CS4615 Systems Security

Simon Foley,
(WGB, Room G-65)
Department of Computer Science,
University College Cork
s.foley@cs.ucc.ie

January 11, 2016

Syllabus

"Access control models. Mandatory access control models and mechanisms. Operating system security, including Unix and Java2. Network Access Controls. Code-level vulnerabilities. Malicious software. Security risk management and audit."

- While CS4614 focussed on providing end-to-end security across an untrusted network, this course will look at the principles of securing the individual systems. This includes models of operating system security, securing services, secure software development and some aspects of security governance.
- The course will focus more on understanding the principles that underly the design of security mechanisms than provide instruction on particular security technologies.
- The Java security model will be examined in some depth, as an example of a practical security system that embodies many important security design principles.

Learning Outcomes

On successful completion of this module students should be able to:

- ☐ Distinguish between different types of security policy model
- ☐ Compromise existing systems by exploiting common vulnerabilities
- ☐ Develop applications that avoid basic security vulnerabilities
- ☐ Use the Java security architecture to provide support for secure application systems
- ☐ Conduct a security assessment of a system.

Prerequisites

Since we'll be looking at the Java security model CS2500 (Java) is a prerequisite.

It is also assumed that you have an understanding of computer operating systems, elementary discrete mathematics, application development and the usual problem solving skills.

Recommended Material/Textbooks

Notes will be provided in class. Note that *it is the students' responsibility to augment these with their own notes of material covered in class and tutorials*.

There are a number of good textbooks available and these can provide a second opinion and more in-depth coverage of material discussed in lectures.

Useful text books (in library) for the course include the following.

- Matt Bishop, *Introduction to Computer Security*. Addison Wesley.
- Dieter Gollmann, *Computer Security*, Wiley Publishers.

Excellent books on computer security in general:

- Bruce Schneier, Applied Cryptography, Wiley Publishers.
- Ross Anderson, Security Engineering, `http://www.cl.cam.ac.uk/~rja14/book.html`

Also checkout: `http://security.stackexchange.com`,

Logistics

Two lectures each week, Semester 2. These are currently scheduled as: Monday 09h00-10h00, WGB G02, and Tuesday 13h00-14h00, WGB G15. You are expected to attend all lectures.

Some tutorials will be scheduled, during which I'm happy further clarify class material, discuss exam strategy, work on problem sheets, past exam questions, and so forth. You should attend all tutorials.

Total marks for this course is 100, including 10 marks for continuous assessment, which will be in the form of one in-lab exercises (5 marks) and one hand-up/programming exercise (5 marks).

Course Website hosted at `http://cs4.ucc.ie/moodle/`

If you decide to take this module then you **must** register on the module website *before* the end of January 2013.

Logistics II (rough outline/subject to change)

Weeks and Lectures:

W1 Introduction
W1-4 Security models and access control
W5-7 Java security
W7-W9 Security Risk and Compliance
W10-W12 Various systems and networks security mechanisms

Weeks and Assignments (exact deadlines announced in lectures):

W5 Security modeling exercise in lab
W8 Java security programming exercise/handup

Final Examination

Course runs during Semester 2 and examined in the summer examinations.

This module is 5 ECTS credits. The exam paper is graded out of 90 marks with 10 marks for Continuous Assessment.

Past papers available on library website (also look for CS4253). Exam paper/solutions will be discussed at end of semester.

Exam questions cover: straightforward regurgitation of material; a reasonably familiar problem that requires application of knowledge, or intended to stretch the student with more challenging/unfamiliar problems.

The intention is that a student who can regurgitate material can pass; a student who not only 'knows' the material but can apply it in straightforward ways can achieve a second class honours student. A first class honours fits the two previous categories and can apply the knowledge in more challenging ways to trickier and unfamiliar problems.

Semesterization

According to National Framework of Qualifications guidelines and European Credit Transfer and Accumulation System (ECTS) Users Guide 2009 a 5-credit module can correspond to between 100 and 150 hours of student effort. This includes lectures, labs, tutorials and independent study. Therefore, you should typically spend at least 6.6 hours of your time per week on CS4615.

"By failing to prepare, you are preparing to fail" [Benjamin Franklin]

Attendance [UCC regulations]

Every student registered for a diploma or degree is expected to attend all lectures, tutorials, laboratory classes etc. In the case of absence through illness, a student must, if possible, give notice of each absence in writing to the Lecturer concerned and/or Head of Department responsible. In the case of such absence for more than four lecture days the student must, on resuming attendance, notify the Lecturer concerned and/or Head of Department in writing and, if required by the Lecturer and/or Head of Department to do so, lodge a medical certificate with the Head of Department, who in turn will send a copy to the Student Records and Examinations.

A student will not be permitted to enter for an examination at the conclusion of a module if attendance at that module is not considered satisfactory by the Registrar and Senior Vice-President Academic following a report by the Lecturer concerned and/or Head of Department responsible for the module. The decision of the Registrar and Senior Vice-President Academic is subject to the appeal of the Academic Council of the University.

UCC Plagiarism Policy

"1.1 Plagiarism is the presentation of someone elses work as your own. When done deliberately, it is cheating, since it is an attempt to claim credit for work not done by you and fails to give credit for the work of others. Plagiarism applies not just to text, but to graphics, tables, formulae, or any representation of ideas in print, electronic or any other media. "

Read
`http://www.ucc.ie/en/exams/procedures-regulations/plagiarism/`