THOMPSON RIVERS UNIVERSITY

**Course Outline**

Computing Science Department
Faculty of Science

**COMP 3260 – 3 Credits**
**Computer Network Security (3,1,0)**
**Fall 2015**

**Instructor:** Phone/Voice Mail: Office:
E-Mail: Office Hours:

## CALENDAR DESCRIPTION

Students explore how information is exchanged on the Internet and the security issues that arise due to information exchange between different technologies. Students learn concepts of authentication, authorization, access control in computer networks. Students gain knowledge about Use of cryptography for data and network security. Students are introduced to the topics such as firewalls, public key infrastructure, security standards and protocols, virtual private networks, and wireless network security. Students also explore privacy, legal issues and ethics in context of network security.

## PREREQUISITES

- COMP 3270

## EDUCATIONAL OBJECTIVES/OUTCOMES

Upon successful completion of the course, the student will demonstrate the ability to:

1. Understand vulnerability in a computer system.
2. Explain useful and common tools used by the attacker
3. Understand basic concept of how to protect and design private network.
4. Understand how to protect security of information.
5. Use theoretical and practical knowledge in securing data transfer and authentication.

## TEXTS/MATERIALS

The course uses the following texts:
**B1**. Network Security, Firewalls, and VPNS, by J. Michael Stewart, 2010, ISBN 10: 076379130X
**B2**. Cryptography and Network Security: Principles and Practices by W.Stallings, Prentice Hall, 5th Edition, ISBN-10: 0136097049
**B3.** Principles of Computer Security: CompTIA Security+ and Beyond by Wm.A. Conklin et al., McGraw Hill, 3rd Edition, ISBN-10: 0071786198
**B4**. CompTIA Security+ Guide to Network Security Fundamentals, Mark Ciampa, 5th Edition, ISBN-10: 1305093917
**Ref5**. Privacy Legislation in Canada, [online] https://www.priv.gc.ca

**SYLLABUS - Lecture & Lab Topics:**

| Course Topics | | Reference to TextBook | Duration |
|---|---|---|---|
| 1. Introduction | 1.1 Computer Security Concepts<br>1.2 The OSI Security Architecture<br>1.3 Security Attacks<br>1.4 Security Services<br>1.5 Security Mechanisms<br>1.6 A Model for Network Security<br>1.7 Recommended Reading and Web Sites | B2-Chapter 1 | 1 |
| 2. Network Security | 2.1 Security Through Network Devices<br>2.2 Security Through Network Technology<br>2.3 Security Through Network Design Elements | B4-Chapter 6 | 1 |
| 3. Firewalls | 3.1 The Need for Firewalls<br>3.2 Firewall Characteristics<br>3.3 Types of Firewalls<br>3.4 Firewall Basing<br>3.5 Firewall Location and Configurations<br>3.6 Recommended Reading and Web Sites | B2-Chapter 22 | 1.5 |
| 4. Cryptography | 4.1 Algorithms<br>4.2 Hashing Functions<br>4.3 Symmetric Encryption<br>4.4 Asymmetric Encryption<br>4.5 Quantum Cryptography<br>4.6 Steganography<br>4.7 Cryptography Algorithm Use | B3-Chapter 5 | 2 |
| 5. Public Key Infrastructure | 5.1 The Basics of Public Key Infrastructures<br>5.2 Certificate Authorities<br>5.3 Registration Authorities<br>5.4 Certificate Repositories<br>5.5 Trust and Certificate Verification<br>5.6 Digital Certificates<br>5.7 Centralized and Decentralized Infrastructures<br>5.8 Public Certificate Authorities<br>5.9 In-House Certificate Authorities<br>5.10 Certificate-Based Threats | B3-Chapter 6 | 1 |
| 6. Security Standards and Protocols | 6.1 PKIX and PKCS<br>6.2 X.509<br>6.3 SSL/TLS<br>6.4 ISAKMP<br>6.5 CMP | B3-Chapter 7 | 2 |

