Establishing Modern Master-level Studies
in Information Systems
561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

Co-funded by the
Erasmus+ Programme
of the European Union

Information Systems Security

Objective	In this course you will explore information security through some introductory material and gain an appreciation of the scope and context around the subject. This includes a brief introduction to cryptography, security management and network and computer security that allows you to begin the journey into the study of information security and develop your appreciation of some key information security concepts. The course concludes with a discussion around a simple model of the information security industry and explores skills, knowledge and roles so that you can determine and analyse potential career opportunities in this developing profession and consider how you may need to develop personally to attain your career goals. After completing the course you will have gained an awareness of key information security principles regarding information, confidentiality, integrity and availability. You will be able to explain some of the key aspects of information risk and security management, in addition, summarise some of the key aspects in computer and network security, including some appreciation of threats, attacks, exploits and vulnerabilities. You will also gain an awareness of some of the skills, knowledge and roles/careers opportunities within the information security industry.
Level of course unit	Masters level
Lecturer	**Name**_____ **Email:**_____
Course Learning Outcomes	After completing this course, students should be able to: 1. to identify appropriate strategies to assure confidentiality, integrity, and availability of information; 2. to identify the role of information systems security (ISS) policy framework; 3. to apply current/common cryptographic technologies and controls for authentication and encryption; 4. to apply and operationalize network security technologies and techniques; 5. to evaluate and justify security technology selections and designs; 6. to provide contingency operations including administrative planning processes for incident response, disaster recovery, and business continuity within information security; 7. to analyze social, legal and ethical issues represented by information technology environments; 8. to argue, justify and present their decision and plans;

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

	9. to make decision and take responsibility for them
Format	5 Credits (150 hours of student work)
Workload	Credit weighting: 5 ECTS Lecture hours: 20 Group assignment work: 28 Independent study: 100 Examination: 2 Total Student Effort: 150 hours
Assessment	Cass participation 20% (participation and presentation of minimum 5 case studies) - Project 40% (Preparation of the project 70% and its presentation (30%)). The group responsible for the project will get the total grade. Students will distribute the grade among the group members internally. - Written exam 40%.
Course Material	Content is available at https://www.moodle.hneu.edu.ua/course/view.php?id=34
Other Information	Classes will be integrated with students' direct involvement in teaching activities. Students will be subdivided into groups of 3-5 people and they will be asked to rehearse course content with teaching cases. - The groups will be also responsible for the development of projects in certain topics. Labs We wanted to have a unified lab environment that is consistent for different lab exercises, so students do not need to learn a new lab environment for each lab. The environment used for these labs must be affordable to enable wider adoption. With these constraints in mind, we are going to use "Hands-on Labs for Security Education" SEED labs. Started in 2002, funded by a total of 1.3 million dollars from United States National Science Foundation (NSF), and now used by hundreds of educational institutes worldwide, the SEED project's objective is to develop hands-on laboratory exercises (called SEED labs) for computer and information security education and help instructors adopt these labs in their curricula. Since the actual lab description for each lab ranges between 2 pages to 10 pages. The detailed lab descriptions is shown on web page http://www.cis.syr.edu/_wedu/seed/

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

COURSE DESCRIPTION

Topic	*Learning Objectives*	*Theoretical component*	*Practical component*
1	*2*	*3*	*4*
Topic 1. Identity and Access Management	To learn: how to use identification methods and technologies; how to implement authentication methods, models and technologies; how to manage and monitor with Access Control Administration; how to recognize different threats to Access Control	*The main sub-topic:* 1.1. Security Principles Identification, Authentication, Authorization and Accountability 1.2. Access Control Models 1.3. Access Control Techniques and Technologies 1.4. Access Control Administration and Monitoring 1.5. Threats to Access Control	Pluggable Authentication Module Lab
Topic 2. Security Frameworks	To learn: how to implement security frameworks, models, standards and best practices; how to model cyber threats; how to manage with cyber threats; how to use Risk Management frameworks	*The main sub-topic:* 2.1. Policies, Standards, Baselines, Guidelines and Procedures 2.3. Risk Management 2.4. Threat Modeling 2.5. Risk Management Frameworks	General Software Vulnerabilities Lab
Topic 3. Cryptography definition and concept	To learn: how to use different types of Encrypting methods; how to check message integrity using different types of hash algorithms; how to understand structure of Public Key Infrastructure and how to use Digital sign for different purpose; how to recognize attacks on cryptography	*The main sub-topic:* 3.1. Methods of Encryption (Symmetric, Asymmetric) 3.2. Message Integrity 3.3. Public Key Infrastructure 3.4. Attacks on Cryptography 3.5. Block chain technologies	Linux Capability Lab. Encrypted File System Lab VPN Lab.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

