FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și 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 Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	1.

2. Date despre disciplină

2.1 Denumirea disciplinei	***Probleme de securitate la nivel de cod sursă***				
2.2 Titularii de curs	Conf. dr.ing. Adrian COLEȘA - (adrian.colesa@cs.utcluj.ro)				
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect	Drd.ing. Gheorghe HĂJMĂȘAN - (ghajmasan@bitdefender.com)				
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar		Laborator	1	Proiect	
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar		Laborator	14	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										18
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										18
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										45
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	83
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

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

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	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 informatice • 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 • 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 C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • 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 • 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 • 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 • 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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	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. 2. Cunoașterea principalelor tipuri de vulnerabilități software, precum: utilizarea datelor utilizator nevalidate corespunzător, interacțiunea necontrolată directă sau indirectă cu mediul exterior aplicației etc. 3. Deprinderea unor tehnici eficiente de studiere și evaluare a unui cod sursă din perspectiva securității și capacitatea de a identifica posibile vulnerabilități. 4. Capacitatea de a evalua implicațiile unei vulnerabilități descoperite. 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.

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
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	2	Expunere la tablă, prezentare cu video-proiectorul, discuții, probleme scurte	
Vulnerabilități de corupere a memoriei (*buffer/integer overflow etc.*)	2		
Vulnerabilități specifice limbajului C: limite aritmetice (de reprezentare), conversii de tip, pointeri etc.	2		
Vulnerabilități în componentele structurale ale unei aplicații software (*Program building blocks*)	2		
Vulnerabilități în utilizarea și manipularea șirurilor de caractere și meta-caractere	2		
Vulnerabilități specifice sistemelor de operare UNIX	2		

Vulnerabilități specifice sistemelor de operare Windows	2		
Vulnerabilități de sincronizare (în situații de concurență)	2		
Vulnerabilități Web: injectare cod SQL, XSS, XSRF etc.	2		
Vulnerabilități de criptografie: parole vulnerabile, numere aleatoare previzibile etc.	2		
Vulnerabilități specifice codului aplicațiilor ce folosesc comunicarea în rețelele de calculatoare	2		
Metode de proiectare corectă a aplicațiilor din perspectiva securității: principii de proiectare, definirea modelului de riscuri (threat modeling), evaluare design etc.	2		
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 (*defensive coding techniques*)	2		
Metode de evaluare a (codului) unei aplicații din perspectiva securității: asigurarea calității, testare, gestiunea vulnerabilităților identificate	2		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziția studenților într-un număr de exemplare corespunzător)*

1. M. Down, J. McDonald, J. Schuh, „*The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities*”, Addison-Wesley, 2007
2. M. Howard, D. LeBlanc, J. Viega, „*24 Deadly Sins of Software Security. Programming* Flows *and How to Fix Them*”, McGraw Hill, 2010
3. M. Howard, D. LeBlanc, „*Writing Secure Code for Windows Vista*”, Microsoft Press, 2007
4. G. McGraw, „*Software Security: Building Security In*”, Addison-Wesley, 2006
5. R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems”, Addison-Wesley, 2nd edition, 2014
6. -, „*Common Weaknesses Enumeration* (WCE)”, on-line: http://cwe.mitre.org/data/index.html

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Unelte utile în identificarea și evaluarea vulnerabilităților unui cod sursă: navigatoare prin codul sursă, depanatoare, navigatoare prin codul executabil (binar), testare *fuzzy*	1	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	
Tehnici de evitare, detecție și evaluare a vulnerabilităților de corupere a memoriei si specifice limbajului C	1		
Tehnici de evitare, detecție și evaluare a vulnerabilităților de utilizare și gestionare a șirurilor de caractere și meta-caractere	1		
Tehnici de evitare, detecție și evaluare a vulnerabilităților specifice sistemului de operare Linux	1		
Tehnici de evitare, detecție și evaluare a vulnerabilităților sistemelor de operare Windows	1		
Tehnici de evitare, detecție și evaluare a vulnerabilităților de sincronizare	1		
Tehnici de evitare, detecție și evaluare a vulnerabilităților aplicațiilor Web si aplicațiilor de rețea	1		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)*

1. M. Down, J. McDonald, J. Schuh, „*The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities*”, Addison-Wesley, 2007
2. M. Howard, D. LeBlanc, J. Viega, „*24 Deadly Sins of Software Security. Programming* Flows *and How to Fix Them*”, McGraw Hill, 2010
3. M. Howard, D. LeBlanc, „*Writing Secure Code for Windows Vista*”, Microsoft Press, 2007
4. G. McGraw, „*Software Security: Building Security In*”, Addison-Wesley, 2006
5. R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems”, Addison-Wesley, 2nd edition, 2014
6. -, „*Common Weaknesses Enumeration* (WCE)”, on-line: http://cwe.mitre.org/data/index.html

