SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Masters
1.6 Program of study / Qualification	Cybersecurity Engineering / Masters
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	***Virtualization and Hardware-Based Security***			Subject code	**9.2**
2.2 Course responsible / lecturer	Dr. eng. Dan Lutas - dan.lutas@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Dr. eng. Dan Lutas - dan.lutas@cs.utcluj.ro				
2.4 Year of study	I	2.5 Semester	2	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DF – fundamental, DS – speciality, DC – complementary				DS
	Optionality: DOB – mandatory, DOP – optional (alternative), DFA – optional (free choice)				DOP

3. Estimated total time

3.1 Number of hours per week	4	of which:	Course	2	Seminars	-	Laboratory	2	Project	-
3.2 Number of hours per semester	56	of which:	Course	28	Seminars	-	Laboratory	28	Project	-
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										24
(b) Supplementary study in the library, online and in the field										12
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										56
(d) Tutoring										-
(e) Exams and tests										2
(f) Other activities:										-

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	94
3.5 Total hours per semester (3.2+3.4)	150
3.6 Number of credit points	6

4. Pre-requisites (where appropriate)

4.1 Curriculum	computer programming, data structure and algorithms, operating systems
4.2 Competence	C programming, basic knowledge of (x86) computer architecture, basic Web programming

5. Requirements (where appropriate)

5.1. For the course	blackboard, beamer, computers
5.2. For the applications	blackboard, beamer, computers

6. Specific competence

6.1 Professional competences	• manage system security • implement ICT security policies • perform ICT security testing • perform risk analysis • identify ICT security risks • ensure information privacy • execute ICT audits • ensure compliance with legal requirements • establish an ICT security prevention plan • monitor developments in field of expertise • keep up with the latest information systems solutions
6.2 Cross competences	• develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded

7. Expected Learning Outcomes

Knowledge	• ICT security standards • security engineering • cyber attack counter-measures • cyber security • information confidentiality • information security strategy • ICT encryption • cloud technologies • cloud security and compliance • cloud monitoring and reporting • attack vectors • operating systems • risk management • assessment of risks and threats
Skills	• analyse ICT systems • define security policies • define technical requirements • identify ICT security risks • identify ICT system weaknesses • keep up with the latest information systems solutions • manage IT security compliances • perform ICT security testing • perform risk analysis • implement ICT security policies • implement cloud security and compliance • manage ICT virtualisation environments • respond to incidents in cloud environments • collect cyber defence data • handle cybersecurity incidents • protect ICT devices • ensure information security • implement ICT risk management • manage systems • develop with cloud services

Responsibilities and autonomy	• develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	Have knowledge regarding the ways different modern hardware mechanisms, in particular hardware virtualization support, could be used for an improved security of computers and their software.
8.2 Specific objectives	1. Understand the main, security aimed, hardware mechanisms provided by the x86_64 architecture. 2. Understand the hardware virtualization support provided by the x86_64 architecture. 3. Be able to develop a mini-hypervisor using hardware virtualization support provided by the x86_64 architecture. 4. Have detailed knowledge regarding the different ways virtualization mechanisms could be used to improve the security of computers and their software. 5. Be able to asses and implement in a hypervisor different virtualization-based security mechanisms.

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Course Introduction. Context and Virtualization Fundamental Aspects	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	
Different Types of Virtualization. Hardware Support for Virtualization	2		
Memory Virtualization	2		
Virtual Machine Introspection (VMI). VMI Overview and Formalization	2		
Reducing the Semantic Gap of VMI by Using Guest OS Semantic Knowledge	2		
Reducing the Semantic Gap of VMI by Using Architectural Semantic Knowledge	2		
Reducing the Semantic Gap of VMI by Using Hardware Performance Counters and Virtualization Events	2		
Reducing the Semantic Gap of VMI by Using Guest Assisted Methods	2		
I/O Virtualization Mechanisms. Security Challenges and Solutions	2		
Trusted Computing. Protection of Security-Sensitive Applications by Using Separated Red-Green VMs	2		
Trusted Computing. Protection of Trusted (Parts of) Applications inside Untrusted OS	2		
Trusted Computing. System Integrity Checking and Attestation	2		
Trusted Computing. Providing Trusted I/O Paths	2		
Cloud Security	2		

Bibliography

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
   - Articole indicate pe parcurs. Vezi http://www.citeulike.org/group/18034 cu etichete precum: *virtualization*, *introspection*, *light-virtualization*, *trusted*, *hvs-course (to be added)*

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Introduction. Administrivia. Understand the architecture of the mini-hypervisor used during lab-related activity. Build the development environment. Configure, build, run and update the mini-HV development project.	2	Brief reviews, blackboard illustrations and explanations, tutorials, roadmaps, short live demos and guidance of code development, discussions, homework.	
Get familiar to tge mini-HV architecture and code structure. Logging mechanisms, dynamic memory allocation, linked lists, synchronization.	2		
Memory virtualization. EPT structure	2		
Memory virtualization. EPT-configured permission rights	2		
Booting a simplified virtual machine (VM). VM enters and exists (1)	2		
Booting a simplified virtual machine (VM). VM enters and exists (2)	2		
Handling a VMCALL from a VM	2		
Booting a Windows VM	2		
VM-HV inter-communication mechanisms	2		
Implement an in-guest agent to communicate to the HV and execute given commands. Get the running process list	2		
Get the in-guest running process list from the HV	2		
Hidden process detection	2		
Attack prevention using EPT-based protection	2		
Subject review, demos, discussions. Lab evaluation	2		

Bibliography

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
   - D. Weinstein, „*Advanced x86: Virtualization with Intel VT-x*", 2012, online: http://opensecuritytraining.info/AdvancedX86-VTX.html

10. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

It is performed by periodic talks with important cybsersecurity industry representatives.
We also take a look and keep in touch with good ideas and proposals of other academic institutions in our country and abroad that run cybersecurity related study programs or/and research projects.

11. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to define and explain concepts and methods specific to hardware-based security field. Attendance frequency, interest, and interactivity during lecture classes.	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of different subjects / paper in the course's field during semester time. *(summative assessment)* In exceptional cases, which	50%

		imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	
Laboratory	Capability and ability to give correct and functional solutions to problems specific to hardware-based security field. Attendance frequency, interest, and interactivity during lecture classes.	Evaluate lab activity. *(continuous assessment)* Evaluate lab assignments. *(continous assessment)* Evaluate solutions of problems given in a final lab exam. *(summative assessment)* In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	50%

Minimum standard of performance

***Lecture*.** Attending **minimum 50%** of lecture classes, to be allowed to take the final examination. Students must be able to define and explain the main concepts related to hardware virtualization support on Intel x86_64 architecture.
Minimum final grade must be 5 for the exam to be considered passed.

***Lab*.** Attending **all lab classes** (one lab could be recovered during the semester, and one more during re-examination sessions). Students must be able to extend the given min-HV functionality such as booting a Windows VM and get the list of running processes from the VM. This kind of assessment could happen in relation to assignments given during semester or subjects given during the final lab evaluation.
Minimum lab grade must be 5 for being allowed at final exam.

Date of filling in 29.04.2026	**Responsible**	**Title First name Last name**	**Signature**
	Course	Dr. eng. Dan LUTAS	
	Applications	Dr. eng. Dan LUTAS	

Date of approval in the department	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council	Dean, Prof.dr.eng. Vlad Mureșan