

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1	Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Automatică și Calculatoare
1.3	Departamentul	Calculatoare
1.4	Domeniul de studii	Calculatoare și Tehnologia Informației
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de Calcul / Master
1.7	Forma de învățământ	IF – învățământ cu frecvență
1.8	Codul disciplinei	01

### 2. Date despre disciplină

2.1	Denumirea disciplinei	Probleme de securitate la nivel de cod sursă									
2.2	Aria tematica (subject area)	Calculatoare și Tehnologia Informației									
2.3	Responsabil de curs	Șef lucrări dr.ing. Adrian COLEȘA ( <a href="mailto:adrian.colesa@cs.utcluj.ro">adrian.colesa@cs.utcluj.ro</a> )									
2.4	Titularul activităților de laborator	Drd.ing. Gheorghe HĂJMĂȘAN ( <a href="mailto:ghajmasan@bitdefender.com">ghajmasan@bitdefender.com</a> )									
2.5	Anul de studii	I	2.6	Semestrul	1	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/OB

### 3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]			[ore/semestru]							
				S	L	P		S	L	P			
I/1	Probleme de securitate la nivel de cod sursă	14	2		1		28		14		88	130	5

3.1	Număr de ore pe săptămână	3	3.2	din care curs	2	3.3	Aplicații	1
3.4	Total ore din planul de învățământ	42	3.5	din care curs	28	3.6	Aplicații	14
<b>Studiul individual</b>								<b>Ore</b>
Studiul după manual, suport de curs, bibliografie și notițe								18
Documentarea suplimentară în bibliotecă, pe platformele electronice și pe teren								18
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri								50
Tutoriat								0
Examinări								2
Alte activități								0
3.7	Total ore studiul individual			88				
3.8	Total ore pe semestru			130				
3.9	Număr de credite			5				

### 4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Programarea calculatoarelor, Structuri de date și algoritmi, Sisteme de operare
4.2	De competențe	Programare în C, cunoștințe de bază ale arhitecturii Intel x86, elemente de bază în programarea web

### 5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2	De desfășurare a aplicațiilor	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

## 6. Competențe specifice acumulate

Competențe profesionale	<p>C1 - Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatică</p> <ul style="list-style-type: none"> <li>• C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității</li> <li>• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</li> </ul> <p>C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> <li>• C4.3 – Dezvoltarea unor module software complexe respectând principiile metodologiilor de dezvoltare corectă a unui software din perspectiva securității. Dezvoltarea unor utilitare de analiză sau de validare a securității</li> <li>• C4.4 – Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare</li> <li>• C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității</li> </ul>
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Capacitatea evaluării caracteristicilor de securitate ale unei aplicații software la nivelul codului ei sursă. Dobândirea deprinderilor fundamentale de scriere a unui cod sursă fără vulnerabilități.
7.2	Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Cunoașterea mecanismelor de bază ce definesc securitatea sistemului și a mediului software în care se execută o aplicație (i.e. modelul de securitate), cum ar fi: permisiunile de acces, politicile de securitate, interacțiunea cu mediul exterior etc.</li> <li>2. Cunoașterea principalelor tipuri de vulnerabilități software, precum: utilizarea datelor utilizator nevalide corespunzător, interacțiunea necontrolată directă sau indirectă cu mediul exterior aplicației etc.</li> <li>3. Deprinderea unor tehnici eficiente de studiere și evaluare a unui cod sursă din perspectiva securității și capacitatea de a identifica posibile vulnerabilități.</li> <li>4. Capacitatea de a evalua implicațiile unei vulnerabilități descoperite.</li> <li>5. Cunoașterea tehnicilor și a bibliotecilor de funcții utile în scrierea unui cod sursă fără vulnerabilități și capacitatea de a le utiliza în situații reale.</li> </ol>

## 8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Concepte și aspecte de bază referitoare la vulnerabilitățile software și la metodele și uneltele de dezvoltare a unui software fără vulnerabilități și de evaluare a unui software din perspectiva posibilelor vulnerabilități	Expunere la tablă, prezentare cu video-proiectorul, discuții,	
2	Vulnerabilități de corupere a memoriei ( <i>buffer/integer overflow etc.</i> )		
3	Vulnerabilități specifice limbajului C: limite aritmetice (de reprezentare), conversii de tip, pointeri etc.		

4	Vulnerabilități în componentele structurale ale unei aplicații software ( <i>Program building blocks</i> )	probleme scurte		
5	Vulnerabilități în utilizarea și manipularea șirurilor de caractere și meta-caractere			
6	Vulnerabilități specifice sistemelor de operare UNIX			
7	Vulnerabilități specifice sistemelor de operare Windows			
8	Vulnerabilități de sincronizare (în situații de concurență)			
9	Vulnerabilități Web: injectare cod SQL, XSS, XSRF etc.			
10	Vulnerabilități de criptografie: parole vulnerabile, numere aleatoare previzibile etc.			
11	Vulnerabilități specifice codului aplicațiilor ce folosesc comunicarea în rețelele de calculatoare			
12	Metode de proiectare corectă a aplicațiilor din perspectiva securității: principii de proiectare, definirea modelului de riscuri (threat modeling), evaluare design etc.			
13	Metode de implementare corectă a unei aplicații software din perspectiva securității: metode și modele de dezvoltare a aplicațiilor (Waterfall, Agile), cele mai frecvente și mai periculoase riscuri și vulnerabilități, tehnici de defensive de scriere a codului ( <i>defensive coding techniques</i> )			
14	Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate			
8.2. Aplicații (lucrări de laborator)			Metode de predare	Observații
1	Unelte utile în identificarea și evaluarea vulnerabilităților unui cod sursă: navigatoare prin codul sursă, depanatoare, navigatoare prin codul executabil (binar), testare fuzzy		Scurte expuneri la tablă, tutoriale, ghiduri de lucru, demonstrații live, explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate	
2	Tehnici de evitare, detecție și evaluare a vulnerabilităților de corupere a memoriei și specifice limbajului C			
3	Tehnici de evitare, detecție și evaluare a vulnerabilităților de utilizare și gestionare a șirurilor de caractere și meta-caractere			
4	Tehnici de evitare, detecție și evaluare a vulnerabilităților specifice sistemului de operare Linux			
5	Tehnici de evitare, detecție și evaluare a vulnerabilităților sistemelor de operare Windows			
6	Tehnici de evitare, detecție și evaluare a vulnerabilităților de sincronizare			
7	Tehnici de evitare, detecție și evaluare a vulnerabilităților aplicațiilor Web și aplicațiilor de rețea			
<b>Bibliografie</b>				
1. M. Down, J. McDonald, J. Schuh, „ <i>The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities</i> ”, Addison-Wesley, 2007				
2. M. Howard, D. LeBlanc, J. Viega, „ <i>24 Deadly Sins of Software Security. Programming Flows and How to Fix Them</i> ”, McGraw Hill, 2010				
3. M. Howard, D. LeBlanc, „ <i>Writing Secure Code for Windows Vista</i> ”, Microsoft Press, 2007				
4. G. McGraw, „ <i>Software Security: Building Security In</i> ”, Addison-Wesley, 2006				
5. R. Seacord, „ <i>CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems</i> ”, Addison-Wesley, 2 <sup>nd</sup> edition, 2014				
6. -, „ <i>Common Weaknesses Enumeration (WCE)</i> ”, on-line: <a href="http://cwe.mitre.org/data/index.html">http://cwe.mitre.org/data/index.html</a>				

