COURSE : FP611 INFORMATION SYSTEM SECURITY
CREDIT(S) : 3
PRE REQUISITE(S) : NONE

SYNOPSIS

INFORMATION SYSTEM SECURITY course is designed to focus on the overall security processes based on security policy emphasizing on hands-on skills in the areas of a secure perimeter, secure connectivity, identity services and intrusion detection. The knowledge delivered shall enable students to identify some of the security approaches to design a defensive strategy in a network environment. Discussion on the security features of Microsoft Windows Server and Open Source Software network operating systems are also included.

COURSE LEARNING OUTCOMES (CLO)

Upon completion of this course, students should be able to:

1. explain information security vulnerabilities, threats and attacks in a network environment according to international standard such as Open Web Application Security Project (OWASP). (C4, PLO1)

2. configure security environment to secure information using various tools effectively. (P4, C3, PLO2, PLO1)

3. work efficiently with proper techniques and procedures to create a secured environment in an organization. (A4, C3, PLO8, PLO1)
SUMMARY

(LECTURE : PRACTICAL)

SST

1.0 INTRODUCTION TO INFORMATION SYSTEM SECURITY

This topic introduces the need of information system security, security policy and security information organization. Students are introduced to identifying potential risks to network security.

2.0 INTRODUCTION TO VULNERABILITIES, THREATS AND ATTACK

This topic provides an overview of essential network security concepts, common vulnerabilities, threats, attacks and vulnerability analysis.

3.0 SECURITY DEVICES AND TECHNOLOGIES

This topic covers the end-point protection and management to secure host and server devices. Different methods of protection are also covered such as anti-virus, firewall, intrusion detection system and intrusion prevention system. This topic also covers installation and configuration of firewalls running on Linux platform and ISA Server.

4.0 OPERATING SYSTEMS AND SECURITY

This topic covers the following areas: Microsoft Windows security approaches, Linux security approaches and Linux based Proxy Servers.

5.0 AUTHENTICATION AND ENCRYPTION TECHNOLOGY

This topic deals with authentication and encryption technology in securing a communication session. It discusses on the various methods of encryption and covers on the solutions available in providing authentication and encryption services such as Virtual Private Network (VPN).

6.0 DISASTER PREVENTION AND RECOVERY

This topic covers disaster prevention and recovery in servers.

DEPENDENT LEARNING COURSEWORK ASSESSMENT

RTA – Recommended Time Allocation
SST – Suggested Sequence of Topics
SYLLABUS

1.0 INTRODUCTION TO INFORMATION SYSTEM SECURITY

1.1 Understand the need for information system security.
   1.1.1 Describe the need for information system security.
   1.1.2 Identify characteristics of information system security (CIA):
      a. Confidentiality (C)
      b. Integrity (I)
      c. Availability (A)

1.1.3 Apply the characteristics of CIA in real environment.
1.1.4 Identify potential risks to information system security.
1.1.5 Explain the goals of security policies.
1.1.6 Describe Open Security Models.
1.1.7 Describe Restrictive Security Models.
1.1.8 Describe Closed Security Models.
1.1.9 Identify the roles of the information security organizations:
      a. CERT/CC (The CERT Coordination Center)
      b. US-CERT (United States Computer Emergency Readiness Team)
      c. SANS Institute (SysAdmin, Audit, Network, Security Institute)
      d. ISC² (International Information Systems Security Certification Consortium, Inc)
      e. FIPS (Federal Information Processing Standards)
      f. ICSA (International Computer Security Association)

1.2 Describe the increasing issues of on-line security.
   1.2.1 Identify threats issues of on-line security medium:
      a. Electronic Mail and news
      b. File transfer
      c. Remote Access to hosts
      d. Real time conferencing services

1.2.2 Describe the following terms:
      a. Information theft
      b. Unauthorized disclosure
      c. Information warfare
      d. Accidental data loss
      e. Data disclosure
      f. Data modification
      g. Data availability

