IT5204 - 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: 04

LEARNING OUTCOMES

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

- Recognize the concept of symmetric key and asymmetric key cryptography.
- Describe the different encryption and decryption algorithms and technologies.
- Recognize the security requirements of an information system.
- Describe the functionality of practical cryptographic protocols.
- Identify the security requirements of operating systems, databases and programs.
- Describe the various existing security solutions in an open network environment.
- Design new security solutions to address the security issues in open network environments.

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- Basic Encryption and Decryption	06
2- Secure Encryption Systems	15
3- Applied cryptography, protocols and practice	15
4- Operating systems, database and program security	12
5- Security in networks and distributed systems	12
Total for the subject	**60**

** 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: "Digital Certificates and Applied Internet Security", Jalal Feghhi, Jalli Feghhi and Peter Williams, Addison Wesley Longman, Inc.

Ref 4: "Security Technologies for the World Wide Web", Rolf Oppliger, Artech House, Inc.

Online References:

Ref 5: Cryptography A-Z, http://ncsi-net.ncsi.iisc.ernet.in/cyberspace/nd/ssh.com/support/cryptogr/index.htm

Ref 6: The Handbook of Applied Cryptography, http://www.cacr.math.uwaterloo.ca/hac/

Ref 7: "W3C Security Resources", World Wide Web Consortium,

http://www.w3.org/Security/security-resource

Ref 8: Cryptographic Message Syntax Standard, Public-Key Cryptography Standards, RSA Laboratories, http://www.rsa.com/rsalabs/node.asp?id=2124

Ref 9: Computer Emergency Response Team (CERT), http://www.cert.org

[The pages of the web addresses mentioned above last accessed on 09th August 2011. The content of the above addresses are on the LMS.]

DETAILED SYLLABUS:

Section 1 : Basic Encryption and Decryption (06 hrs)

Instructional Objectives

- Recognize the concept of encryption/decryption
- Describe the different types of ciphers
- Identify the characteristics of a good cipher

Material /Sub Topics

1.1 Terminology and Background

1.1.1 Encryption, Decryption and Cryptosystems [Ref1: pg.25-39]

1.1.2 Plain Text and Cipher Text [Ref1: pg.39-40]

1.1.3 Encryption Algorithms [Ref1: pg.39-42]

1.1.4 Cryptanalysis [Ref1: pg.40-46]

1.2. Introduction to Ciphers

1.2.1 Monoalphabetic Substitutions such as the Caesar Cipher [Ref1: pg.44]

1.2.2 Cryptanalysis of Monoalphabetic Ciphers [Ref1: pg.45]

1.2.3 Polyalphabetic Ciphers such as Vigenere Tableaux [Ref1: pg.50]

1.2.4 Cryptanalysis of Polyalphabetic Ciphers [Ref1: pg.48-49]

1.2.5 Perfect Substitution Cipher such as the Vernam Cipher [Ref1: pg.50]

1.2.6 Stream and Block Ciphers [Ref1: pg.62,63]

1.3. Characteristics of 'Good' Ciphers

1.3.1. Shannon Characteristics [Ref1: pg.60]

1.3.2. Confusion and Diffusion [Ref1: pg.63]

Section 2 : Secure Encryption Systems (15 hrs)

Instructional Objectives

- Handle properties of arithmetic, which are the fundamental of encryption systems
- Recognise the concept of symmetric and asymmetric key cryptography
- Describe the different symmetric and asymmetric key and hash algorithms

Material /Sub Topics

2.1. Properties of Arithmetic Operations
- 2.1.1. Inverses [Ref1: pg.725]
- 2.1.2. Primes [Ref1: pg.725]
- 2.1.3. Greatest Common Divisor [Ref1: pg.726]
- 2.1.4. Euclidean Algorithm [Ref1: pg.726]
- 2.1.5. Modular Arithmetic [Ref1: pg.726]
- 2.1.6. Properties of Modular Arithmetic [Ref1: pg.727]
- 2.1.7. Computing the inverse in modular arithmetic [Ref1: pg.728]
- 2.1.8. Fermat's Theorem [Ref1: pg.729]
- 2.1.9. Algorithm for Computing Inverses [Ref1: pg.729]
- 2.1.10. Random number generation [Ref2: pg.44-46]

2.2. Public Key (Asymmetric key) Encryption Systems
- 2.2.1. Concept and Characteristics of Public key Encryption System [Ref1: pg.757]
- 2.2.2. Introduction to Merkle-Hellman Knapsacks [Ref1: pg.758-767]
- 2.2.3. Rivest-Shamir-Adelman (RSA) Encryption in Detail [Ref1: pg.767-773]
- 2.2.4. Introduction to Digital Signature Algorithms [Ref1: pg.773, 774]
- 2.2.5. The Digital Signature Standard (DSA) [Ref1: pg.773]
- 2.2.6. Introduction to Elliptic Curve (EC) Cryptography [Ref2: pg.480,481]

2.3. Hash Algorithms
- 2.3.1. Hash Concept [Ref1: pg.79,80,Ref2: pg.30]
- 2.3.2. Description of Hash Algorithms [Ref2: pg.435-455]
- 2.3.3. Message Digest Algorithms [Ref2: pg.31]

