Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti

Facultatea de Electronică, Telecomunicaţii şi

Tehnologia Informaţiei

FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti**
1.2 Facultatea	**Electronică, Telecomunicaţii şi Tehnologia Informaţiei**
1.3 Departamentul	**Telecomunicaţii**
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Comunicaţii Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Protocoale de securitate pentru comunicaţii wireless Wireless Communications Security Protocols			
2.2 Titularul activităţilor de curs				Conf. Dr. Octavian Catrina			
2.3 Titularul activităţilor de seminar / laborator				Conf. Dr. Octavian Catrina			
2.4 Anul de studiu	2	2.5 Semestrul	I	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DS	2.9 Codul disciplinei	UPB.04.M3.O.21-22		2.10 Tipul de notare	Nota

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	2.5	Din care: 3.2 curs	1.5	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	35.00	Din care: 3.5 curs	21	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii şi eseuri					55
Tutorat					0
Examinări					3
Alte activităţi (dacă există):					0

3.7 Total ore studiu individual	65.00
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Algoritmi criptografici, Reţele de calculatoare, Programarea calculatoarelor.
4.2 de rezultate ale învăţării	Noţiunile de bază asociate disciplinelor listate mai sus.

5. Condiţii necesare pentru desfăşurarea optimă a activităţilor didactice (acolo unde este cazul)

5.1 Curs	Sală de curs dotată cu videoproiector.

5.2 Seminar/ Laborator/Proiect	Laborator dotat cu calculatoare și videoproiector. Software-ul utilizate în lucrările de laborator este gratuit (emulator de rețele GNS, Java JDK, Eclipse IDE).

6. Obiectiv general *(Se referă la intențiile profesorilor pentru studenți, la ceea ce studenții vor fi învățați în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului științific abordat, precum și la rolul pe care acesta îl are în cadrul specializării studiate. Vor fi descrise de o manieră generală tematicile abordate, justificarea includerii cursului în planul de învățământ al specializării studiate etc.)*

Obiectivul general al acestei discipline este familiarizarea studenților cu concepte, tehnologii, arhitecturi și protocoale utilizate în practică pentru a asigura securitatea comunicațiilor de date și a rețelelor de telecomunicații. Motivația studierii securității comunicațiilor derivă din faptul că utilizarea pe scară largă a tehnologiei informației, în toate domeniile de activitate, nu a adus doar avantaje importante, ci și riscuri de securitate fără precedent. Securitatea comunicațiilor de date are o importanță deosebită, deoarece acestea au rol esențial în funcționarea sistemelor informatice distribuite și, în același timp, oferă principalele căi de atac asupra acestor sisteme.
Cursul prezintă concepte și tehnologii fundamentale de securitate, precum și arhitecturi și protocoale de securitate standardizate, folosite în rețelele de telecomunicații, rețelele de întreprindere și în Internet:
- Funcții de securitate: autentificarea datelor, autentificarea participanților, confidențialitatea datelor, controlul accesului. Soluții criptografice utilizate pentru a implementa aceste funcții, împreună cu modelele lor de securitate, proprietățile standard de securitate și exemple de atacuri.
- Protocoale pentru canale de comunicație care asigură autentificarea și confidențialitatea datelor.
- Protocoale de autentificare și de distribuție a cheilor: principii de proiectare, atacuri și analiza securității.
- Protocoale de securitate pentru nivelul Rețea: IPsec, IKE; rețele private virtuale securizate folosind IPsec.
- Protocoale de securitate pentru nivelul Transport: TLS, SSH; rețele private virtuale securizate folosind TLS.
Cursul oferă cunoștințe teoretice și practice care să permită înțelegerea aspectelor fundamentale ale protocoalelor de securitate, pentru a le putea proiecta, implementa, configura și întreține. Prezentarea conceptelor teoretice este însoțită de o suită de lucrări de laborator: într-o primă lucrare, studenții se familiarizează cu exemple reprezentative de protocoale de securitate standardizate (IPsec, IKE), iar în următoarele lucrări implementează și testează o serie de protocoale de securitate, folosind construcții tipice și algoritmi criptografici standardizați.

7. Competențe *(Capacitatea dovedită de a utiliza cunoștințe, aptitudini și abilități personale, sociale și/sau metodologice în situații de muncă sau de studiu și pentru dezvoltarea profesională și personală. Reflectă cerințele angajatorilor.)*

Specifice	- Definirea riguroasă a cerințelor și funcțiilor de securitate a comunicațiilor, a tipurilor de algoritmi criptografici utilizați pentru implementarea lor și a proprietăților standard de securitate pe care trebuie să le îndeplinească (și pe care se bazează proiectarea și analiza securității protocoalelor). - Descrierea, analiza și explicarea soluțiilor tipice de construcție a protocoalelor de securitate (în special a proprietăților lor de securitate), a avantajelor și dezavantajelor diferitelor categorii de soluții în contextul unor aplicații practice cu cerințe diferite (de exemplu, protocoale bazate pe criptografie cu cheie secretă, protocoale bazate pe criptografie cu cheie publică și soluții mixte). - Elaborarea unor soluții de securitate a comunicațiilor care îndeplinesc ceințele de securitate, scalabilitate și performanțe ale aplicațiilor, folosind componente standard.

