SE4C03: Computer Networks and Computer Security
Winter 2005

1 Instructor:

Dr. Kartik K. Sivaramakrishnan
Coordinates: ITB 106
Phone: (905) 525-9140 ext. 27765
Email: kartik@optlab.mcmaster.ca
URL: http://optlab.mcmaster.ca/~kartik

2 Teaching Assistants:

1. Xinjun Wu (wux8@mcmaster.ca)
2. Shu Wang (shuw@mcmaster.ca)

Xinjun and Shu will post their office coordinates and office hours on the course webpage shortly.

3 When and Where:

Tuesday, Thursday, and Friday between 8.30-9.20 AM at ABB 164. Kartik’s office hours are Tuesday, Thursday, and Friday between 1-2 PM, and by appointment. To set up an appointment, please send me email. We will have a lab session every Wednesday between 2.30-5.20 pm.

4 Course webpage:

The webpage for this course is located at http://optlab.cas.mcmaster.ca/~kartik/sfwr4c03/spring2005.html.
Please check the webpage regularly for announcements regarding the course. I will also post all the course material, including course handouts, homeworks, exams etc here. I will try and keep this webpage up to date. Please inform me about missing links and necessary updates by sending email to kartik at optlab.mcmaster.ca.
5 Course Outline:

The first part of the course is concerned with the design of software for efficient communication between computers. In particular, we will learn how computer networks comprising the internet are organized, and the various protocols (TCP/IP) used in computer communication. Network security has become increasingly important with the growth in the number and importance of computer networks, and we will also discuss a variety of security techniques and services in the second part of the class. In particular, we will look at encryption techniques for ensuring confidentiality, which includes the use of conventional and public-key encryption. The two important encryption algorithms DES and RSA are examined. We will also discuss IP security standards, and firewall design. I intend to follow this outline closely, but, if appropriate, and as time permits, shall alter what is included in the course. The first part of the course on networking will cover sections of Chapters 1-13, 20-21, 24-28, and 31-33 in the book by Comer. The 2nd half of the course on network security will cover sections of Chapters 1-6, 9-10, 17, 19-21, 23, 25 in the book by Kaufman, Perlman, and Speciner.

Here is a tentative list of topics we will cover during the course.

1. Preliminaries
2. Review of physical networks and underlying network technologies
3. The Internet Protocol (IP)
4. The Transmission Control Protocol (TCP)
5. Routing protocols and algorithms
6. Applications (TELNET, FTP, SMTP, HTTP)
8. Internet Security and Firewall Design

6 Lab exercises:

There will be five lab exercises performed by the students outside of class usually working in groups of two or three people. The lab exercises will be performed on an experimental internet of Intel computers running Linux located in ITB 238. Your job includes configuring and securing this internet of workstations. The lab exercises are normally run by the two TA’s. You are welcome to discuss the lab exercises with other students, but the final work should be your own. If you encounter any problems in the lab exercises, please send me email, or discuss them with me during office hours.
7 Course Project:

Each student will individually do a research project on some new network or security technology. The project will consist of two parts:

1. A proposal for what technology to investigate.
2. A 2-3 page summary presenting the technology.

You are encouraged to come up with research projects of your own. I will also provide a listing of tentative research projects after the midterm exam. The proposals are due in the middle of March, while the final report is due in mid April. More details will be available soon.

8 Exams:

We will have two in-class open book exams: a midterm, and a final. The midterm exam is about an hour long and will be held in class on Friday, the 18th of February 2005 between 8.30-9.20 AM. The final exam is a two hour exam, and will take place on the date scheduled by the University. The term open book refers to open book and notes. As you would expect, each exam has to be your own work.

9 Honor Code Policy:

1. You are encouraged to discuss the lab exercises, research project with other students, but the final work should be your own. It is part of your professional responsibility to give credit to all those who have contributed to your work, and a description of the information you received.

2. Your research proposal and report must be your own. Copying and plagiarism will not be tolerated, and will be considered as academic dishonesty.

3. It is your responsibility to meet the deadlines for the lab exercises, and research project. You may not turn these in late, or take the midterm or final exams at a later date without getting a prior approval from the instructor.

4. Finally, my aim as an instructor is to see you do well in the course. If you have any comments regarding the course material, or my teaching methods feel free to let me know.
10 Grades:

The grades are determined by four elements: lab exercises, research project, midterm and final exams. The breakup will be: 20% for the five lab exercises, 20% for the research project, 20% for the midterm, and 40% for the final exam.

11 Textbooks:

There are two required textbooks for the course:

   This will serve as the required textbook for the course and is the definitive reference for TCP/IP protocols. Actually available in a three volume series.

   This will serve as the required textbook for network security.

These books can be purchased from the campus bookstore and are available on reserve in the library.

Other references include:

   Another three volume series providing a comprehensive treatment of the TCP/IP protocol suite illustrated by examples. Complements the book by Comer very well.

   Another good reference for computer security.

   An excellent introduction to computer networks. Covers protocols more from the OSI standpoint though. There is also a short discussion on network security.

   In particular, this is a good introduction to both networking protocols and network security. Topics, however, are treated sparingly, and not in much detail.

   A mathematically oriented introduction to cryptography.
I will also post lecture notes and selected papers on the course webpage.

12 Discrimination:

The Faculty of Engineering is concerned with ensuring an environment that is free of all adverse discrimination. If there is a problem that cannot be resolved by discussion among the persons concerned individuals are reminded that they should contact their Department Chair, the Sexual Harassment/Anti-Discrimination Officer (SHADO) or the Human Rights Consultant, as soon as possible.

13 Academic Dishonesty:

Students are reminded that they should read and comply with the Statement on Academic Ethics and the Senate Resolutions on Academic Dishonesty as found in the Senate Policy Statements distributed at registration and available in the Senate Office (see Senate Secretariat, Gilmour Hall, Room 104, 525-9140 or 529-7070, ext. 24337).

14 Requisites:

No background prerequisite other than a general curiosity on what makes the internet tick!. Significant study and reading outside of class is required. You are also strongly encouraged to attend class. Finally, if you have any questions, feel free to drop by, and talk to me about it.