

FISA DISCIPLINEI

DENUMIREA DISCIPLINEI		PROTOCOALE DE SECURITATE: MODELARE ȘI VERIFICARE				COD:MSI1208		
CICLUL DE STUDII (L-licență/M-master/D-doctorat) ȘI ANUL DE STUDIU (1,2,3,4)			M 2	Semestrul	2	STATUTUL DISCIPLINEI (OB-obligatorie/OP-opțională/F-facultativă)		OB
NUMĂRUL ORELOR PE SAPTĂMÂNĂ		TOTAL ORE SEMESTRU	TOTAL ORE ACTIVITATE INDIVIDUALĂ	NUMĂR DE CREDITE	TIPUL DE EVALUARE (P-pe parcurs, C-colocviu, E-examen, M-mixt)		LIMBA DE PREDARE	
C	S	L	Pr.					
2	1	1	-	56	124	8	M	Română, Engleză

TITULARUL ACTIVITĂȚILOR DE CURS	GRADUL DIDACTIC ȘI ȘTIINȚIFIC, PRENUMELE, NUMELE	DEPARTAMENTUL
	ASIST. DR. CĂTĂLIN BÎRJOVEANU	INFORMATICA

TITULARUL ACTIVITĂȚILOR DE SEMINAR/L.P.	GRADUL DIDACTIC ȘI ȘTIINȚIFIC, PRENUMELE, NUMELE	DEPARTAMENTUL
	ASIST. DR. CĂTĂLIN BÎRJOVEANU	INFORMATICA

DISCIPLINE ABSOLVITE ANTERIOR	Securitatea informației
-------------------------------	-------------------------

OBIECTIVE	Înțelegerea necesității metodelor formale pentru modelarea și verificarea protocoalelor de securitate. Însușirea principalelor tehnici de modelare și verificare a protocoalelor de securitate.
COMPETENȚE SPECIFICE ACUMULATE	
COMPETENȚE PROFESIONALE	Cunoștințe: Modul de funcționare al protocoalelor de securitate. Diferite tehnici de modelare a protocoalelor de securitate, specificarea proprietăților de securitate, tehnici de verificare a protocoalelor de securitate. Abilități: Abilitatea de a modela protocoale de securitate utilizând diversele tehnici studiate, abilitatea de a utiliza instrumente existente de verificare a protocoalelor de securitate, abilitatea de a depista erori și de a propune corecții în protocoalele de securitate. Abilitatea de a dezvolta un instrument de verificare a protocoalelor de securitate.
COMPETENȚE TRANSVERSALE	Utilizarea unor metode și tehnici eficiente de învățare, informare, cercetare și dezvoltare a capacităților de valorificare a cunoștințelor.
CONTINUTUL CURSULUI	Elemente de bază în teoria protocoalelor de securitate, proprietăți de securitate, vulnerabilități în protocoale de securitate. Modelarea protocoalelor de securitate: Modelul Ramanujam-Suresh, Multiset Rewriting, etc. Rezultate de nedecidabilitate pentru problema confidențialității. Protocoale de securitate mărginite. Complexitatea confidențialității pentru protocoale de securitate mărginite. Tehnici de verificare a protocoalelor de securitate: logica BAN, metoda inductivă, spații de strand-uri, etc. Instrumente de verificare automată a protocoalelor de securitate: Isabelle/HOL, Scyther, Avispa, etc.
BIBLIOGRAFIE (SELECTIVĂ)	1. P. Ryan and S. Schneider. Modelling and Analysis of Security Protocols. Addison-Wesley, 2001. 2. C. Cremers. Scyther -- Semantics and Verification of Security Protocols. Ph.D.Thesis, 2006. 3. M. Burrows, M. Abadi and R. Needham. A Logic of Authentication. 1989. 4. G. Bella. Formal Correctness of Security Protocols. Springer, 2007. 5. Avispa Web Page: http://www.avispa-project.org/
CONȚINUTUL LUCRĂRILOR DE SEMINAR/LABORATOR	Sunt analizate noi exemple de protocoale pentru tehnicile discutate în cadrul cursului și, de asemenea, sunt prezentate instrumente de verificare automată a protocoalelor de securitate: Isabelle/HOL, Scyther, Avispa, etc. Studenții participă în echipe la realizarea unui proiect în care implementează un instrument de verificare a protocoalelor de securitate. Prezentarea de articole recente din domeniul cursului.
BIBLIOGRAFIE (SELECTIVĂ)	1. P. Ryan and S. Schneider. Modelling and Analysis of Security Protocols. Addison-Wesley, 2001. 2. C. Cremers. Scyther -- Semantics and Verification of Security Protocols. Ph.D.Thesis, 2006. 3. M. Burrows, M. Abadi and R. Needham. A Logic of Authentication. 1989. 4. G. Bella. Formal Correctness of Security Protocols. Springer, 2007. 5. Avispa Web Page: http://www.avispa-project.org/ 6. Isabelle Web Page: http://www.cl.cam.ac.uk/research/hvg/Isabelle/ 7. Scyther Web Page: http://people.inf.ethz.ch/cremersc/scyther/index.html
REPERE METODOLOGICE	Predare cu utilizarea combinată a videoproietorului și a tablei (curs). Studii de caz, problematizare, exerciții, prezentări și dezbateri de articole/proiecte (laborator și seminar).

EVALUARE	metodele	activitate seminar, proiecte, test scris.
	forme	Activitate seminar: punerea de întrebări, participarea la discuții, referate. Activitatea laborator: proiect. Test scris.
	ponderea formelor de evaluare în formula notei finale	Activitate seminar: 30% Activitatea laborator: 30% Test scris: 40%
	standardele minime de performanță	Înțelegerea tehnicilor de bază de modelare și verificare a protocoalelor de securitate Următoarele condiții trebuie îndeplinite simultan: Activitate seminar: minim nota 6 Activitatea laborator: minim nota 6 Test scris: minim nota 5