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor importanți din domeniul securității informației.

Cursuri referitoare la aspecte de securitate în dezvoltarea aplicațiilor și domenii adiacente (de exemplu, teste de penetrare) sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, la universități din țară și străinătate, cum ar fi:

- *Securitatea sistemelor software*, Master de Securitatea informației, Universitatea Al. I. Cuza, Iași, Facultatea de calculatoare, <http://profs.info.uaic.ro/~webdata/planuri/master/MISS1FS03.pdf>
- *Securitatea sistemelor și aplicațiilor*, Master de Securitatea tehnologiei informației, Academia Tehnică Militară, București, <http://mta.ro/masterat/masterinfosec/curricula2014.html>
- *Secure Software Systems*, Master of Science in Information Security, Carnegie Mellon University, SUA, <http://www.ini.cmu.edu/degrees/msis/courses.html>
- *Software Security*, Master in Information Security, Royal Holloway University of London, Information Security Group, [https://www.royalholloway.ac.uk/isg/documents/pdf/coursespecs\(msc\)/modules201314/iy5607softwaresecurityspec1314.pdf](https://www.royalholloway.ac.uk/isg/documents/pdf/coursespecs(msc)/modules201314/iy5607softwaresecurityspec1314.pdf)

## 10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de definire a conceptelor specifice problemelor de securitate la nivel de cod sursă și de expunere a metodelor de evaluare și dezvoltare corectă a unui cod sursă din perspectiva securității. Abilitatea de rezolvare a unor probleme specifice domeniului. Prezență, (inter)activitate în timpul orelor de curs.		Examen scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului		50%
Aplicații		Abilitatea de rezolvare a unor probleme specifice domeniului. Prezență, (inter)activitate în timpul orelor de laborator.		Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme în cadrul unui examen practic		50%
<b>10.4 Standard minim de performanță</b>						
Capacitatea de a defini vulnerabilitățile software fundamentale, precum: buffer-overflow, injectare code SQL, XSS etc. Capacitatea de a identifica vulnerabilitățile software fundamentale și de a corecta codul (demonstrate în cadrul exercițiilor de laborator și a examenului final).						

Responsabil curs  
Ș.I. dr.ing. Adrian Colesa

Director departament  
Prof.dr.ing. Rodica Potolea

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1	Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Automatică și Calculatoare
1.3	Departamentul	Calculatoare
1.4	Domeniul de studii	Calculatoare și Tehnologia Informației
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Securitatea informațiilor și sistemelor de calcul / Master
1.7	Forma de învățământ	IF – învățământ cu frecvență
1.8	Codul disciplinei	02

### 2. Date despre disciplină

2.1	Denumirea disciplinei	Securitatea informațiilor									
2.2	Aria tematica (subject area)	Calculatoare și Tehnologia Informației									
2.3	Responsabil de curs	S.I.dr.ing. Marius JOLDOȘ ( <a href="mailto:marius.joldos@cs.utcluj.ro">marius.joldos@cs.utcluj.ro</a> )									
2.4	Titularul activităților de seminar	S.I.dr.ing. Marius JOLDOȘ ( <a href="mailto:marius.joldos@cs.utcluj.ro">marius.joldos@cs.utcluj.ro</a> )									
2.5	Anul de studii	I	2.6	Semestrul	1	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/OB

### 3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs			Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]			[ore/semestru]					
				S	L	P		S			
I/1	Securitatea informațiilor	14	2	1		28	14		88	130	5

3.1	Număr de ore pe săptămână	3	3.2	din care curs	2	3.3	aplicații	1
3.4	Total ore din planul de învățământ	42	3.5	din care curs	28	3.6	aplicații	14
<b>Studiul individual</b>								<b>Ore</b>
Studiul după manual, suport de curs, bibliografie și notițe								50
Documentare suplimentară în bibliotecă, pe platformele electronice și pe teren								20
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri								16
Tutoriat								0
Examinări								2
Alte activități								0
3.7	Total ore studiul individual				88			
3.8	Total ore pe semestru				130			
3.9	Număr de credite				5			

### 4. Precondiții (acolo unde este cazul)

4.1	De curriculum	N/A
4.2	De competențe	Arhitectura sistemelor de operare, Arhitectura calculatoarelor, Cunoștințe de bază de rețele de calculatoare

### 5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2	De desfășurare a aplicațiilor	Prezență obligatorie 100% la orele de seminar pentru admiterea la examenul final

## 6. Competențe specifice acumulate

Competențe profesionale	<p><b>C1</b> Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatică</p> <ul style="list-style-type: none"> <li>• C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității</li> <li>• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</li> <li>• C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor</li> <li>• C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior</li> <li>• C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții</li> </ul> <p><b>C4</b> Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior</li> <li>• C4.4 – Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare</li> <li>• C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității</li> </ul> <p><b>C5</b> Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente ingineriei și informaticii specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• C5.2 – Analiza și interpretarea de situații noi complexe din lumea reală, prin prisma cunoștințelor fundamentale din domeniul securității informațiilor și sistemelor de calcul. Identificarea și corelarea unor soluții similare cu cele cunoscute, precum și plasarea corectă a ideilor noi în domeniul cercetării și dezvoltării de soluții de securitate informatică</li> <li>• C5.4 – Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate</li> </ul>
Competențe transversale	<p><b>CT1</b> Cunoașterea contextului economic, etic, legal și social de exercitare a profesiei pentru identificarea sarcinilor, planificarea activităților și optarea pentru decizii responsabile. Abilități de a evalua impactul social, etic și legal a desfășurării activităților profesionale</p>

