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

PENS
Pathway in Enterprise Systems Engineering

Systems Security and Availability - (PENS)

Project Ref. No.: 586301-EPP-1-2017-1-PS-EPPKA2-CBHE-JP

http://www.pens.ps

Course Specification

Course Specification

I. **Course details**

Course Name	Systems Security and Availability
Course Code	To be assigned later
Number of Credit Hours	[4 CHs → 3 CHs lectures, 1CH coursework]
ECTS Credits	5.5 (140 learning hours)
Course type (core / elective)	Core
Pre-requisites	Computer Networks Information Systems
Weekly Hours • Theoretical • Practical • Total	 • [3] • [3] • [6]
Course Description (provide 60-100 words describing the focus of the syllabus)	
This course provides a comprehensive overview of the foundational security principles, techniques and best practices, in both management and technical aspects, which are associated with the design, development and deployment of enterprise information systems. It includes the following topics: elements of information security, cryptograph concepts and algorithms, symmetric and asymmetric ciphers, data integrity algorithms, systems and Web applications security, mobile security, enterprise mobility management systems, Internet authentication applications, network and Internet security, IT security management, security plans and procedures, risk management systems, and ethical and legal aspects.	
Course aim(s) (provide 30-50 words describing the aim of the course)	
The main objectives of this course are (*i*) To learn students the foundational principles of information, application and network security concepts and the best practices applied in an enterprise information system; (*ii*) To familiarize them with the software tools, polices, regulations, and risk management processes that are necessary for ensuring information and systems availability, integrity, and confidentiality.	

II. Intended Learning Outcomes of the Course (ILOs)

On completing the course, students should be able to (provide 4-6 learning outcomes):

LO.1: Understand the foundational security requirements of confidentiality, integrity and availability, and the various access control models, terminologies, best practices, tools, and network considerations to control accessing to network services and information.

LO.2: Describe the common cryptographic encryption and decryption algorithms and the tools to ensure data integrity such as hashing, symmetric and asymmetric encryption, and methods of implementing cryptography.

LO.3: Apply knowledge of various security aspects of operations, physical, human, audit, network, securing Web applications, and concerns about networking software to protect an organization's assets.

LO.4: Implement mechanisms to secure systems, information, applications, and services such as implementing access control lists, certificates, firewalls, data encryption, and implementing Web application secure protocols.

LO.5: Explain security classification levels, documents, business continuity plans, risk management considerations, incident response, software development concerns, and ethical and legal issues related to information systems.

LO.6: Examine software tools that can be used to test and monitor the vulnerability of systems, networks and logs that provide systems administrator with facilities to track and audit a variety of events on systems.

III. Course Matrix Contents

Week	Main Topics / Chapters	Learning Hours	Intended Learning Outcome (s)
	Part 1: Introduction / *(Refs. [1] & [3])*	**12 CHs**	LO.1
1	**Course overview** – Navigating the syllabus	2 CHs	
2	**Introduction /** *(Ch.(1)-Ref.[1], Ch.(2)-Ref.[3])* – Goals of security – Security concepts and services – Functional requirements – Information assurance – Examples of security attacks **Elements of information system security /** *Chs.(16,17,18)-Ref.[1]* – Physical security – Infrastructure security – Human resource security – Security auditing **Students' coursework (Internet search)** – Student will use Internet resources to search for common IT security breaches and study their impacts on organizations' assets.	10 CHs	LO.1
	Part 2: Cryptography / *(Refs. [1] & [2])*	**10 CHs**	LO.2 & LO.4
3	**Symmetric ciphers** – Data Encryption Standard (DES) / *Ch.(20)-Ref.[1], Ch.(3)-Ref.[2]* – Advanced Encryption Standard (AES) *Ch.(20)-Ref.[1], Ch.(5)-Ref.[2]* **Asymmetric ciphers** – Public key cryptography and RSA / *Ch.(21)-Ref.[1], Ch.(9)-Ref.[2]* – Diffie-Hellman key exchange / *Ch.(21)-Ref.[1], Ch.(10)-Ref.[2]* **Students' coursework (practical part)** – Students will implement and analyze some well-known encryption and decryption algorithms. – They will also build simple client/server applications using symmetric/asymmetric ciphers encryption.	6 CHs	LO.2 & LO.4