2.4. Secret Key (Symmetric Key) Encryption Systems
- 2.4.1. The Data Encryption Standard (DES) [Ref1: pg.68-71,732-742]

2.4.2. Analyzing and Strengthening of DES [Ref1: pg.742-748]

2.4.3. Key Escrow and Clipper [Ref1: pg.691,Ref2: pg.97-100]

2.4.4. Advance Encryption Standard (AES) [Ref1: pg.72-75,748-754]

2.4.5. Introduction to Quantum Cryptography [Ref1: pg.774-778]

Section 3 : Applied Cryptography, Protocol and Practice (15 hrs)

Instructional Objectives

- Describe different key management protocols
- Recognize the concept of public key infrastructure and related technologies
- Describe the advance cryptographic protocols
- Recognize the legal issues related to security of information systems

Material /Sub Topics

3.1. Key Management Protocols

3.1.1. Diffie-Hellman Algorithm [Ref2: pg.513-515]

3.1.2. Key Exchange with Public Key Cryptography [Ref2: pg.48-51]

3.2. Public Key Infrastructure (PKI)

3.2.1. Concept of Digital Certificate [Ref2: pg.185-186]

3.2.2. Certificate Authorities and their roles [Ref2: pg.186-187]

3.2.3. Types of Public Key Infrastructures [Ref1: pg.450-453]

3.3. Legal Issues

3.3.1. Copyrights [Ref1: pg.652-654]

3.3.2. Patents [Ref1: pg.655-658]

3.3.3. Trade Secrets [Ref1: pg.658-659]

3.3.4. Computer Crime [Ref1: pg.679-689]

3.3.5. Cryptography and the Law [Ref1: pg.689-692]

Section 4 : Operating systems, database and program security (12 hrs)

Instructional Objectives

- Identify the security features of ordinary and trusted operating system
- Evaluate the operating system security
- Recognize the security requirement of databases
- Describe the types of computer virus and protection methods

Material /Sub Topics

4.1. Operating Systems Security

4.1.1. Security Policies [Ref1: pg.245-252]

4.1.2. Models of Security [Ref1: pg.252-263]

4.1.3. Security Features of Ordinary Operating Systems [Ref1: pg.266-287]

4.1.4. Security Features of Trusted Operating Systems [Ref1: pg.287-311]

4.2. Database Security

4.2.1. Security Requirements of Databases [Ref1: pg.324-329]

4.2.2. Reliability and Integrity [Ref1: pg.329-335]

4.2.3. Protection of Sensitive Data [Ref1: pg.335-341]

4.2.4. Inference Problem: Direct and Indirect Attacks [Ref1: pg.341-345]

4.2.5. Disaster Recovery [Ref1: pg.563-566]

4.3. Program Security

4.3.1. Types of Malicious Code [Ref1: pg.114-116]

4.3.2. Viruses Attach and Gain Control Mechanisms [Ref1: pg.117-121]

4.3.3. Homes for Viruses [Ref1: pg.121-123]

4.3.4. Virus Signatures [Ref1: pg.124-128]

4.3.5 Preventing Virus Infection [Ref1: pg.129-131]

4.3.6. Trapdoors [Ref1: pg.141-144]

4.3.7. Covert Channels [Ref1: pg.150-160]

4.3.8. Controls Against Program Threats [Ref1: pg.160-181]

4.3.9. Mobile codes [Ref1: pg.433-438]

Section 5 : Security in networks (12 hrs)

Instructional Objectives

- Describe the authentication mechanisms and protocols required in a open network environment
- Design security polices and network protection systems to prevent unauthorized access in open network environment
- Identify the security requirement of the internet
- Describe the existing security solutions and protocols
- Design new solutions to address the security problems in open network environment

Material /Sub Topics

5.1. Network Security

5.1.1. Network Security Issues such as Impersonation, Message Confidentiality, Message Integrity, Code Integrity, Denial of Service [Ref1: pg.415-439]

5.1.2. IP Security (IPSec) protocol and Virtual Private Networks (VPN) [Ref1: pg.449-450, 454-456,]

5.1.3. Securing wireless (IEEE 802.11) networks [Ref1: pg.466-468]

5.1.4. PKI based Authentication and Kerberos Authentication [Ref1:pg.213-214, Ref2: pg.53-54]

5.1.5. Biometrics Authentication Mechanisms [Ref1: pg.234-236]

5.1.6. Access Control Mechanisms [Ref1: pg.469-474]

5.1.7. Firewalls [Ref1: pg.474-484]

5.2. Web Security

5.2.1. Solving Privacy Problems [Ref1: pg.606-608]

5.2.2. Solving Authentication Problems [Ref1: pg619-623]

5.2.3. Secure Socket Layer (SSL) Protocol [Ref1: pg.453-454]

5.2.4. Securing Online Payments [Ref1: pg.627-628]

5.2.5. Precautions for Web Surfing [Ref1: pg.629-635]

5.3. Secure Electronic Mail

5.3.1. Privacy Enhanced Email (PEM) [Ref2: pg.577-584]

5.3.2. Pretty Good Privacy (PGP) [Ref2: pg.584-587]

5.3.3. Public Key Cryptography Standards [Ref2: pg.588-589]

5.3.4. Secure/Multipurpose Internet Mail Extensions (S/MIME) [Ref1: pg.490-496]

PLATFORM

No practical required.