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	06

2. Date despre disciplină

2.1	Denumirea disciplinei					Dezvoltarea și securitatea modulelor kernel					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Drd. Sándor LUKÁCS (slukacs@bitdefender.com)					
2.4	Titularul activităților de seminar / laborator / proiect					Drd. Sándor LUKÁCS (slukacs@bitdefender.com)					
2.5	Anul de studii	I	2.6	Semestrul	2	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/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/2	Dezvoltarea și securitatea modulelor kernel	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 si notițe	12
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	12
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	48
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	Sisteme de operare
4.2	De competențe	Programare C, Programare în limbaj de asamablare x86, Arhitectura calculatoarelor, 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

Competente profesionale	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 • C5.2 – 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 • 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
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Dobândirea de către studenți a unei bune înțelegeri generale a dezvoltării modulelor kernel (driver), în special sub SO Windows. Se urmărește însușirea unei experiențe practice și o familiarizare cu conceptele specifice, utilitarele și metodele de dezvoltare și depanare de bază, precum și înțelegerea diferențelor dintre dezvoltarea aplicațiilor și dezvoltarea modulelor kernel. Un accent particular se pune pe înțelegerea arhitecturii kernelului Windows și de funcționare a modulelor kernel din punct de vedere a implicațiilor de securitate.
7.2	Obiectivele specifice	Se urmărește înțelegerea și dobândirea abilității de manipulare și dezvoltare a: 1. arhitecturii generale a kernelului Windows, 2. diferitelor tipuri de module kernel, 3. metodelor de dezvoltare și depanare a modulelor kernel, 4. interacțiunii dintre modulele kernel și aplicații, 5. implicațiilor dpdv al securității a modulelor kernel, 6. posibilităților de a îmbunătății securitatea unui sistem de calcul folosind module kernel.

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Arhitectura Windows Kernel; Utilitare pentru dezvoltarea și depanarea modulelor kernel pentru Windows	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Depanarea modulelor kernel; Concepte fundamentale specifice dezvoltării modulelor kernel Windows, partea 1 și 2		
3			
4	Operații I/O sub Windows (I/O Manager, IRP processing); Managementul memoriei (Memory Manager), partea 1 și 2		
5			
6	Topic-uri specifice driverelor pentru filtrarea operațiilor kernel (Operații registry, file-system, procese etc.), partea 1 și 2		
7			
8	Întreruperi și excepții (Interrupts, APCs, DPCs)		
9	Modelele de drivere tip KMDF / UMDF		
10	Programarea driverelor USB		
11	Dezvoltarea driverelor de filtrare rețea. Platforma WFP		
12	Securitatea modulelor Kernel în Windows		
13	Analiza structurilor interne specifice kernel-ului Windows		
14	Recapitulare		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Familiarizarea cu utilitarele de dezvoltare și depanare	Expuneri la tablă, discuții, explicații suplimentare, coordonarea realizării exercițiilor de laborator	
2	Dezvoltarea unui driver NT Legacy, a unui DLL user-mode și a unei aplicații de control tip command-line – partea 1 și 2		
3			
4	Dezvoltarea unui driver tip anti-virus – studierea exemplelor de drivere minifilter din WDK. Dezvoltarea modulului inițial și a utilitarului de control și test tip command-line		
5	Dezvoltarea unui driver tip anti-virus – filtrări de operații file system		
6	Dezvoltarea unui driver tip anti-virus – filtrări de operații registry		
7	Dezvoltarea unui driver tip anti-virus – interceptarea și filtrarea unor alte operații (e.g. notificări de pornire procese, operații cu handel-uri de procese)		
8	Dezvoltarea pe parcursul a mai multor laboratoare a unor drivere Windows diverse, din mai multe teme posibile: • drivere de filtrare USB, • drivere de filtrare, emulare sau criptare storage, • drivere anti-rootkit (identificarea proceselor și a fișierelor ascunse, invizibile din Windows Explorer / Task Manager), • drivere de filtrare rețea (WFP).		
9			
10			
11			
12			
13	Prezentarea și evaluarea soluțiilor temelor de laborator și a activităților de laborator		
14			

Bibliografie

1. Windows Internals (Russinovich, Mark – 2012 – Microsoft Press) (6th ed)
2. Windows NT File System Internals (Nagar, Rajeev – 2006 – OSR Reprint)
3. Windows Driver Kit (WDK) (Microsoft – 2010-2014 – electronic)
4. Windows Operating System Internals Curriculum Resource Kit (CRK) (Microsoft – 2006 – electronic)
5. Windows Research Kernel 1.2 (Microsoft – 2006 – electronic)

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.