4	**Data integrity algorithms** – Cryptographic hash functions – Secure hash algorithm / *Ch.(11)-Ref.[2]* – Message authentication codes – Digital signatures and key management / *Ch.(12)-Ref.[2]* **Students' coursework (practical part)** – Students will implement the following algorithms MD5, SHA-1, SHA-2 and SHA-3. – Also, they will implement functions for creating and verifying RSA signatures.	4 CHs	LO.2 & LO.4
	Part 3: Systems Security / *(Refs. [1] & [3])*	**24 CHs**	LO.3, LO.4 & LO.6
5	**Software security /** *Ch.(11)-Ref.[1], Chs.(24,26)-Ref.[3]* – Buffer overflow problem – Handling program inputs – Handling program outputs – Systems calls – Writing safe program codes **Students' coursework (practical part)** – Students will study several programming codes that implement buffer-overflow problems, and experiment with several schemes to handle them. – They will also apply several tools to test program safety using a large set of automatically generated inputs.	6 CHs	LO.3, LO.4 & LO.6
6	**Operating system security /** *Ch.(12)-Ref.[1], Chs.(24, 26)-Ref.[3]* – System security planning – Operating system hardening – Application security – Security maintenance – Virtualization security **Students' coursework (practical part)** – Students will apply and evaluate several mechanisms to secure operating systems. – They will also apply software penetrations tools to test systems security breaches.	6 CHs	LO.3, LO.4 & LO.6
7	**Securing common operating systems /** *Ch.(12)-Ref.[1], Chs.(20,24)-Ref.[3]* – Windows security – Linux/Unix security – Hypervisor security **Students' coursework (practical part)** – Students will deploy, configure, and analyze the output of different mechanisms to secure operating systems.	6 CHs	LO.3, LO.4 & LO.6

8	**Wireless and mobile security** *Ch.(24)-Ref.[1]* – Wireless security measures – WiFi and Bluetooth security – SIM/UICC security – Mobile malware and app security – Android security model – IOS security model **Student's coursework (practical part)** – Students will work on some security toolkits to evaluate different mobile device security aspects.	6 CHs	LO.4 & LO.6
	Part 4: Web Application Security / *(Refs. [1] & [2])*	**22 CHs**	LO.3, LO.4 & LO.6
9	**Web application security/** *Ch.(22)-Ref.[1], Chs.(16,18, 19)-Ref.[2]* – Secure Sockets Layer (SSL) – Transport layer Security (TLS) – Web security and HTTPs – Secure Shell (SSH) **Students' coursework (practical part)** – Students will implement programming codes to secure HTTP traffic using SSL certificate. – They will configure devices to support SSH connections. – Also, they will configure devices to support a site-to-site IPsec and VPN service.	12 CHs	LO.3, LO.4 & LO.6
10	**Internet authentication applications /** *Ch.(22)-Ref.[1], Chs.(14,15)-Ref.[2]* – Kerberos – X.509 – Public-Key Infrastructure **Students' coursework (practical part)** – Students will install and configure Kerberos and X.509 authentication services. – They will also configure devices to support a site-to-site IPsec and VPN.	10 CHs	LO.3, LO.4, LO.6
	Part 5: Network Security / *(Refs. [1] & [2])*	**22 CHs**	LO.3, LO.4 & LO.6
11	**Firewall and intrusion prevention /** *Chs.(8,9)-Ref.[1], Ch.(22)-Ref.[2]* – AAA server – Access Control Lists (ACLs) – Firewall technologies – Intrusion Detection Systems (IDSs) – Intrusion Prevention Systems (IPSs) **Students' coursework (practical part)** Students will use network simulation tools to do the following labs: – Configure server-based AAA authentication using RADIUS.	22 CHs	LO.3, LO.4 & LO.6

	– Configure, apply and verify an extended Access control Lists (ACLs) – Configure a Zone-based Policy (ZPF) firewall. – Configure Intrusion Prevention System (IPS).		
	Part 6: IT Security Management / *(Ref. [1])*	**18 CHs**	LO.5 & LO.6
12	**Risk Management Systems (RMSs) /** *Ch.(14)-Ref.[1]* – Risk management process – Risk identification – Risk assessment – Risk control	6 CHs	LO.5
12	**Security plans and procedures /** *Ch.(15)-Ref.[1]* – Approaches to risk analysis – Monitoring threats	6 CHs	LO.5
13	**Computer security incident response plan** *Chs.(15,16)-Ref.[1]* - Incident response process - Incident response phases **Students' coursework (case study)** Students will be divided into groups to work on a case study to evaluate risk management process implemented in real cases. This includes the following steps: – Identify organization's information assets. – Analyze security risk plan and evaluation. – Apply risk treatment procedures. – Present obtained results.	6 CHs	LO.5 & LO.6
	Part 7: Enterprise Mobility Management	**16 CHs**	LO.5 & LO.6
14	**Enterprise mobility management systems** *Chs.(3,4, 7, &8)-Ref.[4]* – iOS and Android operating systems – Mobile device management – Mobile application management – Mobile email clients – Mobile file syncing – Secure mobile browsers **Student's coursework (practical part)** They will also experiment with an Enterprise Mobility Suite (EMS) to manage devices, users, and data for Windows-based, iOS, and Android devices, and they will implement some mechanisms to secure mobile data and applications.	16 CHs	LO.3, LO.4 & LO.6
	Part 8: Legal and Ethical Aspects / *(Ref. [1])*	**16 CHs**	LO. 5 & LO.6