| | | | |
|---|---|---|---|
| | 6.6 XKMS<br>6.7 S/MIME<br>6.8 PGP<br>6.9 HTTPS<br>6.10 IPsec<br>6.11 CEP<br>6.12 FIPS<br>6.13 Common Criteria for Information Technology Security (Common Criteria or CC)<br>6.14 WTLS<br>6.15 PPTP<br>6.16 WEP<br>6.17 ISO/IEC 27002 | | |
| 7. Authentication and Remote Access | 7.1 The Remote Access Process<br>7.2 IEEE 802.1X<br>7.3 RADIUS<br>7.4 TACACS+<br>7.5 Authentication Protocols<br>7.6 FTP/FTPS/SFTP<br>7.7 VPNs<br>7.8 IPsec<br>7.9 Vulnerabilities of Remote Access Methods | B3- Chapter 11 | 1 |
| 8. Virtual Private Networks | 8.1 VPN Fundamentals<br>8.2 VPN Management<br>8.3 VPN Technologies | B1-Chapter 3 & B1- Chapter 11 & B1- Chapter 12 | 1.5 |
| 9. Wireless Network Security | 9.1 Introduction to Wireless Networking<br>9.2 Mobile Phones<br>9.3 Bluetooth<br>9.4 802.11: Attacking, New Security Protocols, and Implementation | B3-Chapter 12 | 1 |
| 10. Privacy, Legal Issues and Ethics | 10.1 Cybercrime<br>10.2 Ethics<br>10.3 Personally Identifiable Information (PII)<br>10.4 U.S. Privacy Laws<br>10.5 Privacy Legislation in Canada | B3-Chapter 24 & B3-Chapter 25 & Ref 5 | 1 |

| **Lab Topics** | | **Duration** |
|---|---|---|
| Examining and Implementation of a Simple Block Cypher | | 1 |
| Firewall Implementation and Testing | | 2 |
| Implementation of Public Key Crypto-System | | 1 |
| Demonstration of Security Protocols | | 2 |

| | | |
|---|---|---|
| Exercise on Authentication Protocols | | 1 |
| Demonstration and Setup VPN | | 2 |
| Experiments on Wireless Security | | 2 |

## ACM / IEEE Knowledge Area Coverage

### IEEE Knowledge Areas that contain topics and learning outcomes covered in the course

| Knowledge Area | Total Hours of Coverage |
|---|---|
| IAS/Foundational Concepts in Security | |
| IAS/Threats and Attacks | |
| IAS/Network Security | |
| IAS/Cryptography | |

### IEEE Body of Knowledge coverage

| KA | Knowledge Unit | Topics Covered | T1 hours | T2 hours | Elective hours |
|---|---|---|---|---|---|
| | IAS/Foundational Concepts in Security | CIA (Confidentiality, Integrity, Availability)<br>• Concepts of risk, threats, vulnerabilities, and attack vectors (cros- reference SE/Software Project Management/Risk)<br>• Authentication and authorization, access control (mandatory vs. discretionary)<br>• Concept of trust and trustworthiness<br>• Ethics (responsible disclosure). (cross-reference SP/Professional Ethics/Accountability, responsibility and liability) | 6 | | |
| | IAS/Threats and Attacks | Attacker goals, capabilities, and motivations (such as underground economy, digital espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats)<br>• Examples of malware (e.g., viruses, worms, spyware, botnets, Trojan horses or rootkits)<br>• Denial of Service (DoS) and Distributed Denial of Service (DDoS)<br>• Social engineering (e.g., phishing) (cross-reference SP/Social Context/Social implications of computing in<br>a networked world and HCI/Designing Interaction/Handling human/system failure) | 3 | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Describe likely attacker types against a particular system. [Familiarity]<br>2. Discuss the limitations of malware countermeasures (e.g., signature-based detection, behavioral detection). [Familiarity]<br>3. Identify instances of social engineering attacks and Denial of Service attacks. [Familiarity]<br>4. Discuss how Denial of Service attacks can be identified and mitigated. [Familiarity] | | | |
| | IAS/Network Security | Network specific threats and attack types (e.g., denial of service, spoofing, sniffing and traffic redirection,<br>man-in-the-middle, message integrity attacks, routing attacks, and traffic analysis)<br>• Use of cryptography for data and network security<br>• Architectures for secure networks (e.g., secure channels, secure routing protocols, secure DNS, VPNs, anonymous communication protocols, isolation)<br>• Defense mechanisms and countermeasures (e.g., network monitoring, intrusion detection, firewalls, spoofing and DoS protection, honeypots, tracebacks)<br><br>Describe the different categories of network threats and attacks. [Familiarity]<br>2. Describe the architecture for public and private key cryptography and how public key infrastructure (PKI)<br>supports network security. [Familiarity]<br>3. Describe virtues and limitations of security technologies at each layer of the network stack. [Familiarity]<br>4. Identify the appropriate defense mechanism(s) and its limitations given a network threat. [Familiarity] | 24 | | |
| | IAS/Cryptography | Basic Cryptography Terminology covering notions pertaining to the different (communication) partners,<br>secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their | 6 | | |

| | | | | | |
|---|---|---|---|---|---|
| | | characteristics, signatures<br>• Cipher types (e.g., Caesar cipher, affine cipher) together with typical attack methods such as frequency analysis<br>• Public Key Infrastructure support for digital signature and encryption and its challenges | | | |