



## BAZA MATERIALĂ A LABORATORULUI DE

### Rețele și Software de Telecomunicații - Arhitecturi și protocoale de rețea, Securitatea rețelelor de telecomunicații

#### afereent disciplinei Securitatea rețelelor și serviciilor

Laboratorul de Rețele și Software de Telecomunicații afereent disciplinei Securitatea Rețelelor și Serviciilor predată în anul III, semestrul 2, la Facultatea de Electronică, Telecomunicații și Tehnologia Informației, specializările "Tehnologii și Sisteme de Telecomunicații" și "Rețele și Software de Telecomunicații", se află în Localul Leu, Corpul A și aparține Universității POLITEHNICA București, Facultatea de Electronică, Telecomunicații și Tehnologia Informației, Departamentul de Telecomunicații.

Sala a fost renovată recent (ferestre termopan, transperante, mobilier recondiționat, tablă nouă, videoproiector, aer condiționat). Calculatoare actuale au fost instalate în septembrie 2018. În septembrie 2022 a fost instalat un ecran de 190 cm pentru a înlocui proiectorul.

Teme de laborator:

- Laboratorul este utilizat pentru disciplina Securitatea Rețelelor și Serviciilor (SRS) și câteva alte discipline din domeniul rețelelor de calculatoare.
- În cadrul lucrărilor de laborator de la disciplina SRS, studenții implementează, testează și analizează o suită de aplicații care asigură servicii de securitate a comunicațiilor folosind algoritmi criptografici. Aplicațiile sunt implementate în Java folosind mediul integrat de dezvoltare Eclipse și bibliotecile criptografice standard oferite de JDK. Îndrumarul de laborator este disponibil în format electronic pe fiecare calculator

#### Informații laborator

- Indicativ sală: **A315**
- Categorie laborator: **Tehnologic**
- Suprafața laboratorului este de aproximativ: **47.00 m<sup>2</sup>**
- Volumul laboratorului este de aproximativ: **139.94 m<sup>3</sup>**
- Laboratorul poate deservi până la: **18 studenți**

#### Resurse

- 9 PC-uri pentru studenți (Intel I5, 4 nuclee); 1 PC pentru instructor.
- ecran de 190 cm.
- videoproiector.

#### Teme de laborator

- Comunicații protejate prin criptare cu cheie secretă (aplicația SeCom1): <br /> 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.



- Transportul cheilor secrete folosind criptarea RSA (aplicația SeCom2): <br /> 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 este distribuită în prealabil.
- Autentificarea mesajelor folosind criptografie cu cheie secretă (aplicația SeCom3): <br /> Studenții extind SeCom0 pentru a proteja autenticitatea datelor transmise folosind criptografie cu cheie secretă (cod de autentificare a mesajelor). Varianta SeCom3A va asigura doar autenticitatea datelor. Varianta SeCom3AE va proteja atât autenticitatea datelor, cât și confidențialitatea lor, prin criptare autentificată.
- 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).
- 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).
- Protocoale de stabilire a cheilor și autentificare bazate pe criptografie cu cheie publică (aplicația SeCom6): Studenții vor extinde SeCom3AE astfel încât să permită stabilirea cheilor de sesiune folosind un protocol bazat pe criptografie cu cheie publică (Diffie-Hellmann cu autentificare mutuală prin semnătură și certificate).
- Colocviu final de laborator.

### Discipline deservite

- Protocoale de securitate pentru comunicații wireless (Comunicații Wireless Avansate - AWC, Masterat, Anul 2, Semestrul 1)
- Protocoale și tehnologii pentru servicii de comunicații în Internet (Managementul Serviciilor și Rețelelor - MSR, Masterat, Anul 1, Semestrul 1)
- Arhitecturi pentru rețele și servicii (Tehnologii Software Avansate pentru Comunicații - TSAC, Masterat, Anul 1, Semestrul 1)
- Securitatea informației și a rețelelor de comunicații (Tehnologii Software Avansate pentru Comunicații - TSAC, Masterat, Anul 1, Semestrul 2)
- Specificarea, modelarea și validarea protocoalelor de telecomunicații (Tehnologii Software Avansate pentru Comunicații - TSAC, Masterat, Anul 2, Semestrul 1)
- Securitatea rețelelor și serviciilor (Tehnologii și Sisteme de Telecomunicații - TST, Licență, Anul 3, Semestrul 2)
- Securitatea rețelelor și serviciilor (Tehnologii și Sisteme de Telecomunicații - TSTen, Licență, Anul 3, Semestrul 2)
- Arhitecturi și protocoale de comunicații (Rețele și Software de Telecomunicații - RST, Licență, Anul 3, Semestrul 2)
- Securitatea rețelelor și serviciilor (Rețele și Software de Telecomunicații - RST, Licență, Anul 3, Semestrul 2)