15	**Security policy and governance /** *Ch.(19)-Ref.[1]* – Cybercrime and cybersecurity – Intellectual property – Privacy – Digital forensics – Reference standards (ISO27001, the NIS and GDPR) **Students' coursework (Reviewing papers)** Students will be provided with scientific papers and be asked to: – Write summaries – Analyze main ideas – List main findings – Propose future research directions	16 CHs	LO. 5 & LO.6
15	Summary		
Total Learning Hours	140		

IV. Assessment Methods, Schedule and Grade Distribution

Assessment type	Used	Formative	Weight	Week	ILO(s)
Written exam (midterm)	Y	Y	30%	7	LO.1 to LO.3
Written exam (final)	Y	Y	40%	16	All learning outcomes
Written coursework (individual)	Y	Y	10%	per-topic	All learning outcomes
Written coursework (group)	Y	Y	5%	14	LO.5 & LO.6
Oral presentation (individual)	N	N			
Oral presentation (group)	Y	Y	5%	15	LO.5 & LO.6
Test/Quiz	Y	Y	5%	per-topic	All learning outcomes
Other (Class attendance)	Y	Y	5%		

V. List of References

Essential textbook(s)	[1] W. Stallings, L. Brown, Computer Security: Principles and Practice, 4th Edition, 2017, ISBN-13: 978-0134794105. [2] W. Stallings, Cryptography and Network Security – Principles and Practice, 7th Edition, 2017, ISBN-13: 978-0134444284. [3] B. Matt, Introduction to Computer Security, 1st Edition Addison-Wesley, 2004, ISBN-13: 978-0321247445. [4] J. Madden, Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD, Kindle Edition, 2014.
Recommended textbook (s)	[5] B. Forouzan and D. Mukhopadhyay, Cryptography and Network Security, 2nd Edition, 2011, McGraw Hill Education, ISBN: 9780070702080. [6] W. A. Conklin, Principles of Computer Security, 5th Edition, 2018, McGraw-Hill Publishing, ISBN: 9781260025989. [7] M. E. Whitma and H. J. Mattord, Principles of Information Security, 6th Edition, 2017, Cengage Learning, ISBN-13: 978-1337102063. [8] OWASP Testing Guide.
Course notes	• Books' slides used in lectures. • From time to time, there will be other material assigned as well.

Journal(s) / periodical(s)	• Journal of Computers & Security, Elsevier, *https://www.journals.elsevier.com/computers-and-security* • IET Information and Security, IEEE, *https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=4149673* • Journal of Information Security and Applications (JISA), Elsevier, *https://www.journals.elsevier.com/journal-of-information-security-and-applications*
Specific article(s)	• M., Pendleton, R., Garcia-Lebron, J., Cho, and S., Xu. 2016. A Survey on Systems Security Metrics. ACM Comput. Surv. 49, 4, Article 62 (December 2016), 35 pages. DOI: https://doi.org/10.1145/3005714 • Dhillon G., Torkzadeh G., Chang J. (2018) Strategic Planning for IS Security: Designing Objectives. In: Chatterjee S., Dutta K., Sundarraj R. (eds) Designing for a Digital and Globalized World. DESRIST 2018. Lecture Notes in Computer Science, vol 10844. Springer, Cham. • H. Huang, Z. Zhang, H. Cheng and S. W. Shieh, "Web Application Security: Threats, Countermeasures, and Pitfalls," in *Computer*, vol. 50, no. 6, pp. 81-85, 2017. DOI: 10.1109/MC.2017.183 • Dixit P., Gupta A.K., Trivedi M.C., Yadav V.K. (2018) Traditional and Hybrid Encryption Techniques: A Survey. In: Perez G., Mishra K., Tiwari S., Trivedi M. (eds) Networking Communication and Data Knowledge Engineering. Lecture Notes on Data Engineering and Communications Technologies, vol 4. Springer, Singapore.
Websites and other online resources	• CCNA Security & CCNA Cybersecurity Operations Curricula, *https://www.netacad.com/*. • Khan Academy. Free Online Courses, Lessons & Practice, *https://www.khanacademy.org/*

VI. **Facilities required for teaching and learning**

- Computer lab with some software tools.
- Real case studies: Companies' business plans, risk management plans, and datasets.
- Physical tours to some well-known organizations' data centers.