FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea “Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Informatică**
1.3 Departamentul	**Informatică**
1.4 Domeniul de studii	**Informatică**
1.5 Ciclul de studii	**Master**
1.6 Programul de studii / Calificarea	**Securitatea Informației**

2. Date despre disciplină

2.1 Denumirea disciplinei			**PROTOCOALE DE SECURITATE:MODELARE ŞI VERIFICARE**				
2.2 Titularul activităţilor de curs			**LECT. DR. CĂTĂLIN BÎRJOVEANU**				
2.3 Titularul activităţilor de seminar			**LECT. DR. CĂTĂLIN BÎRJOVEANU**				
2.4 An de studiu	**I**	**2.5** Semestru	**2**	**2.6** Tip de evaluare	**M**	**2.7** Regimul disciplinei*	**OB**

** OB – Obligatoriu / OP – Opţional*

3. Timpul total estimat (ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**4**	din care: **3.2** curs	**2**	**3.3** seminar/laborator	**2**
3.4 Total ore din planul de învăţământ	**56**	din care: **3.5** curs	**28**	**3.6** seminar/laborator	**28**

Distribuţia fondului de timp	ore
Studiu după manual, suport de curs, bibliografie şi altele	**30**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	**30**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	**60**
Tutoriat	**-**
Examinări	**4**
Alte activităţi	**-**

3.7 Total ore studiu individual	**120**
3.8 Total ore pe semestru	**180**
3.9 Număr de credite	**6**

4. Precondiţii (dacă este cazul)

4.1 De curriculum	**Securitatea informației**
4.2 De competenţe	

5. Condiţii (dacă este cazul)

5.1 De desfăşurare a cursului	-
5.2 De desfăşurare a seminarului/ laboratorului	**Prezența obligatorie la laborator**

6. Competenţe specifice acumulate

Competenţe profesionale	**C1.** Capabilitatea de a cunoaște modul de funcționare al protocoalelor de securitate. **C2.** Cunoașterea tehnicilor de bază de modelare a protocoalelor de securitate, specificarea proprietăților de securitate, tehnici de verificare a protocoalelor de securitate. **C3.** 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. **C4.** Abilitatea de a dezvolta un instrument de verificare a protocoalelor de securitate.
Competenţe transversale	**CT1.** Capabilitatea de a proiecta și verifica protocoale de securitate utilizate ca parte a aplicațiilor din diverse domenii. **CT2.** Capacitatea de a utiliza noțiuni de logică, grafuri, algebră, pentru modelarea și verificarea protocoalelor de securitate.

7. Obiectivele disciplinei (din grila competenţelor specifice acumulate)

7.1 Obiectivul general	Înțelegerea necesității metodelor formale pentru modelarea și verificarea protocoalelor de securitate. Însuşirea principalelor tehnici de modelare şi verificare a protocoalelor de securitate.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Explice necesitatea metodelor formale în analiza protocoalelor de securitate ▪ Descrie principalele metode de verificare a protocoalelor de securitate ▪ Utilizeze tehnicile studiate pentru a verifica diverse protocoale de securitate ▪ Analizeze corectitudinea protocoalelor de securitate prin utilizarea de instrumente de verificare specifice ▪ Implementeze/dezvolte instrumente de verificare a protocoalelor de securitate

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	Introducere în modelarea și verificarea protocoalelor de securitate	Expunere	2
2.	Atacuri în protocoale de securitate	Expunere	2
3.	Spații de strand-uri	Expunere	2
4.	Verificarea protocoalelor de securitate utilizând spații de strand-uri	Expunere	2
5.	Semantici operaționale, proprietăți de securitate	Expunere	2

6.	Verificarea protocoalelor de securitate utilizând tehnici hibride	Expunere	2
7.	Atacuri type flaw, Atacuri multi-protocol, Scheme de etichetare	Expunere	2
8.	Recapitulare	Dezbatere	2
9.	Metoda inductivă	Expunere	2
10.	Isabelle/HOL	Expunere	2
11.	Verificarea protocoalelor de securitate în Isabelle/HOL	Expunere	2
12.	Fairness in protocoale e-commerce	Expunere	2
13.	Logica BAN	Expunere	2
14.	Verificarea protocoalelor de securitate utilizând logica BAN	Expunere	2