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi 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

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere 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%
Seminar			
Laborator	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%
Proiect			
Standard minim de performanţă: 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
Conf.dr.ing. Adrian Colesa

Director departament
Prof.dr.ing. Rodica Potolea

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și 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 Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	2.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Securitatea Informatiilor***	
2.2 Titularii de curs				S.l.dr.ing. Marius JOLDOȘ (marius.joldos@cs.utcluj.ro)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				S.l.dr.ing. Marius JOLDOȘ (marius.joldos@cs.utcluj.ro)	
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar	1	Laborator		Proiect	
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar	14	Laborator		Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										50
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										20
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										11
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	83
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

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

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență obligatorie 100% la orele de seminar pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	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 informatice • 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 • 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 • 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 • 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 • C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • 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 • 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 • 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 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 inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • 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 informatice • 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
6.2 Competenţe transversale	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

7. Obiectivele disciplinei

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	1. Familiarizarea cu terminologia specifică domeniului securității informațiilor și folosirea corectă a acestei terminologii 2. Înțelegerea diverselor aspecte și moduri în și prin care criminalitatea

	cibernetică și securitatea informațiilor este legată de activitățile zilnice 3. Dobândirea unei abilități de a analiza un sistem informatic din punctul de vedere al securității informatice (de ex. a avea o atitudine critică) 4. Dobândirea unei viziuni de ansamblu și de a putea face legătură între variate arii inginerești, variate tipuri de proiecte software, domeniul și elementele specifice securității informațiilor și procedurile și standardele aplicabile 5. Familiarizarea cu cele 10 domenii fundamentale (conform CISSP) a securității informațiilor.

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Introducere în securitatea informaților. Contextul istoric	2	Expunere la tablă, prezentare cu videoproiectorul, discuții	
Impactul criminalității cibernetice asupra vieții reale. O prezentare generică a tehnicilor și modalităților de atac cibernetic. Clasificarea malware-ului și a căilor de infecție	2		
Etica profesională în securitatea cibernetică	2		
Securitatea informațiilor și managementul riscurilor (CISSP 1)	2		
Controlul accesului (CISSP 2)	2		
Arhitectura și proiectarea sistemelor de securitate (CISSP 3)	2		
Securitatea fizică și de mediu (CISSP 4)	2		
Securitatea telecomunicațiilor și a rețelelor (CISSP 5)	2		
Criptografie (CISSP 6)	2		
Planificarea tratării evenimentelor critice și continuitatea operațiilor (CISSP 7)	2		
Aspecte legale, regulamente, proceduri de investigație și conformitate (CISSP 8)	2		
Securitatea în procesul de dezvoltare a aplicațiilor (CISSP 9)	2		
Operații de securitate (CISSP 10)	2		
Recapitulare	2		
Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)* 1. CISSP Exam Guide – Harris, S. – McGraw-Hill, 2012, 6th edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2013, 2nd 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.			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Impactul economic și social al atacurilor informatice	1	Explicații suplimentare, prezentarea unor exemple, discuții	
Ingineria socială și încrederea acordată celorlalți	1		
Legătura dintre confidențialitate și securitate	1		
Analiza unor rapoarte tehnice și articole recente (1)	1		
Analiza unor rapoarte tehnice și articole recente (2)	1		
Analiza unor rapoarte tehnice și articole recente (3)	1		
Analiza unor rapoarte tehnice și articole recente (4)	1		
Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)* 1. CISSP Exam Guide – Harris, S. – McGraw-Hill, 2012, 6th edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2013, 2nd 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.			

** Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi 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	Criterii de evaluare	Metode de evaluare	Pondere 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%
Seminar	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%
Laborator			
Proiect			
Standard minim de performanţă: 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 si analizate la curs sau seminar și posibilitatea de a defini și explica termenii specifici folosiți.			

