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	9.2

2. Date despre disciplină

2.1 Denumirea disciplinei				***Sisteme de securitate bazate pe hardware şi virtualizare***	
2.2 Titularii de curs				Conf.dr.ing. Adrian COLEȘA (adrian.colesa@cs.utcluj.ro)	
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect				Conf.dr.ing. Adrian COLEȘA (adrian.colesa@cs.utcluj.ro)	
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*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

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										24
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										12
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										56
(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	Programarea calculatoarelor, Programare în limbaj de asamblare, Sisteme de operare, Arhitectura calculatoarelor, Securitatea informațiilor
4.2 de competenţe	Programare în C și limbaj de asamblare x86, cunoașterea funcționalității unui SO, cunoașe terea conceptelor fundamentale referitoare la securitatea sistemelor și informației

5. Condiţii (acolo unde este cazul)

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

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	C2 - Investigarea și analiza situațiilor de criminalitate informatică și a software-ului malițios prin metode avansate de tip inginerie inversă și monitorizare comportament • C2.1 – Cunoașterea aprofundată a clasificării, caracteristicilor și particularităților aferente diferitelor tipuri de atacuri informatice și softurilor malițioase • C2.2 – Analiza și înțelegerea a noi clase de software malițios, noi tehnici de

	atac, persistență, escaladarea privilegiilor etc., precum și compararea lor cu tehnicile cunoscute • C2.4 – 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
6.2 Competenţe transversale	N/A

7. Obiectivele disciplinei

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. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Conceptele fundamentale ale virtualizării și principalele tehnici de implementare	2	Expunere la tablă, prezentare cu video-proiectorul, discuții	
Funcționalitatea de bază oferită de arhitecturile hardware pentru virtualizare (ex. Intel VT-X)	2		
Funcționalitatea de virtualizare a memoriei oferită de arhitecturile hardware (ex. Intel EPT)	2		
Introspecția memoriei ca tehnică de securitate a sistemelor	2		
Metode de protecție a datelor și aplicațiilor folosind virtualizarea	2		
Metode de detecție a aplicațiilor și codului malițios folosind virtualizarea (lista proceselor ascunse, cod injectat etc.)	2		
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	2		
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	2		
Problema nivelurilor multiple de virtualizare (*nested virtualization*) și suportul hardware oferit în acest sens	2		
Tehnici de izolare și protecție a integrității aplicațiilor și datelor (ex. virtualizarea, Intel SGX)	2		
Tehnologii hardware pentru protecția sistemelor (1): Intel MPX, Intel Anti-Theft Technology, Intel IPT, etc.	2		
Tehnologii hardware pentru protecția calculatoarelor (2): funcționalitatea TPM-urilor, UEFI Secure Boot, etc.	2		
Funcționalitatea hardware de verificare și asigurare a integrității (ex. Intel TXT) și utilizarea în tehnicile de securitate bazate pe virtualizare	2		
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.	2		

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

1. 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)*

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Componente de bază ale unui mini-HV: încărcător, organizarea memoriei, unelte de depanare, suport pentru sisteme multiprocesor.	2	Scurte expuneri la tablă, tutoriale, ghiduri de lucru, demonstrații *live*,	
Pornirea unei MV de testare (1): setarea structurilor VCPU/PCPU și	2		

VMCS, trecerea cu toate procesoarele în VMXROOT		explicații suplimentare, discuții, propunerea spre rezolvare a unor probleme de diferite tipuri și grade de complexitate	
Pornirea unei MV de testare (2): controlul MV, tratarea unor evenimente VMEXIT de test	2		
Pornirea unei MV Windows (1): tratare evenimente VMEXIT pentru pornire cod MBR	2		
Pornirea unei MV Windows (2): tratare evenimente VMEXIT pentru pornire cod MBR	2		
Pornirea unei MV Windows (3): injectare harta E820 modificată, redirectare INT 0x15	2		
Pornirea unei MV Windows (4): tratarea tuturor evenimentelor VMEXIT generate de pornirea SO din MV	2		
Izolarea și protecția memoriei folosind EPT (1): izolarea și protecția hipervizorului	2		
Izolarea și protecția memoriei folosind EPT (2): metode de protecție	2		
Introspecția (1): detecția proceselor ascunse folosind structuri de date din Windows	2		
Introspecția (2): protejarea diferitelor structuri de date din SO (spațiul kernel) și din aplicațiile utilizator (spațiul utilizator) in Windows	2		
Introspecția (3): tehnici de detecție/protecție independente de SO	2		
Protecția datelor cu Intel SGX, MPX	2		
Prezentări, demonstrații, discuții, evaluare	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. 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 conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Se realizează prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Acest curs este unul de 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	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de definire a conceptelor specifice problemelor de securitate la nivelul unei arhitecturi hardware și de	Prezentarea unei teme de cercetare din domeniul cursului.	50%

	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 pe calculator, folosind platforme dedicate precum Moodle sau Teams, din subiectele prezentate la curs. În condiții excepționale (ex. izolare socială și activități didactice de la distanță impuse de guvern), examenul se poate da de la distanță.	
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. În cazul în care se va da și colocviu de laborator, acesta se va da pe calculator, folosind platforme dedicate precum Moodle sau Teams, din subiectele studiate la laborator. În condiții excepționale (ex. izolare socială și activități didactice de la distanță impuse de guvern), colocviul se poate da de la distanță	50%
Proiect	-	-	-

Standard minim de performanţă

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

Data completării:	**Titulari**	**Titlu Prenume NUME**	**Semnătura**
	Curs	Conf.dr.ing. Adrian COLEȘA	
	Aplicații	Conf.dr.ing. Adrian COLEȘA	

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