Subject Description Form

Subject Code	EIE4115
Subject Title	Intrusion Detection and Prevention
Credit Value	3
Level	4
Pre-requisite	For 42480: EIE3120 Network Technologies and Security For 42470: EIE4106 Network Management and Security
Co-requisite/ Exclusion	Nil
Objectives	1. To provide a solid foundation to the students in network security and intrusion detection and prevention 2. To enable the students to master the knowledge about intrusion detection and prevention in the context of real-life applications 3. To prepare the students for understanding, evaluating critically, and assimilating new knowledge and emerging technology in network security
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand the physical location, the operational characteristics and the various functions performed by the intrusion detection/prevention system 2. Describe how components in different layers inter-operate in the intrusion detection/prevention system 3. Understand the current and effective procedures to deal with network security threats 4. Learn new techniques and to align new security technologies to existing network infrastructure Category B: Attributes for all-roundedness 5. Present ideas and findings effectively 6. Learn independently
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Vulnerabilities and Security Threats to Computer Networks Sources of vulnerabilities, types of attacks, attacks against various security objectives, countermeasures of attacks. 2. Intrusion Detection and Prevention Technologies Host-based intrusion detection system (IDS) / intrusion prevention system (IPS), network-based IDS/IPS. Data collection for IDS/IPS. Intrusion detection techniques, misuse detection: pattern matching, rule-based and state-based; anomaly detection: statistical based, machine learning based, data mining based; hybrid detection. 3. IDS and IPS Architecture Tiered architectures, single-tiered, multi-tiered, peer-to-peer. Sensor: sensor functions, sensor deployment and security. Agents: agent functions, agent deployment and security. Manager component: manager functions, manager deployment and security. Information flow in IDS and IPS, defending IDS/IPS.

4. Alert Management and Correlation
Data fusion. Alert correlation, pre-process, correlation techniques, post-process, alert correlation architectures. Cooperative intrusion detection, cooperative discovery of intrusion chain, abstraction-based intrusion detection, interest-based communication and cooperation, agent-based cooperation.

5. Deployment of IDS/IPS
Case study on CISCO IDS and Snort.

Possible Laboratory Experiments:

1. Network monitoring
2. Protocol and traffic analysis
   Intrusion detection using Snort

Teaching/Learning Methodology

Teaching and Learning Method	**Intended Subject Learning Outcome**	**Remarks**
Lectures	1, 2, 3, 4	Fundamental principles and key concepts of the subject are delivered to students.
Tutorials	1, 2, 3, 4, 5, 6	Supplementary to lectures and are conducted with smaller class size; Students will be able to clarify concepts and to have a deeper understanding of the lecture material; Problems and application examples are given and discussed.
Laboratory sessions	5, 6	Students will conduct practical exercises in intrusion detection and prevention to reinforce concepts and techniques learned.

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	40%						
• Tests		✓	✓	✓	✓	✓	
• Assignments		✓	✓	✓	✓	✓	
• Laboratories				✓		✓	✓
2. Examination	60%	✓	✓	✓	✓	✓	
Total	100%						

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

Specific Assessment Methods/Tasks	Remark
Short quizzes	Mainly objective tests conducted to measure the students' understanding of the theories and concepts as well as their comprehension of subject materials
Assignments, tests and examination	End-of-chapter type problems used to evaluate students' ability in applying concepts and skills learnt in the classroom; Assignments of reading report type to assess students' ability in acquiring new knowledge related to computer networks; Students need to think critically and creatively in order to come with an alternate solution for an existing problem.
Laboratory sessions	Each group of students is required to produce a written report; Accuracy and the presentation of the report will be assessed; Oral examination based on the laboratory exercises will be conducted for each group member to evaluate his technical knowledge and communication skills.

Student Study Effort Expected	**Class contact (time-tabled):**	
	1. Lecture	24 Hours
	2. Tutorial/Laboratory/Practice Classes	15 Hours
	Other student study effort:	
	3. Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination	36 Hours
	4. Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing	30 Hours
	Total student study effort:	**105 Hours**

Reading List and References

Reference Books:

1. C. Endorf, E. Schultz and J. Mellander, *Intrusion Detection & Prevention,* McGraw-Hill/Osborne, 2004.
2. Ali A. Ghorbani, *Network intrusion detection and prevention concepts and techniques,* Springer, 2010.
3. J. M. Kizza, *Computer Network Security*, Springer, 2005.
4. D. Jacobson, *Introduction to Network Security*, CRC Press, 2009.

Last Updated	December 2016
Prepared by	Dr H. Hu