SUBJECT DESCRIPTION FORM

Subject title: Security in Data Communication

Subject code: EIE553

Credit value: 3

Responsible staff and department:
Dr C.K. Leung, EIE

Pre-requisite:
Nil

Recommended background knowledge:
The students are expected to have some background knowledge about TCP/IP protocol suite.

Mutual exclusions: Nil

Learning approach:
This subject adopts an exploratory and hands-on approach to learning and teaching. Case studies, projects, hands-on exercises, and practical works will be adopted to ensure deep learning for the students. Problem-solving and application with consideration of constraints will be emphasized. Students will be motivated and given a variety of opportunities to apply what they have learned in order to strengthen their learning.

<table>
<thead>
<tr>
<th>Lecture/Tutorial</th>
<th>30 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical</td>
<td>12 hours</td>
</tr>
</tbody>
</table>

Assessment:

<table>
<thead>
<tr>
<th>Continuous Assessment*</th>
<th>70%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examination</td>
<td>30%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

* Continuous assessment suggestive distribution: 3 homework/Assignments: 15%, 2 laboratory reports: 20%, 2 tests: 20%, 1 case Study (report and presentation): 15% (Total=70%)

Objectives:
This subject aims at providing senior students, practicing engineers and information system professionals, who will study network security for the first time, a solid foundation about information security in the context of data communication and computer networking. After attending this course, the students will master the basic principles of network and information security. They will also learn to apply these principles in various scenarios. They will be able to design simple solutions to meet different security requirements in networking applications by using suitable tools and selecting the appropriate parameters.
**Keyword syllabus:**

1. **Communication Theory of Secrecy Systems**
   Shannon’s theory of communication secrecy: structure of secrecy systems, criteria of secrecy systems valuations, theoretical secrecy, unicity distance, perfect security and conditional security.

2. **Cryptography Basis**
   Basic mathematical tools for cryptographic applications: Private key encryption, public key encryption, secure hash function, digital signature, certification authority, public key infrastructure.

3. **Secure Communication in The Internet**
   Security issues and threats, secure communication protocols, authentication, ITU-T X.509 standard and Kerberos, network address translation, packet filtering, firewall design and implementation.

4. **Virtual Private Networks**
   Data confidentiality and authenticity in the Internet, tunnelling protocols, Virtual Private Network installation and configuration with VPN routers.

5. **IP Security Architecture and Protocols**
   The IP Security (IPSec) architecture and protocols, authentication (Authentication Header, AH), confidentiality (IP Encapsulating Security Payload, ESP), security association, key management.

---

**Text book and references:**

**Text Book:**

**General References and standards:**

**Classics Paper**

---

**Practical Works:**

**Laboratory Exercise:**
1. A Study of Internet Security by Packet Analysis
2. A Study of IPSec and VPN with VPN routers.

**Practical works and Case Studies:**
3. English redundancy analysis and security evaluation
4. Cryptanalysis of keyword cipher
5. Email attack analysis

**Case Study Project:**
6. An in-depth study of a selected topic on network security, with report writing and presentation.

June 2009