Subject Description Form

Subject Code	EIE3130
Subject Title	Network Security
Credit Value	3
Level	3
Pre-requisite/ Co-requisite/ Exclusion	Pre-requisite: EIE3333 Data and Computer Communication
Objectives	This course aims to train students to master basic network security knowledge and skills. They will learn how to apply security services of confidentiality, integrity, availability and authentication in various scenarios. They also need to design solutions for network management and solve security problems using the software tools.
Intended Subject Learning Outcomes	**Upon completion of the subject, students will be able to:** Category A: Professional/academic knowledge and skills 1. Describe common security issues arising from the use of telecommunication and data networks for the transmission of information; 2. Analyse a network security problem and identify and define the requirements appropriate to its solution; 3. Identify and solve network security problems by applying knowledge learnt and by using appropriate tools and techniques; 4. Use current techniques, skills, and tools necessary for the practices in network security with an understanding of the limitations. Category B: Attributes for all-roundedness 5. Function effectively on teams to accomplish a common goal; 6. Communicate effectively and understand the importance of life-learning as well as continual professional development.
Subject Synopsis/ Indicative Syllabus	**Syllabus:** 1. Introduction to basic network technologies and components 1.1 Computer security objectives, security services and mechanisms 1.2 X.800 classifies security attacks 1.3 Network and cryptography basics 1.4 Introduction to Public and Private key encryption 1.5 Security at the transport layer 1.6 Understanding the operations of secure sockets layer (SSL) and secure shell (SSH)/Open SSH 1.7 Basic secure design principles 2. Network threats and mechanisms 2.1 Vulnerabilities and attacks of internet protocols 2.2 Review the IP protocol, TCP functions, data formats and basic security problems 2.3 The concepts of DNS lookup, DNS caching and DNS packet formats 2.4 IP spoofing mechanisms, DNS cache poisoning and DNS rebinding attack 2.5 Denial-of-Service (DoS) vulnerability and DoS at SSL handshake 2.6 The concepts of SYN cookies 3. Network security applications and services 3.1 Introduction to IP security using AH, ESP and IKE 3.2 Symmetric key distribution and user authentication 3.3 Public key certification and public key infrastructure (X.509) 3.4 Introduction to firewalls and packet filtering principle 3.5 Federated identity management 4. Web application security and web tracking 4.1 Introduction to web threat models 4.2 Same origin policy (SOP) for document object model (DOM) and cookies 4.3 Cross-site scripting (CSS) and cross-site request forgery (CSRF)

4.4 Third-party tracking techniques; cookie syncing; sticky tracking and fingerprinting in web browsers
4.5 The concepts of “Do Not Track” (DNT)
4.6 Single Sign-on (SSO)
4.7 Security Assertion Markup Language (SAML) for web SSO

5. Network access control and cloud security
   5.1 Introduction to network access control system using EAP
   5.2 Cloud service models: IaaS, PaaS and SaaS
   5.3 The basic concepts of data encryption and crypto management in cloud environment
   5.4 Access control tokens
6. Network management
   6.1 Factors in network management and simple network management protocols (SNMP)
   6.2 Management information base (MIB) concepts and usages

Laboratory Experiments:

1. Linux firewall/pfSense firewall
2. SSH key authentication
3. IPsec configuration and usages

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 and to be supplemented with interactive discussion, self-learning videos and website information.
Tutorials	1, 2, 3, 4, 5, 6	Students will be able to clarify concepts and to have a deeper understanding of the lecture materials; practical exercises and Q&A will be provided to strengthen students’ understanding about taught materials.
Laboratory	3, 4, 5, 6	Students will perform hands-on tasks to practice what they have learned. They will analyse network security issues, ethical hacking and implementing security mechanisms.
Quizzes/Tests	1, 2	Students require to solve network security problems within a specific time and without access to other materials.
Case studies project	1, 2, 3, 4, 5, 6	Students will be able to design and solve a real-life security issue through hands-on activities.

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**
Continuous Assessment (total 100%)							
• Tutorials	15%	√	√	√	√	√	√
• Lab works/reports	25%			√	√	√	√
• Quizzes/Tests	32%	√	√				
• Case study project (Peer-review, presentation, and report)	28%	√	√	√	√	√	√
Total	100%						

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

Specific Assessment Methods/Tasks	Remark
Laboratory sessions and lab reports	Students are required to complete three hands-on activities such as setting up a firewall, generate the SSH keys and configure the IPsec on Windows/Linux and analyse network packets during the lab sessions. They are also required to write reports to explain the network security issues and describe the network packets passing. Students will be accessed based on (1) their ability to apply the knowledge that they learn in classes to deal with network security issues and (2) their ability to write a clear report that explains the principle of operation and architecture of the network security environment that they have created.
Quizzes/Tests	Quizzes/Tests are given to students to assess their competence level of knowledge and comprehension and their ability to apply knowledge within a specific time and without access to other materials. This is a good way to assess students' mastery of knowledge and understanding.
Case study project	Case studies will be used to enable students to probe into a real-life security issue deeply through extensive hands-on activities, readings and research. Students communication skills and function effectively on teams will also be cultivated with project demonstration, peer-review, presentation and report writing.

Student Study Effort Expected	**Class contact (time-tabled):**	
	• Lectures	21 Hours
	• Tutorial/Laboratory/Practice Classes	18 Hours
	Other student study effort:	
	• Lecture: preview/review of notes; homework/assignment; preparation for tests/quizzes	30 Hours
	• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing, presentation and peer-review	36 Hours
	Total student study effort:	**105 Hours**

Reading List and References

A set of comprehensive lecture notes will be provided to students for the study of this subject, together with tutorial materials and laboratory hand-outs. Students may refer to the following suggested reading lists for more in-depth and extensive discussion of topics covered and end-of chapter problem sets (when applicable):

Reference Books:

1. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody, Software-Defined Networking and Security 1st Edition, c2021.
2. J. Michael Stewart, Denise Kinsey, Network Security, Firewalls, and VPNs (Issa) 3rd Edition, c2020.
3. Russell Scott, Computer Networking Beginners Guide: An Easy Approach to Learning Wireless Technology, Social Engineering, Security and Hacking Network, Communications Systems, c2020.
4. Quinn Kiser, Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering, c2020.
5. Ben Malisow, CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide & Practice Tests Bundle 2nd Edition, c2020.
6. Mark Ciampa, CompTIA Security+ Guide to Network Security Fundamentals (MindTap Course List) 7th Edition, c2020.

	7. Ian Neil, CompTIA security+ certification guide: master IT security essentials and exam topics for CompTIA security+ SY0-501 certification, Birmingham: Packt Publishing 2018, (eBook, online access) 8. Manuj Aggarwal, Network Security with pfSense: Architect, deploy, and operate enterprise-grade firewalls, c2018. 9. Stallings, William, Cryptography and Network Security: Principles and Practice (7th Edition): Pearson, c2016. **Classics Materials:** 1. ITU-T Recommendation X.800 Data Communication Networks: Open System Interconnection (OSI); Security, Structure and Applications, ITU-T CCITT, Geneva, 1991 (PDF version available from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-I!!PDF-E&type=items) 2. "Communication theory of secrecy systems" in Claude Elwood Shannon: collected papers, Shannon, Claude Elwood, 1916-2001, New York: Institute of Electrical and Electronics Engineers, c1993., PolyU Lib. Acc. No.: TK5101 .S448 1993, (p.84-143)
Last Updated	October 2022
Prepared by	Dr Doris Lin