Applicable to 42480-2 and above Students

The Hong Kong Polytechnic University
Department of Electronic and Information Engineering

Minor Changes to the BSc(Hons) in Information Security (42480) (BSc in INS) Programme Curriculum

1. Adding an elective subject "EIE4121 Machine Learning for Cyber-security" to the BSc in INS Curriculum

Machine learning techniques have become popular in many different fields. In recent years, machine learning techniques have been applied to cyber-security tasks. There is a growing trend of using these techniques to cyber-security tasks such as application and endpoint security. Currently, the BSc in INS programme does not offer any subject that covers machine learning techniques in cyber-security. It is beneficial to students to learn these techniques and develop skills to apply these techniques to solve various problems in cyber-security.

Besides, during the student feedback collection exercise in 2018/19 Semester 2, the Department sought students' views on the area(s) of subject(s) they preferred if the Department had resources to offer new technical elective subjects for the undergraduate degree programmes it offered. Most students who had given comments preferred new subjects in the areas of Artificial Intelligence, Big Data and Machine Learning. The Department considered that a new subject in the field of Machine Learning could be offered to cater to students' interests and respond to the Departmental Review panel members' suggestions.

The Department therefore introduces a new 3-credit subject "EIE4121 Machine Learning in Cyber-security" (Appendix I) to the BSc in INS programme as a technical elective subject. This subject intends to introduce concepts about machine learning techniques in cyber-security to students and develop students' skills of using recent techniques for solving practical problems in cyber-security. Topics such as machines learning techniques, machine learning development environments, malware analysis, phishing detection and anomaly detection will be covered in this subject.

Adding EIE4121 to the curriculum provides BSc in INS students with more choices of elective subjects. Currently, students of the BSc in INS programme are required to select any two subjects from among the pool of five elective subjects offered by the COMP Department, and another two subjects from among the pool of three elective subjects offered by the EIE Department. This arrangement will expand the elective subject choices of students as they now have one more EIE elective subjects to choose from.

Such change will be applicable to all students of the BSc in INS programme with effect from 2019/20 Semester 2.

2. Removing "COMP4435 Dependable Computing" from and Adding "COMP4334 Principles and Practice of Internet Security" to the BSc in INS Curriculum

The undergraduate degree programmes offered by the Department of Computing (COMP) have gone through a revamping recently and some of the COMP subjects would be phased out effective from 2019/20 academic year. Among them, "COMP4435 Dependable Computing", which is a 3-credit elective subject offered in Year 2 of the BSc in INS programme, will cease to be offered by the COMP Department from 2019/20 academic year. COMP4435 has thus been removed from the BSc in INS (42480) programme with effect from 2019/20 academic year.

After considering the knowledge and skills that may be of interest to BSc in INS students as well as reviewing the subjects on offer by the COMP Department, the EIE and COMP Departments have identified the 3-credit subject, "COMP4334 Principles and Practice of Internet Security" (Appendix II), as an appropriate replacement for COMP4435. COMP4334 aims to equip students with a foundational understanding of the threats to the Internet infrastructure. Students will be equipped to: (i) understand the practical principles, models, cryptographic methods for protecting Internet from various forms of attacks; (ii) understand the major security issues and problems in the TCP/IP protocol suite and the lower layers, and the countermeasures to mitigate the corresponding attacks; and (iii) acquire practical skills in using various tools and resources to analyze the security of Internet protocols.

Such changes, i.e. removing the 3-credit elective subject "COMP4435 Dependable Computing" from and adding the 3-credit subject "COMP4334 Principles and Practice of Internet Security" to the BSc in INS (42480) programme curriculum as an elective subject, are applicable to all students of the BSc in INS programme with effect from 2019/20 academic year. According to the subject offering schedule of the COMP Department, COMP4334 will be offered in 2019/20 Semester 2.

