Subject Description Form

Subject Code	EIE3120
Subject Title	Network Technologies and Security
Credit Value	3
Level	3
Pre-requisite	The students are expected to possess basic knowledge about network protocols (Ethernet and TCP/IP) and cryptography (public-key and private-key encryption, hash function, digital signature).
Co-requisite/ Exclusion	Nil
Objectives	This subject teaches students the features and technologies about public and private telecommunication and data networks for the provision of security services of confidentiality, integrity, availability, and authentication.
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. Describe methods for dealing with security issues as described in (1) 3. Identify and solve network security problems by applying knowledge learnt and by using appropriate tools and techniques 4. Communicate effectively and understand the importance of life-learning as well as continual professional development
Subject Synopsis/ Indicative Syllabus	**Syllabus:** **Fundamentals:** 1. Basic network technologies and components: Internet, Ethernet, VPN, hub, switch, router, network layer protocols (IP, ICMP, DHCP, NAT), transport layer protocols (TCP, UDP) 2. The network security model, services, mechanisms, and threats: authentication, key exchange, access control, data confidentiality, data integrity, availability, eavesdropping, DOS (denial-of-service), application layer security **Applications:** 3. Authentication and Key Distribution for protected communication: Kerberos, X.509, Public Key Infrastructure, Certification Authority 4. Firewalls: packet filtering, application-level gateway, encrypted tunnels 5. Internet Protocol Security: ESP and IKE 6. Transport layer security: Secure Sockets Layer (SSL) and Transport Layer Security (TLS), SSH

Teaching/Learning Methodology

Assessment Method	Intended Subject Learning Outcomes	Descriptions/Remarks
Lectures	1, 2, 4	Lectures will be used as the main instruction mechanism, to be supplemented with interactive discussion, multimedia (video, edX, website information), and presentation materials.
Tutorials/Practical Works	1, 2, 3, 4	The tutorials require students to apply learned knowledge in different scenarios.
Laboratory	2,3	Students are required to identify and solve network security problems by applying knowledge learnt and by using appropriate tools and techniques.
Case Study Project	1, 2, 3, 4	Students are required to set up the company network and describe the common security issues arising from SME and data networks. They need to identify and solve the network security problems by applying knowledge learnt and using appropriate tools and techniques in the demonstration.

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
1. Continuous Assessment	50%				
• Case Study Project	25%	√	√	√	√
• Laboratory	10%		√	√	
• Tutorials	5%	√	√	√	√
• Test	10%	√	√		√
2. Examination	50%	√	√	√	√
Total	100%				

The continuous assessment consists of laboratory reports, project report and test.

<table>
<tr><td rowspan="6">Student Study Effort Expected</td><td colspan="2">Class contact (time-tabled):</td></tr>
<tr><td>• Lecture</td><td>21 Hours</td></tr>
<tr><td>• Tutorial/Laboratory/Practice Classes</td><td>18 Hours</td></tr>
<tr><td colspan="2">Other student study effort:</td></tr>
<tr><td>• Lecture: preview/review of notes; homework/assignment; preparation for test/quizzes/examination</td><td>30 Hours</td></tr>
<tr><td>• Tutorial/Laboratory/Practice Classes: preview of materials, revision and/or reports writing</td><td>36 Hours</td></tr>
<tr><td colspan="2">Total student study effort:</td><td>105 Hours</td></tr>
<tr><td>Reading List and References</td><td colspan="2">Reference Books:

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

1. Stewart, J., & Kinsey, D., Network security, firewalls, and VPNs (Third ed., Jones & Bartlett Learning information systems security & assurance series). Burlington, MA: Jones and Bartlett Learning, ISBN: 9781284183696, c2021.
2. Fiedelholtz, The Cyber Security Network Guide (Vol. 274, Studies in Systems, Decision and Control). Cham: Springer International Publishing AG, (online access from PolyU Library), ISBN: 3030615901, ISBN: 9783030615901, c2020.
3. Stallings, W., Cryptography and network security: Principles and Practice (Seventh ed.). Hoboken, New Jersey: Pearson, c2017. ISBN: 0134444280.
4. Stallings, William, Upper Saddle River, Network security essentials: applications and standards, 5th ed., N.J.: Pearson Education, c2014.
5. Jacobs, Stuart, Books24x7. ; Wiley (DDA)_d., Hoboken, N.J. : John Wiley & Sons; Piscataway, Security management of next generation telecommunications networks and services, NJ: IEEE Press, c2014.

Classics reading materials:
6. 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 http://www.itu.int/rec/T-REC-X.800-199103-I/e)
7. “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)</td></tr>
<tr><td>Last Updated</td><td colspan="2">June 2022</td></tr>
<tr><td>Prepared by</td><td colspan="2">Dr Doris Lin</td></tr>
</table>