

University of Computer Studies, Yangon
B.C.Sc./B.C.Tech.

CT-406	: Computer Security	Second Semester
Text Book	: Computer Security Fundamentals By Chuck Easttom	
Period	: 45 periods for 15 weeks (3 periods/week) (Lecture +Lab)	

Course Description

The focus of the course is to provide a set of practices the students can deploy immediately to secure their computers and to maintain safe security practices. The lectures cover the necessary security concepts and methods to prevent security breaches and what to do if such a breach is detected. The students will learn about securing popular computer platforms and applications running on these platforms.

Course Objectives

- introduce concepts of Computer security;
- provide an overview of principles and practices of Cybersecurity;
- study Denial of Service Attack, Cyber Stalking, Fraud, and Abuse
- present properties of malicious software;
- study tools and techniques used to defend computer systems; and
- Be able to understand and follow security and privacy policies

Assessment Plan for the Course

Paper Exam:	60%
Attendance:	10%
Test/ Quiz:	10%
Lab:	10%
Lab Assessment:	10%

Tentative Lecture Plan

No.	Chapter	Page	Period	Detail Lecture Plan
	Chapter 1 Introduction to Computer Security	2-21	6	All Examples and Questions

No.	Chapter	Page	Period	Detail Lecture Plan
1.	Introduction How Seriously Should You Take Threats to Network Security? Identifying Types of Threats Assessing the Likelihood of an Attack on Your Network	2-7	2	
2.	Basic Security Terminology Concepts and Approaches How Do Legal Issues Impact Network Security? Online Security Resources	8-14	2	
3.	Summary Exercises		2	
	Chapter 3 Cyber Stalking, Fraud, and Abuse	48-71	7	All Examples and Questions
4.	Introduction How Internet Fraud Works Identity Theft	48-55	2	
5.	Cyber Stalking Protecting Yourself against Cyber Crime	55-59	3	
6.	Summary Exercises		2	
	Chapter 4 Denial of Service Attacks	72-91	4	All Examples and Questions
7.	Introduction Denial of Service Illustrating an Attack	72-84	2	
8.	Summary Exercises		2	
	Chapter 5 Malware	92-115	6	All Examples and Questions
9.	Introduction Viruses	92-98	2	
10.	Trojan Horses The Buffer-Overflow Attack The Sasser Virus/Buffer Overflow	98-101	1	
11.	Spyware Other Forms of Malware Detecting and Eliminating Viruses and Spyware	101-109	2	
12.	Summary Exercises		1	
	Chapter 6 Techniques Used by Hackers	116-131	6	All Examples

No.	Chapter	Page	Period	Detail Lecture Plan
13.	Introduction Basic Terminology The Reconnaissance Phase	116-118	2	and Questions
14.	Actual Attacks	123-125	2	
15.	Summary Exercises		2	
	Chapter 9 Computer Security Software	178-199	7	All Examples and Questions
16.	Introduction Virus Scanners	178-181	2	
17.	Firewalls	182-187	2	
18.	Antispyware Intrusion-Detection Software	187-194	2	
19.	Summary Exercises		1	
	Chapter 11 Network Scanning and Vulnerability Scanning	220-253	7	All Examples and Questions
20.	Introduction Basics of Assessing a System	220-228	2	
21.	Securing Computer Systems	229-233	2	
22.	Scanning Your Network	235-238	2	
23.	Summary Exercises		1	
24.	Revision for All Chapters		2	