



Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT

Department: INFORMATION TECHNOLOGIES

Professional Field: 5.3. COMMUNICATION AND COMPUTER TECHNIQUE

Specialty: CYBERSECURITY IN COMMUNICATION TECHNOLOGY

Educational-scientific degree: BACHELOR

LEARNING COURSE DESCRIPTION

1. Course title: *Anonymous communications (TOR networks)*

2. Course code: B.43.045.2

3. Type of the course: elective

4. Level: Bachelor

5. Number of credits: 6

6. Name of the lecturer: Assoc. Prof. Pavlinka Radoyska PhD

7. Course learning outcomes:

The aim of the course is to acquaint students with the challenges in building anonymous communications and the main approaches to their construction, as well as the types of attacks that crash this type of communications and the approaches to their prevention.

Students who have completed their studies in the discipline must acquire:

Basic knowledge of the theoretical foundations of building anonymous communications, the working principles of anonymous communications built through proxy servers, TOR networks and using the Invisible Internet Project (I2P), as well as modern trends in building anonymous communications.

Practical skills in using TOR browsers and other applications to implement anonymous communications.

Competencies: Choosing an approach to building anonymous communications; choosing, installing and configuring applications to build anonymous communications for solving specific practical tasks.

8. Teaching methods:

The material is presented in the form of theory, which is accompanied by examples from academic practice. Significant attention is given to discussions, examples and practical cases related to the subject of the lecture course. The lectures are conducted by introducing the students to the material provided in the curriculum. The lectures are illustrated with graphic and video material, which are presented through presentations with a multimedia projector. Practical exercises are conducted in the form of group assignments to explore various aspects of anonymous communications. Students do their studies and research as an extracurricular activity and report their results during the laboratory exercises. The obtained results are discussed.

9. Prerequisites:

Security Fundamentals and Information Security Standards, Programming Fundamentals, Operating Systems Fundamentals, Databases, Information and Technology Security Workshop, Networks and Protocols 1 and 2, Cryptography Fundamentals, Hacking Attacks and Tools.

10. Course contents:

The course examines the basic requirements for anonymous communications and different approaches for their realization. The principles of building anonymizers, MIX net, Onion routing, TOR network, Invisible Internet Project (I2P), anonymous e-mail (Remailers), ensuring anonymity in AD-HOC networks are represented. The types of threats and attacks aimed at revealing anonymity and approaches to overcome them are discussed.

11. Bibliography

Basic literature:

1. Grahm, K. J., Forss, T., & Pulkkis, G. (2014). Anonymous communication on the internet. Proceedings of Informing Science & IT Education Conference (InSITE) 2014 (pp. 103-120). Retrieved from <http://Proceedings.InformingScience.org/InSITE2014/InSITE14p103-120Grahm0483.pdf>
2. (PDF) Anonymous Communication on the Internet. Available from: https://www.researchgate.net/publication/320663877_Anonymous_Communication_on_the_Internet [accessed Feb 15 2023].
3. Bingdong Li, Esra Erdin, Mehmet Hadi Gunes, George Bebis, Todd Shipley, An Overview of Anonymity Technology Usage, Computer Communications, Volume 36, Issue 12, 1 July 2013, Pages 1269-1283, <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2f4702128959fcd838a41577fa442b1aa97cf6dc> [accessed Feb 15 2023].

4. Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula, Technical and Legal Overview of the Tor Anonymity Network, Tallin 2015, http://195.222.11.251/uploads/2018/10/TOR_Anonymity_Network.pdf [accessed Feb 15 2023].
5. Z. Ling, X. Fu, W. Jia, W. Yu, D. Xuan and J. Luo, "Novel Packet Size-Based Covert Channel Attacks against Anonymizer," in IEEE Transactions on Computers, vol. 62, no. 12, pp. 2411-2426, Dec. 2013, doi: 10.1109/TC.2012.
https://www.cs.ucf.edu/~xinwenfu/paper/Journals/13_TC_62_12_NovelPacketSizeBasedCovertChannelAttacksagainstAnonymizer.pdf [accessed Feb 15 2023].
6. T. Lu, Z. Du and Z. Jane Wang, "A Survey on Measuring Anonymity in Anonymous Communication Systems," in IEEE Access, vol. 7, pp. 70584-70609, 2019, doi: 10.1109/ACCESS.2019.2919322, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8723335> [accessed Feb 15 2023].
7. Huang, Z., Joshi, S.K., Aktas, D. et al. Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network. npj Quantum Inf 8, 25 (2022). <https://doi.org/10.1038/s41534-022-00535-1> [accessed Feb 15 2023].

Additional literature:

1. Anonymous Communication, <https://www.youtube.com/watch?v=OgGTJlgNewE> [accessed Feb 15 2023].
2. Скритият Интернет – Dark Net и Deep Web, <https://postvai.com/seo/dark-net-deep-web.html> [accessed Feb 15 2023].

12. Assessment methods and criteria:

An assessment of the discipline is formed on the basis of a point system, the maximum number of points that students can receive is 100. For each test, as well as for the group task, up to 100 points are awarded, and each of these components has the following weight in formation of the final grade:

- TEST 1 – 25%;
- TEST 2 – 25%;
- Presentation of personal participation in the group task - 50%.

13. Language of instruction: *Bulgarian/English*