1. Overview

Description

This module develops an appreciation of the fundamentals and design principles for information assurance and security. Students will develop a clear understanding of the basic information security services and mechanisms, which will enable them to design and evaluate the integration of solutions into the user application environment. Emphasis will be placed on services such as authorisation and confidentiality. Students will acquire knowledge and skills of Security Models such as the Bell-LaPadula, Harrison-Ruzzo-Ullman and Chinese Wall Model. Students will develop a detailed understanding of the confidentiality services by focusing on cryptology and the practical implication thereof. Students will be introduced to professional and philosophical ethics. At the end of the module students will be able to engage in a debate regarding the impact (local and global) of computers on individuals, organisations and society. The professionalism of IT staff will be discussed against national and international codes of practice such as those of the CSSA, ACM and IEEE.
Prerequisites

COS 110 (Program Design: An Introduction) must be completed before this module may be taken.

Related modules

This module assumes knowledge of topics covered in the following courses: Netcentric Computer Systems (COS 216), Operating Systems (COS 222), Database Systems (COS 326), Computer Networks (COS 332). Information Science: Social and ethical impact (INL240) is related to some of the material covered in this course. Computer Security (COS720) and Information Security (COS721) will follow on this course on honours level.

Study units

This module will broadly look at some of the following units as central to the main themes in Computer Security:
- Access control models
- Cryptography
- Program Security
- Operating System Security
- Network Security
- Administering Security
- Professional and ethical responsibilities
- Intellectual property
- Privacy and civil liberties
- Social context of computing

2. Outcomes

Career

The aim of the course is to equip students with a broad knowledge of Computer Security and Ethics. This will equip students for any ICT career where computer security is used or developed on a continuous basis.

Course

During the course we will focus on the following outcomes subject to be modified at the discretion of the lecturer:
- Discuss the fundamental ideas of public-key cryptography. Discuss how public-key cryptography works. Distinguish between the use of private-and public-key algorithms. Summarise common authentication protocols. Generate and distribute a PGP package to send an encrypted e-mail message. Summarise the capabilities and limitations of the means of cryptography that are conveniently available to the general public.
- Identify progressive stages in a whistle-blowing incident (Sarbanes-Oxley general case). Specify the strengths and weaknesses of relevant professional codes as expressions of professionalism and guides to decision-making. Identify ethical issues that arise in software development and determine how to address them technically and ethically. Develop a computer use policy with enforcement measures. Analyse a global computing issue, observing the role of professionals and government officials in managing the problem. Evaluate the professional codes of ethics from the ACM, The IEEE Computer Society, and other organisations.

- Identify appropriate access control models for different operating environments. Understand the formal specification of access control models such as Bell-LaPadula.

- Distinguish among patent, copyright, and trade secret protection. Discuss the legal background of copyright in national and international law. Describe how patent and copyright laws may vary internationally. Outline the historical development of software patents. Discuss the consequences of software piracy on software developers and the role of relevant enforcement organisations.

- Summarise the legal bases for the right to privacy and freedom of expression in one's own nation and how those concepts vary from country to country. Describe current computer-based threats to privacy. Explain how the internet may change the historical balance in protecting freedom of expression. Explain both the disadvantages and advantages of free expression in cyberspace. Describe trends in privacy protection as exemplified in technology.

- Outline the technical basis of viruses and denial-of-service attacks. Enumerate techniques to combat “cracker” attacks. Discuss several different “cracker" strategies. Identify the professional's role in security and the trade-offs involved.

- Summarise the rationale for anti-monopoly efforts, such as the Microsoft case. Describe several ways in which the information technology industry is affected by shortages in the labour supply. Suggest and defend ways to address limitations on access to computing. Outline the evolution of pricing strategies for computing goods and services.

- Summarise and apply the basic concepts of virtue ethics, utilitarianism, and deontological ethics. Distinguish between what is ethical and what is legal. Identify the strengths and weaknesses of the “hired agent" approach, strict legalism, extreme individualism, and relativism as ethical frameworks.


- Introduction to social implications of computing and the digital revolution.

- Students will be introduced to a few varying ethical decision-making models.

- Identify typical pitfalls in 'ethics talk': Extreme individualism and relativism, group think and passing the buck.
3. Plagiarism policy

The Department of Computer Science considers plagiarism as a serious offence. Disciplinary action will be taken against students who commit plagiarism. Plagiarism includes copying someone else’s work without consent, copying a friend’s work (even with consent) and copying material (such as text or program code) from the Internet.

Copying will not be tolerated in this course. For a formal definition of plagiarism, the student is referred to http://www.ais.up.ac.za/plagiarism/index.htm. (From the main page of the University of Pretoria site, follow the Library quick link, and then click the Plagiarism link). If you have any form of question regarding this, please ask one of the lecturers. Also note that the OOP principle of code re-use does not mean that you should copy and adapt code to suit your solution.

4. Study Material

You are advised to regularly monitor the COS330 website at http://www.cs.up.ac.za/courses/COS330 for any updates and new announcements. You should treat this website as part and parcel of this study guide.

