Course title: INTERNET SECURITY

Lecturers	Full Prof. Miroslav Bača, Ph.D. Asst. Prof. Igor Tomičić, Ph.D.
Language of instruction	Croatian and English
Study level	Master
Study programme	Databases and Knowledge Bases
Semester	2nd (summer)
ECTS	4th (summer)
Goal	This course focuses on the acquisition of main informatics knowledge and skills which are necessary for working with Internet security and networked systems, especially in an environment which is networked on a daily basis, and the implementation of the knowledge and skills in everyday life. Students are acquainted with the most common failures, weaknesses, safety risks, precautions and means of protection, as well as the ways of gathering, processing, storing and comparing of related data and their usage in complete security systems. In addition, they learn about the latest accomplishments in Internet security. The course is structured in a way that provides a solid introduction into of the most important characteristics of Internet security. Nowadays it is impossible to imagine any kind of business activity without a computer network. Development of computer networks is limited by development and connections within the Internet, which is another assumption this course is based on. Internet security has implications on security of all computer networks, either existing on the Internet or connected to or through the Internet. Most of the companies know very little about flaws of the networks they are using, so education about it will be of great help in raising the level of knowledge and awareness of security in general. The course is targeted on the end user in a networked environment. It deals with principal threats, safety risks, weaknesses, precautions and protection of networked computers. The course is divided into lectures, seminars and exercises. The course objectives can be classified in four groups: 1. to introduce the students to failures in Internet security, 2. to explain failure development with a special focus on development of software, 3. to increase the level of ethics when using the Internet, 4. to introduce the students to legal assumptions and encourage them to think about these assumptions.
General and specific learning outcomes	
Content	**1. Introduction (2 hours)** Definitions of security and protection terms in the context of computer networks. Analysis of current status of computer security in Croatia and the world. Goals which are to be achieved by security aspects. Categories of people and actions which can threat Internet security. Current status of software for securing the safety of computer networks. Responsibilities and obligations of users. Threats identification and risk comprehension. **2. Computer networks (2 hours)** Computer networks in general. Kinds and types of computer networks. Ethernet and its monitor. Transceiver. Repeater. Package-switch. Bridge. Router. OSI model. **3. TCP/IP protocols (2 hours)**

The importance of understanding TCP/IP protocols for Internet security. Research of addresses, networks and servers. Work with networked monitor. Inspection of network configurative databases. Comprehension of accessible network databases. Address resolution protocols. DNS. UDP. Network and transportable layer. WWW. Data transport.

4. Internet coding (2 hours)

Usage of coding in the work with the Internet. Usage of coding in network operating systems and applications. DES; IDEA, RC5, Hash functions, Asymmetrical public key and infrastructure.

5. Basic hypotheses about Internet security (2 hours)

Internet security and computer networks in achieving absolute security. Principal terms and the most threatened parts of the Internet. The ethic of using the Internet and its security. Elementary tools and methods for threatening Internet security. Potential goal observing and noting down the activities. Logging on the system and searching for the weakest users. Objectives selection.

6. Discovery of weaknesses and failures (2 hours)

Internet protocols TCP/IP, UDP, DNS. Systems saving, Internet systems saving, scanning, discovering ‘live systems’. Operating system recognition, listing, passwords, appropriate system configurations. Controlling systems of computer networks, security on a network layer, computer networks on several locations. WWW, e-mail, news, FTP, telnet, LDAP. Human failures and technical mistakes, spying of network infrastructure.

7. Attacks on network operating systems (2 hours)

Network operating systems Windows NT, Windows 2000, Windows Me, Windows XP. Network operating systems UNIX, Linux, open source. Cryptography within operating systems. Using mechanisms of authentication. Finding and stopping the usage of rear door in operating systems.

8. Attacks on network applications (2 hours)

Differences between commercial and open source network applications. Deficiencies in remote controlling and managing. Advanced techniques in remote controlling. Attacks on WWW. Attacks on the ultimate user of network applications. Usage of rear door in network applications. Attacks on e-mail.