Cunoașterea bună a arhitecturii Windows Kernel este esențială pentru înțelegerea corespunzătoare a multor tehnici de atac și vulnerabilități relevante în ultimii ani. Cunoașterea dezvoltării driverelor este esențială pentru a putea înțelege arhitectura, funcționarea și limitările multor soluții de securitate pe larg folosite astăzi (cum ar fi soluții de securitate tip anti-virus sau firewall).

Cursuri de driver development sunt prezente în relativ puține alte universități, exemple fiind:

- *ECE 446 – Device Driver Development*, George Mason University, Fairfax, USA

http://catalog.gmu.edu/preview_course_nopop.php?catoid=19&coid=226124
- *COP 5641 – Linux Kernel & Device Driver Programming,* Florida State University, USA http://www.cs.uni.edu/~diesburg/courses/dd/syllabus.html

O parte din detaliile cursului sunt prezentate în alte facultăți în cadrul cursurilor de Sisteme de Operare.

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 (e.g. în cadrul examenului, în cadrul interacțiunii de laborator) înțelegerii noțiunilor de bază specifice arhitecturii Windows kernel, a modulelor / driverelor kernel, și a dezvoltării driverelor kernel sub Windows. Dezvoltarea unui driver Windows de tip anti-virus și înțelegerea funcționării lui.						

Responsabil curs
Drd. Sándor Lukacs

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	07

2. Date despre disciplină

2.1	Denumirea disciplinei					Auditul sistemelor informatice și managementul riscurilor de securitate					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Drd.ing. Dan LUȚAȘ (dlutas@bitdefender.com)					
2.4	Titularul activităților de seminar					Drd.ing. Dan LUȚAȘ (dlutas@bitdefender.com)					
2.5	Anul de studii	I	2.6	Semestrul	2	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/2	Auditul sistemelor informatice și managementul riscurilor de securitate	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

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	48
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	18
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	20
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	Securitatea informațiilor
4.2	De competențe	Arhitecturi de calculatoare, Sisteme 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 orele de seminar obligatorie 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente 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 C3 Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • C3.1 – Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice • C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității • C3.3 – Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc. • C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Familiarizarea studenților cu noțiunile și elementele de bază ale activităților de audit și management de securitate a sistemelor informaționale și conferirea capacității de a înțelege procesul de audit al sistemelor informaționale, conform standardelor internaționale (ISACA)
7.2	Obiectivele specifice	1. Înțelegerea procesului de auditare a sistemelor informaționale, cu referire la standardele internaționale (ISACA) 2. Înțelegerea procesului de guvernare și management IT, împreună cu activitatea de audit al guvernării și managementului IT 3. Înțelegerea proceselor de achiziție, dezvoltare și implementare a sistemelor informaționale, împreună cu activitatea de audit al acestor procese 4. Înțelegerea proceselor de operare, întreținere și suport a sistemelor informaționale, asigurarea continuității afacerii și planurilor de recuperare în caz de dezastru, împreună cu

		activitatea de audit al acestor procese 5. Înțelegerea procesului de asigurare a protecției sistemelor informaționale (managementul securității sistemelor informaționale, controlul accesului, securitatea infrastructurii de rețea, securitatea fizică), împreună cu activitatea de audit aferentă

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Introducere în managementul securității și auditul sistemelor Informatice	Expunere la tablă, prezentare cu video-proiectorul, discuții	
2	Guvernarea IT (roluri și responsabilități, strategii de securitate, politici, standarde și proceduri, metrici de guvernare)		
3	Auditul guvernării IT		
4	Managementul riscului (evaluarea riscului - evaluarea vulnerabilităților, evaluarea amenințărilor, analiză, monitorizare) și auditul managementului riscului		
5	Planificarea continuității afacerii și recuperarea după dezastru (audit și administrare - analiza Impactului, RPO/RTI, copii de siguranță)		
6	Tratarea incidentelor (proceduri de răspuns la incidente, dezvoltarea unui plan de răspuns la incidente, testarea răspunsului la incidente/BCP/DRP)		
7	Managementul proiectelor software: ciclul de viață a dezvoltării software, fazele de certificare și acreditare, sisteme de aplicații business (comerț electronic, schimbul electronic de date, aplicații bancare, transfer electronic de fonduri)		
8	Auditul managementului de proiect		
9	Operațiuni de securitate informațională (administrarea patch-urilor, administrarea configurațiilor) și întreținere, audit (sisteme de operare, infrastructură de rețea)		
10	Administrarea securității informaționale (framework-uri, audit), acces logic (controlul accesului software, identificare, autorizare), acces fizic și audit		
11	Securitatea infrastructurii de rețea (LAN, WAN, Wireless, Firewall, IDS, IPS, VoIP, PBX, testarea vulnerabilităților de rețea)		
12	Auditul infrastructurii de rețea (a componentelor prezentate în cursul 11)		
13	Managementul securității informației (guvernare, managementul riscului, dezvoltarea și gestionarea unui program de securitate a informației)		
14	Prezentare de sinteză a subiectelor studiate, evidențierea concluziilor esențiale, discuții si prezentări pe subiecte propuse de studenți		
8.2. Aplicații (seminar)		Metode de predare	Observații
1	Importanța securității & auditului sistemelor informatice	Expuneri la tablă, explicații suplimentare, discuții	
2	Management-ul riscului. Recuperarea după dezastru: tehnici și principii		
3	Importanța patch-urilor de securitate. Securitate de rețea		
4	Analiza unor rapoarte tehnice și articole recente: vulnerabilități în sistemele de operare		
5	Analiza unor rapoarte tehnice și articole recente: vulnerabilități în infrastructura de rețea		
6	Analiza unor rapoarte tehnice și articole recente: vulnerabilități în aplicații		
7	Analiza unor rapoarte tehnice și articole recente: atacuri avansate		

