FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Automatică
1.4 Domeniul de studii	Ingineria sistemelor
1.5 Ciclul de studii	Licenţă
1.6 Programul de studii / Calificarea	Automatica si Informatica Aplicata / Satu Mare
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	56.30 – AIA Ro 55.30 – AIA SM

2. Date despre disciplină

2.1 Denumirea disciplinei	***Securitate digitală***				
2.2 Titularul de curs	Conf.dr.ing. Ovidiu Stan, Ovidiu.stan@aut.utcluj.ro				
2.3 Titularul/Titularii activităţilor de seminar/laborator/proiect	Conf.dr.ing. Ovidiu Stan, Ovidiu.stan@aut.utcluj.ro				
2.4 Anul de studiu	4	2.5 Semestrul	2	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	C
2.7 Regimul disciplinei	*DF – fundamentală, DD – în domeniu, DS – de specialitate, DC – complementară*				DS
	DI – impusă, DO – opțională, DFac – facultativă				DO

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar	0	Laborator	0	Proiect	1
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar	0	Laborator	0	Proiect	14
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie și notițe										20
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren										19
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii și eseuri										33
(d) Tutoriat										6
(e) Examinări										4
(f) Alte activităţi:										1

3.4 Total ore studiu individual (suma (3.3(a)…3.3(f)))	83
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Algebră matematică, Matematici speciale, Probabilități • Programarea într-un limbaj obiectual de nivel înalt
4.2 de competențe	• C1. Utilizarea de cunoștințe de matematică, fizică, tehnica măsurării, grafică tehnică, inginerie mecanică, chimică, electrică și electronica în ingineria sistemelor

5. Condiţii (acolo unde este cazul)

5.1. de desfășurare a cursului	• Sală de curs cu minim 90 locuri, calculator, videoproiector, tablă, conexiune la Internet
5.2. de desfășurare a seminarului / laboratorului / proiectului	• Sală cu minim 20 locuri, minim 10 calculatoare, videoproiector, tablă, 4 X SEcube dev board, 20 x Raspberry Pi 3+

6. Competențele specifice acumulate

6.1 Competențe profesionale	• C1. Utilizarea de cunoștințe de matematică, fizică, tehnica măsurării, grafică tehnică, inginerie mecanică, chimică, electrică și electronică în ingineria sistemelor.

	• C2. Operarea cu concepte fundamentale din știința calculatoarelor, tehnologia informației și comunicațiilor. • C3. Utilizarea fundamentelor automaticii, a metodelor de modelare, simulare, identificare și analiză a proceselor, a tehnicilor de proiectare asistată de calculator. • C4. Proiectarea, implementarea, testarea, utilizarea și mentenanţa sistemelor cu echipamente de uz general și dedicat, inclusiv reţele de calculatoare, pentru aplicații de automatică și informatică aplicată. • C5. Dezvoltarea de aplicații și implementarea algoritmilor și structurilor de conducere automată, utilizând principii de management de proiect, medii de programare și tehnologii bazate pe microcontrolere, procesoare de semnal, automate programabile, sisteme încorporate.
6.2 Competențe transversale	• CT2. Identificarea rolurilor și responsabilităților într-o echipă plurispecializată, luarea deciziilor și atribuirea de sarcini, cu aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei. • CT3. Identificarea oportunităților de formare continuă și valorificarea eficientă a resurselor și tehnicilor de învățare pentru propria dezvoltare. • Competențe de comunicare scrisă și orală • Competențe privind managementul resurselor materiale și de timp • Competențe de utilizare a terminologiei științifice din domeniu • Competențe de utilizare interdisciplinară a cunoștințelor și terminologiei din domeniu

