2.6. Értékelés módja	Vizsga	2.7 Tantárgy típusa	kötelező

3. Teljes becsült idő (az oktatási tevékenység féléves óraszáma)

3.1 Heti óraszám	3	melyből: 3.2 előadás	2	3.3 szeminárium/labor	1
3.4 Tantervben szereplő össz-óraszám	42	melyből: 3.5 előadás	28	3.6 szeminárium/labor	14

A tanulmányi idő elosztása:	óra
A tankönyv, a jegyzet, a szakirodalom vagy saját jegyzetek tanulmányozása	35
Könyvtárban, elektronikus adatbázisokban vagy terepen való további tájékozódás	15
Szemináriumok / laborok, házi feladatok, portofóliók, referátumok, esszék kidolgozása	35
Egyéni készségfejlesztés (tutorálás)	14
Vizsgák	4
Más tevékenységek:	

3.7 Egyéni munka össz-óraszáma	103
3.8 A félév össz-óraszáma	175
3.9 Kreditszám	7

4. Előfeltételek (ha vannak)

4.1 Tantervi	• nincs
4.2 Kompetenciabeli	• Java és/vagy C++ programozási ismeretek, objektumorientált programozás alapelvei,

5. Feltételek (ha vannak)

5.1 Az előadás lebonyolításának feltételei	• vetítőgép
5.2 A szeminárium / labor lebonyolításának feltételei	• saját felhasználói fiók a kar szerverén,

6. Elsajátítandó jellemző kompetenciák

Szakmai kompetenciák	– A biztonság, az információvédelem és az informatikai biztonság összefüggéseinek ismerete – Az informatikai biztonsági feladatok megtervezése, megszervezése és irányítása – Események kezelése (számítógépes bűnözés, események észlelése, elemzése, helyreállítása, intézkedések) – Napjaink adathordozóival és általános eszközeivel összefüggő informatikai biztonsági kockázatok azonosítása és kezelése
Transzverzális kompetenciák	– Hatékony információgyűjtés, összegzés képessége – Problémamegoldó készség, kreativitás fejlesztése

7. A tantárgy célkitűzései (az elsajátítandó jellemző kompetenciák alapján)

7.1 A tantárgy általános célkitűzése	– A kurzus célja megismertetni a diákokat a számítási rendszerek biztonságával kapcsolatos terminológiát, alapvető megoldandó feladatokat. – A diákok megtanulnak információt gyűjteni illetve összegezni a biztonsággal kapcsolatos témákról. – A diákok ráérezzenek az IT szakember felelősségére a biztonsággal kapcsolatos kérdésekben.
7.2 A tantárgy sajátos célkitűzései	A félév végére a hallgatók kell – ismerjék a számítási rendszerek biztonsága témakörébe tartozó terminológiát és alapfogalmakat – értsék a gyakoribb támadási technikákat és védekezési mechanizmusokat – ismerjék a modern kriptográfiát és ennek alkalmazásait – értsék a „biztonság” szó jelentéseit a különféle alkalmazásokban

8. A tantárgy tartalma

8.1 Előadás	Didaktikai módszerek	Megjegyzések
1. hét Bevezető. Alapfogalmak, fenyegetés-modellek, biztonsági célkitűzések.	előadás, vetítés, magyarázat, dialógus	
2–6. hét Kriptográfia és kriptográfiai protokollok: – történelmi áttekintés – matematikai háttér – pseudorandom bitek és sorozatok – folyamrejtjelek – blokk rejtjelek – nyilvános kulcsú titkosítás – hash függvények és az adatok integritása – azonosítás és hitelesítés	előadás, vetítés, példán keresztül történő szemléltetés	

– digitális aláírás – kulcs-csere protokollok – kulcs management		
7–8. hét Biztonsági modellek: – Bell-LaPadula modell – Biba modell – kínai fal modell – Clark Wilson modell – más modellek	előadás, vetítés, magyarázat	
9–10. hét Software biztonság. – „Secure software engineering”, – defenzív programozás, – puffer túlcsordulás és más implementációs problémák. – programozási nyelvekhez kapcsolódó biztonsági kérdések: – kód ellenőrzése a biztonsági rések felismerésére, – biztos nyelvek, – „sandboxing” technikák.	előadás, vetítés, konkrét példán keresztül történő szemléltetés, magyarázat	
11. hét Operációs rendszerek biztonsága. – a memória védelme, – belépés ellenőrzése, – felhasználók hitelesítése, – biztonság kiértékelése, – digitális jogok.	előadás, vetítés, konkrét példán keresztül történő szemléltetés, magyarázat	
12. hét Hálózatok biztonsága. – tűzfal, – biztonságos szolgáltatások – támadások és kivédésük.	konkrét példán keresztül történő szemléltetés, dialógus	
13. hét Rosszindulatú kód elemzése és védelem. Férgek, spyware, rootkit, botnet, stb.	vetítés, előadás, konkrét példán keresztül történő szemléltetés, magyarázat	
14. hét Web biztonság. XSS támadások és kivédésük, stb.	vetítés, előadás, konkrét példán keresztül történő szemléltetés, magyarázat	

