SYLLABUS / FIŞA DISCIPLINEI

1. Information on the study programme / Date despre programul de studii

1.1. Institution / Instituţia de învăţământ superior	Universitatea de Vest din Timişoara
1.2. Faculty / Facultatea	Matematică şi Informatică
1.3. Department / Departamentul	Computer Science (Informatică)
1.4. Study program field	Computer Science (Informatică)
1.5. Study cycle/ Ciclul de studii	MSc / master
1.6. Study programme / Programul de studii / calificarea*	Artificial Intelligence and Distributed Computing / *Analyst / Analist - 251201; Research assistant in computer science / Asistent de cercetare în informatica - 214918; Teacher in secondary schools / Profesor în învatamântul gimnazial - 233002; Programmer / Programator - 251202; Software systems designers / Proiectant sisteme informatice - 251101*

2. Information on the course / Date despre disciplină

2.1. Title of the course / Denumirea disciplinei	Network Security Models and Architectures						
2.2. Teacher in charge of the course / Titularul activităţilor de curs	Stelian Mihalas						
2.3. Teacher in charge of the seminar / Titularul activităţilor de seminar	Stelian Mihalas						
2.4. Study year / Anul de studii	1	2.5. Semester / Semestrul	2	2.6. Examination type / Tipul de evaluare: E(xam)/C(olloquim)	C	2.7. Course type / Regimul disciplinei: M(andatory)/ E(lective)/ F(acultative)	DE

3. Estimated study time (number of hours per semester) /Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1. Attendance hours per week / Număr de ore pe săptămână	3	out of which din care: 3.2 lecture/ curs	2	3.3. seminar/laborator	1
3.4. Attendance hours per semester / Total ore din planul de învăţământ	42	out of which: 3.5 lecture / curs	28	3.6. seminar/laborator	14

Distribution of the allocated amount of time / Distribuţia fondului de timp*	**hours/ ore**
Individual study /Studiu după manual, suport de curs, bibliografie şi notiţe	14
Supplementary documentation at library or using electronic repositories / Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate	7
Preparing for laboratories, homework, reports etc. /Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	28
Exams / Examinări	7
Tutoring / Tutorat	14

3.7. Total number of hours of individual study / Total ore studiu individual	70

3.8. Total number of hours per semester / Total ore pe semestru	112
3.9. Number of credits (ECTS) / Număr de credite	6

4. Prerequisites (if it is the case) / Precondiţii (acolo unde e cazul)

4.1. curriculum / de curriculum	
4.2. skills / de competenţe	

5. Requirements (if it is the case) / Condiţii (acolo unde e cazul)

5.1. for the lecture / de desfăşurare a cursului	Lecture room with a video-projector
5.2. for the seminar, laboratory / de desfăşurare a seminarului/laboratorului	C or Java development environment installed on the workstations, internet connection

6. Acquired skills / Competenţe specifice acumulate

Professional skills / Competenţe profesionale	• The knowledge and the capacity of applying security principles in designing and implementing security policies • Ability of applying hash functions to guarantee the integrity of a file system or of message exchanges • Ability to use digital certificates in the authentication process and in secure communication • Knewledge and ability to protect data systems by enforcing the use secure communication channels • Recognizing the importance of data backup, protection and integrity preservation • Skills in identifying, preventing and blocking internet specific threats – viruses, trojans, phishing, spoofing
Transversal skills / Competenţe transversale	• Realizing the importance of personal data protection in general • Understanding the necessity of secure communication in day to day life • Recognizing the general internet threats and implementing mesures to prevent them

7. Objectives of the course / Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1. General objective / Obiectivul general al disciplinei	Getting to know and use security policies standards and issues – authentication techniques, key exchange protocols, encryption and decryption algorithms, digital signatures, public key certificates and infrastructure, data protection principles, secure communication, internet threats prevention.
7.2. Specfic objectives / Obiectivele specifice	*Knowledge objectives (KO)*: (1) Good understanding of data protection issues (2) Understanding the steps to implement security policies *Ability objectives (AO)*: (1) Ability to implement secure communication and data protection policies (2) Ability to recognize and prevent threats *Skills wise objectives (SO)*: (1) Implementation of basic data protection, backup and restoration; (2) Ability to use antivirus and other threat prevention and removal software

