UNIVERSITATEA „POLITEHNICA”DIN TIMIŞOARA

SYLLABUS
pentru disciplina:

“TEHNICI AVANSATE DE SECURIZAREA DATELOR SI PROGRAMELOR”

FACULTATEA DE AUTOMATICĂ ŞI CALCULATOARE
DOMENIUL/SPECIALIZAREA: INGINERIA SISTEMELOR / AUTOMATICĂ ŞI INFORMATICĂ APLICATĂ
DENUMIRE MASTER: SISTEME INFORMATICE APLICATE IN PRODUCTIE SI SERVICII
FORMA DE INVĂȚĂMÂNT ZI

Anul de studii: *I*

Semestrul *II*

Titularul cursului: *S.l. dr. ing. Bogdan Groza*
Colaboratori:

Numar de ore/saptamana/Verificarea/Credite					
Curs	**Seminar**	**Laborator**	**Proiect**	**Examinare**	**Credite**
2	**0**	**0**	**1**	**E**	**6**

A. OBIECTIVELE CURSULUI

Obiectivul principal este formarea unui mod de a gandi asupra problemelor de securitatea informatiei, care apar in sisteme informatice de uz comun si industriale, precum si asupra rezolvarii acestora. Se consolideaza totodata cunostintele de software si hardware, in special in zone ca: Java, .NET, retele de calculatoare, micocontrolere; prin dezvoltarea de aplicatii practice care contin elemente de securitate. Liniile de competenta ale domeniului sunt acoperite procentual dupa cum urmeaza: 40% linia 1, 30% linia 2, 20% linia 3, 10% linia 4.

B. SUBIECTELE CURSULUI

1. Fundamente ale securitatii informatiei: *Securitatea ca sistem, Sisteme de protectie, Sisteme criptografice, Probleme computationale, Teoria Informatiei, Teoria Complexitatii (8 ore de curs);* ***2. Securitate Software:*** *Politici de control a accesului, Protejarea secretelor, Protectia socketurilor, Atacuri DoS, Securitate in .NET, Protectia propritetatii intelectuale (copyright), Tehnici de obfuscarea a codului sursa pentru software industrial (2 ore de curs);* ***3. Securitate Hardware:*** *Hardware rezistent la alterare, Atacuri hardware (side-channel), Hardware Criptografic, Designul coprocesoarelor criptografice, Reprezentari numerice, Implementarea operatiilor elementare, Calculul in F2 (4 ore de curs);* ***4. Securitate in sisteme informatice complexe:*** *Controlul Accesului, Securitate in sisteme distribuite si grid, Securitate multinivel si multilaterala, Sisteme de monitorizare, Biometrie, Securitate in sisteme de telecomunicatii, Securitate in sisteme bancare, Securitate in sisteme de comert electronic (4 ore de curs);* ***5. Securitate in sisteme industriale si de control:*** *Standarde pentru asigurarea securitatii in sisteme industriale (2 ore de curs);* ***6. Securitate in medii constranse:*** *Securitate in sisteme SoC, Securitate in telefonia mobila, Securitate in retele de senzori (4 ore de curs);* ***7. Standarde si realizari practice de actualitate in securitatea informatiei:*** *Standarde in securitate retelelor si comunicare prin Internet, Standarde in Criptografie, Studii de caz (SSL, IPsec) (4 ore de curs).*

C. SUBIECTELE APLICATIILOR (laborator, seminar, proiect)

Implementari software (7 ore de laborator): Socketuri cu securitate cripografica, Securitate in .NET, Securitate in Java, Elemente de criptografie in .NET si Java, Implementarea primitivelor simetrice in Java si .NET, Criptografie cu cheie publica in Java si .NET, Implementarea firewal-urilor, Atacuri asupra sistemelor de parole din sistemul UNIX, Obfuscatoare de cod sursa. Implementari hardware (3 ore de laborator): Implementarea criptografiei pe

microcontrollere, Implementari in telefonia mobila, Studii de caz (4 ore de laborator): Protocolul de Autentificare NTLM, SSL si TLS, IPsec, Analiza unui sistem open-source.

D. BIBLIOGRAFIE *Se indică maximum trei titluri bibliografice de referință*

1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, 816 pages, ISBN 0849385237. (disponibil online gratuit la http://www.cacr.math.uwaterloo.ca/hac/)
2. Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, ISBN-10: 0471389226, ISBN-13: 978-0471389224, 640 pagini, John Wiley & Sons, USA, 2001. (disponibil online gratuit la http://www.cl.cam.ac.uk/~rja14/book.html)
3. Bogdan Groza, *Introducere in criptografia cu cheie publică*, 2007, 136 pagini, Editura Politehnica, ISBN 978-973-625-654-9. (disponibil la BUPT si online la http://www.aut.upt.ro/~bgroza/iccp.pdf)
4. Bogdan Groza, *Constructii criptografice hibride, bazate pe tehnici simetrice si asimetrice - aplicatii in sisteme de conducere*, 132 pagini, ISBN 978-973-625-688-2, 2008. (disponibila la BUPT si online la http://www.aut.upt.ro/~bgroza/teza.pdf)

E. PROCEDURA DE EVALUARE

Examen scris, 3 ore. Structura examenului: 3 subiecte cu pondere egala in nota care corespund la: teorie (probleme si concepte fundamentale in securitate), teorie aplicata (elemente de securitate software, hardware, sisteme informatice complexe etc.), studii de caz (unul dintre sistemele discutate in curs sau laborator, de ex. SSL, TLS etc.). Pondere 70% examen, 30% activitate pe parcurs in nota finala.

F.COMPATIBILITATE INTERNATIONALA

Stanford University, UC Berkeley, Massachusetts Institute of Technology (MIT).

Data: 1.09.2008

DIRECTOR/SEF DEPARTAMENT/CATEDRA
Prof. dr. ing. Ioan Silea

TITULAR DE DISCIPLINĂ,
S.l.dr. ing. Bogdan Groza