COURSE DESCRIPTION CARD - SYLLABUS

Course name
Malicious Software Analysis

Course

Field of study	Year/semester
Computer Science	2/3
Area of study (specialization)	Profile of study
Cybersecurity	general academic
Level of study	Course offered in
Second-cycle studies	English
Form of study	Requirements
full-time	compulsory

Number of hours

Lecture	Laboratory classes	Other (e.g. online)
15	30	
Tutorials	Projects/seminars	

Number of credit points

3

Lecturers

Responsible for the course/lecturer:
dr hab. inż. Piotr Zwierzykowski
Piotr.zwierzykowski@put.poznan.pl
tel: 61 665 39 03
Faculty of Computing and Telecommunications

Responsible for the course/lecturer:
mgr inż. Błażej Nowak
blazej.nowak@put.poznan.pl
tel: 61 665 39 20
Faculty of Computing and Telecommunications

Prerequisites

Student starting this course should have basic knowledge of computer networks, cryptographic algorithms and Windows and Linux operating systems. He should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of the team.

Course objective

Provide students with knowledge in the field of widely understood malware analysis, including methods and tools used for static and dynamic analysis of such software and elements of reverse engineering.

As part of the course, the selected methods of static and dynamic malware analysis and reverse engineering used for this purpose will be discussed. As part of the laboratory exercises, the student will get to know the tools to detect malware in practice

Course-related learning outcomes

Knowledge

Has a structured and theoretically founded general knowledge related to key issues in the field of malware analysis.

Has advanced detailed knowledge of selected issues in the field of broadly understood malware analysis as well as methods and tools used for static and dynamic analysis and reverse engineering.

Has knowledge about development trends and the most important cutting edge achievements in computer science and in the field of malware detection, static and dynamic analysis.

Has advanced and detailed knowledge of the processes occurring in systems used for dynamic malware analysis

Skills

Is able to obtain information on methods of malicious software analysis from literature, databases and other sources (both in Polish and English), integrate them, interpret and critically evaluate them, draw conclusions and formulate and fully justify opinions

Is able to plan and carry out experiments, including computer measurements and simulations, interpret the obtained results and draw conclusions and formulate and verify hypotheses related to malware analysis.

Can integrate knowledge from different areas of computer science (and if necessary also knowledge from other scientific disciplines) when formulating and solving engineering tasks related to the detection and analysis of malware.

Is able to assess the suitability and the possibility of using new ahardware and software solutions for solving engineering tasks consisting in building secure data transmission systems.

Social competences

Understands that in the field of ICT security, knowledge and skills quickly become obsolete.

Understands the importance of using the latest knowledge in the field of ICT security in solving research and practical problems.

Is aware of the need to develop professional achievements and comply with the rules of professional ethics

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired during the lecture is verified by an oral and / or written test.

Passing issues, on the basis of which questions are developed, are sent to students by e-mail using the university's e-mail system, or placed in a subject course in the university's distance learning system.

Oral and / or written test consists of 3 to 5 questions for which a descriptive answer is expected. Each answer to the question is rated on a scale of 0 to 5 points. Each question is scored equally. Passing threshold: 50% of points.

In the case of an oral test, students draw questions from a set of 30 questions. In the case of a written test, questions are asked by the teacher.

The skills acquired during the laboratory classes are verified on an ongoing basis. At each laboratory class, the correctness of the exercises is assessed on a scale from 2 to 5. The final grade is the average of the grades obtained from each laboratory session. The final grade is the average of the grades obtained from each laboratory session.

Programme content

Lecture topics:

- Introduction to Malware Analysis

- Classification of Malware

- Malware Analysis Methodology

- Malware Analysis Techniques

- Static Analysis of Malware

- Dynamic Analysis of Malware

- Reverse Engineering in Malware Analysis

- Identification and Extraction of Hidden Components

- Static and Dynamic Reversing

- Malware Functionalities and Persistence

- Malware Obfuscation Techniques

- Hunting Malware Using Memory Forensics

- Dependence of Malware from the Platform

- Malware Evasion Techniques

Laboratory topics:

Compatible with the lectures

Teaching methods

Informative lecture: multimedia presentation, illustrated with examples given on the board.

Laboratory exercises: practical exercises in groups, using test environments and tools.

Bibliography

Basic

D. Barker: Malware Analysis Techniques, Packt>, 2021

Additional

1. Alexey Kleymenov, Amr Thabet: Mastering Malware Analysis,Packt>, 2019

2. Reginald Wong: Mastering Reverse Engineering, Packet>, 2018

3. K.A. Monnappa: Learning Malware Analysis, Pack>, 2018

4. M. Skikorski, A. Honing: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press; 1st edition , 2012

5.O. Or-Meir, Nir Nissim, Yuval Elovici, and Lior Rokach: Dynamic Malware Analysis in the Modern Era—A State of the Art Survey, ACM Computing Surveys, Vol. 52 Issue 5, October 2019, Article No.: 88, pp 1–48, 10.1145.3329786

Breakdown of average student's workload

	Hours	ECTS
Total workload	75	3,0
Classes requiring direct contact with the teacher	45	1,5
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam) [1]	30	1,5

[1] delete or add other activities as appropriate