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

Director departament
Prof.dr.ing. Rodica Potolea

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și 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 Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	3.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Inginerie inversă și analiza de software malițios***	
2.2 Titularii de curs				Drd.ing. George CABĂU (gcabau@bitdefender.com)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Drd.ing. George CABĂU (gcabau@bitdefender.com)	
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	**Curs**	**1**	Seminar	1	Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	14	Seminar	14	Laborator	28	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										16
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										16
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										35
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	69
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

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

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	C2. Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament • C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase • 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

	• C2.3 – Capacitatea de a face corelări și de a putea identifica obiecte potențial malițioase chiar dacă nu se poate analiza complet obiectul respectiv • 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 • C2.5 – Elaborarea unor noi clase de atacuri sau software malițios, și propunerea unor noi proprietăți potrivite clasificării codurilor malițioase C4. Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • 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 • 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 • 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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	1. Înțelegerea modului de funcționare a unui software malițios 2. Obținerea cunoștințelor necesare pentru identificarea unui software malițios 3. Însușirea abilității de recunoaștere a unui sistem infectat

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Arhitectura sistemelor x86	1	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Limbajul de asamblare x86	1		
Structura sistemelor de operare Microsoft Windows: user-mode, kernel-mode, Win32 APIs	1		
Formatul fișierelor MZPE (1)	1		
Formatul fișierelor MZPE (2)	1		
Dezasamblarea codului compilat	1		
Decompilarea programelor	1		
Rularea in sisteme virtualizate și unelte de monitorizare	1		
Depanare folosind depanatoare (ex. OllyDgb)	1		
Tehnici de anti-analiza si anti-emulare	1		
Packer-e și protectoare	1		
Malware polimorfici și metamorfici	1		
Analiza exploit-urilor	1		
Analiza aplicațiilor mobile	1		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

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 – http://opensecuritytraining.info/LifeOfBinaries.html)

8.2 Aplicații (**seminar**/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Recapitulare elemente de bază în programare în limbaj de asamblare	3	Expuneri la tablă, exerciții pe calculator, discuții și explicații suplimentare	
Elemente specifice de securitate în programare în limbaj de asamblare	3		
Programare folosind Win32-APIs (1)	3		
Programare folosind Win32-APIs (2)	3		
Decompilarea și analiza programelor folosind IdaPro (1)	3		
Decompilarea și analiza programelor folosind IdaPro (2)	3		
Decompilarea și analiza programelor folosind IdaPro (3)	3		
Analiza dinamica în sisteme virtualizate si unelte de monitorizare	3		
Analiza dinamica folosind OllyDbg	3		
Sisteme de sandbox-ing	3		
Analiza sistemelor infectate	3		
Dezinfecția sistemelor infectate	3		
Analiza exploit-urilor	3		
Colocviu de evaluare a cunoștințelor	3		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)*

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 – http://opensecuritytraining.info/LifeOfBinaries.html)

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi 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
- *Malware*, Masters in Cybersecurity, Tallinn University of Technology, Estonia. http://www.ttu.ee/studying/masters/masters_programmes/cyber-security/cyber-security-4/

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere 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%
Seminar Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor	Realizarea activităților de laborator și rezolvarea temelor de casă și/sau a unor probleme	50%

	de laborator	de analiză software malițios în cadrul unui examen practic	
Proiect			
Standard minim de performanţă: 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 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și 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 Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	4.1

2. Date despre disciplină

2.1 Denumirea disciplinei				***Dezvoltarea aplicațiilor Android și securitatea dispozitivelor mobile***	
2.2 Titularii de curs				S.l. Dr.ing. Ciprian OPRIȘA (coprisa@bitdefender.com)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				S.l. Dr.ing. Ciprian OPRIȘA (coprisa@bitdefender.com)	
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DA
	DI – Impusă, DOp – opțională, DFac – facultativă				DOp

3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	Curs	2	Seminar		Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	28	Seminar		Laborator	28	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										18
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										24
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										50
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	94
3.5 Total ore pe semestru (3.2+3.4)	150
3.6 Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

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

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	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 informatice • 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 • 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 nouu • 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 C4. Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • 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 • 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 • 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 • 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 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 inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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	1. Înțelegerea modului de funcționare a sistemelor de operare Android, iOS și Windows Phone precum și a aplicațiilor mobile realizate pentru acestea 2. Însușirea abilității de a dezvolta aplicații mobile 3. Însușirea abilității de a analiza și de a efectua analiză inversă pe o aplicație mobilă 4. Cunoașterea caracteristicilor principalelor market-uri de aplicații mobile (Google Play, Amazon, Apple App Store, Windows Phone Apps Store)