Bibliografie

1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)
2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)

3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)
4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll, Douglas – 2011 – CRC Press) (2nd ed)
5. Diferite articole

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 audit și security risk management sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- IT&C Audit – IT&C Security Master Program - THE BUCHAREST ACADEMY OF ECONOMIC STUDIES, http://ism.ase.ro/files/Curriculum/Y2012-2014/analytical-programs/en/S4/ISM_PA_EN_024.pdf
- Information Technology Auditing - Master of Science in Information Systems Audit and Control – Georgia State University, http://cis.robinson.gsu.edu/academic-programs/ms-is-audit/curriculum/
- Audit & Security - Information Security and Audit, MSc – University of Greenwich http://www2.gre.ac.uk/study/courses/pg/inftec/isa/cms-courses?banner=COMP1431&cyear=1415

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		60%
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		40%

10.4 Standard minim de performanță

Capacitatea de a defini și explica în context noțiunile de bază a activităților de audit al sistemelor informaționale și management al securității sistemelor informaționale, cum ar fi : procesul de audit, procesul de guvernare și management IT, procesele de achiziție, dezvoltare, implementare, operare, întreținere, suport și asigurare a protecției sistemelor informaționale, împreună cu mecanismele de audit specifice fiecărui proces.

Responsabil curs
Drd. Ing. Dan Luţaş

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	08

2. Date despre disciplină

2.1	Denumirea disciplinei					Securitate Web					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					s.l.dr.ing. Teodor ȘTEFĂNUȚ (teodor.stefanut@cs.utcluj.ro)					
2.4	Titularul activităților de laborator					Drd.ing. Vlad Ioan TOPAN (itopan@bitdefender.com)					
2.5	Anul de studii	I	2.6	Semestrul	2	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DA/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/2	Securitate Web	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

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	16
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	16
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	54
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	Probleme de securitate la nivel de cod sursă
4.2	De competențe	Programare web, Baze de date, 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 la laborator obligatorie 100% pentru admiterea la examenul final

6. Competențe specifice acumulate

Competente 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 C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • C3.1 – Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice • C3.2 – Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității • C3.3 – Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei rețele, sistem de calcul sau aplicații software, fără să existe informații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc. • C3.4 – Evaluarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabilităților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție • C3.5 – Propunerea unor noi metode de clasificare, identificare sau analiză pentru vulnerabilitățile și configurările greșite de sisteme. Crearea unor soluții și utilitare software care să identifice și analizeze astfel de cazuri 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 • C4.4 – 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
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Înțelegerea vulnerabilităților comune prezente în aplicațiile Web, a modului în care acestea pot fi exploatate cu intenții malițioase și a tehnicilor de dezvoltare, instalare și configurare a aplicațiilor Web securizate
7.2	Obiectivele specifice	1. Înțelegerea modului de funcționare a aplicațiilor Web 2. Dezvoltarea abilității de a identifica vulnerabilități în implementarea

		aplicațiilor Web 3. Înțelegerea tehnicilor de exploatare a vulnerabilităților aplicațiilor Web (XSS, SQL injection etc.) 4. Dezvoltarea aptitudinilor de scriere de cod securizat pentru aplicațiile Web 5. Dezvoltarea aptitudinilor de configurarea corectă a aplicațiilor Web, din perspectiva securității

