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 și iOS 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, permisiuni, ciclul de viață)	2		
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 desfășurat on-line și/sau on-site 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.			

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
	Curs	S.l.Dr.ing. Ciprian OPRIȘA	
	Aplicații	S.l.Dr.ing. Ciprian OPRIȘA	

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