2.0 INTRODUCTION TO VULNERABILITIES, THREATS AND ATTACK

2.1 Describe vulnerabilities, threats and attacks.
   2.1.1 Define vulnerability in relation to security.
   2.1.2 Describe the following weaknesses in relation to security vulnerabilities:
      a. Technology
      b. Configuration
2.1.3 Define the security threats.
2.1.4 Describe different types of threats:
   a. unstructured threats
   b. structured threats
   c. external threats
   d. internal threats
2.1.5 Identify the attackers in information security:
   a. Hackers
   b. Attackers
   c. Script kiddies
   d. Cybercriminals
2.1.6 Explain various types of attacks:
   a. Reconnaissance attack (e.g sniffing, spoofing)
   b. Access attack (e.g hacking, brute force)
   c. Denial of Service attack
   d. Distributed Denial of Service attacks
   e. Malicious code attack (e.g Worms, Viruses, Trojan horses)
2.1.7 Determine on how to secure assets in banking, business and financial.

2.2 Use various tools in network security.
2.2.1 Use any of the following network scanning tools:
   a. Network Mapper (Nmap)
   b. Netstat tool
   c. NetScan tool
2.2.2 Use various security analysis tools:
   a. open source tools such as Knoppix tools
   b. Microsoft tools such as Microsoft Baseline Security Analyzer (MBSA)

3.0 SECURITY DEVICES AND TECHNOLOGIES

3.1 Apply end point protection and management.
3.1.1 Describe device hardening in host and server based.
3.1.2 Implement the following host and server based security components and technologies:
   a. Anti-virus Software
   b. Personal Firewall
   c. Operating System Patches
   d. Intrusion Detection and Prevention System
   e. Host-based Intrusion Detection Systems

3.2 Understand firewalls.
3.2.1 Describe Firewall architecture.
3.2.2 Explain the various types of firewalls:
a. IP Packet filtering firewall
b. Circuit-level Gateways
c. Application Level Firewall

3.2.3 State the three common technologies employed in building firewalls:
  a. static packet filtering
  b. dynamic packet filtering
  c. proxy

3.2.4 Explain how static packet filtering works.
3.2.5 Explain how dynamic packet filtering works.
3.2.6 Explain how a proxy passes the network traffic.
3.2.7 Compare between static packet filters, dynamic packet filter and proxy-based firewall, in relation to security features that each technology provides.

3.3 Configure firewalls using Microsoft Windows Server and Open Source Software.
3.3.1 Create a firewall that runs on Open Source Software.
3.3.2 Create a proxy that runs on Open Source Software.
3.3.3 Create a firewall that runs on Microsoft Windows Server (ISA server).
3.3.4 Create proxy that runs on Microsoft Windows Server.

4.0 OPERATING SYSTEMS AND SECURITY

4.1 Manage Microsoft Windows security approaches.
4.1.1 Identify and configure minimum system services.
4.1.2 Implement the following System Policy:
  a. Password
  b. Account
  c. Audit
  d. User rights
4.1.3 Configure TCP/IP and IPSEC filtering.
4.1.4 Carry out system updates and hotfixes.
4.1.5 Identify Internet Information Services (IIS) vulnerability.
4.1.6 Configure security enhancement for IIS.
4.1.7 Identify and explain the features of Microsoft Security Server (ISA).
4.1.8 Configure a Microsoft Security Server.

4.2 Manage Open Source Software security approaches.
4.2.1 Perform open source Operating System updates.
4.2.2 Identify and disable unnecessary services and ports.
4.2.3 Describe system hardening with Bastille (Linux Bastion Hosts).
4.2.4 Maintain controlling and auditing of Root Access.
4.2.5 Manage System Log Files using Logging Enhancers.

4.3 Manage Linux based proxy servers.
4.3.1 Explain benefits of Linux based Proxy Server Implementation.
4.3.2 Differentiate between a Packet Filter and a Proxy Server.
4.3.3 Implement a Linux based Proxy Server (*e.g.* Squid Web Proxy Cache Server):
   a. Install the proxy cache server
   b. Configure the proxy cache server

4.3.4 Test and verify the server.

5.0 AUTHENTICATION AND ENCRYPTION TECHNOLOGY

5.1 Explain authentication and encryption technology.
   5.1.1 Define the purpose of authentication.
   5.1.2 Identify various authentication application technologies.
   5.1.3 Describe various attacks that can be launched if authentication is not implemented.