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Obs.
1	Privire de ansamblu asupra tehnologiilor Web (1): concepte generale (clienți/servere, web 2.0, DOM etc.), arhitectura aplicațiilor web (frontend/middleware/backed)	Expunere la tablă, prezentare cu videoproiectorul, discuții	
2	Privire de ansamblu asupra tehnologiilor Web (2): protocoale (stiva ISO-OSI, HTTP, FTO, TCP, SOAP etc.) și limbaje (HTML, CSS, SVG, JS, XML, JSON, PHP, Python, Ruby etc.)		
3	Securitatea Web (1): autentificare (identitate), autorizare, criptare și legislație în domeniu		
4	Securitatea Web (2): confidențialitate, integritate și disponibilitate, nivelul rețea (firewalls, IPS)		
5	Securitatea serverelor (1): vulnerabilități și atacuri (OWASP, atacuri prin injecții SQL/hijack de sesiune/SSL/referințe directe de obiecte/etc.)		
6	Securitatea serverelor (2): asigurarea disponibilității (atacul (D)DoS) și configurarea corectă		
7	Securitatea clienților (browser-e Web) (1): vulnerabilități (browser, pluginuri Flash/Java/etc., cookies, DNS, clickjacking)		
8	Securitatea clienților (browser-e Web) (2): configurare, sandboxing, scripturi utilizator, malware/spyware		
9	Criptografie pentru Web: concepte generale, chei publice/private, certificate, integritatea mesajelor, protocoale (SSL, HTTPS etc.)		
10	Măsuri proactive de securitate: detectarea intruziunilor în aplicații web, gestionarea de incidente, honeytokens		
11	Securitatea pentru Web 2.0: paradigma AJAX, cloud computing etc.		
12	Programare sigură pentru Web (1): validarea intrărilor/sanitizarea erorilor, identitatea, controlul accesului, gestionarea sesiunilor		
13	Programare sigură pentru Web (2): gestionarea datelor cu sensibilitate mare, practici corecte de programare		
14	Prezentare de sinteză a subiectelor studiate, evidențierea concluziilor importante, discutarea unor subiecte propuse de studenți		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Obs.
1	Dezvoltarea unei aplicații minimale Web (frontend/middleware/backend)	Expunere la tablă, explicații suplimentare, discuții, exerciții de laborator	
2	Analiza de pachete de rețea în protocoale Web, implementarea / configurarea unui firewall		
3	Analiza atacurilor Web: OWASP, vulnerabilități de sesiune, injecții SQL		
4	Analiza atacurilor Web: XSS, CSRF, referințe directe nesecurizate, SSL		
5	Analiza și exploatarea de vulnerabilități în browser-ele Web: JavaScript, traversare de path-uri si în plugin-uri de browser-e Web (Flash, Java etc.)		
6	Programare sigură: validarea intrărilor, evitarea expunerii publice a detaliilor cazurilor de eroare, tratarea datelor sensibile, practici corecte etc.		
7	Utilizarea instrumentelor de validare a site-urilor Web: scannere de vulnerabilități cunoscute si fuzzere		

Bibliografie

1. 24 Deadly Sins of Software Security (Howard, Michael – 2010 – McGraw-Hill)
2. Web Penetration Testing with Kali Linux (Muniz, Joseph – 2013 – Packt Publishing)
3. Hacking Exposed: Web Application (Scambray, Joel – 2010 – McGraw-Hill) (3rd ed)
4. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (Stuttard, Dafydd – 2011 – Wiley) (2nd ed)
5. The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration

Testing Made Easy (Engebretson, Patrick – 2013 – Sygress)
6. Web Security Testing Cookbook (Hope, Paco – 2008 – O'Reilly Media)
7. Diferite articole și site-uri Web

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 securitate web sunt prezente în cadrul multor alte masterate din domeniul securității calculatoarelor și a informațiilor, cum ar fi:

- XACS241 - Web Security 2.0 (Stanford) – http://scpd.stanford.edu/search/publicCourseSearchDetails.do?method=load&courseId=1284858
- 06-20009 Network Security (University of Birmingham) – http://www.cs.bham.ac.uk/internal/modules/2010/20009/
- Internet and Security (Nottingham University) – http://targetpostgrad.com/course/31312-internet-and-security
- Master of Science in Cybersecurity (University of Maryland) – http://www.umuc.edu/academic-programs/masters-degrees/cybersecurity.cfm
- Applied Cyber Security (MIT) – http://web.mit.edu/professional/short-programs/courses/applied_cyber_security.html

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

Capacitatea de a defini și explica conceptele elementare de securitate a aplicațiilor Web (SQL injection, XSS, CSRF, configurare) și a riscurilor la care sunt expuse datele și aplicațiile publicate pe Web.
Capacitatea de a identifica vulnerabilități de bază (SQL injection, XSS, CSRF, de configurare) în codul sursă al aplicațiilor web.
Capacitatea de a scrie cod securizat pentru aplicații Web de complexitate mică.

