Course Directive
IN618 Security
Semester One, 2015

Description

If we were to survey a sample of IT professionals all, or very nearly all, of them would say that security is a critically important property for IT systems. If we then asked them how we can build and operate secure systems their responses would be less clear. This is because security is a hard problem. Basically, a secure system is one that *doesn't* suffer from a huge class of design and implementation flaws. This means that we're in the impossible position of trying to prove not just one, but in fact many negatives. Security is hard, and perfect security is completely out of the question.

The news isn't all bad, however. There are concrete things we can do to avoid vulnerabilities and reduce risk. In the process of exploring those things we hope to gain some experience and insight to help us deal with other security problems that may present themselves in the future. That is our plan for this paper. We will not become security experts in this paper. Instead, we will try to introduce some sensible security practices that you can use in your IT work.

Course Information

- 15 Credits
- No prerequisites

Lecturer

Tom Clark

Office:	D311
Phone:	470 4356
Email:	`tom.clark@op.ac.nz`
GitHub:	`https://github.com/tclark`

Course Dates

Term 1 (7 weeks)	16 February - 2 April
Term 2 (9 weeks)	20 April - 19 June

Learning Outcomes

On completion of this paper you will be able to:

1. Assess IT security risks and prioritise risk reduction and mitigation measures;
2. Understand common software and system security vulnerabilities;
3. Write computer programs in a manner that avoids introducing vulnerabilities;
4. Deploy IT systems according to security best practices.

Resources

- Course notes, lecture slides, and lab documents are availble in a GitHub repository published at `https://github.com/tclark/op-papers`.
- Although it is not a required text, much of the material covered in this paper is adapted from the book *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them* by Michael Howard, David LeBlanc, and John Viega.
- Another interesting book on the topic is *Engineering Security* by Peter Gutmann. It is available in draft form at `https://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf`.

Course Content and Schedule

This schedule is subject to change based on the needs of the class.

Week	Week Start	Monday	Thursday
1	16 Feb	Introduction	Risk Analysis
2	23 Feb	Password Hashing	Authentication
3	2 Mar	XSS	XSS
4	9 Mar	XSS	XSS
5	16 Mar	XSRF	XSRF
6	23 Mar	Otago Ann. Day	Other Web Vulnerabilities
7	30 Mar	SQL Injection	SQL Injection
H1	6 Apr	Holiday	Holiday
H2	13 Apr	Holiday	Holiday
8	20 Apr	Buffer Overflows	Buffer Overflows
9	27 Apr	ANZAC Holiday	Error Handling
10	4 May	Information Leakage	Information Leakage
11	11 May	Protecting Data	Protecting Data
12	18 May	Securing Network Traffic	Securing Network Traffic
13	25 May	Server Hardening	Server Hardening
14	1 Jun	Queen's Birthday	Incident response
15	8 Jun	Forensic Analysis	Forensic analysis
16	15 Jun	Vulnerability Reporting	Vulnerability Information

Assessment

Your assessment for this paper is comprised of a set of lab assignments, approximately one each week. Each lab will be marked on a ten point scale and will be averaged over the semester to determine your overall mark. Programming labs will contribute 60% of your final mark while systems administration labs will contribute the remaining 40%

Criteria for Passing

You must earn an overall average mark of 50% or better to pass this paper.

Course Requirements and Expectations

Attendance

- Students are expected to attend all classes, both lectures and labs.
- If you miss a class you should get notes from another student.
- If you cannot attend for two or more consecutive sessions, contact the lecturer.
- You must be present for assessments on the due date at the correct time.

Communication

Important announcements and discussions about the course, assessments, and scheduling may take place during class sessions. It is your responsibility to be informed about them. If you cannot attend a class session, be sure to check with another student.

Your student email is an official communication channel. It is your responsibility to regularly check your student email for important course related material, including changes to class scheduling or assessment details. Not checking will not be accepted as an excuse.

You can manage your email at the Student Hub and download the instructions for forwarding your email at `http://www.op.ac.nz/students/student-hub/`

Polytechnic Closure

In the event that the Polytechnic is closed or has a delayed opening because of snow or bad weather, you should not attempt to attend class if it is unsafe to do so. It is possible that your instructor will not be able to attend either, so classes will not physically be meeting. However, this does not become a holiday. Rather, material will be available on the Cisco Academy web site covering the material for classes affected by the closure. You are responsible for any material presented in this manner. Information about closure will be posted on the Otago Polytechnic facebook page `https://www.facebook.com/OtagoPoly`.

Group Work and Originality

Students in the Bachelor of Information Technology degree are expected to hand in original work. Students are encouraged to discuss assignments with their fellow students. However, all assignments are to be completed as individual works unless group work is explicitly involved. Failure to submit your own unique work will be treated as plagiarism.

Referencing

Appropriate referencing is required for all work. Referencing standards will be specified by your instructor.

Plagiarism

Plagiarism is submitting someone else's work as your own. Plagiarism offences are taken seriously and an assessment that has been plagiarised may be awarded a zero mark. A definition of plagiarism is in the Student Handbook, available online or at the school office.

Submission Requirements

All assignments are to be submitted by the time, date, and method given when the assignment is issued.

Extensions

Extensions are only available for unusual circumstances. These must be applied for, and approved, prior to the submission deadline.

Impairment

In case of sickness contact your lecturer or year co-ordinator as soon as possible, preferably before the test or assignment is due. The policy regarding the granting of a mark that considers impaired performance requires a medical certificate and a medical practitioners signature on a form. You may should refer to the guide on impaired performance on the student handbook.

Appeals

If you are concerned about any aspect of your assessment, please approach the lecturer in the first instance. We support an open door policy and aim to resolve issues promptly. Further support is available from the Programme Manager and Head of School. Otago Polytechnic has a formal process for academic appeals if necessary.

Other Documents

Regulatory documents relating this course can be found on the Polytechnic website.

Special Resources and Requirements

If you have any special needs, whether they relate to the course material, the exercises, the assessment, or anything in the course - then *please* let your instructor know as soon as possible.