IT5205 - Information Systems Security

(Compulsory)

INTRODUCTION

This is one of the compulsory courses designed for Semester 5 of the Bachelor of Information Technology Degree program. This course on Information Systems Security focuses on introducing the concepts, principles, techniques and methodologies required to design and assess the security of information exchange over complex networks, information systems and applications.

CREDITS: 03

LEARNING OUTCOMES

After successful completion of this course students will be able to:

- Explain the relationship between threats, vulnerabilities, countermeasures and attacks.
- Identify the security requirements of an information system.
- Describe the security services and countermeasures.
- Describe the concept of symmetric/asymmetric cryptography and key distribution protocols.
- Describe the different security protocols in the distributed network environments.
- Conduct a risk assessment.
- Prepare a cost benefit analysis and recommend the appropriate countermeasures.
- Describe a disaster recovery scenario.
- Demonstrate the ability to preserve evidence necessary for a forensic investigation.
- Design new security solutions for address the security issues in their organization.

MINOR MODIFICATIONS

When minor modifications are made to this syllabus, those will be reflected in the Virtual Learning Environment (VLE) and the latest version can be downloaded from the relevant course page of VLE. Please inform your suggestions and comments through the VLE.http://vle.bit.lk

ONLINE LEARNING MATERIALS AND ACTIVITIES

You can access all learning materials and this syllabus in the VLE: http://vle.bit.lk, if you are a registered student of BIT degree program. It is very important to participate in learning activities given in the VLE to learn this subject.

FINAL EXAMINATION

Final exam of the course will be held at the end of the semester.Learning activities and tutorial exercises are very important in this course, and they will help students to prepare themselves for the final semester exam. Final exam is a two hour written paper with four compulsory questions.

OUTLINE OF SYLLABUS

Topic	Hours
1- Introduction to Information System Security	03
2- Cryptosystems	08
3- Key Management	06
4- Network Security	10
5- The Internet Security	08
6- Information Assurance	10
Total for the subject	**45**

** Students may need more time to do relevant practical work.*

REQUIRED MATERIALS

Main Reading
Ref 1: "Security in Computing (Fourth Edition)", Charles P. Pfleeger, Prentice-Hall International, Inc.

Ref 2:"Applied Cryptography Protocols, Algorithms, and Source Code in C (Second edition)", Bruce Schneier, John Wiley & Sons, Inc.
Supplementary Reading

Ref 3: Computer Security: Art and Science, Matt Bishop

Online References:

Ref 4: Cryptography, Prof. Dan Boneh, Stanford University
URL: https://www.coursera.org/course/crypto

Ref 5: Network and Computer Security, Prof. Ronald Rivest
URL: http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/

Ref 6: Building an Information Risk Management Toolkit, Barbara Endicott-Popovsky University of Washington
URL: https://www.coursera.org/course/inforisk

[The pages of the web addresses mentioned above last accessed on 16th October 2015. The content of the above addresses are on the VLE.]

DETAILED SYLLABUS:

Section 1: Introduction to Information System Security (03 hrs)

Instructional Objectives

- Describe and explain how different security attacks might be used to compromise an information system
- Identify and distinguish between the different types of Malware (viruses, Trojan horses, worms)
- Explain the role of integrity, confidentiality, availability, authentication, and non-repudiation as security services. Identify the characteristics of a good cipher

Material /Sub Topics

1.1. Attacks

- 1.1.1 Active attacks
- 1.1.2 Passive attacks
- 1.1.3 Social engineering
- 1.1.4 Denial of service attacks
- 1.1.5 Buffer overflow attacks
- 1.1.6 Malware (viruses, Trojan horses, worms)

1.2. Introduction to Security Mechanisms
    1.2.1 Cryptosystems
    1.2.2 Authentication ("Who you are, what you have, what you know")
    1.2.3 Intrusion detection
    1.2.4 Redundancy
    1.2.5 Disaster Recovery
1.3. Security Services
    1.3.1 Availability
    1.3.2 Integrity
    1.3.3 Confidentiality
    1.3.4 Authentication
    1.3.5 Non-repudiation

Section 2: Cryptosystems (08 hrs)

Instructional Objectives

- Describe the concept of encryption/decryption
- Describe the different types of ciphers
- Explain the concept of symmetric and asymmetric key cryptography
- Describe the different symmetric and asymmetric key and hash algorithms