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

7.1	Obiectivul general al disciplinei	Dobândirea unei viziuni ample și globale asupra numeroaselor arii și aspecte ce fac parte din sau sunt direct conexe cu securitatea informațiilor, a sistemelor și a rețelelor de calcul. Se urmărește, totodată, înțelegerea aplicabilității noțiunilor și a elementelor specifice securității informației la diverse procese din lumea reală (și în mod particular la proiecte software și sisteme de calcul) precum și dobândirea unei abilități de a observa, a analiza și a evalua legăturile dintre securitatea informației și lumea reală.
-----	-----------------------------------	---

7.2	Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Familiarizarea cu terminologia specifică domeniului securității informațiilor și folosirea corectă a acestei terminologii</li> <li>2. Înțelegerea diverselor aspecte și moduri în și prin care criminalitatea cibernetică și securitatea informațiilor este legată de activitățile zilnice</li> <li>3. Dobândirea unei abilități de a analiza un sistem informatic din punctul de vedere al securității informatice (de ex. a avea o atitudine critică)</li> <li>4. Dobândirea unei viziuni de ansamblu și de a putea face legătură între variate arii ingineresti, variate tipuri de proiecte software, domeniul și elementele specifice securității informațiilor și procedurile și standardele aplicabile</li> <li>5. Familiarizarea cu cele 10 domenii fundamentale (conform CISSP) a securității informațiilor.</li> </ol>
-----	-----------------------	---

## 8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații	
1	Introducere în securitatea informațiilor. Contextul istoric	Expunere la tablă, prezentare cu videoproiectorul, discuții		
2	Impactul criminalității cibernetice asupra vieții reale. O prezentare generică a tehnicilor și modalităților de atac cibernetic. Clasificarea malware-ului și a căilor de infecție			
3	Etica profesională în securitatea cibernetică			
4	Securitatea informațiilor și managementul riscurilor (CISSP 1)			
5	Controlul accesului (CISSP 2)			
6	Arhitectura și proiectarea sistemelor de securitate (CISSP 3)			
7	Securitatea fizică și de mediu (CISSP 4)			
8	Securitatea telecomunicațiilor și a rețelelor (CISSP 5)			
9	Criptografie (CISSP 6)			
10	Planificarea tratării evenimentelor critice și continuitatea operațiilor (CISSP 7)			
11	Aspecte legale, regulamente, proceduri de investigație și conformitate (CISSP 8)			
12	Securitatea în procesul de dezvoltare a aplicațiilor (CISSP 9)			
13	Operații de securitate (CISSP 10)			
14	Recapitulare			
8.2. Aplicații (seminar)		Metode de predare	Observații	
1	Impactul economic și social al atacurilor informatice	Explicații suplimentare, prezentarea unor exemple, discuții		
2	Ingineria socială și încrederea acordată celorlalți			
3	Legătura dintre confidențialitate și securitate			
4	Analiza unor rapoarte tehnice și articole recente (1)			
5	Analiza unor rapoarte tehnice și articole recente (2)			
6	Analiza unor rapoarte tehnice și articole recente (3)			
7	Analiza unor rapoarte tehnice și articole recente (4)			
<b>Bibliografie</b> 1. CISSP Exam Guide – Harris, S. – McGraw-Hill, 2012, 6 <sup>th</sup> edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2013, 2 <sup>nd</sup> edition 3. Geekonomics. The Real Cost of Insecure Software – Rice, D. – Addison-Wesley, 2008 4. Numeroase articole și rapoarte tehnice elaborate de companiile din domeniu – în format electronic.				

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

Materialul de bază pentru acest curs reprezintă tematica CISSP® (Certified Information Systems Security Professional), una dintre cele mai importante certificări în domeniul securității informațiilor, recunoscut și

apreciat pe plan internațional (<https://www.isc2.org/cissp/default.aspx>).

Se realizează totodată prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.

## 10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		Examen scris și/sau de tip grilă		70%
Aplicații		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de seminar		Prezentarea unei teme de cercetare din domeniul cursului și/sau rezolvarea și prezentarea soluției unor probleme similare cu cele discutate în timpul orelor de seminar		30%

### 10.4 Standard minim de performanță

Demonstrarea prin interacțiunile și discuțiile la orele de seminar a înțelegerii conceptelor și a noțiunilor folosite în domeniul securității informațiilor, precum și aplicarea și folosirea lor corectă. Capacitatea de analiză critică din punct de vedere al securității informatice a unui (studiu de) caz dintre cele prezentate și analizate la curs sau seminar și posibilitatea de a defini și explica termenii specifici folosiți.

Responsabil curs  
S.I. dr.ing. Marius Joldos

Director departament  
Prof.dr.ing. Rodica Potolea



## FIȘA DISCIPLINEI

### 1. Date despre program

1.1	Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Automatică și Calculatoare
1.3	Departamentul	Calculatoare
1.4	Domeniul de studii	Calculatoare și Tehnologia Informației
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de Calcul / Master
1.7	Forma de învățământ	IF – învățământ cu frecvență
1.8	Codul disciplinei	03

### 2. Date despre disciplină

2.1	Denumirea disciplinei	Inginerie inversă și analiza de software malițios									
2.2	Aria tematica (subject area)	Calculatoare și Tehnologia Informației									
2.3	Responsabil de curs	Drd.ing. George CABĂU ( <a href="mailto:gcabau@bitdefender.com">gcabau@bitdefender.com</a> )									
2.4	Titularul activităților de laborator	Drd.ing. George CABĂU ( <a href="mailto:gcabau@bitdefender.com">gcabau@bitdefender.com</a> )									
2.5	Anul de studii	I	2.6	Semestrul	1	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/OB