8. Content / Conţinuturi*

8.1. Lecture / Curs	Teaching strategies / Metode de predare	Remarks/Observaţii
01 - Network security – concepts and approach	Lecture, class discussion, informal debate	
02 - Network security architecture and standards	Lecture, exemplification, class discussion, informal debate	
03 - Security policies implementations	Student presentations, questioning, informal discussion	
04 - Authentication techniques - Kerberos	Student presentations, questioning, informal discussion	
05 - Encryption systems	Lecture on number theory, Student presentation, questioning, informal discussion	
06 - Hash functions	Student presentations, questioning, informal discussion	
07 - The public key infrastructure and DSS	Student presentations, questioning, informal discussion	
08 - IPSec and IPv6 security features	Student presentations, questioning, informal discussion	
09 - Secure communication - VPN, TLS, SSH	Student presentations, questioning, informal discussion	
10 - Secure storage – principles and providers	Student presentations, exemplification, informal discussion	
11 - Point to point secure exchanges	Student presentations, exemplification, informal discussion	
12 - Personal profiles, data verification	Student presentations, questioning, informal discussion	
13 - Electronic payments	Student presentations, exemplification, informal discussion	
14 - Electronic voting systems	Student presentation, exemplification	

Recommended bibliography / Bibliografie:

1. Course Notes - http://web.info.uvt.ro/~smihalas/net_sec/book/netsec.pdf
2. L. Batten, Public Key Cryptography Applications and Attacks, John Wiley and Sons, New Jersey, 2013.
3. Security features in IPv6 – Penny Hermann-Seton, SANS Institute, 2012
4. On the security of cloud storage services – Fraunhofer SIT Technical Report, 2012
5. Building and implementing a successful information security policy – Dancho Dancev, Internet Software Marketing, Ltd., 2003
6. ICT Security Standards – Herbert Rwamibazi, EAST AFRITAC IFMIS Rwanda Workshop, 2012
7. Introducing Traffic Analysis, Attacks, Defenses and Public Policy Issues - http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/TAIntro.pdf
8. Digital Signature Standard (DSS), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
9. ISO/IEC 27033-1:2015 - network security overview and concepts - http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63461
10. Introduction to public key infrastructure - http://www.tomsitpro.com/articles/public-key-infrastructure-introduction,2-884.html

8.2. Seminar, lab / Seminar, laborator	Teaching/learning strategies / Metode de predare/ invăţare	Remarks, details / Observaţii
P1 - Simplified TLS implementation versus normal TLS implementations	Projects will be designed and implemented by teams of 2-4 students. Each team will use the resources they discover and consider necessary for project implementation.	
P2 - Profile data verification mechanisms		
P3 - Architecture specification for an electronic voting system		
P4 – Electoral authority implementation		
P5 - Poll data provisioning		
P6 - Voter interface, voting process implementation		
P7 - Poll data processing, fraud prevention		
P8 - Voting system deployment, simulation and testing		

9. Correlations between the content of the course and the requirements of the IT field / Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

This course provides the theoretical and practical foundation for designing, implmenting and managing the security policies of a company or of a department. Course content is in line with existing graduate courses in this area.

10. Evaluation / Evaluare*

Activity / Tip de activitate	10.1. Evaluation criteria / Criterii de evaluare**	10.2. Evaluation methods / Metode de evaluare***	10.3. Weight in the averaged mark / Pondere din nota finală
10.4. Lecture / Curs	Knowledge levels in all course areas, quality of course presentations	Colloquium in written form or course presentation	50%
10.5. Seminar/ lab	Project implementation	Project execution	20%
	Project details knowledge	Questioning	15%
	Project documentation	Reading, questioning	15%
10.6. Minimal knowledge for passing / Standard minim de performanţă			
Acquiring a passing grade (5) as a combination of the colloquium/presentation and lab projects.			

Date/ Data completării

Signature (lecture) / Semnătura titularului de curs

Signature (seminar) Semnătura titularului de seminar

Signature (director of the department)
Semnătura directorului de departament
Conf.dr. Victoria Iordan