COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of Software Defined Networks

Course

Field of study
Computing

Year/semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

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

Number of credit points

3

Lecturers

Responsible for the course/lecturer:
dr hab. inż. Mariusz Żal

mariusz.zal@put.poznan.pl

tel: 61 665 39 26

Faculty of Computing and Telecommunications

Responsible for the course/lecturer:

Prerequisites

A student starting this course should have basic knowledge of computer networks, routing protocols, cybersecurity, and programing languages (such as C, C++, or Java). 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

Providing students with knowledge in the field of broadly understood security in Software Defined Networks (SDN) and Network Function Virtualization (NFV) as well as challenges facing network developers and administrators. Methods of attacks and threat detections based on the events analysis in SDN will be presented. To acquaint students with challenges facing to application, control and data planes. Protocol-independent Packet Processing Programming (P4) languages, portable NIC and portable

switch architectures will be presented in the context of creation and maintenance of secure SDN networks.

As part of the course, solutions improving security of SDN networks will be discussed. Moreover advanced security techniques, such as microsegmentation, moving target defense (MTD), and AI in SDN security will be presented. Students will be acquainted with a newest ITU-T and ETSI recommendations in the field of security in SDN networks.

Course-related learning outcomes

Knowledge

Has advanced and in-depth knowledge of selected issues in the field of Software Defined Networks, Network Function Virtualization and methods, tools and programming framework used in data collection, analysis, and detection of threat and attacks in SDN.

Has advanced detailed knowledge in the field of NFV security life cycle processes.

Has advanced detailed knowledge regarding the issues and strategies of security in SDN.

Has knowledge about development trends and strategies in the field of security in SDN and the most important cutting edge achievements in broadly understood SDN security.

Skills

Student is able to obtain information regarding SDN and NFV from literature, databases and other sources (both in Polish and English), integrate them, interpret and critically evaluate them

Is able to plan and carry out experiments, interpret the obtained results and draw conclusions and formulate and verify hypotheses related to simple research problems in the field of SDN and NFV security.

Can - when formulating and solving engineering tasks - integrate knowledge from different areas of computer science, including programming and computer networks, in order to build secure SDN networks and implementation of NFV that are resistant to different attacks.

Can assess the usefulness and the possibility of using new hardware and software solutions for solving engineering tasks consisting in building secure SDN networks and implements secure NFV.

Can communicate both in Polish and English using different techniques in a professional environment and in other environments, also using IT tools.

Is able to cooperate in a team responsible for ensuring the security of ICT systems.

Is able to define the directions of further learning in order to meet the challenges posed by people responsible for the security of ICT systems.

Social competences

Student understands that in the field of SDN and NFV security, knowledge and skills very quickly become obsolete.

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

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes are verified with a written or oral test. Test in written form consists 7-10 question (multichoice and open), which are scored in different ways (there are three or four groups of scores). Test in oral form contains 50-60 open questions divided into three or four score groups. Students draw one question from each group. In the oral form, for each question teacher can ask one additional question. Both, main and additional questions are scored, taking into account content range and understanding the issue. Minimum number of scores to pass the exam is equal to 50%.

Skills acquired as part of the laboratory are verified on an ongoing basis. At the end of each laboratory class, the correctness of configuration of network devices is assessed on a scale of 0 to 10 points. Minimum number of scores to pass the exam is equal to 50%.

The assessment levels (lecture and tutorials) are the following:

Number of scores	mark
<=50 %	2,0
51% - 60%	3,0
61% - 70%	3,5
71% - 80%	4,0
81% - 90%	4,5
91% - 100%	5,0

Programme content

1. The following topics will be discussed as part of the lecture:
- Software-Defined Networks: definition, architectures,
- SDN implementation – review
- Security analyses and potential attacks in SDN:
    - Application plane,
    - Control plane,
    - Data plane,
- SDN Security Threat Vectors
- Deep programmability – P4 security challenges
- Network Function Virtualization (NFV) – framework, implementations
- Security challenges in NFV: security classification and security lifecycle
- SDN and NFV security in industry: standards and recommendations
- Review of solutions to security issues in SDN:
    - Unauthorized access,
    - Malicious applications,
    - DoS
    - Configuration issues

- System level SDN security

• Advance techniques of security in SDN:
  - Microsegmentation
  - Moving target defense
  - Attack representation
  - Service function chaining
  - Intelligent SDN security

• Security-Defined Networks - future directions

2. Laboratory topics:
In line with the content of lectures.

Teaching methods

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

Laboratory exercises: practical exercises in groups using network devices and virtualized environment.

Bibliography

Basic

1. Khondoker, Rahamatullah (Ed.): SDN and NFV Security - Security Analysis of Software-Defined Networking and Network Function Virtualization; Springer International Publishing 2018.

2. Guy Pyjolle: Software Networks: Virtualization, SDN, 5G and Security, John Wiley & Sons, 2015

Additional

1. Shao Ying Zhu, Sandra Scott-Hayward, Ludovic Jacquin, Richard Hill: Guide to Security in SDN and NFV - Challenges, Opportunities, and Applications. Computer Communications and Networks, Springer 2017.

2. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody: Software-Defined Networking and Security - From Theory to Practice, CRC Press, 2021

Breakdown of average student's workload

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

[1] delete or add other activities as appropriate