### 3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]			[ore/semestru]							
				S	L	P		S	L	P			
I/1	Inginerie inversă și analiza de software malițios	14	2		2		28		28		74	130	5

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	aplicații	2
3.4	Total ore din planul de învățământ	56	3.5	din care curs	28	3.6	aplicații	28

Studiul individual								Ore
Studiul după manual, suport de curs, bibliografie și notițe								16
Documentarea suplimentară în bibliotecă, pe platformele electronice și pe teren								16
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri								40
Tutoriat								0
Examinări								2
Alte activități								0
3.7	Total ore studiul individual				74			
3.8	Total ore pe semestru				130			
3.9	Număr de credite				5			

### 4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Programarea calculatoarelor, Arhitectura calculatoarelor, Sisteme de operare
4.2	De competențe	Limbaje de asamblare x86, Programare C, Arhitectura sistemelor de operare

### 5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2	De desfășurare a aplicațiilor	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

## 6. Competențe specifice acumulate

Competențe profesionale	<p>C2</p> <p>Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament</p> <ul style="list-style-type: none"> <li>• C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase</li> <li>• C2.2 – Analiza și înțelegerea a noi clase de software malițios, noi tehnici de atac, persistență, escaladarea privilegiilor etc., precum și compararea lor cu tehnicile cunoscute</li> <li>• C2.3 – Capacitatea de a face corelări și de a putea identifica obiecte potențial malițioase chiar dacă nu se poate analiza complet obiectul respectiv</li> <li>• C2.4 – Determinarea limitărilor teoretice și practice oferite de diverse metode de automatizare a analizei software-ului malițios. Propunerea de alternative mai bune unde este posibil</li> <li>• C2.5 – Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase</li> </ul> <p>C4</p> <p>Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior</li> <li>• C4.3 – Dezvoltarea unor module software complexe respectând principiile metodologiilor de dezvoltare corectă a unui software din perspectiva securității. Dezvoltarea unor utilitare de analiză sau de validare a securității</li> <li>• C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității</li> </ul>
	Competențe transversale

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

7.1	Obiectivul general al disciplinei	Familiarizarea studenților cu softurile malițioase, înțelegerea modului de funcționare a atacurilor informatice, obținerea cunoștințelor necesare pentru recunoașterea și investigarea unui sistem infectat
7.2	Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Înțelegerea modului de funcționare a unui software malițios</li> <li>2. Obținerea cunoștințelor necesare pentru identificarea unui software malițios</li> <li>3. Însușirea abilității de recunoaștere a unui sistem infectat</li> </ol>

## 8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Arhitectura sistemelor x86	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Limbajul de asamblare x86		
3	Structura sistemelor de operare Microsoft Windows: user-mode, kernel-mode, Win32 APIs		
4	Formatul fișierelor MZPE (1)		
5	Formatul fișierelor MZPE (2)		
6	Dezasamblarea codului compilat		
7	Decompilarea programelor		
8	Rularea în sisteme virtualizate și unelte de monitorizare		
9	Depanare folosind depanatoare (ex. OllyDgb)		
10	Tehnici de anti-analiza și anti-emulare		
11	Packer-e și protectoare		

12	Malware polimorfici și metamorfici		
13	Analiza exploit-urilor		
14	Analiza aplicațiilor mobile		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Recapitulare elemente de bază în programare în limbaj de asamblare	Expuneri la tablă, exerciții pe calculator, discuții și explicații suplimentare	
2	Elemente specifice de securitate în programare în limbaj de asamblare		
3	Programare folosind Win32-APIs (1)		
4	Programare folosind Win32-APIs (2)		
5	Decompilarea și analiza programelor folosind IdaPro (1)		
6	Decompilarea și analiza programelor folosind IdaPro (2)		
7	Decompilarea și analiza programelor folosind IdaPro (3)		
8	Analiza dinamica în sisteme virtualizate și unelte de monitorizare		
9	Analiza dinamica folosind OllyDbg		
10	Sisteme de sandbox-ing		
11	Analiza sistemelor infectate		
12	Dezinfectia sistemelor infectate		
13	Analiza exploit-urilor		
14	Colocviu de evaluare a cunoștințelor		
<b>Bibliografie</b> 1) Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (Sikorski, Michael – 2012 – No Strach Press) 2) The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler (Eagle, Chris – 2011 – No Strach Press) 3) The Art Of Computer Virus Research And Defense (Szor, Peter - 2005 - Addison-Wesley) 4) Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Dang, Bruce - 2014 - Wiley) 5) The Life of Binaries (Xeno Kovah – 2013 – <a href="http://opensecuritytraining.info/LifeOfBinaries.html">http://opensecuritytraining.info/LifeOfBinaries.html</a> )			

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.

Cursuri de inginerie inversă și analiză de software malițios sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- CS 675 *Reverse Software Engineering*, Masters in Computer Science, Drexel University, Philadelphia, USA.  
<https://www.cs.drexel.edu/~spiros/teaching/CS675/>
- CISC6800 *Malware Analytics and Software Security*, Fordham University, Masters Degree in Cybersecurity, New York, USA  
[http://www.fordham.edu/academics/colleges\\_graduate\\_s/undergraduate\\_colleg/school\\_of\\_profession/pcs\\_home/degrees\\_and\\_programs/ms\\_cybersecurity\\_94711.asp](http://www.fordham.edu/academics/colleges_graduate_s/undergraduate_colleg/school_of_profession/pcs_home/degrees_and_programs/ms_cybersecurity_94711.asp)
- *Malware*, Masters in Cybersecurity, Tallinn University of Technology, Estonia.  
[http://www.ttu.ee/studying/masters/masters\\_programmes/cyber-security/cyber-security-4/](http://www.ttu.ee/studying/masters/masters_programmes/cyber-security/cyber-security-4/)

## 10. Evaluare

Tip activitate	10.1	criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		Examen scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului		50%
Aplicații		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de laborator		Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor		50%

				probleme de analiză software malițios în cadrul unui examen practic		
10.4 Standard minim de performanță						
Demonstrarea înțelegerii modului de funcționare a unui program malițios. Identificarea prin analiză statică a unui software malițios. Identificarea prin analiză dinamică a unui software malițios.						