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	• Identificarea și însușirea principalelor tehnici moderne în securitatea datelor, în contextual tehnologic curent expus prin sintagma Internet of Things • Internet of Things (IoT) este o tehnologie în curs de dezvoltare care ne schimbă lumea cu produsele sale inovatoare, cum ar fi „casele inteligente”, „vehiculele autonome”, etc. Acest curs își propune să introducă studenților conceptul de IoT și impactul acestuia asupra vieții noastre de zi cu zi, să îi facă să înțeleagă arhitectura și componentele IoT și să abordeze provocările și soluțiile implementării IoT în realitate. • Studenții vor învăța cum să facă legătura și schimbul între costurile de comunicare și puterea de calcul, precum și între hardware și software. În plus, securitatea digitală este o problemă critică de proiectare a sistemelor IoT. De la acest curs, studenții vor conștientiza problemele de cyber-securitate ridicate de IoT și vor dobândi cunoștințe despre tehnicile de securitate aferente. De asemenea, studenții vor câștiga experiențe practice despre construirea dispozitivelor IoT și implementarea tehnicilor de securitate prin proiecte de echipă.
7.2 Obiectivele specifice	• Utilizarea algoritmilor/metodelor specifici pentru securizarea datelor prin criptare • Identificarea vulnerabilităților • Evaluarea securității dispozitivelor inteligente • Înțelegerea impactului tehnologiilor IoT • Cunoașterea tehnologiilor emergente ale IoT • Dezvoltarea de abilități de gândire critică (critikal thinking)

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
Curs 1 1. Note introductive, context, structura disciplinei, cerințe examen 2. Introducere: securitatea datelor și aspecte legate de securitatea informației 3. Servicii de securitate	2	Prelegere interactivă, brainstorming, învățare prin descoperire, învățare prin cooperare, argumentarea,	În caz de forță majora, cursurile se vor desfășura

4. Accesul la date și controlul acestuia 5. Tipuri de atacuri (Dictionary and Brute Force, Lookup Tables, Reverse Look Tables, Rainbow Tables) 6. Clasificarea atacurilor 6.1. Atacurile de tip protocol 6.2. Atacurile de estimare 6.3. Atacul de remodulare		învățarea în perechi, dezbaterea, exemplificare video	on-line pe platforma Teams
Curs 2 1. Criptarea clasica – aspecte generale, algoritmi, mesaje de autentificare, semnături digitale 2. Criptarea modernă – principii și algoritmi 3. Critarea cu chei publice – principii, standarde și algoritmi 4. Criptografia cu cheie criptografică (secretă) 5. Funcția Hash (MD5, SHA256, SHA512, RipeMD, Whirlpool)	4		
Curs 3 1. Steganografie 1.1. Aspecte generale 1.2. Steganografia tehnică 1.3. Steganografia lingvistică 2. Utilizarea metodelor steganografice în vederea creșterii securității sistemelor cyber-fizice 3. Principii de bază ale marcării transparente 3.1. Inserţia marcajului 3.2. Detecţia marcajului 3.3. Metoda schimbării celui mai puţin semnificativ bit 4. Marcarea fragilă pentru diverse forme ale informaţiei digitale 4.1. Marcare fragilă pentru imagini 4.2. Marcarea pentru semnalele audio 4.3. Marcarea pentru secvenţe video 5. Stocarea imaginilor 5.1. Stocarea imaginilor în memorie 5.2. Stocarea imaginilor în fişiere	4		
Curs 4 1. Introducere în Internet of Things (IoT) 1.1. Beneficiile și aplicațiile IoT 1.2. Creșterea IoT 1.3. Probleme de securitate cu IoT 1.4. Arhitectura de bază a IoT 2. IoT Attack Surface și amenințări 2.1. OWASP top 10 pentru IoT 2.2. IoT Attack Surface 2.3. Componente software și cloud 2.4. Firmware-ul dispozitivelor 2.5. Tabloul de bord pentru aplicații web 2.6. Aplicație mobilă utilizată pentru controlul, configurarea și monitorizarea dispozitivelor 2.7. Evaluare a amenințărilor 3. Etică și confidențialitate	2		
Curs 5	4		