Responsabil curs
Ş.l.dr.ing. Teodor Ştefănuţ

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	09.1

2. Date despre disciplină

2.1	Denumirea disciplinei					Sisteme de date masive și securitatea calculatoarelor					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					S.l.dr.ing. Camelia LEMNARU (camelia.lemnaru@cs.utcluj.ro)					
2.4	Titularul activităților de seminar / laborator / proiect					Drd.ing. Ciprian OPRIȘA (coprisa@bitdefender.com)					
2.5	Anul de studii	I	2.6	Semestrul	2	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/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/2	Sisteme de date masive și securitatea calculatoarelor	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

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	32
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	18
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	48
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	Baze de date
4.2	De competențe	Statistică și probabilități

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

Competente 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 • C2.3 – 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 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 • C5.5 – 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
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Dobândirea deprinderii de a lucra cu colecții masive de date. Ținând cont că numărul de programe malițioase este în continuă creștere, se dorește ca studenții să fie capabili să le gestioneze, clasifice și să găsească noi modele pentru detecția acestora.
7.2	Obiectivele specifice	• Dobândirea abilității de a utiliza limbaje de scripting și baze de date pentru a manipula colecții masive de date • Înțelegerea paradigmei Map-Reduce și abilitatea de a proiecta și implementa sisteme distribuite • Cunoașterea unor algoritmi și tehnici pentru căutarea datelor în colecții masive • Deprinderea unor modele pentru clasificarea și învățarea

		automată a regulilor de detecție a programelor malițioase

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Introducere în limbaje de scripting: limbajul Python	Expunere la tablă, prezentare cu videoproiectorul, discuții	
2	Procesarea datelor în Python		
3	Baze de date relaționale și nerelaționale: proprietățile ACID, algebra relațională, teorema CAP		
4	Paradigma Map-Reduce		
5	Analiza complexității algoritmilor Map-Reduce		
6	Tehnici simple de căutare în colecții masive: indexare, hashing		
7	Tehnici avansate de căutare în colecții masive:căutarea elementelor similare, identificarea similarităților între programe		
8	Tehnici avansate de căutare în colecții masive: reversed index, locality-sensitive hashing		
9	Analiza link-urilor: algoritmul PageRank, tehnici de SEO		
10	Tehnici de clustering: K-means, clustering ierarhic		
11	Tehnici avansate de clustering penru colecții masive		
12	Construcția de modele pentru predicții: regresie liniară, regresie logistică, arbori de decizie		
13	Clasificatori avansați: perceptronul, Support Vector Machines		
14	Reducerea dimensionalității		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Introducere în limbajul Python	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	Structuri de date în Python		
3	Biblioteci de funcții specifice pentru operarea cu colectii de date		
4	Extragerea de trăsături pentru identificarea programelor potențial malițioase		
5	Stocarea și accesarea colecțiilor de date: baze de date, utilizarea indecșilor		
6	Algoritmi de tip Map-Reduce pentru procesarea colecțiilor de fișiere potențial malițioase		
7	Calculul similarității între programe		
8	Construcția unui reversed index, folosind tehnica Map-Reduce		
9	Regăsirea aplicațiilor similare în colecții masive: locality-sensitive hashing		
10	Tehnici de clustering pentru identificarea familiilor de malware, partea 1		
11	Tehnici de clustering pentru identificarea familiilor de malware, partea 2		
12	Clasificatori pentru malware și spam, partea 1		
13	Clasificatori pentru malware și spam, partea 2		
14	Evaluare și verificare		

Bibliografie

1. Mining of Massive Datasets (Rajarman, Anand – 2011 – Cambridge)
2. Pattern Recognition and Machine Learning (Bishop, Christopher – 2007 – Springer)
3. MongoDB: The Definitive Guide (Chodorow, Kristina – 2013 – O'Reilly) (2nd ed)
4. Data Science for Business: What you need to know about data mining and data-analytic thinking (Provost, Foster – 2013 – O'Reilly)
5. Learning Python (Lutz, Mark – 2013 – O'Reilly) (5th ed)
6. Diferite articole

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 cu topic-uri legate de big data sunt prezente în cadrul multor alte masterate, însă puține dintre ele se focalizează și pe domeniul securității calculatoarelor și a informațiilor. Oricum, atât clasificarea

software-ului malițios, cât și a spam-urilor reprezintă în practică colecții masive de date, a căror prelucrare necesită metode de învățare automată și prelucrare a datelor massive. Exemple ar fi:

- *Big Data*, Masters in Computer and Information Security, University of Liverpool, UK http://www.liv.ac.uk/study/online/programmes/information-technology/msc-computer-and-information-security/module-details/
- *Big Data Management and Security*, Graduate Certificate Program, Missouri University of Science and Technology, USA, http://dce.mst.edu/credit/certificates/bigdatamanagementandsecurity/
- CS246, *Mining Massive Data Sets*, Stanford, http://web.stanford.edu/class/cs246/
  CSE 599, *Machine Learning for Big Data*, Computer Science & Engineering, University of Washington

Există numeroase alte programe de masterat care se specializează pe big data și business analytics, care predau metode și tehnici care se pot aplica cu succes și în cadrul analizei datelor de securitate.

