



## FIȘA DISCIPLINEI

### 1. Date despre program

|                                       |  |
|---------------------------------------|--|
| 1.1 Instituția de învățământ superior | Universitatea “Alexandru Ioan Cuza” din Iași |
| 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 | Sisteme Distribuite                          |

### 2. Date despre disciplină

|  |   |              |   |                     |   |                         |    |  |
|--|---|--------------|---|---------------------|---|-------------------------|----|--|
| 2.1 Denumirea disciplinei              | PROTOCOALE DE SECURITATE:MODELARE ȘI VERIFICARE |              |   |                     |   |                         |    |  |
| 2.2 Titularul activităților de curs    | LECT. DR. CĂTĂLIN BÎRJOVEANU                    |              |   |                     |   |                         |    |  |
| 2.3 Titularul activităților de seminar | LECT. DR. CĂTĂLIN BÎRJOVEANU                    |              |   |                     |   |                         |    |  |
| 2.4 An de studiu                       | I,II  | 2.5 Semestru | 2 | 2.6 Tip de evaluare | M | 2.7 Regimul disciplinei | OB |  |

\* OB – Obligatoriu / OP – Opțional

### 3. Timpul total estimat (ore pe semestru și activități 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 învățământ   | 56 | din care: 3.5 curs | 28 | 3.6 seminar/laborator | 28  |
| Distribuția fondului de timp   |    |                    |    |                       | ore |
| Studiu după manual, suport de curs, bibliografie și altele                                     |    |                    |    |                       | 30  |
| Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren |    |                    |    |                       | 30  |
| Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri                          |    |                    |    |                       | 60  |
| Tutoriat   |    |                    |    |                       | -   |
| Examinări  |    |                    |    |                       | 4   |
| Alte activități  |    |                    |    |                       | -   |
| 3.7 Total ore studiu individual  |    |                    |    |                       | 120 |
| 3.8 Total ore pe semestru  |    |                    |    |                       | 180 |
| 3.9 Număr de credite   |    |                    |    |                       | 8   |

### 4. Precondiții (dacă este cazul)

|                   |                         |
|-------------------|-------------------------|
| 4.1 De curriculum | Securitatea informației |
| 4.2 De competențe |                         |

### 5. Condiții (dacă este cazul)

|                               |   |
|-------------------------------|---|
| 5.1 De desfășurare a cursului | - |
|-------------------------------|---|



5.2 De desfășurare a seminarului/  
laboratorului

**Prezența obligatorie la laborator**

## 6. Competențe specifice acumulate

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

## 7. Obiectivele disciplinei (din grila competențelor specifice acumulate)

|                                  |  |
|----------------------------------|--|
| <b>7.1 Obiectivul general</b>    | <p>Înțelegerea necesității metodelor formale pentru modelarea și verificarea protocoalelor de securitate. Însușirea principalelor tehnici de modelare și verificare a protocoalelor de securitate.</p>   |
| <b>7.2 Obiectivele specifice</b> | <p>La finalizarea cu succes a acestei discipline, studenții vor fi capabili să:</p> <ul style="list-style-type: none"><li>▪ Explice necesitatea metodelor formale în analiza protocoalelor de securitate</li><li>▪ Descrie principalele metode de verificare a protocoalelor de securitate</li><li>▪ Utilizeze tehnicile studiate pentru a verifica diverse protocoale de securitate</li><li>▪ Analizeze corectitudinea protocoalelor de securitate prin utilizarea de instrumente de verificare specifice</li><li>▪ Implementeze/dezvolte instrumente de verificare a protocoalelor de securitate</li></ul> |

## 8. Conținut

| 8.1 | Curs   | Metode de predare | Observații<br>(ore și referințe 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  | Dezbateri | 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                                    | Observații<br>(ore și referințe bibliografice) |
|-----|---|--|--|
| 1.  | PKI pentru protecția împotriva atacurilor MITM  | Experiment, studii de caz, problematizare, exerciții | 2  |
| 2.  | Atacul Heartbleed   | Experiment, studii de caz, problematizare, exerciții | 2  |
| 3.  | Avispa: Modelarea și verificarea protocoalelor de securitate  | Experiment, studii de caz, problematizare, exerciții | 2  |
| 4.  | Avispa: Verificarea protocoalelor de securitate using Constraint-Logic-based Attack Searcher (CL-AtSe) Model-Checker                    | Experiment, studii de caz, problematizare, exerciții | 2  |
| 5.  | Avispa: Verificarea protocoalelor de securitate using CL-AtSe, OFMC   | Experiment, studii de caz, problematizare, exerciții | 2  |
| 6.  | Proiect Avispa (Proiectarea unui protocol de securitate cu obiective specifice și verificarea corectitudinii acestuia utilizând 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 conținutului disciplinei cu așteptările reprezentanților comunității, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului**

Conținutul disciplinei este proiectat și structurat astfel încât să acopere principalele tematici necesare proiectării și 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                          | Înțelegerea 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.<br>Implementarea unui instrument de verificare a protocoalelor de securitate | Exercitii pe parcursul laboratoarelor + 2 Proiecte | 75%                             |
| 10.6 Standard minim de performanță |  |  |                                 |



Simultan trebuie indeplinite conditiile Test scris  $\geq 5$ , Laborator  $\geq 5$

Data completării  
23.03.2018

Titular de curs  
Lect. Dr. Cătălin Bîrjoveanu

Titular de seminar  
Lect. Dr. Cătălin Bîrjoveanu

Data avizării în departament

Director de departament