Subject Description Form

Subject Code	EIE4121
Subject Title	Machine Learning in Cyber-security
Credit Value	3
Level	4
Pre-requisite	Nil
Co-requisite/ Exclusion	Nil
Objectives	1. To introduce concepts about machine learning techniques in cyber-security 2. To develop skills of using recent techniques for solving practical problems in cyber-security
Intended Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Understand different machine learning techniques 2. Use different techniques for solving problems in cyber security Category B: Attributes for all-roundedness 3. Present ideas and findings effectively
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Machine learning techniques Introduction to machine learning; Basic concepts and classification; Supervised learning and unsupervised learning; classification; clustering; Neural Networks; Support vector machines; Dimensionality reduction; Deep learning 2. Machine learning development environments Software tools for implementing machine learning techniques; Generalization performance; Issues of over-fitting. 3. Malware Analysis Introduction to malware analysis; Types of malware analysis; static analysis, dynamic analysis; Behavioral vs code analysis; Use of machine learning techniques for malware detection such as K-Means, support vector machines, convolutional neural networks. 4. Phishing detection Introduction to phishing detection; Analysis of email/websites/message features for phishing characterization; Use of techniques such as logistic regression and decision tree for phishing detection. 5. Anomaly Detection Introduction to the anomaly definition; overview of anomaly detection techniques; static rules technique; use of machine learning techniques such as autoencoder for anomaly detection. **Laboratory Experiments:** Practical Works: 1. Evaluation of machine learning techniques in malware detection 2. Evaluation of machine learning techniques in phishing detection Forensic analysis of digital evidence.

Teaching/Learning Methodology

Teaching and Learning Method	Intended Subject Learning Outcome	Remarks
Lectures	1, 2	Fundamental principles and key concepts of the subject are delivered to students.
Tutorials	1, 2	Supplementary to lectures; 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	2, 3	Students will evaluate different kinds of machine learning techniques.
Mini-project	1, 2, 3	Students are required to study the use of machine learning techniques in cyber-security application. Students will need to submit a written report and make a presentation.

Assessment Methods in Alignment with Intended Learning Outcomes

Specific Assessment Methods/Tasks	% Weighting	Intended Subject Learning Outcomes to be Assessed (Please tick as appropriate)		
		1	2	3
1. Continuous Assessment (total 50%)				
• Tests	17%	√	√	
• Short quizzes	10%	√	√	
• Laboratory sessions	5%		√	√
• Mini-project	18%		√	√
2. Examination	50%	√	√	
Total	100%			

The continuous assessment consists of tests, short quizzes, laboratory exercises and a mini-project.

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

Specific Assessment Methods/Tasks	Remark
Short quizzes	These can measure students' understanding of the theories and concepts as well as their comprehension of subject materials.
Tests and examination	end-of chapter type problems used to evaluate students' ability in applying concepts and skills learnt in the classroom; students need to think critically in order to come with a solution for a problem.
Laboratory sessions, mini-project	oral examination will be conducted to evaluate student's technical knowledge and communication skills.

Student Study Effort Expected	**Class contact (time-tabled):**	
	• Lecture	24 Hours
	• Tutorial/Laboratory/Practice Classes	15 Hours
	Other student study effort:	
	• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination	26 Hours
	• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing	40 Hours
	Total student study effort:	**105 Hours**
Reading List and References	1. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, Chapman and Hall/CRC, 2017. 2. Chiheb Chebbi, Mastering Machine Learning for Penetration Testing, Packt Publishing Ltd, 2018. 3. Sumeet Dua and Xian Du, Data Mining and Machine Learning in Cybersecurity, Auerbach Publications, 2011. 4. Monnappa K A, Learning Malware Analysis, Packt Publishing Ltd, 2018. 5. Dipanjan Sarkar, Raghav Bali and Tushar Sharma, Practical Machine Learning with Python, Apress, 2018.	
Last Updated	1 Feb 2019	
Prepared by	Bonnie Law	

