

# SFWR 4C03 : Computer Networks & Computer Security

## Winter 2004

### 1 Instructor:

Dr. Kartik Krishnan  
Coordinates: ITB 106  
Phone: (905) 525-9140 ext. 27765  
Email: [kartik@optlab.cas.mcmaster.ca](mailto:kartik@optlab.cas.mcmaster.ca)  
Web: <http://optlab.cas.mcmaster.ca/~kartik>

### 2 Teaching Assistants:

Zhihui Dong ([dongz@mcmaster.ca](mailto:dongz@mcmaster.ca))  
Hany Shalaby ([shalabhm@mcmaster.ca](mailto:shalabhm@mcmaster.ca))

### 3 When and Where:

Mondays, Wednesdays and Thursdays between 10.30-11.20 AM at JHE 326H. Kartik's office hours are Monday, Wednesday, Thursday between 1-2 PM and by appointment. To set up an appointment please send me an email.

### 4 Course Webpage:

The course webpage is located at <http://optlab.cas.mcmaster.ca/~kartik/sfwr4c03>. Please check the webpage regularly for announcements regarding the course. I will also post most of the course material, including course handouts, lab exercises, exams here. My intention is to keep this webpage up to date. However, please inform me about missing links, and necessary updates by sending me email.

### 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 course will cover sections of Chapters 1-13, 20-21, 24-28, and 31-33 in the book by Comer. Here is a tentative list of topics to be covered :

1. Preliminaries
2. Review of 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)
7. Cryptography and Network Security (DES, RSA, Digital Signatures, IP Security)
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 Research 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 report is due in mid April. The research projects will be formally assessed by the class and 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 will be held in class on Friday, the 27th of February 2004 between 10.30 - 11.20 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 will be 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:

1. Douglas E. Comer, *Internetworking with TCP/IP : Principles, Protocols and Architectures*, 4th edition, Prentice Hall, 2002.

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.

2. W. Richard Stevens *TCP/IP Illustrated, Vol I : The Protocols*, Addison Wesley, 1994.  
Another three volume series providing a comprehensive treatment of the TCP/IP protocol suite illustrated by examples. Complements the book by Comer very well.
3. Andrew S. Tanenbaum, *Computer Networks*, 4th edition, Prentice Hall, 2002.  
An excellent introduction to computer networks. Covers protocols more from the OSI standpoint though. There is also a short discussion on network security.
4. William Stallings, *Data & Computer Communications*, 6th edition, Prentice Hall, 2000.  
A good introduction to the whole field of data communications, including network technologies and protocols. Topics, however, are treated sparingly and not in much detail.
5. William Stallings, *Cryptography and Network Security*, 3rd edition, Prentice Hall, 2003.  
Recommended as our primary reference for computer security.
6. Douglas Stinson, *Cryptography: Theory and Practice*, Boca Raton, FL: CRC Press, 2002.  
A mathematically oriented introduction to cryptography.

The book by Comer can be purchased from the campus bookstore, and the other references are available on reserve in the library. I will also post lectures, course handouts, 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:**

There is no background prerequisite. However, 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.