Transversale (generale)	- Analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluţii consacrate, asigurând astfel îndeplinirea sarcinilor profesionale. - Capacitatea de a se adapta la noile tehnologii şi de a se documenta (în limba română şi limba engleză), pentru dezvoltarea profesională şi personală, prin formare continuă. - Abilitatea de a gândi în termeni ştiinţifici, de a căuta şi analiza date în mod independent, precum şi de a desprinde şi prezenta concluzii sau de a identifica soluţii. - Capacitatea de analiză şi sinteză: prezentarea în mod sintetic a cunoştinţele dobândite, ca urmare a unui proces de analiză sistematică. - Abilitatea de a coopera cu specialişti din domeniu şi de a lucra în echipă, comunicând eficient şi coordonându-şi eforturile cu ceilalţi pentru soluţionarea problemelor. - Respectare principiilor de etică academică, în particular, citarea corectă a surselor bibliografice utilizate în activitatea de documentare.

8. Rezultatele învăţării *(Sunt enunţuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învăţării reflectă realizările studentului şi mai puţin intenţiile profesorului. Rezultatele învăţării informează studenţii despre ceea ce se aşteaptă de la ei din punct de vedere al performanţei, pentru a obţine notele şi creditele dorite. Sunt definite în termeni concreţi, folosind verbe similare exemplelor de mai jos şi indică ceea ce se va urmări prin evaluare. Rezultatele învăţării vor fi astfel redactate încât să fie evidenţiată clar relaţia faţă de competenţele definite la punctul 7.)*

Cunoştinţe	*Rezultatul asimilării de informaţii prin învăţare. Cunoştinţele reprezintă ansamblul de fapte, principii, teorii şi practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice şi/sau faptice.* - Cunoaşte noţiunile specifice domeniului şi subiectelor tratate în curs: funcţii de securitate, algoritmi criptografici şi proprietăţile lor de securitate, construcţii tipice de protocoale, soluţii standardizate pentru protocoale şi componentele lor. - Cunoaşte modul în care noţiunile de securitate, algoritmii criptografici şi protocoalele de securitate sunt utilizate pentru în practică, pentru a înţelege şi specifica riguros cerinţele sau proprietăţile de securitate şi performanţe ale aplicaţiilor şi pentru a elabora soluţii care îndeplinesc aceste cerinţe.
Aptitudini	*Capacitatea de a aplica cunoştinţe şi de a utiliza know-how pentru a duce la îndeplinire sarcini şi a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive şi creative) sau practice (implicând dexteritate manuală şi utilizarea de metode, materiale, unelte şi instrumente).* - Identifică şi formulează riscurile şi cerinţele (de bază) de securitate a comunicaţiilor. - Analizează, descrie şi explică rolul şi funcţionarea componentelor unei rsoluţii de asigurare a securităţii comunicaţiei (funcţii, algoritmi, protocoale), folosind terminologie specifică. - Identifică, implementează şi testează soluţii de securitate a comunicaţiilor bazate pe componente standard (algoritmi şi protocoale), care să îndeplinească cerinţele aplicaţiilor.

Responsabilitate și autonomie	*Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.* - Selectează surse bibliografice potrivite și le analizează. - Respectă principiile de etică academică (de exemplu, citând corect sursele bibliografice utilizate). - Demonstrează receptivitate pentru contexte noi de învățare. - Manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice - Demonstrează autonomie în organizarea situației de învățare sau în situația problemelor de rezolvat. - Conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile și sustenabile care să rezolve probleme din viața socială și economică (responsabilitate socială). - Analizează și valorifică oportunități de afaceri/de dezvoltare antreprenorială în domeniul de specialitate. - Demonstrează abilități de management al situațiilor din viața reală.

