EE5815: TOPICS IN SECURITY TECHNOLOGY

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Topics in Security Technology

Subject Code
EE - Electrical Engineering
Course Number
5815

Academic Unit
Electrical Engineering (EE)

College/School
College of Engineering (EG)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
Nil

Precursors
MA3150 Advanced Mathematical Analysis or MA3151 Advanced Engineering Mathematics

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

This course aims to provide students with an understanding of the principles of computer security technologies, including the principles of cryptography, side channel attacks forensics and securities for data, communications, cloud computing smart cards embedded systems and IoT.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify the conceptual difference between threats, vulnerabilities and attack.		x	x	
2	Recognize techniques and mechanisms for safeguarding an attack.		x	x	x
3	Identify the use of preventive and logistic techniques for safeguarding a computer system.		x	x	x
4	Describe the current techniques and anticipated trends in Internet security development, cloud computing security.		x	x	x
5	Analyse and explain various security issues in different embedded system & Internet technologies.		x	x	x

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	Students engage with concepts of the security theory and security protocol, cryptography.	1, 2, 3, 4, 5	24 hrs
2	Tutorial	Students develop security implementation examples, and cryptography examples.	1, 2, 3, 4	12 hrs (Some of the tutorials will be conducted in the laboratory)
3	Laboratory	Students work on hands-on example with smart-card systems and digital systems.	5	3 hrs

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Tests (min.: 2)	1, 2, 3, 4, 5	30	-	No
2	#Assignments (min.: 3)	1, 2, 3, 4, 5	10	-	Yes
3	Lab Exercises/ Reports	1, 2, 3, 4, 5	10	-	Yes

Continuous Assessment (%)

50

Examination (%)

50

Examination Duration (Hours)

2

Minimum Continuous Assessment Passing Requirement (%)

30

Minimum Examination Passing Requirement (%)

30

Additional Information for ATs

Remark:
To pass the course, students are required to achieve at least 30% in course work and 30% in the examination. Also, 75% laboratory attendance rate must be obtained.
may include homework, tutorial exercise, project/mini-project, presentation

Assessment Rubrics (AR)

Assessment Task

Examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Achievements in CILOs

Excellent

(A+, A, A-) High

Good

(B+, B, B-) Significant

Fair

(C+, C, C-) Moderate

Marginal

(D) Basic

Failure

(F) Not even reaching marginal level

Assessment Task

Coursework (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Achievements in CILOs

Excellent
(A+, A, A-) High

Good
(B+, B, B-) Significant

Fair
(C+, C, C-) Moderate

Marginal
(D) Basic

Failure
(F) Not even reaching marginal level

Assessment Task
Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Achievements in CILOs

Excellent
(A+, A, A-) High

Good
(B+, B) Medium

Marginal
(B-, C+, C) Low

Failure
(F) Not even reaching marginal level

Assessment Task
Coursework (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Achievements in CILOs

Excellent
(A+, A, A-) High

Good
(B+, B) Medium

Marginal
(B-, C+, C) Low

Failure

(F) Not even reaching marginal level

Additional Information for AR

Constructive Alignment with Programme Outcomes

PILO 1 - An ability to apply knowledge of engineering is appropriate to the degree discipline. Students will learn security techniques for enhancing the safety of computer, network and portable devices and apply these techniques to the solution of engineering problems in class.
PILO 2 - An ability to design and conduct experiments as well as to analyze and interpret data is appropriate to the degree discipline. Students will learn the programming techniques for smart card and analyze new security technologies.
PILO 3 - An ability to design a system, component, or process that conforms to a given specification within realistic constraints is appropriate to the degree discipline. Students will learn design a security system and learn the technique to analysis the risk of the designed system. They are required to work with the constraints specified in the environment including components, interconnectivity and network link.
PILO 4 - An ability to evaluate and formulate solutions to system security problems effectively and responsibly as a team member is appropriate to the degree discipline. Students will work in groups and split the work amongst them and coordinate the design into a workable system.
PILO 5 - An ability to conduct some research, identify, formulate and solve engineering problems is appropriate to the degree discipline. Students will integrate the smart card device and design appropriate software to solve the design/implementation/integration problems.
PILO 6 - An ability to communicate effectively is appropriate to the degree discipline. Students work in groups and they will practice the skill to communicate with each other to prepare the formal laboratory report.
PILO 7 - An ability to learn how to manage a team of technologists using necessary engineering tools is appropriate to the degree discipline. Students will be given a chance to present their work in class and collect feedbacks from other students

Part III Other Information

Keyword Syllabus

Threats to Computer Systems
Threats, Vulnerabilities and Attacks, System Security Engineering, Threat Trees, Categorization of Attacks, Trojan Horse and Viruses, Common Attack Methods.

Preventive Security Approaches
Auditing and Intrusion Detection, Identification and Authentication and Encryption.

Logistic Security Approaches
Key Management Protocols -, Access Control, Convert Channels, Composing Security, Privileges and Roles, Security Kernel.

Basic Cryptography
Classical Encryption Methods, Block Ciphers, Concepts in Number Theory and Finite Fields, Random Number Generation, Public-Key Cryptography (PKC), Advanced Encryption Standard (AES), Message Authentication Codes (MAC), Digital Signatures, Post-Quantum Cryptography, Lightweight Cryptography (LWC)

Computer Security Applications
Network Security Methods, Data Base Security Methods, Trusted Network Interpretations, WiFi and P2P security, Cloud Computing Security.

Card Security Applications
Smart Card ISO standards, Security Methods – encryption, key management and access control.

Embedded System & IoT Security Applications
Trustzone, Secure Boot Architecture, Trusted Execution Environment (TEE), Trusted Computing.

Reading List

Compulsory Readings

	Title
1	Cryptography and Network Security, 7 Edition, William Stallings, Pearson, 2017.

Additional Readings

	Title
1	Ross J. Anderson Security Engineering: A Guide to Building Dependable Distributed Systems (Wiley; 2 edition (April 14, 2008), ISBN-10: 0470068523)
2	William Stalling, Lawrie Brown, Computer Security: Principles and Practice (Prentice Hall, 2008 ISBN 0-13-600424-5)
3	William Stalling, Cryptography and Network Security (Prentice Hall, 2006 ISBN 0-13- 187316-4)
4	E. Amoroso: Cyber Security (Silicon Press 2006 ISBN 0929306384)
5	Matt Bishop Introduction to Computer Security (Addison-Wesley Professional 2005, ISBN 0-32-124744-
6	E. Amoroso: Fundamentals of Computer Security Technology (Prentice Hall, 1994, ISBN 0-13-108929-1)
7	J.A. Cooper: Computer and Communications Security (McGraw Hill, 1989, ISBN0-07-012926-6)
8	S.Muffic: Security Mechanisms for Computer Networks (John Wiley &Sons, 1989, ISBN 0-470-21387-6)
9	J.B. Grimson & H.J. Kugler: Computer Security: the practical issues in a troubled world (North Holland 1985, ISBN 0-444-87801-7)
10	http://csrc.nist.gov/publications/drafts/800-124/Draft-SP800-124.pdf DRAFT Guidelines on Cell Phone and PDA Security (National Institute of Standards and Technology Technology Administration U.S. Department of Commerce SP 800-124, Jul 2008)
11	http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf An Introduction to Computer Security: The NIST Handbook (National Institute of Standards and Technology Technology Administration U.S. Department of Commerce SP 800-12, Oct 1995)
12	https://csrc.nist.gov/projects/post-quantum-cryptography, Post-Quantum Cryptography PQC, NIST: National Institute of Standards and Technology