Zetech University
Faculty of ICT & Engineering
BNT 312: Computer and Information System Security

Lecturer: Dr Daniel Makupi Ph.D.
Office Hours: Wednesdays EAT 2-5pm
Email: Makupidaniel@gmail.com
Contacts: 0727582498

Course Description

General concepts and applied methods of computer security, especially as they relate to confidentiality, integrity, and availability of information assets. Topics include system security analysis, access control and various security models, identification and authentication, protection against external and internal threats, network protocols and Internet security

Course Objectives:

This course provides a broad introduction to a variety of topics in applied computer, network, and system security. These include system/software vulnerabilities, applied cryptography, host-based and network-based security, privacy, anonymity, usability, security economics, risks and vulnerabilities, policy formation, controls and protection methods, and issues of law and privacy

Course Outline

1. **Introduction to Information security**

   Overview of Computer Security Concepts and Foundations and Threats, Attacks, and Assets Computer Security Technology and Principles

2. **Software Security and Trusted Systems**

   User Identification and Authentication and Access Control and Database, Cloud Security and Malicious Software, Denial-of-Service Attacks and Intrusion Detection and Firewalls and Intrusion Prevention Systems

3. **Software Security and Trusted Systems**

   Buffer Overflow and Software Security, Operating System Security and Database Security, Trusted Computing and Multilevel Security

4. **Management Issues**

   Security Management and Risk Assessment, Human Resources Security, Legal and Ethical Aspects

5. **Cryptographic Algorithms**

   Symmetric Encryption and Message Confidentiality and Public-Key Cryptography and Message Authentication

6. **Security Technology: Firewalls and VPN**

   Access control and firewalls, Firewalls and Protecting remote connections.

7. **Information security Maintenance**

   Security Management Maintenance Models; NIST SP 800-100 Information Security Handbook: A Guide for Managers, The Security Maintenance Model, Monitoring the External Environment, Monitoring the Internal Environment. Digital Forensics

Textbook and Reading Materials

The primary text for this class is;

Principles of Information Security 3nd Edition, Whitman and Mattord, Thompson – Course Technology, ISBN: 970-1-4-2390177-0

External reading materials will be made available eLearning Platforms

Other Refrence Materials

1. White, G. L., Hewitt, B., & Kruck, S. E. (June 06, 2013). Incorporating Global Information Security and Assurance in I.S. Education. Journal of Information Systems Education, 24, 1, 11-16.
2. Handbook of research on information security and assurance.(Brief article)(Book review). (January 01, 2008). Scitech Book News.
3. Holzinger, A. (January 01, 2000). Information Security Management and Assurance. Information Systems Security, 9, 32-39.
4. Stahl, B. C. (July 01, 2004). Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics?. Journal of Organizational and End User Computing, 16, 3, 59-77.
5. Optimizing information security and advancing privacy assurance; new technologies. (Brief article) (Book review). (January 01, 2012). Reference & Research Book News.

Projected schedule of homework, labs, quizzes, and tests:

There will be homework assignments and at least 2 lab projects.

There will be assigned readings (mostly research papers) for each week and there will be pop up quizzes (or group discussions) about the readings.

There will be 2 CATs and a final exam

Ethics

During the course of the semester, you will learn techniques and tools that can be used to compromise the security of computer systems and computer networks. It is very important that you never use these techniques or tools without the permission of the computer or network owner. You should never attempt to attack the computers or networks belonging to the computer science department, the university, a classmate, or the course staff. If a student unethically exploited a vulnerability, the student will fail the class.