2012

COURSE OUTLINE FOR COSC425

Computer Forensics and Cybercrime

Course Supervisor:
Ray Hunt ray.hunt@canterbury.ac.nz

Course Lecturer:
Milton Baar, 02 7874 8869, milton.baar@canterbury.ac.nz

Lectures will be held Friday at 1500.

Objectives of the Course

This course is designed to build on the work of COSC331/COSC364 and COSC332/COSC362, which are both strongly recommended preparation courses, and is designed to be taken as part of the Post Graduate Diploma (Computer Security and Forensics) or as a paper for Part 1 Masters or Honours. This course is intended to provide students with greater depth of study in a number of key topics in the area of computer security in society: cybercrime, computer and forensics, analysis. The course also involves significant practical work involving the development and use of forensics analysis tools.

Topics include:

- Accounting Forensics
- Sarbanes-Oxley Financial and Accounting Disclosure Information
- Computer Crime and Criminals
- Computer Forensics
- Network Forensics
- Forensics Tools
- Liturgical Procedures

Learning Outcomes

- Understand financial and accounting forensics, and explain their role in preventing various forms of fraud.
- Distinguish various types of computer crime, and use computer forensic techniques to identify the digital fingerprints associated with criminal activities.
- Know how to apply forensic analysis tools to recover important evidence for identifying computer crime.
- Be able to develop a custom computer forensic analysis tool.

Reference Material

All information relating to this course (including this document) can be found on UCLearn at http://learn.canterbury.ac.nz/course/view.php?id=1176

This course does not have a textbook, but course notes and papers will be handed out prior to the corresponding lectures. For a general overview of computer forensics, please consult:

- Computer Forensics (US-CERT): http://learn.canterbury.ac.nz/mod/resource/view.php?id=139624
- An Overview of Computer Forensics: http://learn.canterbury.ac.nz/mod/resource/view.php?id=139631

Assessment

Students will be required to complete one assignment, which involves developing a computer forensics tool. This assignment requires a written report, code, and demonstration of the tool's operation. The assignment may be completed individually

or in pairs. Development tools are available in Lab 3 (Security and Forensics lab). Some of the tool's functionality will include:

- Disk analysis and cloning
- Physical sector access
- Case management
- File system detection and search operations

You will work on the assignment during Lab time and also, if required, at other times outside this unit. The assignment must be submitted to the lecturer for review in week 8 and in week 9 students will present their work to the class.

Students will also sit for an end of course test that is worth 50% of the final mark.

Teaching Schedule

Teaching will combine lectures, slides and handouts, pre-reading and lab work. Each lecture will be recorded for audio and the mp3 file will be available on Learn after the lecture. Weeks 3, 6 and 7 will have no face-to-face lecture, but there will be the slides, handouts and pre-recorded audio available to replace attendance requirements.

Topic	**Date**	**Contribution to Final Mark**
Introduction/Accounting Forensics (1)	24-FEB-12	
Accounting Forensics (2)	2-MAR-12	
Sarbanes-Oxley Financial and Accounting Forensics	9-MAR-12*	
Cybercrime and Criminals	16-MAR-12	
Liturgical Procedures/Digital Trails and Storage Systems	23-MAR-12	
Application and Appliance Trails/Hidden Evidence	30-MAR-12*	
Network Forensics (1)	27-APR-12*	
Network Forensics (2)	4-MAY-12	
Revision	11-MAY-12	
Code and Proof of Successful Operation	4-MAY-12	35%
Written Report Submission	11-MAY-12	10%
Assignment Presentations	11-MAY-12	5%
End of Course Test (2 hours)	1-JUN-2012	50%

NOTE: *Weeks marked with an * (weeks 3, 6 and 7) will be taught via pre-recorded audio and there will be no lecture to attend that week. Lab work may be undertaken in the Lab or on your own equipment at any location.*

The Computer Science department has the following grading policy.

1. In order to pass a course you must meet the *absolute* passing mark for the class; i.e. the percentage of *all* your scored items must meet the absolute passing mark set for the class. Marks are sometimes scaled to achieve consistency between courses from year to year. Specific passing marks are therefore set on a class-by-class basis. For example, a total mark of 50% would typically be required to achieve a C pass; although this may vary. Passing a course with a C indicates that we believe that you have *just* mastered the relevant material. Your *ranking* in the class may be a more useful indicator of your progress; students ranked above you will receive higher grades, and vice versa.
2. You must average at least 45% on the invigilated assessment items. (Invigilated assessment items are those completed under exam conditions, such as oral and written exams and lab tests.) If you achieve less than 45% over these items, you will receive a C- (for 100- and 200-level courses only), D, or E, depending on your marks.

NOTE: The online notices are the *only* definitive source of information on tests.

Other Important Documents

There are several important documents available online about departmental regulations, policies and guidelines at the following site. We expect all students to be familiar with these.

http://www.cosc.canterbury.ac.nz/regulations

Notices about this class will be posted to the class forum in the Learn system (see learn.canterbury.ac.nz). COSC students will also be made members of a class called "CSSE Notices", where general notices will be posted that apply to all classes (such as information about building access or job opportunities).