Subject Description Form

Subject Code	EIE553
Subject Title	Security in Data Communication
Credit Value	3
Level	5
Pre-requisite/ Co-requisite/ Exclusion	The students are expected to have some basic knowledge about TCP/IP such as addressing, routing, layering. Extra materials will be provided for self-review before the commencement of the course on request for those who do not have the appropriate knowledge. Please contact the subject lecturers for details.
Objectives	This subject aims at providing senior students, practicing engineers and information system professionals, who will study network security for the first time, a solid foundation about information security in the context of data communication and networking. After attending this course, the students will master the basic principles of network and information security. They will also learn to apply these principles in various scenarios. They will be able to identify security problems in the context of data communication, apply basic principles to design and evaluate solutions to meet different security requirements in networking and particularly Internet of things applications.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: **(1) Professional/academic knowledge and skills** a. Identify, formulate, and describe security issues and problems in the context of data communication. b. Understand and describe the basic theories and principles in network security. c. Analyze, design, and evaluate solutions to network security problems. **(2) Attributes for all-roundedness** d. Communicate effectively. e. Think critically and creatively. f. Assimilate new technological development in related field.
Subject Synopsis/ Indicative Syllabus	1. <u>Overview of Security Challenges in Data Communication</u> An introduction to the common security issues related to data communications, with identification on unique security characteristics of Internet of Things applications such as computational and power limits, system vulnerabilities, and high data volume. 2. <u>Applied Cryptography for Data Communication</u> Cryptographic tools for security models: cryptographic hash function for integrity, symmetric and asymmetric encryption for confidentiality, digital signature for authentication. 3. <u>Security Standards and Solutions for Data Communication</u> ISO 27001/2 and similar standards such as NIST SP 800, HIPAA, Public-Key Infrastructure (X.509), IP security (IPSec); firewall, virtual private network, authentication and access control. 4. <u>Case studies of Internet of Things Security Threats and Solutions</u> With a focus on the following Internet of Things technologies: Wi-Fi, Bluetooth, Low-power wide-area network, and 5G.

Teaching/Learning Methodology

Lectures and Tutorials are effective teaching methods:

1. To provide an overview of the subject contents.
2. To introduce, identify and describe common security issues in data communication.
3. To introduce the common approaches and solutions for ensuring data security.
4. To use feedbacks from students for gauging their progress

Assignments and Tests:

1. To supplement the teaching materials.
2. To foster a deeper understanding of the concepts.
3. To test the mastery of the subject matter by the students at different stages.

Case studies, lab sessions:

1. To ensure deep learning and real understanding of the students.
2. To cultivate students' problem-solving skills.
3. To foster deep understanding of the subject.

Teaching/Learning Methodology	Intended Subject Learning Outcomes					
	a	b	c	d	e	f
Lecture	✓	✓	✓		✓	✓
Tutorial	✓	✓	✓	✓	✓	✓
Test/Assignment	✓	✓	✓	✓	✓	
Case study, Labs				✓	✓	✓

Assessment Methods in Alignment with Intended Learning Outcomes

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed (Please tick as appropriate)					
		a	b	c	d	e	f
1. Assignments	10%	✓	✓	✓	✓	✓	
2. Tests	10%	✓	✓	✓	✓		
3. Laboratory demonstration and reports	15%	✓	✓	✓	✓		
4. Mini project	15%	✓	✓	✓	✓	✓	✓
5. Examination	50%	✓	✓	✓	✓	✓	
Total	100%						

Student Study Effort Expected

Class contact:	
▪ Lecture/Tutorial	27 Hrs.
▪ Laboratory	12 Hrs.
Other student study effort:	
▪ Lecture: further reading, doing homework/ assignment, preparing for tests, examination	36 Hrs.
▪ Writing laboratory reports	10 Hrs.
▪ Mini-project: studying, writing report, giving presentation	20 Hrs.
Total student study effort	105 Hrs.

Reading List and References	***Text Book:*** 1. Network Security Essentials: Applications and Standards (6th Edition) 6th Edition, William Stallings, Pearson, August 2016. ***General References and standards:*** 2. Network Security, André Perez, Wiley (DDA), Hoboken, N.J. : Wiley, 2014. (PolyU Library Acc. No.: TK5105.59 .P47 2014, online access available) 3. IPsec virtual private network fundamentals, James Henry Carmouche, Indianapolis, Ind.: Cisco Press, 2007. (PolyU Library Call Number: TK5105.567 .C37 2007). 4. Firewall policies and VPN configurations, Anne Henmi, technical editor; Mark Lucas, Abhishek Singh, Chris Cantrell, Rockland, Mass.: Syngress, 2006. (PolyU Library Call Number: TK5105.59 .F478 2006) 5. Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, Nitesh Dhanjani: O'Reilly Media; 1 edition, April 2015. 6. Practical Internet of Things Security, Brian Russell, and Drew Van Duren, Packt Publishing, June 2016. 7. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, Aaron Guzman and Aditya Gupta, Packt Publishing, November 2017. 8. Wireless Communications Security: Solutions for the Internet of Things, Jyrki T. J. Penttinen, John Wiley & Sons, 2017.

July 2019