5.1.4 Define the following cryptographic terminologies:
   a. Encryption
   b. Cipher text
   c. Decryption
   d. Cryptanalysis

5.1.5 Determine how encryption can protect data from snooping and protect data from being altered.

5.1.6 Differentiate between the two classes of key-based encryption algorithms:
   a. symmetric algorithms (private)
   b. asymmetric algorithms (public)

5.1.7 Use methods of encryption:
   a. Caesar cipher
   b. Substitution cipher
   c. Vigenere tableau/ Vigenere Cipher
   d. Grid encryption

5.2 Explain Virtual Private Network (VPN) fundamentals.
   5.2.1 Describe a VPN session.
   5.2.2 Explain types of VPN:
       a. Intranet VPNs
       b. Remote Access VPNs
       c. Extranet VPNs

5.2.3 Describe VPN tunneling protocols:
   a. Point-to-Point Tunneling Protocol (PPTP)
   b. Layer 2 Tunneling Protocol (L2TP)
   c. Internet Protocol Security (IPSec)

5.2.4 State the procedure to set up a VPN.
5.2.5 Illustrate typical VPN configuration (VPN between two Internet sites).
5.2.6 Identify the various devices for a VPN connection:
       a. Firewall-based VPN
       b. Router-based VPN
       c. Dedicated software or hardware
5.2.7 State the features of good VPN products:
   a. strong authentication
   b. adequate encryption
   c. adherence to standards

6.0 DISASTER PREVENTION AND RECOVERY

6.1 Explain disaster solutions.
   6.1.1 Define disaster.
   6.1.2 Identify type of disaster:
       a. natural
       b. man-made

6.1.3 Explain the two categories of disaster solutions:
   a. maintaining or restoring a service
   b. protecting or restoring the lost, corrupted, or deleted information

6.1.4 Identify the disaster recovery principles.
6.1.5 Explain the types of disaster recovery system:
   a. Synchronous system
   b. Asynchronous system

6.1.6 State the purpose of disaster recovery plan.
6.1.7 Describe the disaster recovery planning:
   a. Security planning
   b. Program budget
   c. Organizing
   d. Training
   e. Implementation

6.2 Manage hardware for disasters handling.
6.2.1 Describe the following hardware and function in handling server disasters:
   a. UPS
   b. RAID (0,1 – 5)
   c. Redundant servers
   d. Clustering
   e. Tape backup (full, incremental, and differential backups)
REFERENCES

Main:

David R. Miller, Michael Gregg (2009), Security Administrator Street Smarts. Wiley Publishing, Inc. (ISDN: 978-0-470-40485-0)


Additional:


JPK (2010), Executive Summary-ICT System Security Technologist Level 4 & 5. Department of Skills Development MOHR
## MATRIX OF COURSE LEARNING OUTCOMES (CLO) VS PROGRAMME LEARNING OUTCOMES (PLO)

<table>
<thead>
<tr>
<th>Course Learning Outcome (CLO)</th>
<th>Compliance to PLO</th>
<th>Recommended Delivery Methods</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Explain information security vulnerabilities, threats and attacks in a network environment according to international standard such as Open Web Application Security Project (OWASP).</td>
<td>✓</td>
<td>Interactive Lecture, Discussion and Presentation</td>
<td>Quiz and Test, Final Examination</td>
</tr>
<tr>
<td>2. Configure security environment to secure information using various tools effectively.</td>
<td>✓ ✓</td>
<td>Interactive Lecture, Discussion and Laboratory Activity</td>
<td>Laboratory Exercises and Test, Final Examination</td>
</tr>
<tr>
<td>3. Work efficiently with proper techniques and procedures to create a secured environment in an organization.</td>
<td>✓ ✓</td>
<td>Interactive Lecture, Laboratory Activity, Discussion and Presentation</td>
<td>Quiz, Test and Problem Based Task, Final Examination</td>
</tr>
</tbody>
</table>

### Remark:
- LD 1 Knowledge
- LD 2 Practical Skills
- LD 3 Communication Skills
- LD 4 Critical Thinking and Problem Solving Skills
- LD 5 Social Skills and Responsibilities
- LD 6 Continuous Learning and Information Management Skills
- LD 7 Management and Entrepreneurial Skills
- LD 8 Professionalism, Ethics and Moral
- LD 9 Leadership and Teamwork Skills
ASSESSMENT

The course assessment comprises two components namely:

i. **Coursework Assessment (CA) – 50%**
   Coursework assessments that measures knowledge, practical skills and generic skills are carried out in the form of continuous assessment. Coursework assessments total score comprises the knowledge and practical marks **ONLY**. It does not include the mark of generic skills.

ii. **Final Examination Assessment (FE) – 50%**
   Final examination is carried out at the end of the semester.