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		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						
La finalul cursului, studenții trebuie să fie capabili să manipuleze colecții mari de date, atât nestructurate cât și structurate în baze de date, folosind algoritmi secvențial și distribuiți, de tip Map-Reduce. Principalele operații pe care studenții trebuie să demonstreze că le-au deprins sunt căutarea în colecții masive, clasificarea și clusterizarea elementelor, respectiv construirea de modele predictive.						

Responsabil curs
Ş.l.dr.ing. Camelia Lemnaru

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	09.2

2. Date despre disciplină

2.1	Denumirea disciplinei					Sisteme de securitate bazate pe hardware și virtualizare					
2.2	Aria tematica (subject area)					Calculatoare și Tehnologia Informației					
2.3	Responsabil de curs					Ș.l.dr.ing. Adrian COLEȘA (adrian.colesa@cs.utcluj.ro)					
2.4	Titularul activităților de laborator					Ș.l.dr.ing. Adrian COLEȘA (adrian.colesa@cs.utcluj.ro)					
2.5	Anul de studii	I	2.6	Semestrul	2	2.7	Evaluarea	examen	2.8	Regimul disciplinei	DS/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/2	Sisteme de securitate bazate pe hardware și virtualizare	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

Studiul individual	**Ore**
Studiul după manual, suport de curs, bibliografie si notițe	24
Documentara suplimentara in biblioteca, pe platformele electronice si pe teren	12
Pregătire seminarii / laboratoare, teme, referate, portofolii, eseuri	62
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	Programarea calculatoarelor, Programare în limbaj de asamblare, Sisteme de operare, Arhitectura calculatoarelor, Securitatea informațiilor
4.2	De competențe	Programare în C și limbaj de asamblare x86, cunoașterea funcționalității unui SO, cunoașe terea conceptelor fundamentale referitoare la securitatea sistemelor și informației

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

Competente 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 • C2.4 – 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 • C4.1 – 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 • C5.2 – 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
Competențe transversale	N/A

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

7.1	Obiectivul general al disciplinei	Cunoașterea modalităților prin care diferite tehnologii hardware moderne (de platformă, de procesor etc.), în general, și cele de virtualizare, în particular, pot fi folosite pentru îmbunătățirea securității sistemelor și informației.
7.2	Obiectivele specifice	1. Înțelegerea principalelor funcționalități hardware oferite de arhitectura x86 pentru securitatea aplicațiilor și informației 2. Înțelegerea principalelor funcționalități hardware oferite de arhitectura x86 pentru virtualizare 3. Capacitatea de dezvoltare a unui mini-hipervizor utilizând funcționalitățile hardware de virtualizare ale arhitecturii x86 4. Cunoașterea principalelor tehnici de utilizare a virtualizării pentru asigurarea securității aplicațiilor și informației

