

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Babeș-Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematică și Informatică
1.3 Departamentul	Departamentul de Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclu de studii	Master
1.6 Programul de studiu / Calificarea	Sisteme Distribuite în Internet

2. Date despre disciplină

2.1 Denumirea disciplinei	Protocoloale de securitate în comunicații						
2.2 Titularul activităților de curs	Lect. Dr. Bufnea Darius-Vasile						
2.3 Titularul activităților de seminar	Lect. Dr. Bufnea Darius-Vasile						
2.4 Anul de studiu	1	2.5 Semestrul	2	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Obligatorie

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe					40
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					50
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					44
Tutoriat					14
Examinări					10
Alte activități:					0
3.7 Total ore studiu individual		158			
3.8 Total ore pe semestru		200			
3.9 Numărul de credite		8			

4. Precondiții (acolo unde este cazul)

4.1 De curriculum	Arhitectura Calculatoarelor, Sisteme de operare, Rețele de calculatoare, Programare Web, Aritmetică modulară și criptografie
4.2 De competențe	Cunoștințe elementare despre structura și modul de funcționare a rețelei Internet, cunoștințe elementare de criptografie, sisteme de operare, arhitectura calculatoarelor, baze de date, programare web, modelul client-server, algoritmică și programare

5. Condiții (acolo unde este cazul)

5.1 De desfășurare a cursului	Sală de curs dotată cu videoproiector
5.2 De desfășurare a seminarului/laboratorului	

6. Competențele specifice acumulate

Competențe profesionale	• Capacitate avansată de modelare a fenomenelor și proceselor specifice din domenii economice, industriale și științifice, folosind cunoștințe fundamentale din matematică, statistică și informatică • Capacitate avansată de analiză, proiectare și construcție a sistemelor informatice, folosind o gamă variată de platforme hardware și software, limbaje și medii de programare și instrumente de modelare, verificare și validare • Modelarea și conceptualizarea modelelor de proiectare / implementare pentru sisteme distribuite pe scară largă și care comunică între ele prin canale nesigure (Internet). • Dezvoltarea de aplicații pe arhitecturi masiv paralele (cloud computing, structuri grid) și a comunicațiilor în timp real, mobile computing, wireless, bluetooth etc. • Conceperea și utilizarea de modele pentru formalizarea conceptului de web semantic. • Capacitatea de a preda elevilor din ciclul liceal concepte și teorii specifice informaticii, în măsura în care titularul diplomei de disertație în informatică posedă un certificat de absolvire a modului de pregătire pedagogică
Competențe transversale	• Cunoașterea aprofundată a dezvoltărilor teoretice, metodologice și practice specifice informaticii • Utilizarea sistematică a cunoștințelor de specialitate în informatică la modelarea și interpretarea unor situații noi, în contexte de aplicare mai largi decât cele cunoscute • Cunoașterea și utilizarea integrată a aparatului conceptual și metodologic specific informaticii pentru soluționarea unor situații incomplet definite, pentru rezolvarea unor probleme teoretice și practice noi • Utilizarea nuanțată și pertinentă a criteriilor și metodelor de verificare, validare și evaluare a soluțiilor software realizate, capacitatea de a formula judecăți de valoare și de a fundamenta deciziile constructive • Elaborarea și conducerea de proiecte software complexe, de natură practică sau de cercetare, utilizând un spectru larg de metode cantitative și calitative • Capacitate avansată de comunicare în medii profesionale diferite, de utilizarea adecvată a vocabularului informatic în comunicarea profesională, în limba engleză • Capacitate de lucru în echipă, asumarea de roluri de execuție și de conducere, realizarea sarcinilor profesionale în condiții de autonomie și responsabilitate

7. Obiectivele disciplinei (reieșind din grila competențelor acumulate)

7.1 Obiectivul general al disciplinei	Cursul își propune aprofundarea de către cursant a celor mai bune mecanisme de securitate care pot fi implementate și utilizate la elaborarea unui protocol, în Internet, la nivelul unui sistem de calcul, în elaborarea unei aplicații software.
---------------------------------------	--