Responsabil curs  
Drd.ing. George Cabău

Director departament  
Prof.dr.ing. Rodica Potolea

## FIȘA DISCIPLINEI

### 1. Date despre program

1.1	Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Automatică și Calculatoare
1.3	Departamentul	Calculatoare
1.4	Domeniul de studii	Calculatoare și Tehnologia Informației
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de Calcul / Master
1.7	Forma de învățământ	IF – învățământ cu frecvență
1.8	Codul disciplinei	04.1

### 2. Date despre disciplină

2.1	Denumirea disciplinei	Dezvoltarea aplicațiilor Android și securitatea dispozitivelor mobile									
2.2	Aria tematica (subject area)	Calculatoare și Tehnologia Informației									
2.3	Responsabil de curs	Drd.ing. Ciprian OPRIȘA ( <a href="mailto:coprisa@bitdefender.com">coprisa@bitdefender.com</a> )									
2.4	Titularul activităților de laborator	Drd.ing. Ciprian OPRIȘA ( <a href="mailto:coprisa@bitdefender.com">coprisa@bitdefender.com</a> )									
2.5	Anul de studii	I	2.6	Semestrul	1	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/OP

### 3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs			Aplicații			Studiu Individual	TOTAL	Credit		
			[ore/săptămână]			[ore/semestrul]							
				S	L	P		S				L	P
V/1	Dezvoltarea aplicațiilor Android și securitatea dispozitivelor mobile	14	2		2		28		28		100	156	6

3.1	Număr de ore pe săptămână	4	3.2	din care curs	2	3.3	aplicații	2
3.4	Total ore din planul de învățământ	56	3.5	din care curs	28	3.6	aplicații	28
<b>Studiul individual</b>								<b>Ore</b>
Studiul după manual, suport de curs, bibliografie și notițe								18
Documentarea suplimentară în bibliotecă, pe platformele electronice și pe teren								24
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri								56
Tutoriat								0
Examinări								2
Alte activități								0
3.7	Total ore studiul individual			100				
3.8	Total ore pe semestrul			156				
3.9	Număr de credite			6				

### 4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Proiectare software, Sisteme de Operare
4.2	De competențe	N/A

### 5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2	De desfășurare a aplicațiilor	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

## 6. Competențe specifice acumulate

Competențe profesionale	<p><b>C1</b> Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatică</p> <ul style="list-style-type: none"> <li>• C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității</li> <li>• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</li> <li>• C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor</li> </ul> <p><b>C4</b> Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> <li>• C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior</li> <li>• C4.3 – Dezvoltarea unor module software complexe respectând principiile metodologiilor de dezvoltare corectă a unui software din perspectiva securității. Dezvoltarea unor utilitare de analiză sau de validare a securității</li> <li>• C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității</li> </ul> <p><b>C5</b> Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente ingineriei și informaticii specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• C5.4 – Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate</li> </ul>
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	În urma acestui curs, studenții trebuie să fie familiari cu conceptele din domeniul securității dispozitivelor mobile, să fie capabili să construiască aplicații pentru platforma Android, respectând normele de securitate și confidențialitate ale utilizatorului. De asemenea, se urmărește deprinderea de a realiza inginerie inversă pe aplicații mobile în vederea recunoașterii programelor malițioase și a depistării eventualelor probleme de securitate sau confidențialitate existente.
7.2	Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Înțelegerea modului de funcționare a sistemelor de operare Android, iOS și Windows Phone precum și a aplicațiilor mobile realizate pentru acestea</li> <li>2. Însușirea abilității de a dezvolta aplicații mobile</li> <li>3. Însușirea abilității de a analiza și de a efectua analiză inversă pe o aplicație mobilă</li> </ol>

		4. Cunoașterea caracteristicilor principalelor market-uri de aplicații mobile (Google Play, Amazon, Apple App Store, Windows Phone Apps Store)
--	--	--

## 8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Arhitecturi pentru device-uri mobile. Componente hardware și funcționarea lor (ecrane capacitive/rezistive, giroscop, unitati de stocare a datelor, senzori)	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Arhitectura sistemului de operare Android (sistemul de fișiere, managementul memoriei, mașina virtuală de Dalvik)		
3	Organizarea unei aplicații Android (format, resurse, manifest, permisiuni, ciclul de viață)		
4	Componente uzuale ale aplicațiilor Android: interfața utilizator, Intent-uri, accesul la rețea, accesul la rețeaua GSM		
5	Înregistrarea și distribuirea aplicațiilor în diverse piețe: studiu comparativ al piețelor Google, Apple, Microsoft		
6	Monetizarea aplicațiilor mobile		
7	Ingineria inversă pe aplicații Android: analiza statică		
8	Ingineria inversă pe aplicații Android: analiza dinamică		
9	Atacuri asupra canalelor de comunicație (GSM, wireless, bluetooth)		
10	Atacuri prin software malițios		
11	Probleme de confidențialitate la nivelul dispozitivelor mobile		
12	Asigurarea confidențialității în cadrul dispozitivelor furate sau pierdute		
13	Escaladarea securității dispozitivelor mobile: rooting și jailbreaking		
14	Asigurarea securității în contextul BYOD		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Introducere în platforma Android și familiarizarea cu mediul de dezvoltare	Scurte expuneri la tablă, ghiduri de lucru, demonstrații <i>live</i> , explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate	
2	Programarea interfeței utilizator în Android: Layout-uri și controale		
3	Programarea interfeței utilizator în Android: Gestiunea evenimentelor		
4	Depanarea și deployment-ul aplicațiilor Android		
5	Interacțiunea cu alte aplicații		
6	Accesarea senzorilor dispozitivului		
7	Utilizarea rețelei și transmisia datelor		
8	Scrierea de aplicații native		
9	Ingineria inversă pe aplicații Android: structura și dezasamblarea aplicațiilor		
10	Ingineria inversă pe aplicații Android: instrumente pentru analiza statică		
11	Ingineria inversă pe aplicații Android: analiza dinamică		
12	Studiu de caz: programe malițioase		
13	Studiu de caz: probleme de confidențialitate în aplicațiile din piață		
14	Evaluare și verificare		
<b>Bibliografie</b> 1. Hacking Exposed: Mobile Security Secrets & Solutions (Berman, Neil – 2013 – McGraw-Hill) 2. Mobile Application Security (Dwivedi, Himanshu – 2010 – Mc-Graw Hill) 3. Android Forensics (Hoog, Andrew – 2007 – Syngress) 4. Android Native Development Kit Cookbook (Liu, Feipeng – 2013 – Packt Publishing) 5. Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It (Zdziarski, Jonathan – 2012 – O'Reilly) 6. Programming Android: Java Programming for the New Generation of Mobile Devices (Mednieks, Zigurad – 2012 – O'Reilly) (2nd ed)			

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.