Bibliografie

1. C. Cremers, S. Mauw. Operational Semantics and Verification of Security Protocols. Information Security and Cryptography series, Springer, 2012.
2. G. Bella. Formal Correctness of Security Protocols. Springer, 2007.
3. C. Cremers. Feasibility of multi-protocol attacks. ARES 2006.
4. J.D. Guttman. Security goals: Packet trajectories and strand spaces. Springer 2001.
5. V. Cortier, S. Delaune and P. Lafourcade. A Survey of Algebraic Properties Used in Cryptographic Protocols. JCS 2006.
6. M. Burrows, M. Abadi and R. Needham. A Logic of Authentication. 1989.

8.2	**Seminar / Laborator**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)
1.	PKI pentru protectia impotriva atacurilor MITM	Experiment, studii de caz, problematizare, exerciții	2
2.	Atacul Heartbleed	Experiment, studii de caz, problematizare, exerciții	2
3.	Avispa: Modelarea si verificarea protocoalelor de securitate	Experiment, studii de caz, problematizare, exerciții	2
4.	Avispa: Verificarea protocoalelor de securitate utilizand Constraint-Logic-based Attack Searcher (CL-AtSe) Model-Checker	Experiment, studii de caz, problematizare, exerciții	2
5.	Avispa: Verificarea protocoalelor de securitate utilizand CL-AtSe, OFMC	Experiment, studii de caz, problematizare, exerciții	2
6.	Proiect Avispa (Proiectarea unui protocol de securitate cu obiective specifice si verificarea corectitudinii acestuia utilizand Avispa)	Experiment, studii de caz, problematizare	2
7.	Proiect Avispa	Experiment, studii de caz, problematizare	2

8.	Proiect Avispa	Experiment, studii de caz, problematizare	2
9.	Evaluare Proiect Avispa	Interviu	2
10.	Modelarea si verificarea protocoalelor de securitate utilizand Scyther	Experiment, studii de caz, problematizare, exerciții	2
11.	Verificarea protocoalelor de securitate utilizand Scyther	Experiment, studii de caz, problematizare, exerciții	2
12.	Proiect: Atacuri multi-protocol utilizand Scyther	Experiment, studii de caz, problematizare	2
13.	Proiect: Atacuri multi-protocol utilizand Scyther	Experiment, studii de caz, problematizare	2
14.	Exaluare Proiect: Atacuri multi-protocol utilizand Scyther	Interviu	2

Bibliografie:

1. Avispa Web Page: http://www.avispa-project.org/
2. Scyther Web Page: http://www.cs.ox.ac.uk/people/cas.cremers/scyther/index.html
3. Isabelle Web Page: http://www.cl.cam.ac.uk/research/hvg/Isabelle/

9. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor comunităţii, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Conținutul disciplinei este proiectat și structurat astfel încât să acopere principalele tematici necesare proiectării si verificării protocoalelor de securitate cu aplicații în practică.

10. Evaluare

Tip activitate	**10.1 Criterii de evaluare**	**10.2 Metode de evaluare**	**10.3 Pondere în nota finală (%)**
10.4 Curs	Înţelegerea tehnicilor de bază de modelare și verificare a protocoalelor de securitate	Test scris	25%
10.5 Seminar/ Laborator	Utilizarea tehnicilor de verificare prezentate la curs/laborator. Implementarea unui instrument de verificare a protocoalelor de securitate	Exercitii pe parcursul laboratoarelor + 2 Proiecte	75%
10.6 Standard minim de performanţă Simultan trebuie indeplinite conditiile: Test scris ≥ 5, Laborator ≥ 5			

Data completării	Titular de curs	Titular de seminar
23.03.2018	Lect. Dr. Cătălin Bîrjoveanu	Lect. Dr. Cătălin Bîrjoveanu

Data avizării în departament

Director de departament