Subject Description Form

Subject Code	EIE3129
Subject Title	IoT Security
Credit Value	3
Level	3
Pre-requisite/ Co-requisite/ Exclusion	Pre-requisite: EIE2113 Introduction to Internet of Things
Objectives	This subject aims at providing senior students with knowledge and skills in the latest developments in the security domain of Internet of Things (IoT). The topics to be covered include cryptographic foundations, wireless security, data security, and IoT system security. The subject will blend theory and practice. After attending this subject, the students will master the basic principles and skills of network and information security for IoT. They will also be able to identify security problems in the context of IoT, apply these principles and skills to design and evaluate solutions to meet different security requirements in IoT applications.
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Identify, formulate, and describe security issues and problems in the context of Internet of Things. 2. Understand and describe the basic theories and principles in IoT security. 3. Analyze, design, and evaluate solutions to IoT security problems. Category B: Attributes for all-roundedness 4. Communicate effectively. 5. Think critically and creatively. 6. Assimilate new technological development in related field.
Subject Synopsis/ Indicative Syllabus	1. Overview of Security Challenges in IoT An introduction to the common security issues in Internet of Things across its whole architecture, including perception layer, network layer, management layer, and application layer, with identification on unique security challenges of IoT systems such as computational and power limits, system vulnerabilities, and high data volume. 2. Applied Cryptography Cryptographic tools for security models: cryptographic hash function for integrity, symmetric and asymmetric encryption for confidentiality, digital signature for authentication. 3. Physical and Hardware Security Trust computing for IoT, such as root of trust and Trusted Platform Module); physical security attacks, side channel attacks, such as differential power analysis and timing attacks; firmware security. 4. Network and Wireless Security Public-Key Infrastructure (X.509), IP security (IPSec); firewall, virtual private network, authentication, and network access control, with a focus on the following wireless radio and communication technologies for IoT: Wi-Fi,

Bluetooth, Low-power wide-area network, 5G, and MQTT.

5. Data and Cloud Security Technologies
   key management, intrusion detection, access control, data anonymization, differential privacy, enterprise data protection

6. Internet of Things Security Standards and Case Studies
   ISO 27001/2 and similar standards such as NIST SP 800 and HIPAA; real-life security threats and solutions of IoT applications, such as smart home, smart grid, connected vehicle, wearable computing and mobile health care.

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 IoT.
3. To introduce the common approaches and solutions for ensuring security in IoT.
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.

Assessment Methods in Alignment with Intended Subject Learning Outcomes

Specific Assessment Methods/Tasks	**% Weighting**	**Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)**					
		1	**2**	**3**	**4**	**5**	**6**
1. Continuous Assessment							
• Assignments	10%	✓	✓	✓	✓	✓	
• Tests	10%	✓	✓	✓	✓		
• Laboratory demonstration and reports	15%	✓	✓	✓	✓		
• Mini project	15%	✓	✓	✓	✓	✓	✓
2. Examination	50%	✓	✓	✓	✓	✓	
Total	100%						

Explanation of the appropriateness of the assessment methods in assessing the intended learning outcomes:

The assessment methods above fully address the intended learning outcomes.

Specific Assessment Methods/Tasks	Remark
Mini project	Students need to think critically and creatively in order to come with a solution for a practical problem.
Test	Mainly objective quizzes conducted to measure the students' understanding of the theories and concepts as well as their comprehension of subject materials.
Examination and Assignment	Hands-on type problems that emulate real-life IoT security scenarios, which are used to evaluate students' ability in applying concepts and skills learnt in the classroom.
Laboratory demonstration and reports	Each student is required to produce a real-life demo and/or a written report to evaluate his/her technical knowledge and communication skills.

Student Study Effort Expected	**Class contact (time-tabled):**	
	• Lectures	24 Hours
	• Tutorial/Laboratory/Practice Classes	15 Hours
	Other student study effort:	
	• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes	24 Hours
	• Tutorial/Laboratory/Mini project: preview of materials, revision and/or reports writing	42 Hours
	Total student study effort:	**105 Hours**

Reading List and References	**Textbook:** 1. "Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem." Brian Russell, and Drew Van Duren. Packt Publishing; 2nd edition (November 30, 2018). **Reference Materials:** 1. "Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things." Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods, No Starch Press, Apr 2021. 2. "The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things." Aditya Gupta, Apress; 1st ed. edition (April 1, 2019). 3. "Hacking Connected Cars: Tactics, Techniques, and Procedures." Alissa Knight, Wiley; 1st edition (March 17, 2020). 4. "The IoT Architect's Guide to Attainable Security and Privacy." Damilare D. Fagbemi, David M Wheeler, and JC Wheeler, Auerbach Publications; 1st edition (October 4, 2019). 5. "IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security." Perry Lea, 2nd Edition, Packt Publishing (March 6, 2020).
Last Updated	October 2022
Prepared by	Dr. Haibo Hu