Könyvészet

1. R. Anderson: *Security Engineering: a guide to building dependable distributed systems*., 2nd Edition (Wiley, 2008) (1. kiadás: http://www.cl.cam.ac.uk/~rja14/book.html)
2. D. Gollmann: *Computer Security*, 2nd Edition (Wiley, 2006)
3. A. Menzes, P. van Oorschot, S. Vanstone, Handbook of Applied Criptography, CRC press, 1996. (Letölthető: http://cacr.uwaterloo.ca/hac/)
4. M. Howard, D. LeBlanc, J. Viega: 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, McGraw-Hill Professional, 2009
5. Charles P. Pfleeger, Shari Lawrence Pfleeger: *Security in Computing*, 4th Edition (Prentice Hall, 2006)

8.2 Szeminárium / Labor	Didaktikai módszerek	Megjegyzések
A diákok a félév során – szemináriumi bemutatót kell tartsanak egy, az előadás anyagához kapcsolódó kiegészítő témában – egy biztonsági rést szemléltető bemutatót és programot kell készítsenek		
1. hét Bevezető beszélgetés, témák kiosztása	megbeszélés	
2. hét „Social engineering”	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
3. hét Fizikai biztonság, felügyelő rendszerek.	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
4. hét Telefonok biztonsága	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
5. hét Banki biztonság	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
6. hét Elektronikus kereskedelem	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
7. hét Biometrikus azonosítás	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
8. hét Copyright	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
9. hét Számítógépes játékok, virtuális valóság	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
10. hét Webes alkalmazások (esettanulmányok): eBay, Google, Facebook	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
11. hét „Privacy Technology”	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
12. hét Terror, igazságszolgáltatás, szabadság	Bemutató, a téma megbeszélése, a bemutató közös kiértékelése	
13–14. hét Biztonsági rések elemzése: buffer overflow, cod injection, SQL injection, cross site scripting, cross-site request forgery,	Bemutató, a téma megbeszélése, a bemutató és programok közös kiértékelése	
Könyvészet – R. Anderson: Security Engineering: a guide to building dependable distributed systems., 2nd Edition (Wiley, 2008) (1. kiadás: http://www.cl.cam.ac.uk/~rja14/book.html) – M. Howard, D. LeBlanc, J. Viega: 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, McGraw-Hill Professional, 2009 – aktuális biztonsági problémákkal kapcsolatos weboldalak		

9. A tantárgy tartalmának összhangba hozása az episztemikus közösségek képviselői, a szakmai egyesületek és a szakterület reprezentatív munkáltatói elvárásaival.

A tantárgy ismerteti a a számítási rendszerek biztonságával kapcsolatos legújabb irányelveket, illetve a napjainkban a szoftverfejlesztésben használt biztonsági technikákat

10. Értékelés

Tevékenység típusa	10.1 Értékelési kritériumok	10.2 Értékelési módszerek	10.3 Aránya a végső jegyben
10.4 Előadás	Válaszok helyessége (a tanult fogalmak/alapelvek/technológiák működési elvének helyes ismerete)	Írásbeli elméleti vizsga (A)	30%
10.5 Szeminárium / Labor	A választott téma átfogó bemutatása: érthetőség, általánosság, használhatóság Kérdésekre adott válasz	Szemináriumi bemutató (B)	20%
	A mások által bemutatott témák megértését segítő aktív részvétel (pl. kérdésfeltevés, kiegészítés, megjegyzés hozzáfűzése)	Évközi tevékenység (C)	30%
	a választott biztonsági rést helyesen bemutató összefoglaló és jól megválasztott, a biztonsági rést bemutató, illetve javított program	Bemutató, program elemzése (D)	20%
10.6 A teljesítmény minimumkövetelményei			
- A tantárgy sikeres letételéhez az A, B, C és D részeredmények esetében el kell érni a minimális pontszámot (ami az elérhető összpontszám fele).			

Kitöltés dátuma	Előadás felelőse	Szeminárium felelőse
2013.04.25.	dr. Robu Judit, docens	dr. Robu Judit, docens

Az intézeti jóváhagyás dátuma	Intézetigazgató,
2013.04.30.	Dr. Szenkovits Ferenc, egyet. docens