9. Metode de predare *(Se vor avea în vedere metode care să asigure predarea centrată pe student. Se va descrie modul în care se asigură participarea studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămâneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)*

Procesul de predare utilizează atât metode de predare expozitive (prelegerea, expunerea), cât și conversative-interactive, bazate pe modele de învățare prin descoperire facilitate de explorarea directă și indirectă a realității (experimente conceptuale sau practice), dar și pe metode bazate pe acțiune, precum exercițiul, activitățile practice și rezolvarea de probleme.
Activitatea de predare utilizează prelegeri bazate pe prezentări PowerPoint ilustrate prin imagini și scheme (arhitecturi, mesaje, diagrame pentru algoritmi și interacțiuni), astfel încât informațiile să fie mai ușor de înțeles și de asimilat. Prezentările PowerPoint sunt completate cu exemple construite interactiv pe tablă. Prezentările introductive ale cursurilor și lucrărilor de laborator scot în evidență legătura cu noțiunile prezentate anterior.
La laborator, studenții explorează, implementează și testează construcții tipice de protocoale de securitate pentru canale securizate de comunicații. Exercițiile de implementare sunt esențiale pentru a înțelege corect operațiile efectuate și mesajele transmise de aceste protocoale, iar experimentele permit urmărirea pas cu pas a evoluției stării protocoalelor și a informației accesibile adversarului. Atât mediul integrat de programare Eclipse, cât și bibliotecile criptografice utilizate sunt disponibile gratuit și studenții le pot instala cu ușurință pe propriul calculator.
Procesul de predare ține seama de diferențele cruciale dintre securitatea comunicațiilor și celelalte discipline din domeniul ingineriei electronice și telecomunicațiilor. În acest domeniu, ne confruntăm cu adversari care doresc să compromită funcționarea sistemului și dispun de cunoștințele, competențele și resursele necesare pentru a înțelege și eventual depăși măsurile de protecție, nu doar cu fenomene fizice al căror comportament este predictibil pe baza unor modele matematice. Mai mult, îndeplinirea proprietăților de securitate este dificil sau imposibil de testat (experimental) deci trebuie să ne bazăm pe analize de securitate teoretice riguroase. Exemplele de atacuri joacă un rol important în înțelegerea vulnerabilităților și a soluțiilor utilizate de protocoalele de securitate.

10. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
1	Introducere. Amenințări și atacuri asupra securității comunicațiilor. Funcții de securitate și soluții criptografice pentru realizarea lor. Exemplu: securitatea rețelelor WiFi.	3

2	Componente ale protocoalelor de securitate (I): Confidențialitatea datelor folosind algoritmi cu cheie secretă (ENCS). Proprietăți de securitate. Cifru bloc. Construcții tipice de scheme ENCS folosind cifru bloc.	3
3	Componente ale protocoalelor de securitate (II): Autentificarea datelor folosind algoritmi cu cheie secretă (MAC). Proprietăți de securitate. Funcții hash criptografice. Construcții tipice de scheme MAC folosind funcții hash sau cifru bloc.	3
4	Protocoale pentru comunicație pe canale sigure ("secure channel"). Criptarea autentificată a datelor. Proprietăți de securitate. Construcții tipice. Exemple de protocoale pentru canale sigure utilizate în practică (IPsec, TLS Record, WiFi).	3
5	Componente ale protocoalelor de securitate (III): Confidențialitatea și autentificarea datelor folosind algoritmi cu cheie publică (ENCP, SIG). Proprietăți de securitate. Construcții tipice de scheme ENCP și SIG folosind funcții cu sens unic bazate pe problema RSA și pe problema logaritmului discret.	4
6	Componente ale protocoalelor de securitate (IV): Generarea și distribuția cheilor. Generarea șirurilor pseudoaleatoare și derivarea cheilor secrete folosind algoritmi MAC. Distribuția cheilor publice. Certificate și infrastructura pentru chei publice.	3
7	Protocoale de autentificare și stabilire a cheilor secrete. Construcții tipice de protocoale pentru autentificarea participanților și pentru stabilirea cheilor secrete folosind criptografie cu cheie secretă și criptografie cu cheie publică. Proprietăți de securitate. Atacuri.	6
8	Protocoale pentru crearea canalelor de comunicație sigure. Exemple tipice de protocoale de autentificare și stabilire a cheilor secrete utilizate în practică (IKEv2, TLS Handshake).	3
	Total:	28

Bibliografie:

1. Catrina Octavian, Protocoale de Securitate pentru Comunicații Wireless, suport de curs electronic (platforma Moodle): https://curs.upb.ro/2021/course/view.php?id=9563
2. Catrina Octavian. Cryptographic Algorithms and Protocols. Editura MATRIX ROM, București, 2016. ISBN 978-606-25-0249-2.
3. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996, 2001. Disponibilă în format electronic (gratuit): http://cacr.uwaterloo.ca/hac/
4. Specificațiile algoritmilor și protocoalelor din curs sunt disponibile online (gratuit) în publicațiile NIST (National Institute of Standards and Technology, https://www.nist.gov/) și IETF (https://www.ietf.org).