Cursuri legate de securitate a aplicațiilor și a dispozitivelor mobile sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, sau în cadrul altor cursuri opționale de facultate, cum ar fi:

- NordSecMob, Master's Programme in Security and Mobile Computing  
[http://nordsecmob.aalto.fi/en/nordsecmob\\_brochure\\_2013-pdf/](http://nordsecmob.aalto.fi/en/nordsecmob_brochure_2013-pdf/)
- XACS215 - Mobile Security, Stanford, USA,  
<http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=13070857>
- T-110.5130 Mobile Systems Programming, Aalto University, Finland - Master's Programme in Mobile Computing - Services and Security,  
[https://into.aalto.fi/download/attachments/16096227/OPS\\_Mobile\\_2014-2015.pdf](https://into.aalto.fi/download/attachments/16096227/OPS_Mobile_2014-2015.pdf)

## 10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		Examen scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului		50%
Aplicații		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de laborator		Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme în cadrul unui examen practic		50%

### 10.4 Standard minim de performanță

Demonstrarea înțelegerii arhitecturilor mobile și sublinierea diferențelor față de arhitecturile clasice.  
 Demonstrarea abilității de a dezvolta o aplicație Android, respectiv evaluarea uneia în vederea respectării normelor de securitate și confidențialitate.  
 Demonstrarea abilității de a efectua analiză inversă asupra unei aplicații și de a recunoaște conținutul malițios.

Responsabil curs  
Drd.ing. Ciprian Oprișa

Director departament  
Prof.dr.ing. Rodica Potolea



## FIȘA DISCIPLINEI

### 1. Date despre program

1.1	Instituția de învățământ superior	Universitatea Tehnică din Cluj-Napoca
1.2	Facultatea	Automatică și Calculatoare
1.3	Departamentul	Calculatoare
1.4	Domeniul de studii	Calculatoare și Tehnologia Informației
1.5	Ciclul de studii	Master
1.6	Programul de studii / Calificarea	Securitatea Informațiilor și Sistemelor de Calcul / Master
1.7	Forma de învățământ	IF – învățământ cu frecvență
1.8	Codul disciplinei	04.2

### 2. Date despre disciplină

2.1	Denumirea disciplinei	Programare și securitate la nivelul arhitecturii x86-64									
2.2	Aria tematica (subject area)	Calculatoare și Tehnologia Informației									
2.3	Responsabil de curs	Prof.dr.ing. Gheorghe SEBESTYEN ( <a href="mailto:gheorghe.sebestyen@cs.utcluj.ro">gheorghe.sebestyen@cs.utcluj.ro</a> )									
2.4	Titularul activităților de laborator	Drd. ing. Gheorghe HĂJMĂȘAN ( <a href="mailto:ghajmasan@bitdefender.com">ghajmasan@bitdefender.com</a> )									
2.5	Anul de studii	I	2.6	Semestrul	1	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/OP

### 3. Timpul total estimat

An/ Sem.	Denumirea disciplinei	Nr. săpt.	Curs	Aplicații			Curs	Aplicații			Studiu Individual	TOTAL	Credit
			[ore/săptămână]			[ore/semestru]							
				S	L	P		S	L	P			
I/1	Programare și securitate la nivelul arhitecturii x86-64	14	2		2		28		28		100	156	6

3.1	Număr de ore pe săptămână	2	3.2	din care curs	2	3.3	aplicații	2
3.4	Total ore din planul de învățământ	56	3.5	din care curs	28	3.6	aplicații	28
<b>Studiul individual</b>								<b>Ore</b>
Studiul după manual, suport de curs, bibliografie și notițe								20
Documentarea suplimentară în bibliotecă, pe platformele electronice și pe teren								18
Pregătire laboratoare, teme, referate, portofolii, eseuri								60
Tutoriat								0
Examinări								2
Alte activități								0
3.7	Total ore studiul individual			100				
3.8	Total ore pe semestru			156				
3.9	Număr de credite			6				

### 4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Programare în limbaj de asamblare, Sisteme de operare
4.2	De competențe	Arhitectura calculatoarelor, Programare în limbaj de asamblare x86, Programare C, Arhitectura sistemelor de operare

### 5. Condiții (acolo unde este cazul)

5.1	De desfășurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2	De desfășurare a aplicațiilor	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

## 6. Competențe specifice acumulate

Competențe profesionale	<p>C1</p> <p>Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatice</p> <ul style="list-style-type: none"> <li>• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</li> <li>• C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor</li> <li>• C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior</li> </ul> <p>C4</p> <p>Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate</p> <ul style="list-style-type: none"> <li>• C4.1 – Cunoașterea principiilor și noțiunilor de bază necesare dezvoltării și testării unui cod sigur din punctul de vedere al securității. Cunoașterea claselor uzuale de software și unelte de securitate. Cunoașterea arhitecturilor de SO și platformelor necesare dezvoltării soluțiilor de securitate</li> <li>• C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior</li> <li>• C4.3 – Dezvoltarea unor module software complexe respectând principiile metodologiilor de dezvoltare corectă a unui software din perspectiva securității. Dezvoltarea unor utilitare de analiză sau de validare a securității</li> <li>• C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității</li> </ul> <p>C5</p> <p>Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente ingineriei și informatice specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• C5.4 – Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate</li> <li>• C5.5 – Realizarea de activități de cercetare cu finalitate practică demonstrată prin prototipuri software și/sau hardware funcționale, cu aplicabilitate în domeniul securității informațiilor și sistemelor de calcul</li> </ul>
	Competențe transversale

