COURSE SYLLABUS

NETWORK SECURITY

1. **Module Code:** CS 4510
2. **Number of credits:** 3
3. **Pre-requisite(s):** CS 3323
4. **Teaching Language:** English
5. **Lecturer Information:**

Luu Quang Trung, PhD,

Department of Communication Engineering,

School of Electrical and Electronic Engineering

Hanoi University of Science and Technology

6. **Main aim(s) of the module:**

The course covers all aspects of network and computer security. It takes an in-depth and comprehensive view of security by examining the attacks that are launched against networks and computer systems, the necessary defense mechanisms, and even offers end-user practical tools, tips, and techniques to counter attackers. A fundamental knowledge of computers and networks is all that is required to follow this course. Its pedagogical features are designed to provide a truly interactive learning experience to help prepare students for the challenges of network and computer security. In addition to the information presented in the lecture, each topic includes hands-on projects that guide students through implementing practical hardware, software, network, and Internet security configurations step by step.

7. **Learning outcomes of the module:**

For knowledge

1. DEFINE information security and EXPLAIN why it is so important, yet so difficult to achieve
2. DESCRIBE the types of attackers, the basic steps of an attack, and the basic principles of defense
3. IDENTIFY the different types of malware
4. DESCRIBE the types of social engineering attacks
5. DESCRIBE cryptographic algorithms and their applications
6. EXPLAIN different cryptographic attacks
7. DESCRIBE how to implement cryptography and manage digital certificates
8. DESCRIBE the different transport cryptographic algorithms
9. EXPLAIN the different attacks that are directed at enterprises, including networking-based attacks as well as server attacks
10. EXPLAIN how to protect networks through standard network devices, network security hardware, network architectures and network technologies
11. DESCRIBE the techniques for administering a network and securing different network platforms
12. DESCRIBE the different types of wireless network attacks, the vulnerabilities

in different wireless security mechanisms, and several secure wireless protections
13. EXPLAIN how to secure the client through hardware and peripherals through hardware and the operating system
14. DESCRIBE application security vulnerabilities and the development of secure applications
15. DESCRIBE the different types of mobile devices, the risks associated with these devices, and the ways to secure mobile devices as well as the Internet of Things devices in general

For skills and attitude

Note: *- The learning outcomes of the module are constructed based on the learning outcomes of the program (Annex 1);*

- Compatibility matrix between learning outcomes of the module and learning outcomes of the program (Annex 2).

8. Assessment methods

No	*Assessment items*	*Value*	*Notes*
1.	Class participation	10%	
2.	Mid-term quiz	10%	20 multiple choice questions, 30 minute duration, on computer
3.	Hands-on projects	20%	
4.	Final exam	60%	40 multiple choice questions, 80 minute duration, on computer
	Total	100%	

9. Required textbook(s):

Required text
Mark Ciampa. *CompTIA Security+ Guide to Network Security Fundamentals, Sixth Edition*. ISBN-10 1337288780, ISBN-13 978-1337288781. Course Technology, 2017.

Required lab manual
Andrew Hurd. *CompTIA Security+ Guide to Network Security Fundamentals, Lab Manual, Sixth Edition*. ISBN-10 1337288799, ISBN-13 978-1337288798. Course Technology, 2017.

10. Module's description:

Topic 1: Introduction to security

Introduces the network security fundamentals, including the current challenges in computer security, the definition of computer security, the types of attackers, the basic steps of an attack, and the basic principles of defense

Topic 2: Malware and social engineering attacks

Examines attacks that use different types of malware and the different types of social engineering attacks

Topic 3: Basic cryptography

Explores how cryptography can be used to protect data, including how to protect data using three common types of encryption algorithms (hashing, symmetric encryption, asymmetric encryption) and how to use cryptography on files and disks to keep data secure

Topic 4: Advanced cryptography and PKI

Examines how to implement cryptography, how to use digital certificates (with a look at public key infrastructure and key management), and how cryptography is used on data that is being transported

Topic 5: Networking and server attacks

Explores the different attacks that are directed at enterprises, including networking-based attacks as well as server attacks

Topic 6: Networking security devices, design, and technology

Examines how to protect networks through standard network devices, network security hardware, network architectures and network technologies

Topic 7: Administering a secure network

Looks at the techniques for administering a network, including understanding common network protocols and the proper placement of security devices and technologies, and analyzing security data and securing network platforms such as virtualization, cloud computing, and software define networks

Topic 8: Wireless network security

Investigates the attacks on common wireless devices, different wireless security mechanisms that have proven to be vulnerable, and several secure wireless protections

Topic 9: Client and application security

Examines securing the client through hardware, peripherals through hardware and the operating system, external perimeter physical security, internal physical access security, application security vulnerabilities and the development of secure applications

Topic 10: Mobile and embedded device security

Looks at the different types of mobile devices, the risks associated with these devices, how to secure them and the applications running on them, and how embedded systems and the Internet of Things devices can be secured

11. Course schedule / Teaching plan:

Week	Content	Reference	Learning Outcomes
1	Course overview Introduction to security	Course syllabus Chapter 1	1, 2
2	Malware and social engineering	Chapter 2	3, 4
3	*Hands-on projects*: Malware and social engineering	Chapter 2	
4	Basic cryptography, Advanced cryptography and PKI	Chapters 3 and 4	5, 6, 7, 8
5	*Hands-on projects*: Basic cryptography, Advanced cryptography and PKI	Chapters 3 and 4	
6	Networking and server attacks	Chapter 5	9
7	*Hands-on projects*: Networking and server attacks Midterm	Chapter 5	
8	Networking security devices, design, and technology	Chapter 6	10
9	*Hands-on projects*: Networking security devices, design, and technology	Chapter 6	
10	Administering a secure network	Chapter 7	11
11	*Hands-on projects*: Administering a secure network	Chapter 7	
12	Wireless network security Mobile and embedded device security	Chapters 8 and 10	12, 15
13	*Hands-on projects*: Wireless network security, Mobile and embedded device security	Chapters 8 and 10	
14	Client and application security	Chapter 9	13, 14
15	*Hands-on projects*: Client and application security	Chapter 9	
	Final Exam		