LABORATOR

Nr. crt.	Conţinutul	Nr. ore
1	Securitate comunicațiilor în practică: Rețele private virtuale care asigură autenticitatea și confidențialitatea datelor ("secure VPN") realizate folosind IPsec, GRE și IKEv2. Implementare, experimente și analiză folosind un emulator de rețele, analizor de protocoale și rutere Cisco.	4
2	Implementarea protocoalelor care asigură autenticitatea și confidențialitatea datelor prin criptare autentificată. Aplicație implementată în Java folosind biblioteca standard de clase criptografice (SecPro1). Experimente și analiză.	2

3	Implementarea protocoalelor de autentificare şi stabilire a cheilor secrete (I): Construcţii bazate pe criptografie cu cheie secretă. Aplicaţie realizată în Java folosind biblioteca standard de clase criptografice (SecPro2). Experimente şi analiză.	4
4	Implementarea protocoalelor de autentificare şi stabilire a cheilor secrete (II): Construcţii bazate pe criptografie cu cheie publică şi infrastructură pentru chei publice. Aplicaţie realizată în Java folosind biblioteca standard de clase criptografice (SecPro3). Experimente şi analiză.	4
	Total:	14

Bibliografie:

1. Catrina Octavian, Protocoale de Securitate pentru Comunicaţii Wireless, Îndrumar de laborator în format electronic şi proiecte Java iniţiale (platforma Moodle): https://curs.upb.ro/2021/course/view.php?id=9563
2. Documentaţia bibliotecilor software folosite, disponibilă online, gratuit: Java Cryptography Architecture Reference Guide, documentaţia claselor Java standard care implementează algoritmii folosiţi.

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	- Cunoaşterea conceptelor, tehnicilor, algoritmilor şi protocoalelor de securitate studiate la curs. - Abilitatea de a descrie, analiza şi explica funcţionarea şi proprietăţile de securitate ale protocoalelor şi componentelor lor în divese situaţii întâlnite în practică (scenarii de comunicaţie, atacuri).	Examen scris	50%
11.5 Seminar/laborator/proiect	Analiza, proiectarea, implementarea şi testarea unor aplicaţii elementare care asigură securitatea comunicaţiilor, pe baza exemplelor realizate pe parcursul lucrărilor de laborator.	Colocviu final de laborator	50%
11.6 Condiţii de promovare			
Studenţii trebuie să obţină minimum 50/100 la examen şi minimum 50/100 la colocviul de laborator.			

12. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor angajatorilor şi asociaţiilor profesionale reprezentative din domeniul aferent programului, precum şi cu stadiul actual al cunoaşterii în domeniul ştiinţific abordat şi practicile în instituţii de învăţământ superior din Spaţiul European al Învăţământului Superior (SEÎS)

Societatea modernă se bazează pe o vastă reţea de sisteme informatice utilizate în economie, finanţe şi administraţie, în infrastructuri şi servicii esenţiale, precum şi în viaţa de zi cu zi a cetăţenilor. Această informatizare masivă a adus atât avantaje importante, cât şi riscuri de securitate fără precedent.
Tehnologiile de securitate au devenit, prin urmare, componente esenţiale ale acestei reţele de sisteme informatice. Aceste tehnologii oferă o gamă largă de funcţii şi servicii de securitate: permit accesul la resurse şi servicii doar utilizatorilor legitimi, protejează integritatea, autenticitatea şi confidenţialitatea datelor, asigură disponibilitatea sistemelor, reţelelor şi serviciilor. În particular, securitatea comunicaţiilor de date are o importanţă deosebită, deoarece acestea au rol esenţial în sistemele informatice distribuite şi, în acelaşi timp, oferă principalele căi de atac asupra acestor sisteme. Industria IT solicită ingineri cu o calificare multidisciplinara, capabili să rezolve problemele de securitate ale sistemelor, reţelelor şi aplicaţiilor distribuite, cu cunoştinţe solide de electronică, tehnologii de comunicaţie şi securitatea informaţiei.

Prin urmare, cursul răspunde cerinţelor actuale şi de perspectiva ale economiei globale în domeniile Electronică şi Telecomunicaţii. El oferă absolvenţilor cunoştinţe teoretice şi practice esenţiale privind securitatea informaţiei, care le îmbunătăţesc competitivitatea şi le permit angajarea rapidă după absolvire, fiind perfect încadrat în politica Universităţii Politehnica din Bucureşti, atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite studenţilor.

Data completării	Titular de curs	Titular(i) de aplicaţii
10.10.2024	Conf. Dr. Octavian Catrina	Conf. Dr. Octavian Catrina

Data avizării în departament	Director de departament
27.10.2024	Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultăţii	Decan
25.10.2024	Prof. Dr. Mihnea Udrea