Securitatea Rețelelor și Serviciilor (SRS)

ETTI - Licenta 3D+3C+3G (curs la alegere), S2, 2019-2020

Plan preliminar

http://discipline.elcom.pub.ro/srs1/

Contact	
Curs, laborator	Octavian Catrina, A317, ocatrina at elcom.pub.ro
Laborator	Radu Lupu, A311b, rlupu at elcom.pub.ro

Curs (sala B312)	**Detalii**	**Durata**
1. Introducere in securitatea comunicațiilor	Amenințări, atacuri, servicii de securitate.	2
2. Confidentialitatea datelor	- Definiții. Modele de securitate pentru confidențialitatea datelor (tipuri de atacuri, cerințe de securitate). - Introducere în criptarea cu cheie secretă: cifru bloc, exemple de scheme de criptare bazate pe cifru bloc. - Introducere în criptarea cu cheie publică: criptare folosind funcția RSA. *Bibliografie: Ch. 1, Encryption Schemes, in [1]. Ch. 3, Private-Key (Symmetric) Encryption, in [1].Ch. 8, Public-Key (Asymmetric) Encryption, in [1].*	8
3. Autentificarea datelor	- Definiții. Modele de securitate pentru autentificarea datelor (tipuri de atacuri, cerințe de securitate). - Funcții hash criptografice: Proprietăți de securitate și exemple. - Introducere în autentificarea datelor cu cheie secretă: exemple de construcții bazate pe cifru bloc și pe funcții hash; criptare autentificată. - Introducere în autentificarea datelor cu cheie publică: semnătură digitală folosind funcția RSA. *Bibliografie: Ch. 4, Hash Functions, in [1]. Ch. 5, Message Authentication Codes, in [1]. Ch. 9, Digital Signatures, in [1].*	8
4. Protocoale de securitate pentru canale de comunicații sigure	- Concepte de bază privind infrastructura pentru chei publice. - Protocoale de autentificare: construcții elementare și atacuri. - Protocoale de stabilire a cheilor secrete: construcții elementare și atacuri. *Bibliografie: Ch. 10, Public-Key Infrastructure, in [1]. Ch. 11, Entitiy Authentication, in [1]. Ch. 12, Key Exchange Protocols, in [1].*	6
5. Controlul accesului	Concepte de bază privind tehnicile de control al accesului în sisteme informatice distribuite.	4
Bibliografie	[1] O. Catrina. Cryptographic Algorithms and Protocols. Ed. Matrix Rom, Bucharest, 2016. [2] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996, 2001.	

Laborator (sala A315)	**Detalii**	**Durata**
1. Comunicații protejate prin criptare cu cheie secretă (aplicația SeCom1)	Studenții extind o aplicație care nu oferă servicii de securitate, numită SeCom0, astfel încât să protejeze confidențialitatea datelor transmise folosind criptare cu cheie secretă. Aplicația va folosi în acest scop chei secrete prestabilite.	2
2. Transportul cheilor secrete folosind criptarea RSA (aplicația SeCom2)	Studenții modifică SeCom1 astfel încât fiecare sesiune de comunicație să folosească o cheie secretă diferită, în locul unei chei prestabilite. La începutul comunicației, un participant generează o nouă cheie secretă și o transmite celuilalt, protejându-i confidențialitatea prin criptare cu cheie publică RSA. Cheia publică RSA va fi distribuită în prealabil.	2

3. Autentificarea mesajelor folosind criptografie cu cheie secretă (aplicația SeCom3)	Studenții extind SeCom0 pentru a proteja autenticitatea datelor transmise folosind criptografie cu cheie secretă (cod de autentificare a mesajelor). SeCom3A va asigura doar autenticitatea datelor. SeCom3AE va proteja atât autenticitatea datelor, cât și confidențialitatea lor, prin criptare autentificată.	2
4. Autentificarea mesajelor folosind criptografie cu cheie publică (aplicația SeCom4)	Studenții extind SeCom0 pentru a proteja autenticitatea datelor transmise folosind criptografie cu cheie publică (semnătură digitală). Pentru distribuirea cheilor publice se vor folosi certificate digitale. În acest scop, studenții vor mai realiza și o infrastructură minimală pentru chei publice (o autoritate de certificare care emite certificatele necesare utilizatorilor).	2
5. Protocoale de stabilire a cheilor și autentificare bazate pe criptografie cu cheie secretă (aplicația SeCom5).	Studenții vor extinde SeCom3AE astfel încât să permită stabilirea cheilor de sesiune folosind un protocol bazat pe criptografie cu cheie secretă (chei secrete prestabilite, cod de autentificare).	2
6. Colocviu	Prezentarea temelor	

Evaluare		**Pondere**
Lucrare de verificare	Scris, sapt 14 (srs1/curs, srs1/probleme/srs_probleme_st.pdf)	50%
Lab + Tema	Colocviu in sapt 13-14.	40%
Participare la curs		10%
Total		**100%**
Conditii minime de promovare: min 50/100 din Total, min 50/100 la lucrarea de verificare, min 50/100 lab/tema.		

Orar laborator	**Sala, instructor**
Luni 13-15	A315, Octavian Catrina
Marti 15-17	A315, Radu Lupu
Joi 15-17	A315, Radu Lupu