Class attendance is vital to maintain a good academic record. Additional material may also be discussed during lectures, not found in the published study material. Please ensure that you attend these forums so that you are aware of important announcements, additional discussions and material not covered in this study guide.

Prescribed book

Title: Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach
Authors: Charles P. Pfleeger and Shari L. Pfleeger
Publisher: Prentice Hall
ISBN: 9780132901062

Additional references

During the course, lecturers may prescribe a number of articles. References will be given, and it is the students’ responsibility to ensure that they obtain a copy. Note that such material is examinable, unless stated otherwise.

Software

All of the software you are required to familiarise yourself with will be available on the computer in the Informatorium. Some software will be made available on the COS330 web site. The prescribed text also lists several websites, where some of the software that is used in this course can be obtained.
5. Assessment

Semester test
One semester test will be written on Friday 18 September 2015, 17:30 in CENT 2. The scope will be announced closer to the test date on the COS330 website.

Class tests
A number of short class tests might be written during the semester. These class tests will be unannounced and students should always be prepared to write a class tests. The scope of a class test can cover any work already discussed during the past lectures.

Examination
All the work covered during the semester will be examinable. Please make sure to check the course website towards the end of the semester for any updates. The exam date will be announced at a later stage. It is imperative to attend lectures to be fully aware of possible exam questions.

Final mark:
Examination mark 50%; semester mark 50%

Semester mark:
Semester test 50%
Class tests 20%
Practical assignments 30%

Subminimum: 40% semester mark; 40% examination

6. Absence from assessment

The Department of Computer Science has the following policy about being absent from any assessment. A valid sick note needs to be handed to one of the lecturers in person NO LATER THAN 3 (three) days to the hour after the assessment opportunity took place. If no such valid documentation has been provided within the three days, the student cannot be accommodated.

Note that, due to EBIT Faculty regulations, lecturers may not accept any sick letters or similar documentation for the absence from the exam. All such valid documentation needs to be handed in at Faculty Administration, Engineering Building 1, level 6.

7. Lecture schedule

There are two (2) lectures per week for COS 330, as follows:

<table>
<thead>
<tr>
<th>Day</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>07:30-08:20</td>
<td>IT 2-26</td>
</tr>
<tr>
<td>Thursday</td>
<td>07:30-08:20</td>
<td>IT 4-4</td>
</tr>
</tbody>
</table>
The detailed schedule is as follows.

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>23/7</td>
<td>Chapter 1: Introduction</td>
</tr>
<tr>
<td>2</td>
<td>27,30/7</td>
<td>Chapter 1: Security theatre</td>
</tr>
<tr>
<td>3</td>
<td>3,6/8</td>
<td>Chapter 2: Knock, Knock. Who’s There?</td>
</tr>
<tr>
<td>4</td>
<td>13/8</td>
<td>Chapter 3: 2+2 = 5 (No class Monday 10 Aug – public holiday)</td>
</tr>
<tr>
<td>5</td>
<td>17,20/8</td>
<td>Chapter 3: 2+2 = 5 (Remainder of chapter)</td>
</tr>
<tr>
<td>6</td>
<td>24,27/8</td>
<td>Chapter 4: A Horse of a Different Color</td>
</tr>
<tr>
<td>7</td>
<td>31/8,3/9</td>
<td>Chapter 5: The Keys to the Kingdom</td>
</tr>
<tr>
<td>8</td>
<td>6,10/9</td>
<td>Chapter 6: My cup runneth over and Interlude A: Cloud computing</td>
</tr>
<tr>
<td>9</td>
<td>14,17/9</td>
<td>Chapter 9: Scanning the Horizon</td>
</tr>
<tr>
<td>10</td>
<td>18/9</td>
<td>Semester Test in CENT 2, 17:30 on Chapters 1-6.</td>
</tr>
<tr>
<td>11</td>
<td>21/9</td>
<td>Guest lecture – to be confirmed. No lecture 24/9 – public holiday.</td>
</tr>
<tr>
<td>12</td>
<td>28/9,1/10</td>
<td>Chapter 10: Do you hear what I hear?</td>
</tr>
<tr>
<td>13</td>
<td>5,8/10</td>
<td>Recess – no lectures</td>
</tr>
<tr>
<td>14</td>
<td>12,15/10</td>
<td>Chapter 7: He Who Steals My Purse ...</td>
</tr>
<tr>
<td>15</td>
<td>19,22/10</td>
<td>Chapter 8: The Root of All Evil</td>
</tr>
<tr>
<td>16</td>
<td>26,29/10</td>
<td>Chapter 11: I hear you loud and clear!</td>
</tr>
<tr>
<td></td>
<td>2/11,5,11</td>
<td>Guest lectures: TBC</td>
</tr>
<tr>
<td>23/11</td>
<td></td>
<td>Exam: 8:00-11:00, covering all work as shown in this schedule.</td>
</tr>
</tbody>
</table>

8. Project Detail

The practical portion will consist of several smaller practicals and may include one or more implementation projects carrying equal weights. Details will be provided separately on the course website.