		5. Capacitatea de implementare și de evaluare critică (context, avantaje, dezavantaje) a metodelor sus amintite

8. Conținuturi

8.1. Curs (programa analitică)		Metode de predare	Observații
1	Conceptele fundamentale ale virtualizării și principalele tehnici de implementare	Expunere la tablă, prezentare cu videoproiectorul, discuții	
2	Funcționalitatea de bază oferită de arhitecturile hardware pentru virtualizare (ex. Intel VT-X)		
3	Funcționalitatea de virtualizare a memoriei oferită de arhitecturile hardware (ex. Intel EPT)		
4	Introspecția memoriei ca tehnică de securitate a sistemelor		
5	Metode de protecție a datelor și aplicațiilor folosind virtualizarea		
6	Metode de detecție a aplicațiilor și codului malițios folosind virtualizarea (lista proceselor ascunse, cod injectat etc.)		
7	Tehnici avansate folosite în introspecției memoriei: introspecția aplicațiilor utilizator, protejarea împotriva tehnicilor de remapare a memoriei virtuale, optimizări, tehnici de generare a codului de introspecție independent de SO din mașina virtuală, tehnici de generare automată a codului de introspecție		
8	Funcționalitatea de virtualizare a spațiului de adrese ale dispozitivelor I/O oferită de arhitecturile hardware (ex. Intel VT-d), și evitarea atacurilor de tip DMA		
9	Problema nivelurilor multiple de virtualizare (*nested virtualization*) și suportul hardware oferit în acest sens		
10	Tehnici de izolare și protecție a integrității aplicațiilor și datelor (ex. virtualizarea, Intel SGX)		
11	Tehnologii hardware pentru protecția sistemelor (1): Intel MPX, Intel Anti-Theft Technology, Intel IPT, etc.		
12	Tehnologii hardware pentru protecția calculatoarelor (2): funcționalitatea TPM-urilor, UEFI Secure Boot, etc.		
13	Funcționalitatea hardware de verificare și asigurare a integrității (ex. Intel TXT) și utilizarea în tehnicile de securitate bazate pe virtualizare		
14	Folosirea virtualizării și a funcționalității hardware de verificare a integrității datelor pentru asigurarea securității și integrității aplicațiilor client ce interacționează cu servicii ce gestionează date confidențiale.		
8.2. Aplicații (lucrări de laborator)		Metode de predare	Observații
1	Componente de bază ale unui mini-HV: încărcător, organizarea memoriei, unelte de depanare, suport pentru sisteme multiprocesor.	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	Pornirea unei MV de testare (1): setarea structurilor VCPU/PCPU și VMCS, trecerea cu toate procesoarele în VMXROOT		
3	Pornirea unei MV de testare (2): controlul MV, tratarea unor evenimente VMEXIT de test		
4	Pornirea unei MV Windows (1): tratare evenimente VMEXIT pentru pornire cod MBR		
5	Pornirea unei MV Windows (2): tratare evenimente VMEXIT pentru pornire cod MBR		
6	Pornirea unei MV Windows (3): injectare harta E820 modificată, redirectare INT 0x15		
7	Pornirea unei MV Windows (4): tratarea tuturor evenimentelor VMEXIT generate de pornirea SO din MV		
8	Izolarea și protecția memoriei folosind EPT (1): izolarea și protecția hipervizorului		
9	Izolarea și protecția memoriei folosind EPT (2): metode de protecție		
10	Introspecția (1): detecția proceselor ascunse folosind structuri de date din Windows		
11	Introspecția (2): protejarea diferitelor structuri de date din SO (spațiul kernel) și din aplicațiile utilizator (spațiul utilizator) in Windows		
12	Introspecția (3): tehnici de detecție/protecție independente de SO		

13	Protecția datelor cu Intel SGX, MPX		
14	Prezentări, demonstrații, discuții, evaluare		

Bibliografie

1. Intel, „*Intel 64 and IA-32 Architectures Software Developer's Manual*”, Volume 1-3, 2014, http://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf
2. B. Parno, J. McCune, A. Perrig, „*Bootstapping Trust in Modern Computers*”, Springer, 2011, http://research.microsoft.com/pubs/154093/bootstrappingtrustbook.pdf
3. Intel, „*Intel Trusted Execution Technology (TXT). Software Development Guide*”, 2014, http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html
4. D. Weinstein, „*Advanced x86: Virtualization with Intel VT-x*”, 2012, online: http://opensecuritytraining.info/AdvancedX86-VTX.html
5. A. Segall, „*Introduction To Trusted Computing*”, 2013, online: http://opensecuritytraining.info/IntroToTrustedComputing.html
6. Articole indicate pe parcurs. Vezi http://www.citeulike.org/group/18034 cu etichete precum: *virtualization*, *introspection*, *light-virtualization*, *trusted*, *hvs-course (to be added)*

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 specializare și de aprofundare a cunoștințelor, într-un domeniu care deocamdată, din câte știm noi, nu este prezent în curricula altor programe de master de securitatea informațiilor. Considerăm, însă, că înțelegerea practică a detaliilor legate de virtualizarea hardware, precum și dobândirea unei înțelegeri generale a diferitelor tehnologii hardware de creștere a securității prezente pe sistemele moderne este esențială. Peste 80% din noile servere x86 sunt servere virtualizate, iar tehnologiile de virtualizare sunt prezente deja nu numai pe servere și calculatoare portabile, dar chiar în unele tablete, telefoane mobile și sisteme industriale. Domeniul securității prin virtualizare a fost și este în continuare intens cercetat atât în zona academică, precum și în domeniul industrial în ultimii 10-15 ani.

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 nivelul unei arhitecturi hardware și de expunere a metodelor de asigurare a securității prin mecanisme hardware și virtualizare. 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

Curs: Cunoașterea și capacitatea de a explica principalele concepte de virtualizare și funcționalitatea de bază oferită de procesoarele Intel pentru securitate (SGX, MPX, TXT etc.) și virtualizare (VT-X). Cunoașterea și capacitatea de a explica tehnica de introspecție bazată pe virtualizare și o metodă de asigurare a securității bazată pe introspecție.
Aplicații: Extinderea mini-hipervizor-ului de laborator furnizat, astfel încât să pornească o mașină virtuală (MV) cu Windows, folosind funcționalitatea EPT și obținerea listei proceselor active din acea MV.