1. Necesitatea securității IoT 1.1. Cerințe și proprietăți de bază 1.2. Principalele provocări 1.3. Probleme principale de securitate 1.4. Confidențialitate, Integritate, Disponibilitate 1.5. Non-repudiere 2. Introducere în hardware-ul IOT și în componentele sale 2.1. Instrumente și tehnici 2.2. Protocoale de comunicare electronică 2.3. JTAG 3. Introducere în HydraBus, Raspberry PI 3.1. Întelegerea Raspberry Pi 3.2. Configurarea Raspberry Pi 3.3. Instalarea sistemului de operare în Raspberry PI (Noobs și Kali Linux) 3.4. Setarea accesului la distanță al Raspberry PI 4. Analiza canalului lateral 5. Analiza firmware-ului 6. Vectori de atac convenționali			
Curs 6 1. Înțelegerea arhitecturii IOT 1.1. Dispozitiv la dispozitiv 1.2. Dispozitiv la Coud 1.3. Dispozitiv către Gateway 1.4. Cloud către Gateway 2. IOT- protocoale de comunicare 2.1. Model de referință OSI vs TCP / IP 2.2. Protocoale de nivel de transport (TCP, UDP) 2.3. Protocoale de nivel de rețea (IPv4, IPv6, LowPAN) 2.4. Protocoale de straturi de legătură (Ethernet, WiFi, WiMax, celular) 2.5. Introducere în modulul RF 2.5.1. Tipuri de module RF 2.5.2. Protocoale wireless utilizate în modulele RF 2.5.2.1. Introducere în BLE 2.5.2.2. Introducere în ZigBee 2.6. Introducere în SDR 2.7. Extragerea datelor sensibile din Semnalele	4		
Curs 7 1. Probleme de securitate a stratului de aplicații IoT 1.1. Transport telemetrie de coadă de mesaje (MQTT) 1.2. Protocol de aplicare restricționat (CoAP) 1.3. Înțelegerea COAP cu Wireshark 1.4. HTTP, Web socket, DDS, AMQP 2. Standarde tehnologice IoT 2.1. Protocoale de comunicare cu fir (UART, USART, I2C, SPI, Ethernet, JTAG) 2.2. Protocoale de comunicare wireless (Bluetooth, Zigbee, 6lowPAN, WiFi, Z-wave)	4		

Curs 8 1. Atacuri și implementare 1.1. Riscul IoT 1.2. Exploatarea vulnerabilității 1.3. Atacuri de confidențialitate (Phishing, Pharming, deturnare DNS, Defacement, Eavesdropping, Spionaj Cyber) 1.4. Atacuri bazate pe web (malware, parolă, acces, inginerie socială, furt de date și identitate, recunoaștere) 2. Managementul identității și accesului 2.1. Managementul cheilor 3. Studii de caz și discuții 3.1. Case inteligente 3.2. Agricultură inteligentă 3.3. Furnizare inteligentă de vânzare cu amănuntul 3.4. Asistență medicală inteligentă 3.5. Retea inteligenta 3.6. Orașe inteligente	4		

Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziția studenților într-un număr de exemplare corespunzător)*

1. Lilya Budaghyan, Construction and Analysis of Cryptographic Functions, 2014, ISBN 978-3-319-12991-4
2. Kristian Beckers, Pattern and Security Requirements, 2015, ISBN 978-3-319-16664-3
3. KPMG International, Security and the IoT ecosystem, 2015
4. Shancang Li, Li Da Xu, Securing the Internet of Things, 2017, ISBN-13: 978-0128044582
5. Perry Lea, Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security, 2018, ISBN-13: 978-1788470599
6. European Research Cluster , Internet of Things: IoT Governance, Privacy and Security Issues"

8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Proiect 1 1. Introducere 1.1. Note introductive 1.2. Context 1.3. Structura laboratorului 1.4. Premise – cunoștințe de bază necesare 1.5. Lecții practice simple pentru premise 1.6. Discuție deschisă 2. Algoritmi de criptare: analiză și sisteme software 3. Generatoare de numere aleatoare 4. Criptarea cu cheie publică. Implementare algoritmi	4	Prelegere interactivă, brainstorming, învățare prin descoperire, învățare prin cooperare, argumentarea, învățarea în perechi, dezbaterea, exemplificare video	În caz de forță majora, cursurile se vor desfășura on-line pe platforma Teams
Proiect 2 1. Steganografia: analiza și aplicații 2. Standardul XML și criptarea cu chei asimetrice 3. Articol științific 3.1. Cerințe 3.2. Template IEEE 3.3. Sugerarea structurii articolului	4		
Proiect 3 1. SEcube 1.1. Ce este SEcube	4		

