Subject Description Form

Subject Code	EIE1D04 (CAR STE Subject)
Subject Title	Cyber Security Essentials
Credit Value	3
Level	1
Pre-requisite /Co-requisite/ Exclusion	NIL
Objectives	This course aims at inspiring students to understand the basic principles, knowledge, andskills about the secure use of IT in daily life. The cybercrime in business scale is universal, and the internet is a platform for e-businessand m-business, the context of information security has begun to gain increased attention,notably where the use of security technologies has failed to protect companies from cyberattacks (Anwar et al., 2016). The role a human plays in cybersecurity is essential, and most research has found that human consistently underestimated the probability of falling victim to a cybersecurity breach (Herath and Rao, 2009b). The issues on safe dataand information below, 1. Cyber security is essential in business as most businesses now turn into online form. 2. Cyber security is essential in day-to-day operations such as e-health, e-government, e-payment, an online teaching. 3. Data security and privacy is an essential need for human rights. The course will introduce symmetric encryption (e.g., DES/AES), asymmetric encryption (e.g., RSA/Elliptic-curve), key exchange (Diffie-Hellman), and cryptographic hash (e.g.,MD5/SHA1/SHA2). They will use relevant techniques and applications to apply in a secure network connection, use the computer and Internet securely, and manage information appropriately.
Intended Learning Outcomes	**Upon completion of the subject, students will be able to:** **<u>Category A: Professional/academic knowledge and skills</u>** 1. Understand the essential security concepts about the importance of secure information and data and identify various forms of attacks. 2. Understand the security issues related to communications including e-mail andinstant messaging. 3. Describe common web security problems arising from the use of the Internet for thetransmission of information. 4. Analyze a computer, device or network from malware and unauthorized access. 5. Analyze the local and global impact of cyber security on individuals, organizations,and society. 6. Identify and solve network security problems by applying knowledge learned and byusing appropriate tools and techniques. 7. Explore the real-life security issues, including security policy, recent security incident, security product, and an international standard or request for comments. **<u>Category B: Attributes for all-roundedness</u>** 8. Think critically, and understand social responsibility and ethics. 9. Acquire critical and independent analytical skills in the process of analyzing thesecurity problems. 10. Write and read English effectively.

Subject Synopsis/ Indicative Syllabus	1. Security Concepts Overview Difference types of attacks; the reasons for protecting the personal information and commercially sensitive information; the types of encryptions; the advantages and limitations of encryption such as symmetric key and asymmetric key; 2. Security for Malware and Wearable Devices Definition and function of malware; types of malware; mobile malware; app security; Android/iOS security model; how anti-virus software works and its limitations; 3. Network Security Difference types of network; the function and limitations of a firewall; Different types of wireless security (i.e. WEP and WPA2); access control; 4. Web Security Digital certificate; one-time password; appropriate settings of cookies; protect private data in browsers; types of content-control software 5. Communications Encrypting and decrypting an e-mail; digital signature; unsolicited e-mail; phishing; backdoor access in instant messaging 6. Secure Data Management Physical security; backup procedures; data destruction utilities
Teaching/Learning Methodology	**Lecture:** Lectures will use as the primary instruction mechanism. An interactive discussion is supplemented instruction (i.e. live group discussion/presentation and online group assessments), multimedia (integrate some videos, edX course(s), games, website information) presentation materials. **Tutorial/Practical Exercise Demo:** Tutorials will be used for strengthening students' understanding of taught materials through online tests/quizzes, in-class practical exercises, further reading, peer learning groups, and discussions. **Analytical Essay and Reading Presentation:** Case studies will be used to enable students to probe into a real-life security issue deeply through extensive readings with 100,000 words or 200 pages, it contains 10% of the reading presentation and research. The student needs to read a comprehensive document on one of the following cyber-security fields: (1) a security policy document for a business/company/organization, (2) a comprehensive analysis on a recent security incident, (3) a comprehensive datasheet or manual on a security product (e.g., a software/hardware or a service), and (4) a snippet of an international standard or request for comments (RFC). The student will learn security services and mechanisms, authentication protocols, digital signature, public key infrastructure and firewall set up in the case study assignment. The student applies what they have learnt to solve the network security problems, and student needs to write a analytical essay of 1,500 to 2500 words in English on recent advances in cyber security and/or data security or privacy.