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

7.1	Obiectivul general al disciplinei	Aprofundarea și înțelegerea arhitecturii x86-64 din punctul de vedere al dezvoltării sistemelor de operare și al mecanismelor de securitate, înțelegerea mecanismelor de nivel jos ale unui sistem de operare, a componentele sale precum și a elementelor de bază necesare dezvoltării acestuia.
7.2	Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Înțelegerea arhitecturii x86-64 la nivel structural și funcțional</li> <li>2. Înțelegerea diferitelor mecanisme de securitate oferite de arhitectura x86-64 precum și a modului lor de folosire în cadrul unui sistem de operare</li> <li>3. Cunoașterea diferitelor componente de nivel jos ale unui sistem de operare; înțelegerea rolului și funcționalității acestora precum și a relațiilor dintre ele.</li> </ol>

		4. Cunoașterea tehnicilor de proiectare și implementare a diferitelor componente ale unui sistem de operare 5. Dobândirea de experiență de programare a unor componente hardware la nivelul de interfață hardware-software
--	--	---

## 8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Recapitularea arhitecturii x86 și a limbajului de asamblare x86 pe 32 de biți. Utilitare de dezvoltare și depanare	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Inițializarea platformelor x86 și procesul de boot. Elemente de bază necesare dezvoltării unui sistem de operare pe platforma x64. Mesaje de debug și I/O elementar		
3	Arhitectura x86-64. Regiștrii, contextul de execuție, modelul de memorie, modul long (1)		
4	Arhitectura x86-64. Regiștrii, contextul de execuție, modelul de memorie, modul long (2)		
5	Înteruperi și excepții		
6	Programarea dispozitivelor hardware (tastatură, ceasuri, disk)		
7	Sisteme multi-procesor și primitive de sincronizare pe platforma x64		
8	Mecanisme hardware pe platforma x64 pentru implementarea de procese, thread-uri și schimbare de context ( <i>context switching</i> )		
9	Mecanisme hardware pe platforma x64 pentru implementarea elementelor de bază din managementul memoriei (fizice și virtuale)		
10	Bus-ul PCI/PCI Express. Plăci de extensie PCI și identificarea resurselor din sistem		
11	Mecanisme de securitate în procesoarele și platforma x64		
12	Modelul de execuție SSE și AVX. Optimizarea subrutinelor în limbaj de asamblare		
13	Modelul de execuție SSE și AVX. Optimizarea subrutinelor în programe C		
14	Recapitulare		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Exerciții de recapitulare pentru programarea în limbajul de asamblare x86 pe 16 și 32 de biți	Expuneri la tablă, discuții, explicații suplimentare, coordonarea realizării exercițiilor de laborator	
2	Folosirea de proiecte mixte, compilate parțial în asamblare și parțial în C. Bootarea <i>MultiBoot</i> folosind <i>GRUB</i> , pe 32 biți mod protejat, fără paginare. Output pe ecran ( <i>direct video memory write</i> ) fără dependență de BIOS. Integrarea unor funcții tip <i>printf</i>		
3	Activarea paginării pe 32 biți. Trecerea în modul de operare pe 64 biți.		
4	Configurarea corectă a unor structuri de control procesor, spații de memorie și paginări inițiale de lucru pentru 64 biți		
5	Configurarea IDT-ului și a PIC-ului pentru tratarea excepțiilor și a întreruperilor. STUB-uri în limbaj de asamblare, rutine tip ISR de tratare a excepțiilor și a întreruperilor în C și legătura între ele. Rutină de dump-at trapframe-uri cu scop de debug-ing		
6	Programarea și tratarea timerelor. Programarea pentru keyboard și implementarea unui I/O interactiv (e.g. command interpreter)		
7	Citire PIO mode ATA. Implementarea unor comenzi de tip "dir", "type" pe un volum FAT32		
8	Intel SMP 1.4 trampoline pentru procesoare AP. Exerciții simple de sincronizare (spinlock), afișare sincronizată SMP. Exerciții cu liste dublu înlănțuite de tipul FIFO cu mai multe procesoare		
9			
10	Treaduri SMP, context switching, scheduling. Salvarea contextului		
11	FPU/SSE. Mutex-uri		
12	Managementul memoriei: alocatori de memorie fizică, virtuală și heap.		
13	Sincronizarea lor. Testcase-uri, cazuri dificile		
14	Exemple de optimizare în SSE. Predarea exercițiilor de laborator		

## Bibliografie

- 1) Intel 64 and IA-32 Architectures Software Developer's Manual, Volume 1-3 (Intel – 2014 – electronic)
- 2) Operating System Concepts (Silberschatz, Abraham – 2012 – Wiley) (9th ed)
- 3) Optimizing subroutines in assembly language: An optimization guide for x86 platforms (Fog, Agner – 2013 – electronic, <http://www.agner.org/optimize/>)
- 4) Windows Operating System Internals Curriculum Resource Kit (CRK) (Microsoft – 2006 – electronic, MSDNAA)
- 5) Diverse site-uri despre dezvoltarea sistemelor de operare (de ex. <http://wiki.osdev.org/>).

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

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.

Acest curs este unul de aprofundare a cunoștințelor legate de arhitectura x86, de arhitectura și implementarea sistemelor de operare, precum și cele de programare hardware la nivel low-level. Multe dintre atacurile informatice complexe din lumea reală se bazează pe detalii foarte specifice unei platforme hardware (e.g. în special arhitectura CPU-ului și a managementului memoriei), și, din acest punct de vedere cursul și realizarea proiectului aferent pot oferi o experiență practică pentru înțelegerea multora dintre mecanismele de bază din spatele acestor atacuri.

## 10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finală
Curs		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs		Examen scris și/sau tip grilă și/sau prezentarea unei teme de cercetare din domeniul cursului		50%
Aplicații		Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de aplicații		Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme în cadrul unui examen practic		50%

### 10.4 Standard minim de performanță

Cunoașterea principalelor mecanisme oferite de arhitectura x86-64.

Cunoașterea principalelor principii de proiectare a sistemelor de operare.

Capacitatea de a folosi cunoștințele dobândite pentru a dezvolta componente din cadrul unui sistem de operare.