1.2. Use-cases 1.3. Prezentare hardware 1.4. Prezentarea generală a bibliotecilor 1.5. Setup 1.5.1. Exemple și analize de cod la nivel scăzut 2. Framework-ul Qt 3. SEfile exemple 4. SElink exemple 5. Construirea unei aplicații simple			
Proiect 4 1. Securizarea aplicațiilor Cloud utilizând SEcube 2. Securizarea protocoalelor de comunicare IoT utilizând SEcube și Raspberry Pi 3+	4		
Proiect 5 1. IP-core manager 1.1. Proiectare bazată pe FPGA utilizând SEcube	4		
Proiect 6 1. Penetration testing 1.1. Renunțarea la răspundere și cum să înveți în siguranță (bounty bug, capture the flag, hack the box) 1.2. Prezentarea fluxului de lucru (detaliat) 1.2.1. Colectarea de informații 1.2.2. Scanarea 1.2.3. Enumerarea 1.2.4. Exploatarea 1.2.5. Post-exploatare 1.2.6. Raportarea 1.3. Exemple 1.4. Crearea unei stații portabile de hacking 1.4.1. Instalarea Kali pe Raspberry Pi 1.4.2. Configurarea SSH pentru conectarea la Raspberry Pi de la distanță 1.4.3. Spargerea unei parole WI-FI, crearea unei rețele false, spionarea traficului unui dispozitiv 1.4.4. Monitorizarea unei rețele	4		
Proiect 7 1. Penetration testing 1.1. Website assessment OR Host assessment 1.2. Solving a Hack-the-box 2. Predarea articolului științific	3		
Proiect 8 1. Predare proiect	1		

Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenţilor într-un număr de exemplare corespunzător)*

1. Fei Hu, Security and Privacy in Internet of Things, 2016, ISBN-13: 978-1-4987-2319-0
2. Francis daCosta, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, 2013, ISBN: 978-1-4302-5740-0
3. Federal Trade Comission , Internet of Things: Privacy & Security in a Connected World, 2015
4. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 2014, ISBN-13: 978-1593275648
5. Wil Allsopp, Advanced Penetration Testing: Hacking the World's Most Secure Networks, 2017, ISBN-13: 978-1119367680
6. Aaron Guzman, IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, 2017, ISBN-13: 978-1787280571

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatorilor reprezentativi din domeniul aferent programului

- Securitatea digitală este o preocupare constantă în aproape toate sectoarele industriale,
- Cunoștințele de securitate digitală a informației sunt importante pentru toate componentele (software sau hardware) din domeniile IT&C.
- Conținutul disciplinei este în concordanță cu cel predat la alte centre universitare din țară și din străinătate;
- Pentru o mai bună adaptare a conținutului disciplinei la cerințele pieței muncii, au loc întâlniri cu reprezentanți ai angajatorilor;
- În dezvoltarea disciplinei s-au avut în vedere cele mai importante realizări teoretice și empirice în domeniu.

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Modul de analiză, sinteză și integrare a informației teoretice	Examen	50%
Laborator	Modul de analiză, sinteză și integrare a informației teoretice	Proiect	30%
	Rezolvarea problemelor corespunzătoare intalnirilor de proiect	Prezentarea rezolvărilor, răspunsuri la întrebări	5%
	Articol științific	1. Organizare - respectarea formatului și a structurii IEEE; concordanța și fluxul lucrării 2. Conținut - relevanța și acoperirea cuprinzătoare a subiectului abordat; aplicarea conceptelor prezentate la curs; reflectarea abilităților de gândire critică 3. Includerea a minim 6 referințe	15%

Standard minim de performanță:

- Participarea la sedințele de proiect și efectuarea tuturor temelor
- Condiții simultane, pentru promovarea examenului
  - Minim 5 puncte din examen
  - Minim 5 puncte din proiect + articol științific

Data completării:	Titulari	Titlu Prenume NUME	Semnătura
30.03.2023	Curs	Conf.dr.ing. Ovidiu Stan	
	Proiect	Conf.dr.ing. Ovidiu Stan	

Data avizării în Consiliul Departamentului Automatică _____	Director Departament Automatică Prof.dr.ing. Honoriu Vălean
Data aprobării în Consiliul Facultății Automatică și Calculatoare _____	Decan Prof.dr.ing. Liviu Miclea