# COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of network services [S2Teleinf2-STRC>BUs]

## Course

Field of study
Teleinformatics

Year/Semester
1/2

Area of study (specialization)
ICT networks and cloud solutions

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

## Number of hours

Lecture
14

Laboratory classes
24

Other (e.g. online)
0

Tutorials
0

Projects/seminars
0

## Number of credit points

3,00

## Coordinators

dr hab. inż. Piotr Zwierzykowski prof. PP
piotr.zwierzykowski@put.poznan.pl

mgr inż. Błażej Nowak
blazej.nowak@put.poznan.pl

## Lecturers

## Prerequisites

Basic networking knowledge: Students should have a basic knowledge of computer networks, including concepts such as IP addressing, routing, switching, network protocols, firewalls and network architecture. Knowledge of application development: Students should be familiar with the concepts and language(s) (e.g. Java, Python, C#, PHP, JavaScript) of web application development. Familiarity with at least one framework related to web application development will be a great advantage. Students should be well acquainted with the creation and use of relational databases. It is also required that the student knows the basics of the http / https protocol. Security basics: Students should have a basic understanding of general security principles and concepts, including authentication, encryption, access control and typical security threats.

## Course objective

The aim is to educate students on the basic concepts, principles and best practices related to network service security and application layer security. The subject aims to increase the participants' awareness of the potential risks, threats and vulnerabilities in these areas and to provide them with the knowledge to make informed decisions on security measures. By understanding the risks and vulnerabilities arising from the given solutions discussed in this subject, Students will learn effective strategies to mitigate risks and protect their networks and applications from unauthorised access, data breaches and other security incidents..

## Course-related learning outcomes

Knowledge:
1. Detailed knowledge of basic authentication processes such as OAuth and BasicAuth
2. Knowledge of the operation of basic encryption algorithms at the application layer
3. Knowledge of session management and storage of sensitive data
4. Knowledge of the principle of operation, effects and countermeasures of basic application layer attacks such as:
a. SQL injection
b. Cross site request forgery
c. Cross site scripting
d. DNS poisoning
e. WiFi SSID spoofing
f. Session hijacking
g. Brute force
5. knowledge of the architecture of standard web applications
6. knowledge of basic attacks, their effects and preventive measures of the network layer and data link such as:
a. ARP poisoning
b. WiFi SSID spoofing
c. IP spoofing
d. DDoS
e. ICMP flood
f. Routing table poisoning
g. Ping death
Has a broadened and deepened knowledge of [K2_W02]:
- modern data transmission and processing systems,
- devices included in data communications systems.
Knows and understands the algorithms used in ICT systems from the area of specialisation [K2_W05].
Has in-depth knowledge of information processing and security in data communication systems [K2_W08].

Skills:
1. Ability to develop simple web applications resistant to basic attacks
2. Ability to use encryption to secure data
3. Ability to design networks and use routing protocols while protecting against basic attacks
4. Ability to exploit application vulnerabilities to selected attacks
Be able to prepare detailed documentation of the results of an experiment, project or research task; be able to prepare a paper discussing these results [K2_U03].
Is able to use the known methods and mathematical models, modifying them if necessary, to carry out projects in the field of Information and Communication Technology [K2_U06].
Can propose improvements or alternatives to existing ICT design solutions and systems [K2_U09].
Is able to assess the usefulness and possibility of using new developments in techniques, design methods for the design and manufacture of ICT systems and systems containing solutions of an innovative nature [K2_U10].

Social competences:
Students know and understand the importance and impact of security vulnerabilities, understand that new attacks, vulnerability exploitation and defence against them is an ongoing process.
Is ready to recognise the importance of knowledge in solving cognitive and practical problems and to critically evaluate received content[K2_K01].

## Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The skills acquired in the laboratory classes are verified on the basis of a credit colloquium consisting of 5-10 tasks scored differently depending on their level of difficulty or on the basis of an elaborated project of a sample application or network. Credit threshold: 50+% of the points.
The knowledge acquired in the lecture is verified by a final colloquium held in the last lecture. Each colloquium consists of 10-15 questions (test and open), variously scored. Pass mark: 50+% marks. The credit issues on which the questions are based will be sent to students by e-mail using the university e-mail system or the eCourses platform.

## Programme content

The subject covers issues related to ensuring the security of network services. Security of web services presented mainly based on the security of web-based services.

## Course topics

Lectures:
1. introduction to web services security.
2. Discussion of standard web applications and the most common vulnerabilities.
3. Discussion of basic ways to exploit / protect against the most common vulnerabilities and web applications.
4. Discuss ways and practices related to session management and storage of sensitive data.
5. Discuss basic authentication methods.
6. Discussion of basic attacks, how to protect yourself and exploit vulnerabilities at the network and data link layer.
7. Colloquium.

Labs:
1. Introduction to web services security / organisational activities.
2. Creation of a sample web application without using the framework.
3. Creation of a sample web application using the framework.
4. Design and create databases related to the written applications.
5. Locate vulnerabilities in written applications.
6. Carry out attacks, using the vulnerabilities located, on your own applications.
7. Modification of written applications to protect against the attacks carried out at that time.
8 Securing and redundancy of sensitive data.
9. Use of basic encryption algorithms.
10. Creating a sample application using one of the standard authentication methods.
11. Conducting a man in the middle attack using WiFi SSID spoofing.
12. Carry out an ICMP flood attack on one of your applications/machines.
13. Conduct a brute force attack on a selected proprietary WiFi network.
14. Passing colloquium or discussion of projects.

## Teaching methods

Lecture: multimedia presentation, illustrated by examples given on the blackboard and practical demonstrations.
Laboratory exercises: practical exercises carried out alone or in groups using a computer.

## Bibliography

Basic:
1. Sekurak: Bezpieczeństwo aplikacji webowych, Sekurak, 2019, ISBN:10010302135.
2. A.Muller, M. Meucci: OWASP Testing Guide v4, OWASP, 2014.
3. W. Stallings: Network Security Essentials: Applications and Standards, Pearson, 2016.

Additional:
1. C. Sanders: Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, No Starch Press, 2011.
2. J. Wright, J. Cache: Hacking Exposed Wireless: Wireless Security Secrets & Solutions, McGraw Hill,

2015.
3. C. McNab: Network Security Assessment. Know Your Network, O'Reilly Media, 2016.
4. D. Stuttard, M. Pinto: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition, Wiley, 2011.

## Breakdown of average student's workload

| | Hours | ECTS |
|---|---|---|
| Total workload | 78 | 3,00 |
| Classes requiring direct contact with the teacher | 38 | 1,50 |
| Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation) | 40 | 1,50 |