9. Attacks on network hardware(2 hours)

Differences between wired and wireless communication and network architecture development. Security on a network layer. Security on a transport layer. Telephone exchanges and VPN networks. Network devices and firewalls. Attacks through distributed withholding of services. Package filtering and port scanning. TCP/IP failures.

10. Malicious computer programs (2 hours)

Types of malicious computer programs and their effect on Internet security. The most frequent ways of using network weaknesses. Types of malicious computer programs-viruses, worms, Trojan horse, hoax, spam. Software and hardware for prevention and stopping of malicious computer programs spread.

11. Hacking techniques into networked systems and the Internet (2 hours)

	Hacking techniques into computer system. Hack tracking. Techniques and methods of detection of hacks into computer systems. Methods of prevention and stopping of hacks into computer system. **12. Forensics and hack proving (2 hours)** Attacker detecting. Attacker tracking. Evidence gathering and documentation. Definition of digital proof for the purpose of proving the act. Ways of communicating with authorities. Ways of accepting, storing and delivery of evidence material. **13. Prevention and Internet protection (2 hours)** Organizational, technological and technical assumptions of Internet security. Net applications without security failures. Complete methods of risk evaluation. Software and hardware firewalls. Software and hardware protection models. New models and techniques in keeping and securing Internet safety. **14. Ethics and legal regulations (2 hours)** Ethics in using the Internet and its meaning. Legal regulations in Croatia and the world. Systems for detection of unauthorized hacks, diary analysis. Digital signatures. Privacy on the Internet. Inspection of legal regulations concerning computer crime in Croatia. **15. Conclusion (2 hours)** Review of current developing projects in Croatia and the world for securing the safe Internet. Comparative analysis of the newest practical accomplishments in securing undisturbed Internet activity. Comparative analysis of the newest methods for undisturbed Internet activity. Directions for development of security systems. Biometrics implementation into security systems on the Internet.
Exercises	**Auditory + practical exercises** Practical exercises are based on working with security tools and detecting security failures and threats on PC oriented computers in a networked environment. The follow-up includes setting up prevention systems and networked environment protection and operating them; detection, tracking and analyzing of hack traces in computer system. Upon completing the exercises students have to perform individual monitoring of a certain computer system, and give a qualitative assessment. **1. Internet domains** Ways of determining an Internet domain owner. Whois service. DNS enquiries. Nslookup application. **2. Package route determination** Package route determination by tracer and retrace express applications. **3. Internet address cover-up** Usage of web-based proxy server. Connecting to proxy server. Using ftp service. **4. Using e-mail clients** Analysis of e-mail messages. Sending and hiding data. Using samspade application. **5. Using Usenet service and web server** Analysis of Usenet messages headings. Text search on web servers using logical criteria.

	6. Group searching Using WinMX service and Gnutell service. **7. IRC** IRC IceChat clients installation, database transfer. Using ICQ services. **8. Protection** PGP. Web-based remailer.
Realization and examination	Classes: lectures, seminars and exercises Examination: written examination and seminars
Related courses	1. Carnegie Mellon University (Electronic Commerce Institute) http://www.andrew.cmu.edu/user/mml 2. University of Notre Dame (Illinois Institute of Technology) http://www.nd.edu/~dcnoway/mgt425 3. Columbia University (Department of Computer Science) http://www.cs.columbia.edu/~hgs/teachnig/security 4. University of Virginia (Department of Computer Science) http://www.cs.virginia.edu/~evans/cs551 5. Wright State University, College of Engineering & CS, Dayton, Ohio http://www.cs.wright.edu/~pmateti 6. The University of Arkon, Wayne College http://www.eng.wayne.edu/coe 7. Universitat Trier, Trier, Deutschland http://www.uni-trier.de/uni
Literature	Basic: Lecture materials available on: http://www.foi.hr/studiji/dodiplomski/IS/kolegiji/si Du, Wenliang. Internet Security: A Hands-on Approach 2nd Edition, 2019. Bača, M. Uvod u računalnu sigurnost (Introduction to Computer Security), Narodne novine, 2004. Garfinkel, S., Spafford, G., Practical UNIX and Internet Security, O'Reilly & Associates, Inc., Sebastpol, CA, 1996 Additional: Garbis, J., & Chapman, J. W. (2021). Zero Trust Security: An Enterprise Guide. Apress. Bellovin, S., Cheswick, B., Firewalls and Internet Security, Addison Wesley, Reading, MA, 1994. Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computer and Internet, Academic Press, San Francisco, CA, 2000. Lockhart, A., Network Security Hacks, O'Reilly Media, Inc., Gravenstein Highway North, Sebastopol, 2004. Rhee, M.J., Internet Security, John Wilwy & Sons Ltd, England, 2003. Hunt, C., Networking Personal Computers with TCP/IP, O'Reilly & Associates, Inc. Sebastopol, 1995. **Unit 1.** Garfinkel, S., Spafford, G. Practical UNIX & Internet Security, O'Reilly & Associates, Inc., Sebastopol, CA 1996.