### ASSESSMENT SPECIFICATION TABLE (AST)

<table>
<thead>
<tr>
<th>COURSE LEARNING OUTCOMES (CLO)</th>
<th>TOPICS</th>
<th>ASSESSMENT TASKS FOR COURSEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 2 3 4 5 6</td>
<td>Test</td>
</tr>
<tr>
<td>1. Explain information security vulnerabilities, threats and attacks in a network environment according to international standard such as Open Web Application Security Project (OWASP). (C4,PLO1)</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>2. Configure security environment to secure information using various tools effectively. (P4,C3,PLO2,PLO1)</td>
<td>• •</td>
<td></td>
</tr>
</tbody>
</table>
| 3. Work efficiently with proper techniques and procedures to create a secured environment in an organization. (A4,C3,PLO8,PLO1) | | | | | | | **√**

**Remark**

- Topic 1 : Introduction to Information System Security
- Topic 2 : Introduction to Vulnerabilities, Threats and Attack
- Topic 3 : Security Devices and Technologies
- Topic 4 : Operating Systems and Security
- Topic 5 : Authentication and Encryption Technology
- Topic 6 : Disaster Prevention and Recovery

√ Refers to the CLO to be assessed through the indicated assessment task.

*(#) # refers to the quantity of assessment

• Indicates the topic (s) to be covered under the assigned/identified assessment tasks. For merged topics, lecturers have the options of choosing the preferred topic (s).

** The generic skills are to be assessed separately. The total score for generic skills is 100%. However, it is NOT PART of the coursework assessment mark.
### DISTRIBUTION OF STUDENT LEARNING TIME (SLT)

**ACCORDING TO COURSE LEARNING - TEACHING ACTIVITY**

<table>
<thead>
<tr>
<th>No.</th>
<th>Learning and Teaching Activity</th>
<th>SLT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEPENDENT LEARNING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>Delivery Method</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Lecture</td>
<td>30</td>
</tr>
<tr>
<td>1.2</td>
<td>Practical</td>
<td>30</td>
</tr>
<tr>
<td>1.3</td>
<td>Tutorial</td>
<td>0</td>
</tr>
<tr>
<td>2.0</td>
<td>Coursework Assessment (CA)</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Lecture-hour-assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Test</td>
<td>[1]</td>
</tr>
<tr>
<td></td>
<td>- Quiz</td>
<td>[3]</td>
</tr>
<tr>
<td>2.2</td>
<td>Practical-hour-assessment</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>- Laboratory Exercises</td>
<td>[3]</td>
</tr>
<tr>
<td>2.3</td>
<td>Tutorial-hour-assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- None</td>
<td></td>
</tr>
<tr>
<td><strong>INDEPENDENT LEARNING</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.0</td>
<td>Coursework Assessment (CA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Problem Based Task</td>
<td>[1]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>4.0</td>
<td>Preparation and Review</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Lecture</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>- Preparation before theory class eg: download lesson notes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Review after theory class eg: additional references, discussion group,discussion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Preparation for quizzes.</td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Practical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Preparation before practical class/field work /survey eg: review notes, check list/ labsheets and/or tools and equipment.</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>- Post practical activity eg: lab report, additional references and discussion session</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Preparation before studio work presentation/critique.</td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>Tutorial</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Preparation for tutorial</td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>Assessment</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>- Preparation for test.</td>
<td>[1]</td>
</tr>
<tr>
<td></td>
<td>- Preparation for final examination.</td>
<td>4</td>
</tr>
<tr>
<td><strong>FINAL EXAMINATION</strong></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>120</td>
</tr>
<tr>
<td></td>
<td>Credit = SLT/40</td>
<td>3</td>
</tr>
</tbody>
</table>

### Remark:
1. Suggested time for
   - Quiz : 10 - 15 minutes
   - Test (Theory) : 30 - 60 minutes
2. Laboratory Exercises are conducted during practical hours
3. 40 hours is equivalent to 1 credit