Material /Sub Topics

2.1. Terminology and Background
    2.4.1. Encryption, Decryption
    2.4.2. Plain Text and Cipher Text
    2.4.3. Encryption Algorithms
2.2. Hash Algorithms
    2.4.1. Hash Concept
    2.4.2. Description of Hash Algorithms
    2.4.3. Message Digest Algorithms
2.3. Secure Secret Key (Symmetric) Systems
    2.4.1. The Data Encryption Standard (DES)
    2.4.2. Advance Encryption Standard (AES)

2.4.3. Block Cipher Operational Modes

2.4. Public Key (Asymmetric key) Encryption Systems

2.4.1. Concept and Characteristics of Public key Encryption System

2.4.2. Rivest-Shamir-Adelman (RSA) Encryption in Detail

2.4.3. Introduction to Digital Signature Algorithms

2.4.4. The Digital Signature Standard (DSA)

2.4.5. Introduction to Elliptic Curve (EC) Cryptography

Section 3: Key Management (06 hrs)

Instructional Objectives

- Describe different key management protocols
- Explain the concept of public key infrastructure and related technologies

Material /Sub Topics

3.1. Key Management Protocols

3.1.1. Solving Key Distribution Problem

3.1.2. Diffie-Hellman Algorithm

3.1.3. Key Exchange with Public Key Cryptography

3.2. Public Key Infrastructure (PKI)

3.2.1. Concept of Digital Certificate

3.2.2. Certificate Authorities and it's roles

3.2.3. Digital Certificates

3.2.4. Types of Public Key Infrastructures

Section 4: Network Security (10 hrs)

Instructional Objectives

- Explain the authentication mechanisms
- Describe security protocols in open network environment
- Describe the types of malware and protection methods

Material /Sub Topics

4.1. Network Security Protocols

4.1.1. Authentication Protocols (Password, challenge-response, S/Key, PKI based strong authentication and Kerberos)

4.1.2. Secure Shell (SSH)

4.1.3. IP Security (IPSec) protocol

4.1.4. Virtual Private Networks (VPN)

4.1.5. Securing wireless (IEEE 802.11) networks (WEP, WPA, WPA2 protocols)

4.2. Intruder Detection and Prevention

4.2.1. Malicious Code (virus, worms, zombies etc.)

4.2.2. Preventing Malware Attacks

4.2.3. Firewalls

4.2.4. Intruder detection and prevention mechanisms

Section 5: The Internet Security (08 hrs)

Instructional Objectives

- Identify the security requirement of the Internet
- Describe the existing Web and e-mail security solutions and protocols
- Design new solutions to address the security problems in open network environment

Material /Sub Topics

5.1. Web Security

5.1.1. Solving Privacy Problems

5.1.2. Solving Authentication Problems

5.1.3. Secure Socket Layer (SSL) Protocol

5.1.4. Secure Payment Protocols (SET, 3D Secure)

5.2. Secure Electronic Mail

5.2.1. Pretty Good Privacy (PGP)

5.2.2. Public Key Cryptography Standards-PKCS#7

5.2.3. Secure/Multipurpose Internet Mail Extensions (S/MIME)

5.2.4. Spams (hoax, phishing, chain mails, financial) detection and prevention

Section 6: Information Assurance (10 hrs)

Instructional Objectives

- Describe the role of security policy in an organization
- Describe the importance of and key elements involved in incident tracking to develop an incident handling and reporting process.
- Describe legal and ethical considerations related to the handling and management of information systems.

Material /Sub Topics

6.1. Security Policy

- 6.1.1. Creation of policies (Password, Internet, e-mail and social network access policies etc.)
- 6.1.2. Maintenance of policies
- 6.1.3. Domainintegration (physical, network, Internet, etc.)

6.2. Threat Analysis Model

- 6.2.1. Risk assessment
- 6.2.2. Cost / benefit analysis

6.3. Operational Issues

- 6.3.1. Security Auditing
- 6.3.2. Enforcement Legal issues (Copyrights, Patents, Trade Secrets)
- 6.3.3. Disaster recovery (natural and man-made)
- 6.3.4. Incident response (forensics)
- 6.3.5. Security awareness

PLATFORM

No practical required.