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Arhitecturi pentru device-uri mobile. Componente hardware si funcționarea lor (ecrane capacitive/rezistive, giroscoape, unitati de stocare a datelor, senzori)	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Arhitectura sistemului de operare Android (sistemul de fisiere, managementul memoriei, masina virtuala de Dalvik)	2		
Organizarea unei aplicații Android (format, resurse, manifest,	2		

permisiuni, ciclul de viață)			
Componente uzuale ale aplicațiilor Android: interfața utilizator, Intent-uri, accesul la rețea, accesul la rețeaua GSM	2		
Înregistrarea și distribuirea aplicațiilor în diverse piețe: studiu comparativ al piețelor Google, Apple, Microsoft	2		
Monetizarea aplicațiilor mobile	2		
Ingineria inversă pe aplicații Android: analiza statică	2		
Ingineria inversă pe aplicații Android: analiza dinamică	2		
Atacuri asupra canalelor de comunicație (GSM, wireless, bluetooth)	2		
Atacuri prin software malițios	2		
Probleme de confidențialitate la nivelul dispozitivelor mobile	2		
Asigurarea confidențialității în cadrul dispozitivelor furate sau pierdute	2		
Escaladarea securității dispozitivelor mobile: rooting și jailbreaking	2		
Asigurarea securității în contextul BYOD	2		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziția studenților într-un număr de exemplare corespunzător)*

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)

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Introducere în platforma Android și familiarizarea cu mediul de dezvoltare	2	Scurte expuneri la tablă, ghiduri de lucru, demonstrații *live*, explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate	
Programarea interfeței utilizator în Android: Layout-uri și controale	2		
Programarea interfeței utilizator în Android: Gestiunea evenimentelor	2		
Depanarea și deployment-ul aplicațiilor Android	2		
Interacțiunea cu alte aplicații	2		
Accesarea senzorilor dispozitivului	2		
Utilizarea rețelei și transmisia datelor	2		
Scrierea de aplicații native	2		
Ingineria inversă pe aplicații Android: structura și dezasamblarea aplicațiilor	2		
Ingineria inversă pe aplicații Android: instrumente pentru analiza statică	2		
Ingineria inversă pe aplicații Android: analiza dinamică	2		
Studiu de caz: programe malițioase	2		
Studiu de caz: probleme de confidențialitate în aplicațiile din piață	2		
Evaluare și verificare	2		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)*

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)

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi 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/
- *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

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere 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%
Seminar			
Laborator	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%
Proiect			
Standard minim de performanţă: 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
S.l.Dr.ing. Ciprian Oprişa

Director departament
Prof.dr.ing. Rodica Potolea

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și 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 Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	4.2

2. Date despre disciplină

2.1 Denumirea disciplinei	***Programare și securitate la nivelul arhitecturii x86-64***				
2.2 Titularii de curs	Prof.dr.ing. Gheorghe SEBESTYEN (gheorghe.sebestyen@cs.utcluj.ro)				
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect	Drd. ing. Gheorghe HĂJMĂȘAN (ghajmasan@bitdefender.com)				
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DA
	DI – Impusă, DOp – opțională, DFac – facultativă				DOp

3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	Curs	2	Seminar		Laborator	2	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	28	Seminar		Laborator	28	Proiect	
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										20
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										18
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										54
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0
3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))										94
3.5 Total ore pe semestru (3.2+3.4)										150
3.6 Numărul de credite										6

4. Precondiţii (acolo unde este cazul)

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

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență la laborator obligatorie 100% pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	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 informatice • 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 • 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 • 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 C4. Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • 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 • 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 • 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 • 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 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 inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • 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 • 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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	1. Înțelegerea arhitecturii x86-64 la nivel structural și funcțional 2. Înțelegerea diferitelor mecanisme de securitate oferite de arhitectura x86-64 precum și a modului lor de folosire în cadrul unui sistem de operare 3. Cunoașterea diferitelor componente de nivel jos ale unui sistem de operare; înțelegerea rolului și funcționalității acestora precum și a relațiilor dintre ele. 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. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Recapitularea arhitecturii x86 și a limbajului de asamblare x86 pe 32 de biți. Utilitare de dezvoltare și depanare	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
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	2		
Arhitectura x86-64. Regiștrii, contextul de execuție, modelul de memorie, modul long (1)	2		
Arhitectura x86-64. Regiștrii, contextul de execuție, modelul de memorie, modul long (2)	2		
Întreruperi și excepții	2		
Programarea dispozitivelor hardware (tastatură, ceasuri, disk)	2		
Sisteme multi-procesor si primitive de sincronizare pe platforma x64	2		
Mecanisme hardware pe platforma x64 pentru implementarea de procese, thread-uri și schimbare de context (*context switching*)	2		
Mecanisme hardware pe platforma x64 pentru implementarea elementelor de bază din managementul memoriei (fizice și virtuale)	2		
Bus-ul PCI/PCI Express. Plăci de extensie PCI și identificarea resurselor din sistem	2		
Mecanisme de securitate în procesoarele și platforma x64	2		
Modelul de execuție SSE și AVX. Optimizarea subrutinelor în limbaj de asamblare	2		
Modelul de execuție SSE și AVX. Optimizarea subrutinelor în programe C	2		
Recapitulare	2		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziția studenților într-un număr de exemplare corespunzător)*

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/).