7.2 Obiectivele specifice	Cursul grupează câteva subiecte avansate din domeniul securității în rețele de calculatoare. Cursul este structurat pe baza arhitecturii TCP/IP de organizare a rețelelor de calculatoare, aspectele teoretice orientându-se spre fiecare nivel și set de protocoale din cadrul stivei TCP/IP. Cursul își propune: • să prezinte și familiarizeze studentul cu algoritmi de criptare cei mai des întâlniți precum și cu diferitele protocoale de la diverse nivele din stiva TCP/IP ce implementează acești algoritmi; • să familiarizeze studentul cu cele mai grave vulnerabilități în domeniu, precum și cu mecanismele și măsurile de luptă împotriva acestor vulnerabilități; • să prezinte cursanților principalele provocări de securitate pe care le ridică comerțul electronic pe Internet; • să abordeze din punct de vedere legal și moral diferite subiecte precum infraționalitatea pe Internet și intimitatea utilizatorului; • să contribuie la înțelegerea acestor domenii prin studierea și dezvoltarea unor aplicații practice relevante.
---------------------------	--

8. Conținuturi

8.1 Curs	Metode de predare	Observații
1. Prezentarea bibliografiei și structurii cursului. Cerințe și evaluare. Vulnerabilități informatice. Politici de securitate informatică la diferite nivele ale stivei TCP/IP.	Expuneri, explicații, exemple, studii de caz	
2. Istoria atacurilor informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Expuneri, explicații, exemple, studii de caz	
3. Securitatea sistemelor de operare. Securitatea sistemelor server în Internet. Arhitecturi de securitate în rețelele Enterprise. Atacuri locale și atacuri remote. Spyware și adware. Aplicații ale acestora în e-commerce.	Expuneri, explicații, exemple, studii de caz	
4. Anatomia unui exploit. Shell-code. Exemple.	Expuneri, explicații, exemple, studii de caz	
5. Mecanisme Firewall.	Expuneri, explicații, exemple, studii de caz	
6. Securitatea aplicațiilor Web. SQL Injection. JavaScript Injection. SMTP Injection. Cross Site Scripting.	Expuneri, explicații, exemple, studii de caz	
7. Algoritmi de criptare bazați pe chei publice și chei private. Semnături digitale. Certificate digitale.	Expuneri, explicații, exemple, studii de caz	
8. Infrastructuri bazate pe chei publice și servicii asociate acestora.	Expuneri, explicații, exemple, studii de caz	
9. Securitatea poștei electronice. DKIM. Mecanisme antispam: bayesian spam filters, DNS based black lists. PGP.	Expuneri, explicații, exemple, studii de caz	
10. Protocoale de securitate la nivel rețea și transport. IPSec. SSL și TLS. Securitate la nivel fizic și legătura de date.	Expuneri, explicații, exemple, studii de caz	
11. Vulnerabilități de tip Social Engineering. Infraționalitatea informatică. Asigurarea intimității	Expuneri, explicații, exemple, studii de	

utilizatorului.	caz	
12. Smartcard-uri. Biometrice.	Expuneri, explicații, exemple, studii de caz	
13. Securitate în sistemul bancar și plăți electronice în Internet.	Expuneri, explicații, exemple, studii de caz	
14. Mecanisme și scheme de autentificare. Kerberos.	Expuneri, explicații, exemple, studii de caz	