Assessment Methods inAlignment with Intended Learning Outcomes

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to beassessed (Please tick as appropriate)									
		1	2	3	4	5	6	7	8	9	10
1.Continuous Assessment	100%										
Analytical Essay	40%	✓		✓	✓	✓	✓	✓	✓	✓	✓
Reading Presentation	10%	✓		✓	✓	✓	✓	✓	✓	✓	✓
Tutorials/Practical Exercise with Demonstrations	15%	✓	✓	✓	✓		✓			✓	
Tests (with short questions)	20%	✓	✓	✓	✓		✓		✓		✓
Quizzes	15%	✓	✓	✓	✓		✓		✓		
Total	100 %										

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

Essay, reading presentation and tutorials/exercises require students to apply what they have learned to solve problems. They are required to evaluate the recent incidents on the security breach, writea analytical essay between 1,500 to 2,500 words on recent advances in cyber security and/or data security or privacy (**with 10% of this essay contributed by ELC and student must obtain a D or above on the writing assignment to pass the subject**). The student needs to read around 100,000 words or 200 pages of the comprehensive document on one of the following cyber-security fields: (1) a security policy document for a business/company/organization, (2) a comprehensive analysis on a recent security incident, (3) a comprehensive datasheet or manual on a security product (e.g., a software/hardware or a service), and (4) a snippet of an international standard or requestfor comments (RFC).

Tests and quizzes require students to solve security problems within a specific time and without access to other materials. This is a good way to assess students' masteryof knowledge and understanding. The two quizzes cover some materials and the format includes MC and fill-in the blank or multiple blanks. The two tests cover all materials taught in the course, and the format includes short questions.

Student Study Effort Expected

Class contact:	
• Lecture	22 Hours
• Tutorials/Seminars/Practical Classes	15 Hours
Other student study effort:	
• Lecture: preview/review of notes; homework/assignment; preparation for tests/quizzes	36 Hours
• Tutorial/Practice Classes: preview of materials, revisionand/or reports writing	32 Hours
The total student study effort:	**105 Hours**

Reading List and References

Reading Presentation

The student needs to select one of the following cyber-security fields for reading presentation. The following are the reading references for each field:

(1) A security policy document for a business/company/organization

a. Fiedelholtz. (2020). 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.

b. Fiedelholtz, G. (2021). The cyber security network guide (Studies in systems, decision and control; v. 274). Cham: Springer, (online access from PolyU Library), ISBN: 9783030615918, ISBN: 303061591X.

c. Johnson, Easttom, & Easttom, Chuck. (2022). Security policies and implementation issues (Third ed., Jones & Bartlett Learning information systems security & assurance series). Burlington, MA: Jones & Bartlett Learning, (online access from PolyU Library), ISBN: 9781284199925.

d. Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. IEEE Transactions on Engineering Management, 68(1), 87-100, (online access from PolyU Library), ISSN: 0018-9391, EISSN: 1558-0040, DOI: 10.1109/TEM.2020.2977815

e. Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System Security Management Based on ISO 27001 Guidelines (1st ed. 2020, ed.). Berkeley, CA: A press: Imprint: A press, (online access from PolyU Library), ISSN: 0018-9391, EISSN: 1558-0040, DOI: 10.1109/TEM.2020.2977815.

(2) A comprehensive analysis of a recent security incident

a. Danda B. Rawat, Bhed B. Bista, Gongjun Yan. (2014). Security, privacy, trust, and resource management in mobile and wireless communications, Hershey, PA: Information Science Reference (chapter 9 to chapter 13 (mobile network and wireless communications)), (chapter 11 to chapter 13, chapter 16 to chapter 18, and chapter 19 tochapter 20 (cloud and mobile communications and wireless network management)) (eBook, online access)
(No. of pages required: 260 pages)

b. Ozkaya, E. (2021). Incident Response in the Age of Cloud. Birmingham: Packt Publishing, Limited, (online access from PolyU Library), ISBN: 9781800569218, ISBN: 180056921.

c. Birch, M. (2022). CompTIA CASP CAS-004 Certification Guide. Birmingham: Packt Publishing, Limited, (online access from PolyU Library), EISBN: 9781801814485, EISBN: 180181448.

(3) A comprehensive datasheet or manual on a security product

a. Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. Journal of Cloud Computing, 10(1), 1-34, (online access from PolyU Library), ISSN: 2192-113X, EISSN: 2192-113X, DOI: 10.1186/s13677-021-00247-5.

b. Vacca, & Vacca, John R. (2021). Cloud computing security: Foundations and challenges (Second ed.). Boca Raton, FL: CRC Press, ISBN: 9780367151164, ISBN: 0367151162, PolyU Library Call Number: QA76.585 .C5825 2021.

c. Wu, C. (2021). IoT Network Layer Security. In Internet of Things Security (Advances in Computer Science and Technology, pp. 107-123). Singapore: Springer Singapore, (online access from PolyU Library), ISBN: 9811613710 ISBN: 9789811613715, DOI: 10.1007/978-981-16-1372-2_7.

d. Security for VPNs with IPsec Configuration Guide Cisco IOS Release https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/12-2sy/sec-sec-for-vpns-w-ipsec-12-2sy-book.pdf (No. of pages required: 95 pages).

e. Ian Neil. (2018). CompTIA security+ certification guide: master IT security essentials and exam topics for CompTIA security+ SY0-501 certification, Birmingham: Packt Publishin. (online access from PolyU Library) (No. of words required: 10,000 words).

(4) A snippet of an international standard or request for comments (RFC)

a. Stewart, James Michael, Burlington. (2014) Network security, firewalls, and VPNs, 2nd ed.,Mass.: Jones & Bartlett Learning. (chapter 4 to chapter 6 (network security andnetwork security management)), (chapter 8 to chapter 10 (firewall deployment and management)) (ISBN: 9781284188851) (No. of words required: 10,000 words).

b. Bartlett, G., & Inamdar, A. (2017). *IKEv2 IPsec virtual private networks : Understanding and deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS* (1st ed.). Indianapolis, Indiana: Cisco Press, PolyU Library Call Number: TK5105.875.E87 B37 2017, ISBN : 1587144603, ISBN : 9781587144608.

c. IPsec Security Policy Database Configuration MIB https://tools.ietf.org/html/rfc4807 (No. of pages required: 70 pages)

d. X.800 : Security architecture for Open Systems Interconnection for CCITT applications https://www.itu.int/rec/T-REC-X.800-199103-I (No. of pages required: 48 pages)

Other references

Technical:

1. Ian Neil. (2018). CompTIA security+ certification guide: master IT security essentials and exam topics for CompTIA security+ SY0-501 certification, Birmingham: Packt Publishing. (eBook, online access)
2. Robin M. Abernathy, Troy McMillan (2016). Certified information systems security professional Cert guide, Indianapolis, Indiana: Pearson Education Second edition.
3. James Henry Carmouche. (2007). IPsec virtual private network fundamentals, Indianapolis,Ind.: Cisco Press. (PolyU Library Call Number: TK5105.567 .C37 2007).
4. IBM Security Products https://www.ibm.com/support/pages/identity-adapters-product-documentation-pdfs

	Network security: 5. Perez, Andre. (2014). Network Security, London: Hoboken, NJ: ISTE; Wiley. (eBook,online access) 6. Stewart, J., & Kinsey, D. (2021). Network security, firewalls, and VPNs (Third ed., Jones & Bartlett Learning information systems security & assurance series). Burlington, MA: Jones and Bartlett Learning, ISBN : 9781284183696. 7. Boston. (2013). Guide to network security, Mass. : Course Technology/Cengage Learning. **General:** 8. Danda B. Rawat, Bhed B. Bista, Gongjun Yan. (2014). Security, privacy, trust, and resourcemanagement in mobile and wireless communications, Hershey, PA: Information Science Reference. (eBook, online access) 9. Chen Lidong, Boca Raton. (2012). Communication system security, FL: CRC Press/Taylor& Francis Group. **Classics reading materials:** 10. 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)
Last Updated	May 2022
Prepared by	Dr Doris Lin