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Exerciții de recapitulare pentru programarea în limbajul de asamblare x86 pe 16 și 32 de biți	2	Expuneri la tablă, discuții, explicații suplimentare, coordonarea realizării exercițiilor de laborator	
Folosirea de proiecte mixte, compilate parțial în asamblare și parțial în C. Bootarea *MultiBoot* folosind *GRUB*, pre 32 biți mod protejat, fără paginare. Output pe ecran (*direct video memory write*) fără dependență de BIOS. Integrarea unor funcții tip *printf*	2		
Activarea paginării pe 32 biți. Trecerea în modul de operare pe 64 biți. Configurarea corectă a unor structuri de control procesor, spații de memorie și paginări inițiale de lucru pentru 64 biți	4		
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	2		
Programarea și tratarea timerelor. Programarea pentru keyboard și implementarea unui I/O interactiv (e.g. command interpreter)	2		
Citire PIO mode ATA. Implementarea unor comenzi de tip “dir”, “type” pe un volum *FAT32*	2		
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	4		
Treaduri SMP, context switching, scheduling. Salvarea contextului FPU/SSE. Mutex-uri	4		

Managementul memoriei: alocatori de memorie fizică, virtuală și heap. Sincronizarea lor. Testcase-uri, cazuri dificile	4		
Exemple de optimizare în SSE. Predarea exercițiilor de laborator	2		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)*

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/).

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi 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 oferii o experiență practică pentru înțelegerea multora dintre mecanismele de bază din spatele acestor atacuri.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere 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%
Seminar			
Laborator	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%
Proiect			

Standard minim de performanţă:
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

FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și 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 Informatiilor si Sistemelor de calcul/ Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	5.

2. Date despre disciplină

2.1 Denumirea disciplinei	***Activitate de cercetare 1***				
2.2 Titularii de curs	Nu e cazul				
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect	Nu e cazul				
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	V
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	14	din care:	Curs		Seminar		Laborator		Proiect	14
3.2 Număr de ore pe semestru	196	din care:	Curs		Seminar		Laborator		Proiect	196
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										25
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										
(d) Tutoriat										
(e) Examinări										4
(f) Alte activităţi:										

3.4 Total ore studiu individual (suma (3.3(a)…3.3(f)))	29
3.5 Total ore pe semestru (3.2+3.4)	225
3.6 Numărul de credite	9

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de competenţe	Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Nu este cazul
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Echipamente si programe specifice temei de proiect

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	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 informatice • 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 • 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 • 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 • 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 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 inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 - Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • 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 informatice • 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 • 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 • 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
6.2 Competenţe transversale	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

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Deprinderea de abilități și competente de cercetare, proiectare, dezvoltare și evaluare în domeniul securității informațiilor și sistemelor de calcul, calculatoarelor și al tehnologiei informațiilor.
7.2 Obiectivele specifice	1. Identificarea unei probleme concrete de securitate (la nivelul unei aplicații particulare sau la nivel general al unei strategii, mecanism, protocol etc.) 2. Elaborarea specificațiilor/cerințelor de rezolvare a problemei identificate 3. Elaborarea unei strategii de investigare și cercetare a problemei abordate și a unui plan de lucru 4. Cunoașterea stării actuale a domeniului problemei alese

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
-			
Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)* -			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
1. Stabilirea temei proiectului de disertație 2. Stabilirea principalelor direcții de investigat 3. Documentare asupra temei de disertație		Colaborare îndrumător - student	

4. Realizarea unei sinteze privind documentația bibliografică 5. Elaborarea unui raport tehnic de descriere a activității desfășurate și a sintezei bibliografice			
Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziţia studenţilor într-un număr de exemplare corespunzător)* Se stabilește de către fiecare îndrumător de proiect de disertație în parte.			

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

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

Se realizeaza prin întâlniri periodice cu reprezentanții mediului economic.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs			
Seminar			
Laborator			
Proiect	Pe baza cunoștințelor și rezultatelor obținute și a referatului elaborat	Evaluare orala Evaluare referat	60% 40%
Standard minim de performanţă: 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