Subject Description Form

Subject Code	COMP4334
Subject Title	Principles and Practice of Internet Security
Credit Value	3
Level	4
Pre-requisite / Co-requisite / Exclusion	**Pre-requisite:** COMP3334
Objectives	To equip students with a foundational understanding of the threats to the Internet infrastructure. Students will be equipped to: 1. Understand the practical principles, models, cryptographic methods for protecting Internet from various forms of attacks; 2. Understand the major security issues and problems in the TCP/IP protocol suite and the lower layers, and the countermeasures to mitigate the corresponding attacks; and 3. Acquire practical skills in using various tools and resources to analyze the security of Internet protocols.
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Acquire a foundational understanding of the three cryptographic primitives: secret-key encryption, public-key encryption, and one-way hash functions; 2. Understand the major security issues in implementing the four major security functions: secrecy, identity authentication, message authentication, and nonrepudiation; 3. Understand the major security issues and problems in the TCP/IP protocol suite and the lower layers, and the countermeasures to mitigate the corresponding attacks; 4. Acquire practical skills, such as setting up a secure private network using firewalls, secure tunnels, and end-to-end secure applications, implementing and/or integrating security functions, and assessment of system security; and 5. Understand the major threats to the Internet-wide security today, such as denial- of-service attacks and DNS insecurity. Category B: Attributes for all-roundedness 6. Acquire critical and independent analytical skills in the process of analyzing the security problems in the Internet; and 7. Acquire the skill of synthesizing various security problems into a small set of fundamental security issues and solutions.
Subject Synopsis/ Indicative Syllabus	**Topic** **1. Overview** Types of attacks; threat models; the role of cryptography in network security. **2. Cryptographic Functions and Services**

Symmetric encryption, block cipher; hash functions; message authentication codes; public-key encryption, digital signatures, and authentication protocols.

3. **IP and Link-Layer Security**
   IP security and Internet key exchange protocols; routing security; wireless network security.

4. **End-to-End Security**
   TCP security; Secure Socket Layer; examples of secure application protocols; e.g., Secure Shell, Kerberos, and Pretty Good Privacy.

5. **Other Topics**
   DNS security, denial-of-service attacks, botnet, firewalls and intrusion detection/prevention systems.

Workshops:

A series of workshops on Web security will be given to let students acquire practical experience.

Teaching/Learning Methodology

The course will emphasize on both the principles and practices of network and system security. The principles will be covered mainly through the lectures and problem-solving activities in the tutorials, whereas the practice aspects will be taught through a series of workshops on Web security which are designed to reinforce what has been taught in the lectures and to help students acquire practical skills and group projects.

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**	**7**
Continuous Assessment	**60%**							
1. Assignments	25%	✓	✓	✓		✓	✓	✓
2. Workshops	10%				✓			
3. Project	25%				✓	✓	✓	✓
Examination	**40%**	✓	✓	✓		✓	✓	✓
Total	100%							

The examination and assignments are designed to evaluate the students' understanding on the principles undergirding the network and system security. The workshops on Web security and group projects, on the other hand, are designed to evaluate the students' practical skills on solving Internet security problems.

Student Study Effort Expected

Class contact:	
• Lecture	39 Hours
• Tutorials/Workshops	0 Hours
Other student study effort:	
• Self-study (around 7 hours per week)	94 Hours

	Total student study effort	**133 Hours**
Reading List and References	**Textbooks:** 1. Stallings, William*, Cryptography and Network Security: Principles and Practice*, 6th Edition, Pearson, 2013. **Reference Books:** 1. Anderson, Ross J., *Security Engineering*, 2nd Edition, Wiley, 2008. 2. Kaufman, Charlie, Perlman, Radia and Speciner, Mike, *Network Security: Private Communication in a Public World*, 2nd Edition, Prentice Hall PTR 2003. 3. Zwicky, Elizabeth D., Cooper, Simon and Chapman, D. Brent, *Building Internet Firewalls,* 2nd Edition, O'Reilly & Associates, 2000. 4. Cheswick, William and Bellovin, Steven M., *Firewalls and Internet Security*, 2nd Edition, Addison Wesley, 2003. 5. Schneier, Bruce, *Applied Cryptography*, 2nd Edition, Wiley, 1996. 6. Schneier, Bruce, *Secrets and Lies*, Wiley, 2000. 7. Young, Adam and Yung, Moti, *Malicious Cryptography*, Wiley, 2004. 8. Stinson, Douglas R., *Cryptography: Theory and Practice*, 3rd Edition, Chapman and Hall/CRC, 2006. 9. Forouzan, Behrouz A., *Cryptography and Network Security*, McGraw-Hill, 2008. *10.* Boyd, Colin and Mathuria, Anish*, Protocols for Authentication and Key Establishment,* Springer, 2003.	
Last Updated	Dec 2018	
Prepared by	COMP Department	