Bibliografie

1. V. V. Patriciu, M. Ene-Pietrosanu, C. Vaduva, I. Bica, N. Voicu, Securitatea Comerțului Electronic, Editura ALL
2. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnături Electronice și Securitate Informatică, Editura ALL, 2006
3. Stalling William, Cryptography and Network Security, Prentice Hall, 1999
4. Oskar Andreasson, Iptables Tutorial, <http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html>
5. F. Cohen, A Short Course on Computer Viruses, Wiley Professional Computing, 2 edition, April 1994
6. Mostafa Hashem, Protocols for Secure Electronic Commerce, CRC Press, 2004
7. B. Gladman, C. Ellison, N. Bohm, Digital Signatures, Certificates and Electronic Commerce, <http://jya.com/bg/digsig.pdf>
8. O'Mahony D., Electronic Payment Systems for E-Commerce, Artech House, 2001
9. Ford W., Secure Electronic Commerce, Prentice Hall, 2001
10. Weidong Kou, Payment Technologies for E-Commerce, Springer Verlag 2003
11. Vancea, Al. si altii, Programarea în limbaj de asamblare 80x86, Exemple si aplicatii, pag. 317-323, Ed. Risoprint, 2005
12. Martin Boldt, Privacy-Invasive Software, cap. 2, cap. 7, Blekinge Institute of Technology, ISBN 978-91-7295-100-6

8.2 Seminar / laborator	Metode de predare	Observații
1. Vulnerabilități informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Dezbateri, dialogul, exemple, conversații de aplicare	Seminarul se desfășoară din două în două săptămâni
2. Exploit-uri. Shell-code.	Dezbateri, dialogul, exemple, conversații de aplicare	
3. Mecanisme Firewall.	Dezbateri, dialogul, exemple, conversații de aplicare	
4. Securitatea aplicațiilor Web	Dezbateri, dialogul, exemple, conversații de aplicare	
5. Algoritmi de criptare bazați pe chei publice și chei private. Semnături digitale. Certificate digitale.	Dezbateri, dialogul, exemple, conversații de aplicare	
6. Securitatea poștei electronice	Dezbateri, dialogul, exemple, conversații de aplicare	
7. Protocoale de securitate la nivel rețea și transport.	Dezbateri, dialogul, exemple, conversații de aplicare	

Bibliografie

1. E. Rescorla, HTTP Over TLS, RFC 2818, May 2000
2. Kerberos: The Network Authentication Protocol, <http://web.mit.edu/Kerberos/>
3. T. Ylonen, C. Lonvick, The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006
4. P. Hoffman, SMTP Service Extension for Secure SMTP over TLS, RFC 2487, January 1999

5. OpenSSL: The Open Source toolkit for SSL/TLS, www.openssl.org
6. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006
7. S. Kent, Security Architecture for the Internet Protocol, RFC 2401, S. Kent, R. Atkinson

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Cursuri cu un conținut similar există în planul de învățământ al tuturor marilor universități din România și din străinătate.
- Cursul abordează probleme fundamentale de securitate și deosebit de actuale în Internet.
- Conținutul cursului acoperă principalele aspecte necesare a fi însușite de către cursant pentru a ocupa cu succes o poziție corespunzătoare în cadrul unei companii de profil.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoașterea principalelor aspecte teoretice prezentate la curs	Examen parțial din prima jumătate a materiei	1/4
	Cunoașterea principalelor aspecte teoretice prezentate la curs	Examen final din a doua jumătate a materiei	1/4
10.5 Seminar/laborator	Elaborarea unui referat și a unui proiect pe o temă de securitate stabilită de comun acord de cursant cu cadrul didactic dintre cele discutate la seminar.	Susținere orală de către cursant	1/2
10.6 Standard minim de performanță			
Pentru promovare trebuie cumulate următoarele două condiții:			
• prezentarea referatului și a proiectului, activitate ce trebuie notată cel puțin cu nota 5; • minim media 5 între nota examenului parțial și cea obținută la examenul din sesiune.			

Data completării

.....

Semnătura titularului de curs

Lect. Dr. Bufnea Darius-Vasile

Semnătura titularului de seminar

Lect. Dr. Bufnea Darius-Vasile

Data avizării în departament

.....

Semnătura directorului de departament

.....