Responsabil curs  
Prof.dr.ing. Gheorghe Sebestyen

Director departament  
Prof.dr.ing. Rodica Potolea

## FISA DISCIPLINEI

### 1. Date despre program

1.1	Institutia de invatamint superior	Universitatea Tehnica din Cluj-Napoca
1.2	Facultatea	Automatica si Calculatoare
1.3	Departamentul	Calculatoare
1.4	Domeniul de studii	Calculatoare si Tehnologia Informatiei
1.5	Ciclul de studii	Master
1.6	Programul de studii/Calificarea	Securitatea Informațiilor și Sistemelor de Calcul / Master
1.7	Forma de invatamint	IF – invatamant cu frecventa
1.8	Codul disciplinei	05

### 2. Date despre disciplina

2.1	Denumirea disciplinei	Activitate de cercetare 1		
2.2	Aria tematica (subject area)	Calculatoare si Tehnologia Informatiei		
2.3	Responsabil de curs	Nu e cazul		
2.4	Titularul activităților de proiect	Nu e cazul		
2.5	Anul de studii	I	2.6 Semestrul	1
2.7	Evaluarea	A/R	2.8 Regimul disciplinei	DS/OB

### 3. Timpul total estimat

An/ Sem	Denumirea disciplinei	Nr. sapt.	Curs			Aplicații			Stud. Ind.	TOTAL	Credit
			[ore/săpt.]			[ore/sem.]					
			S	L	P	S	L	P			
I/1	Activitate de cercetare 1	14			3			42	192	234	9

3.1	Numar de ore pe săptămână	3	3.2	din care curs	-	3.3	aplicatii	3
3.4	Total ore din planul de inv.	42	3.5	din care curs	-	3.6	aplicatii	42
Studiul individual								Ore
Studiul după manual, suport de curs, bibliografie și notițe								0
Documentare suplimentară în bibliotecă, pe platformele electronice și pe teren								110
Pregătire referate, portofolii, eseuri, rapoarte tehnice și articole științifice								30
Tutoriat								14
Examinări								3
Alte activități (implementare aplicații și prototipuri de validare, testare și evaluare)								35
3.7	Total ore studiul individual	192						
3.8	Total ore pe semestru	234						
3.9	Numar de credite	9						

### 4. Precondiții (acolo unde este cazul)

4.1	De curriculum	Nu este cazul
4.2	De competente	Nu este cazul

### 5. Condiții (acolo unde este cazul)

5.1	De desfasurare a cursului	Nu este cazul
5.2	De desfasurare a aplicatiilor	Echipamente si programe specifice temei de proiect

### 6. Competente specifice acumulate

Competențe profesionale	<p>C1 - Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatică</p> <ul style="list-style-type: none"> <li>• C1.1 - Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității</li> <li>• C1.2 - Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou</li> <li>• C1.3 - Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor</li> <li>• C1.4 - Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior</li> </ul> <p>C5 - Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente ingineriei și informaticii specifice domeniului securității informațiilor și sistemelor de calcul</p> <ul style="list-style-type: none"> <li>• C5.1 - Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate</li> <li>• C5.2 - Analiza și interpretarea de situații noi complexe din lumea reală, prin prisma cunoștințelor fundamentale din domeniul securității informațiilor și sistemelor de calcul.</li> <li>• Identificarea și corelarea unor soluții similare cu cele cunoscute, precum și plasarea corectă a ideilor noi în domeniul cercetării și dezvoltării de soluții de securitate informatică</li> <li>• C5.3 - Aplicarea unor modele matematice și informatice teoretice sau cu o arie mai generală de aplicabilitate pentru a analiza, evalua și rezolva probleme diverse de securitate/confidențialitate din lumea reală</li> <li>• C5.4 - Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate</li> <li>• C5.5 - Realizarea de activități de cercetare cu finalitate practică demonstrată prin prototipuri software și/sau hardware funcționale, cu aplicabilitate în domeniul securității informațiilor și sistemelor de calcul</li> </ul>
Competențe transversale	<p>CT1 - Cunoașterea contextului economic, etic, legal și social de exercitare a profesiei pentru identificarea sarcinilor, planificarea activităților și optarea pentru decizii responsabile. Abilități de a evalua impactul social, etic și legal a desfășurării activităților profesionale</p>

## 7. Obiectivele disciplinei (reiesind din grila competențelor specific acumulate)

7.1	Obiectivul general al disciplinei	Deprinderea de abilități și competențe de cercetare, proiectare, dezvoltare și evaluare în domeniul securității informațiilor și sistemelor de calcul, calculatoarelor și al tehnologiei informațiilor.
7.2	Obiectivele specifice	<ol style="list-style-type: none"> <li>1. Identificarea unei probleme concrete de securitate (la nivelul unei aplicații particulare sau la nivel general al unei strategii, mecanism, protocol etc.)</li> <li>2. Elaborarea specificațiilor/cerințelor de rezolvare a problemei identificate</li> <li>3. Elaborarea unei strategii de investigare și cercetare a problemei abordate și a unui plan de lucru</li> <li>4. Cunoașterea stării actuale a domeniului problemei alese</li> </ol>

## 8. Continuturi

8.1. Curs (programa analitica)		Metode de predare	Observatii
1	Nu e cazul.		
8.2. Aplicații (proiect)		Metode de predare	Observatii
	<ol style="list-style-type: none"> <li>1. Stabilirea temei proiectului de disertație</li> <li>2. Stabilirea principalelor direcții de investigat</li> <li>3. Documentare asupra temei de disertație</li> <li>4. Realizarea unei sinteze privind documentația bibliografică</li> <li>5. Elaborarea unui raport tehnic de descriere a activității desfășurate și a sintezei bibliografice</li> </ol>	Colaborare îndrumător - student	
<b>Bibliografie</b> Se stabilește de către fiecare îndrumător de proiect de disertație în parte.			

## 9. Coroborarea continuturilor disciplinei cu asteptarile reprezentantilor comunitatii epistemice, asociatiilor, profesionale si angajatori din domeniul aferent programului

Se realizeaza prin întâlniri periodice cu reprezentanții mediului economic.

## 10. Evaluare

Tip activitate	10.1	Criterii de evaluare	10.2	Metode de evaluare	10.3	Ponderea din nota finala
Curs		Nu este cazul				
Aplicații		Pe baza cunoștințelor și rezultatelor obținute și a referatului elaborat		Evaluare orala Evaluare referat		60% 40%
<b>10.4 Standard minim de performanta</b>						
Stabilirea unei direcții de cercetare, parcurgerea bibliografiei asociate, elaborarea documentației aferente și a raportului tehnic.						

Responsabil curs  
Îndrumătorii de disertație

Director departament  
Prof.dr.ing. Rodica Potolea