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	6.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Dezvoltarea și securitatea modulelor kernel***	
2.2 Titularii de curs				Drd. Ing. Radu-Marian PORTASE (rportase@bitdefender.com)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Drd. Ing. Radu-Marian PORTASE (rportase@bitdefender.com)	
2.4 Anul de studiu	I	2.5 Semestrul	2	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 – facultative				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	4	din care:	Curs	1	Seminar		Laborator	3	Proiect	
3.2 Număr de ore pe semestru	56	din care:	Curs	14	Seminar		Laborator	42	Proiect	

3.3 Distribuţia fondului de timp (ore pe semestru) pentru:	
(a) Studiul după manual, suport de curs, bibliografie şi notiţe	12
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren	12
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri	43
(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	Sisteme de operare
4.2 de competenţe	Programare C, Programare în limbaj de asamablare x86, Arhitectura calculatoarelor, Arhitectura sistemelor de operare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Tabla, proiector, calculatoare
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Tabla, proiector, calculatoare

6. Competenţele specifice acumulate

6.1 Competenţe 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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 implicaților 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. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Arhitectura Windows Kernel; Utilitare pentru dezvoltarea și depanarea modulelor kernel pentru Windows	1	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Depanarea modulelor kernel; Concepte fundamentale specifice dezvoltării modulelor kernel Windows, partea 1 și 2	2		
Operații I/O sub Windows (I/O Manager, IRP processing);	2		

Managementul memoriei (Memory Manager), partea 1 și 2			
Topic-uri specifice driverelor pentru filtrarea operațiilor kernel (Operații registry, file-system, procese etc.), partea 1 și 2	2		
Întreruperi și excepții (Interrupts, APCs, DPCs)	1		
Modelele de drivere tip KMDF / UMDF	1		
Programarea driverelor USB	1		
Dezvoltarea driverelor de filtrare rețea. Platforma WFP	1		
Securitatea modulelor Kernel în Windows	1		
Analiza structurilor interne specifice kernel-ului Windows	1		
Recapitulare	1		

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. Windows Kernel Programming (Yosifovich, Pavel – 2019 - CreateSpace Independent Publishing Platform)
2. Windows Internals (Russinovich, Mark – 2012 – Microsoft Press) (6th ed)
3. Windows NT File System Internals (Nagar, Rajeev – 2006 – OSR Reprint)
4. Windows Driver Kit (WDK) (Microsoft – 2010-2014 – electronic)
5. Windows Operating System Internals Curriculum Resource Kit (CRK) (Microsoft – 2006 – electronic)
6. Windows Research Kernel 1.2 (Microsoft – 2006 – electronic)

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Familiarizarea cu utilitarele de dezvoltare și depanare	3	Expuneri la tablă, discuții, explicații suplimentare, coordonarea realizării exercițiilor de laborator	
Dezvoltarea unui driver NT Legacy, a unui DLL user-mode și a unei aplicații de control tip command-line – partea 1 și 2	6		
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	3		
Dezvoltarea unui driver tip anti-virus – filtrări de operații file system	3		
Dezvoltarea unui driver tip anti-virus – filtrări de operații registry	3		
Dezvoltarea unui driver tip anti-virus – interceptarea și filtrarea unor alte operații (e.g. notificări de pornire procese, operații cu handel-uri de procese)	3		
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).	15		
Prezentarea și evaluarea soluțiilor temelor de laborator și a activităților de laborator	6		

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. 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 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.

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	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 pe platforma Moodle și/sau prezentarea unei teme de cercetare din domeniul cursului. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	50%
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. In situații excepționale, care necesită desfășurarea activităților didactice de la distanță, examinarea poate avea loc online, de la distanță, folosind platformele Moodle și Teams.	50%

Standard minim de performanţă

***Curs*.** Prezența la **minim 50%** din orele de curs, pentru admiterea la examenul final. 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.

***Aplicații*.** Prezența la laborator **obligatorie 100%** (2 laboratoare se pot recupera în timpul semestrului, iar alte 2 în sesiunile de restanțe) pentru admiterea la examenul final. Dezvoltarea unui driver Windows de tip anti-virus și înțelegerea funcționării lui.

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Drd. Radu-Marian PORTASE	
	Aplicații	Drd. Radu-Marian PORTASE	

Data avizării în Consiliul Departamentului Calculatoare	Director Departament Prof.dr.ing. Rodica Potolea
Data aprobării în Consiliul Facultății de Automatică și Calculatoare	Decan Prof.dr.ing. Liviu Miclea