1	*2*	*3*	*4*
Topic 4. Communication and Network Security	To learn: how to identify some of the factors driving the needs for network security; how to identify and classify particular examples of network attacks; how to identify physical points of vulnerability in simple networks; how to compare and contrast symmetric and asymmetric encryption systems, their vulnerability to attack, and explain the characteristics of hybrid systems.	*The main sub-topic:* 4.1. Open system Interconnection 4.2. Reference Model 4.3. TCP/IP Model 4.4. Networking Foundations 4.5. Network devices 4.6. Wireless Networks 4.7. Network Encryption 4.8. Security Protocols 4.9. Network Attacks	Network Protocol Vulnerabilities. IPSec Lab
Topic 5. Software Development Security	To learn: security characteristics of different software development models; security requirements for mobile application; security requirements for web-based application; security issue of databases; different malware types, attacks and how to protect IT system from malicious software.	*The main sub-topic:* 5.1. Software Development Models 5.2. Programming Languages and Concepts 5.3. Mobile Code 5.4. Web Security 5.5. Database Management 5.6. Malicious Software	Web Application Vulnerabilities. Web Browser Access Control Lab.
Topic 6. Security Operations	To learn: how to organize physical security; how to implement appropriate preventive measures; how to organize incident management processes; how to implement disaster recovery procedures; how to realize investigation process after cyber-attacks.	*The main sub-topic:* 6.1. Administrative Management 6.2. Operational Management 6.3. Physical Security 6.4. Preventive Measures 6.5. The Incident Management Process 6.6. Disaster Recovery 6.7. Investigation	Packet Sniffing and Spoofing Lab. MinixFirewall Lab

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

1	*2*	*3*	*4*
Topic 7. Asset Security	To learn: how to manage and protect information according with their classification; importance of clear definition of layers' responsibilities; how to provide privacy and protect assets.	*The main sub-topic:* 7.1. Information Life Cycle 7.2. Information Classification 7.3. Layers of Responsibility 7.4. Data Breaches 7.5. Protecting Privacy 7.6. Protecting Assets	Role-Based Access Control (RBAC) Lab

RECOMMENDED OR REQUIRED READING

Main:

1. Information Security Management Handbook/ CISSP (All in one – Exam guide 7th Edition), ISBN-13: 978-0071849272, ISBN-10: 0071849270.
2. Fundamentals of Information Systems Security (Information Systems Security & Assurance Series)

Additional:

1. Meltdown / Lipp M., Schwarz M., Gruss D. [et al.]. [Electronic resource]. – Access mode: https://meltdownattack.com/meltdown.pdf
2. Spectre / Kocher P., Genkin D., Gruss D. [et al.]. [Electronic resource]. – Access mode: https://spectreattack.com/spectre.pdf 3. Horn J. Reading privileged memory with a side-channel / Project Zero at Google. [Electronic resource]. – Access mode: https://googleprojectzero. blogspot.co.at/2018/01/reading-privileged-memory-with-side.html
3. Akhmetov, B., Lakhno, V., Boiko, Y., Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, Eastern-European Journal of Enterprise Technologies, 1(2 (85)), 4–15. DOI: 10.15587/1729-4061.2017.90506.
4. Rees, L. P., Deane, J. K., Rakes, T. R., Baker, W. H. (2011). Decision support for Cybersecurity risk planning. Decision Support Systems, 51(3), 493– 505. DOI: 10.1016/j.dss.2011.02.013.
5. Chang, L. Y., Lee, Z. J. (2013). Applying fuzzy expert system to information security risk Assessment-A case study on an attendance system. IEEE 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY), 346–351. DOI: 10.1109/iFuzzy.2013.6825462.
6. Mahmood, T., & Afzal, U. (2013). Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools. In Information assurance (ncia), 2013 2nd national conference on (pp. 129-134). IEEE. 7. Kim, K., Kim, I., Lim, J. (2017). National cyber security enhancement scheme for intelligent surveillance capacity with public IoT environment, The Journal of Supercomputing, 73(3), 1140–1151. DOI: 10.1007/s11227-016-1855-z.
7. Medhat, K., Ramadan, R. A., Talkhan, I. (2017). Security in Mission Critical Communication Systems, Multimedia Services and Applications in Mission Critical Communication Systems, 270. DOI: 10.4018/978-1-5225- 2113-6.ch012

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

8. Radziwill, N., Benton, M. (2017). Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management [Electronic resource] Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf

9. Jalali, M., Siegel, M., Madnick, S. (2017). Decision Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. [Electronic resource]. Available at: https://arxiv.org/ftp/arxiv/papers/1707/1707.01031.pdf.

10. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F. (2016). Decision support approaches for cyber security investment, Decision Support Systems, 86, 13–23. DOI:10.1016/j.dss.2016.02.012. 12. Lakhno, V., Petrov, A., & Petrov, A. (2017). Development of a Support System for Managing the Cyber. Benaroch, M. (2017). Real Options Models for Proactive UncertaintyReducing Mitigations and Applications in Cybersecurity Investment DecisionMaking. Information Systems Research. P. 39.

11. Wagner, N., Şahin, C. Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D., & Streilein, W. W. (2016, December). Towards automated cyber decision support: A case study on network segmentation for security. Computational Intelligence (SSCI), 2016 IEEE Symposium Series on (pp. 1–10). IEEE.

12. Atymtayeva, L., Kozhakhmet, K., & Bortsova, G. (2014). Building a knowledge base for expert system in information security. In Soft computing in artificial intelligence, 57–76. Springer, Cham.

13. Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. International Journal of Information Management, 34(6), 733–740.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. Computers & Security, 43, 19–34.

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein