Course Content

Academic Year	AY2022 Summer 2023
Course Coordinator	Assoc Prof Mohammed Yakoob Siyal
Course Code	EE5084
Course Title	Cyber Security
Pre-requisites	Nil
No of AUs	3
Contact Hours	Lecture (39 hours)

Course Aims

The objective of this course is to provide you with basic appreciation and understanding of the underlying security issues and implications of the use of various networked systems and electronic devices in the modern cyber-society from both user and management perspectives. Topics to be covered include overview of information systems and devices in a global network environment, threats to information systems and devices, security models, and concepts for secrecy, integrity and availability. Other topics of security concerns will also be explored: security tools and devices, cryptology, hard ware security concerns, personnel security standards and legal implications.

Intended Learning Outcomes (ILO)

By the end of this course, students are expected to be able to:

1. Describe the history and evolution of cyber security.
2. Explain the need for security, in particular the Confidential, Integrity and Availability (CIA) Triads.
3. Differentiate various types of threats and their potential damages: virus, worms, Trojan horses, human engineering attacks, etc..
4. Explain the legal and planning issues of cyber security.
5. Describe the use of security tools and devices such as firewalls, IDPS and other scanning tools.
6. Explain the basic concepts of cryptology and the encryption standards.
7. Identify security concerns with regards to hard ware, personnel and implementation issues.

Course Content

Introduction to Security Issues in a Cyber-environment. Need for security. Legal and Planning. Tools, Firewalls and VPN. IDPS Tools. Cryptology. Hardware. Physical Security. Security and Personnel. Implementation.

Course Outline

S/N	Topic	Hours
1.	Introduction to Security Issues in a Cyber-environment	3

	• Describe the history of computer security and how it evolved into information security • Define information security • Define key terms and critical concepts of information security • Explain the information security roles of professionals within an organization	
2.	Need for Security • Explain the need for Cyber Security • Explain why an organization's general management and IT management are responsible for a successful information security program • Describe various types of threats and attacks • Describe various types of malwares, antivirus and patch	6
3.	Legal and Planning • Describe the functions of and relationships among laws, regulations, and professional organizations in information security • Explain the differences between laws and ethics • Explain role of culture as it applies to ethics in information security	3
4.	Tools, Firewall and VPN • Differentiate various types of security tools • Explain important role of access control in computer-based information systems • Identify and discuss widely used authentication factors • Describe firewall technology and the various approaches to firewall implementation • Explain approaches to control remote and dial-up access by authenticating and authorizing users • Describe content filtering technology • Describe virtual private networks (VPN)	5
5.	IDPS Tools • Identify various categories and models of intrusion detection and prevention systems (IDPS) • Describe honeypots, honeynets, and padded cell systems • Define categories of scanning and analysis tools, and describe the specific tools used within each category	4
6.	Cryptology • Describe the most significant events and discoveries in the history of cryptology • Explain the basic principles of cryptography • Describe the operating principles of the most popular cryptographic tools • Explain the major protocols used for secure communications	6
7	Hardware • Identify the hardware components of a computer • Identify the security concerns of the various hardware components of a computer • Describe the organization of storage devices, in particular, the hard disk with regards to security • Explain proper ways to dispose a used or old computer	3
8	Physical Security	3

	• Explain the relationship between information security and physical security • Describe key physical security considerations, including fire control and surveillance systems • Identify critical physical environment considerations for computing facilities, including uninterruptible power supplies	
9	Security and Personnel • Describe where and how the information security function should be positioned within organizations • Explain the issues and concerns related to staffing the information security function • Enumerate the credentials that information security professionals can earn to gain recognition in the field • Discuss how an organization's employment policies and practices can support the information security effort • Identify the special security precautions that must be taken when using contract workers • Explain the need for separation of duties • Describe the special requirements needed to ensure the privacy of personnel data	3
10	Implementation • Explain how an organization's information security blueprint becomes a project plan • Discuss the many organizational considerations that a project plan must address • Explain the significance of the project manager's role in the success of an information security project • Describe the need for professional project management for complex projects • Describe technical strategies and models for implementing a project plan • List and discuss the nontechnical problems that organizations face in times of rapid change	3

Assessment (includes both continuous and summative assessment)

Component	Course LO Tested	Related Programme LO or Graduate Attributes *	Weighting	Team/ Individual	Assessment rubrics
1. Final Examination	1-7	a, b, f	60%	Individual	
2. Continuous Assessment 1: Quiz 1	1-4	a, b, f	20%	Individual	
3. Continuous Assessment 2: Quiz 2	1-7	a, b, f	20%	Individual	
Total			**100%**		

* From the school website: EEE & IEM Programme Accreditation (Refer to Student Learning Outcomes) http://www.eee.ntu.edu.sg/Programmes/CurrentStudents/undergraduate/accreditation/Pages/Home.aspx

Mapping of Course SLOs to EAB Graduate Attributes

Course Student Learning Outcomes	**Cat**	**EAB's 12 Graduate Attributes* (indicate full/partial/weak moon/blank for the whole course for SLO a-l)**											
		(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)
EE5084 Cyber Security	GER-PE (STS); GER-UE	●	●				◐		○				

1. Describe the history and evolution of cyber security.	EAB SLO*a, f
2. Explain the need for security, in particular the Confidential, Integrity and Availability (CIA) Triads.	EAB SLO*a, b
3. Differentiate various types of threats and their potential damages: virus, worms, Trojan horses, human engineering attacks, etc…	EAB SLO*a, b, f
4. Explain the legal and planning issues of cyber security.	EAB SLO*a, f
5. Describe the use of security tools and devices such as firewalls, IDPS and other scanning tools.	EAB SLO*a, b
6. Explain the basic concepts of cryptology and the encryption standards.	EAB SLO*a, b
7. Identify security concerns with regards to hardware, personnel and implementation issues.	EAB SLO*a, b, f

Legend: ● Fully consistent (contributes to more than 75% of Student Learning Outcomes)
◐ Partially consistent (contributes to about 50% of Student Learning Outcomes)
○ Weakly consistent (contributes to about 25% of Student Learning Outcomes)
Blank Not related to Student Learning Outcomes

Formative feedback

(1) The lectures include discussions that provide immediate feedback of your understanding.
(2) Quiz 1 and quiz 2 are conducted using OASIS, which will provide immediate feedback on your performance.
(3) Based on the quiz results, lecturers will reviewed those topics that your cohort did not performed very well.
(4) Weekly consultations with lecturer, in addition to the scheduled class.
(5) Course websites will be provided with supplementary reading materials and interesting websites.

Learning and Teaching approach

Approach	How does this approach support students in achieving the learning outcomes?
LECTURE	Lectures will be conducted systematically from basic to more advanced knowledge. Course materials are carefully designed to meet the skill level of students, especially those who have no engineering background.
TUTORIAL	There are no tutorials. Instead there will be discussion per week after one of the lectures. This discussions are designed to review the subject matters and to highlight the key points.
LABORATORY(if any)	Nil

Reading and References

Textbooks

1. Principles of Information Security, 6th Edition, Michael E. Whitman and Herbert J. Mattord, Cengage Learning, 2018.
2. Tsai Flora S and Chan Chee Keong, Cyber Security, Pearson Custom, 2006. (TK5105.59.C994)

References

1. Volonino Linda, Robinson Stephen R and Volonino Charles P, Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers, 1st Edition, Pearson/Prentice-Hall, 2004. (TK5105.59.V929)
2. Stallings William, Network Security Essentials: Applications and Standards, 5th Int'l Edition, Pearson Prentice- Hall, 2013. (TK5105.59.S782N 2013)
3. Maiwald Eric, Fundamentals of Network Security, McGraw-Hill, 2004. (TK5105.59.M232F)

Course Policies and Student Responsibilities

Course policies:
http://www.ntu.edu.sg/Students/Undergraduate/AcademicServices/Pages/AcademicUnitSystem(AUS).aspx

CA guidelines:
http://www.eee.ntu.edu.sg/programmes/CurrentStudents/undergraduate/undergraduatefull-time/Documents/assessments/EEE%20CA%20Guidelines%28St%29_Aug2018.pdf

Instructions to Examination Candidates:
http://www.ntu.edu.sg/Students/Undergraduate/AcademicServices/Examination/pages/instructionstoexamcand.aspx

Academic Integrity

Good academic work depends on honesty and ethical behaviour. The quality of your work as a student relies on adhering to the principles of academic integrity and to the NTU Honour Code, a set of values shared by the whole university community. Truth, Trust and Justice are at the core of NTU's shared values.

As a student, it is important that you recognize your responsibilities in understanding and applying the principles of academic integrity in all the work you do at NTU. Not knowing what is involved in maintaining academic integrity does not excuse academic dishonesty. You need to actively equip yourself with strategies to avoid all forms of academic dishonesty, including plagiarism, academic fraud, collusion and cheating. If you are uncertain of the definitions of any of these terms, you should go to the academic integrity website for more information. Consult your instructor(s) if you need any clarification about the requirements of academic integrity in the course.

Course Instructors

Instructor	Office Location	Phone	Email
The contact info will be provided to students at the beginning of the programme.			

Planned Lesson Schedule

Lesson	Topic	Course LO	Readings/ Activities
1	Introduction to Security Issues in a Cyber environment	1-2	Video/Discussions
2	Need for Security	1-2	Discussions
3	Need for Security	1-2	Discussions
4	Legal and Planning	1-3	Discussions
5	Tools, Firewall and VPN	5, 6	Discussions
6	Tools, Firewall, VPN and IDPS Tools	5, 6	Quiz 1
7	IDPS Tools	5, 6	Discussions
8	Cryptology	5, 6	Illustrative examples
9	Cryptology	5,6	Illustrative examples
10	Hardware	7	Invited speaker (depends on availability)
11	Physical Security	7	Quiz 2
12	Security and Personnel	7	Discussions

13	Implementation	7	Summary & Revision