Responsabil curs
Ş.l.dr.ing. Adrian Coleşa

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	10

2. Date despre disciplina

2.1	Denumirea disciplinei					Activitate de cercetare 2					
2.2	Aria tematica (subject area)					Calculatoare si Tehnologia Informatiei					
2.3	Responsabil de curs					Nu e cazul					
2.4	Titularul activităţilor de proiect					Nu e cazul					
2.5	Anul de studii	I	2.6	Semestrul	2	2.7	Evaluarea	A/R	2.8	Regimul disciplinei	DS/OB

3. Timpul total estimat

An/ Sem	Denumirea disciplinei	Nr. sapt.	Curs	Aplicaţii			Curs	Aplicaţii			Stud. Ind.	TOTAL	Credit
			[ore/săpt.]				[ore/sem.]						
				S	L	P		S	L	P			
I/2	Activitate de cercetare 2	14		3				42			192	234	9

3.1	Numar de ore pe saptamina	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	60
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)	85

3.7	Total ore studiul individual	192
3.8	Total ore pe semestru	234
3.9	Numar de credite	9

4. Preconditii (acolo unde este cazul)

4.1	De curriculum	Activitatea de cercetare 1
4.2	De competente	Competentele disciplinei de mai sus

5. Conditii (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

Competente 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 C3 - Analiza și evaluarea proprietăților de securitate a unui sistem de calcul. Identificarea erorilor de configurare și a vulnerabilităților software • C3.1 - Cunoașterea teoretică și practică a diverselor scenarii de configurare sau mentenanță greșită a sistemelor de calcul, precum și a claselor de vulnerabilități software și atacuri informatice tipice • C3.2 - Analiza și înțelegerea unor protocoale de comunicare și module software noi, pentru identificarea unor vulnerabilități posibile. Utilizarea listelor dedicate, recunoscute în domeniu, de clase și tipuri de vulnerabilități și configurări greșite pentru analiza și validarea unui sistem informatic nou din punct de vedere al securității • C3.3 - Capacitatea de a analiza critic, din punctul de vedere al testării vulnerabilității, configurarea unei relețe, sistem de calcul sau aplicații software, fără să existe infor¬mații anterioare. Capacitatea de a identifica informații vizibile, servicii expuse etc. • C3.4 - Evauarea limitărilor teoretice și practice oferite de diverse metode și tehnologii de detectare a vulnerabili¬tăților și configurărilor greșite ale sistemelor de calcul. Determinarea unor corelări constructive între diverse metode de detecție • C3.5 - Propunerea unor noi metode de clasificare, identificare sau analiză pentru vulnerabilitățile și configurările greșite de sisteme. Crearea unor soluții și utilitare software care să identifice și analizeze astfel de cazuri 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 • C4.4 - 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
Competențe transversale	**N/A**

7. Obiectivele disciplinei (reiesind din grila competentelor specific acumulate)

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. Definirea obiectivelor activității de cercetare corespunzătoare temei lucrării de disertație 2. Cunoașterea exactă a soluțiilor existente pentru diverse aspecte ale problemei abordate 3. Stabilirea unor direcții concrete de cercetare 4. Propunerea unor posibile soluții viabile ale problemelor identificate

8. Continuturi

8.1. Curs (programa analitica)		Metode de predare	Observații
1	Nu e cazul.		
8.2. Aplicații (proiect)		Metode de predare	Observații
	1. Documentarea suplimentară asupra temei de disertație, realizarea unei clasificări pe principii critice a soluțiilor existente pentru diverse aspecte ale problemei abordate 2. Enunțarea unor ipoteze de lucru, posibile soluții și justificarea lor teoretică 3. Estimarea efortului necesar implementării și validării soluțiilor propuse 4. Stabilirea programului de cercetare teoretică și experimentală 5. Elaborarea schemei generale sau a arhitecturii sistemului ce urmează a fi dezvoltat 6. Proiectarea componentelor sistemului dezvoltat 7. Efectuarea de experimente, teste și verificări 8. Elaborarea unui raport tehnic de descriere a activităților derulate și a rezultatelor obținute	Colaborare îndrumător - student	
Bibliografie 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				
Aplicatii		Pe baza cunoștințelor și rezultatelor obținute și a referatului elaborat		Evaluare orala Evaluare referat		60% 40%
10.4 Standard minim de performanta						
Propunerea a cel puțin unei soluții, stabilirea planului de cercetare și lucru, elaborarea arhitecturii generale a sistemului, elaborarea raportului tehnic.						

Responsabil curs
Indrumătorii de disertaţie

Director departament
Prof.dr.ing. Rodica Potolea