Unit 2.

McClure, S., Scambray, J., Kurtz, G., Hacking Exposed:Network Security Secrets & Solutions, McGraw-Hill, Osborne, 2003

Tanenbaum, A.S., Computer Networks, Prentice Hall, 2002.

Unit 3.

Blank, A.G., Blank, A., TCP/IP JumpStart: Internet Protocol Basics, Sybx, 2002.

Hunt, C., TCP/IP Network Administration, O'Reilly, 1997.

Unit 4.

Buchmann, J.A., Introduction to Cryptography, Springer-Verlag, 2000.

Srallings, W. Cryptography and Network Security: Principles and Practice, Prentice Hall, 2002.

Unit 5.

Cheswick, W.R., Bellovin, S.M., Rubin, A.D., Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Professional, 2003.

Northcutt, S., Zeltser, L., Winters, S., Fredrick, K., Ritchey, R.W., Inside Network Perimeret Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection systems, Sams, 2002.

Unit 6.

Blank, A.G., Blank, A., TCP/IP JumpStart: Internet Protocol Basics, Sybx, 2002

McClure, S., Scambray, J., Kurtz, G., Hacking Exposed:Network Security Secrets & Solutions, McGraw-Hill, Osborne, 2003.

Unit 7.

Fogie, S., Peikari, C., Windows Internet Security, Prentice Hall, PRT, 2001.

Schetina, E., Green, K., Carlson, J., Internet Site Security, Addison-Wesley, 2002.

Unit 8.

Fogie, S., Peikari, C., Windows Internet Security, Prentice Hall, PRT, 2001.

Stallings, W., Cryptography and Network Security: Principles and Practice, Prentice Hall, 2002.

Schetina, E., Green, K., Carlson, J., Internet Site Security, Addison-Wesley, 2002.

Unit 9.

Twicky, E.D., Cooper, S., Champman, D.B., Building Internet Firewalls, O'Reilly, 2000.

Cheswick, W.R., Bellovin, S.M., Rubin, A.D., Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Professional, 2003.

Unit 10.

Icove, D., Seger, K., VonStorch, W., Computer Crime-A Crimefighter's Handbook, O'Reilly & Associates, Inc. Sebastopol, 1995.

Skoudis, E., Zeltser, L., (2003.): Malware: Fighting Malicious Code, Prentice Hall PTR, Upper Saddle River, New Jersey

Unit 11.

	Northcutt S, Novak, J. Network Intrusion Detection, New Riders Publishing, 2002. **Unit 12.** Icove, D., Seger, K., VonStorch, W., Computer Crime-A Crimefighter's Handbook, O'Reilly & Associates, Inc. Sebastopol, 1995. Northcutt S, Novak, J. Network Intrusion Detection, New Riders Publishing, 2002. **Unit 13.** Icove, D., Seger, K., VonStorch, W., Computer Crime-A Crimefighter's Handbook, O'Reilly & Associates, Inc. Sebastopol, 1995. **Unit 14.** Dragičević, D., Kompjuterski kriminal i informacijski sustavi (Computer Crime and Information Systems), Informator, 1999. Saunders, K. M. Practical Internet Law for Business, Artech House, 2001