COMP 3825: Networking and Information Assurance – Spring 2007
Instructor: Prof. Santosh Kumar

2:40pm –4:05pm, Tuesday, Thursday in FIT 324

Contact Information:

Office: 376 Dunn Hall	**Department Office:** 209 Dunn Hall
Phone: (901) 678 2487	**Department Phone:** (901) 678-5465
E-mail: santosh.kumar@memphis.edu	**URL:** http://www.cs.memphis.edu/~santosh
TA: Madhu Kumar Kolli (mkkolli@memphis.edu)	

Office Hours:

Monday	Tuesday	Wednesday	Thursday	Friday
4pm – 5pm		4pm – 5pm		
Also by Appointment				

Course Description:

COMP 3825. Net-centric computing; communication and networking; world wide web; multimedia networking; network management; basic issues in computer security; threat modeling; basic methods and protocols in cryptography; web security; security policies; cyber ethics and netiquette. PREREQUISITE: MATH 2701 and COMP 3410

Why take this course?

1. To gain a basic understanding of computer networks such as the Internet, Wireless and Mobile Networks, Wireless Sensor Networks (Smart Dust), etc.;
2. To learn the principles of network protocol and application design;
3. To learn the basic notions and importance of computer and network security;
4. To understand the legal and ethical issues arising from computer and Internet use in society;
5. To learn programming for smart dust (wireless sensor networks).

Resources:

Required Text

- Computer Networking: A Top-Down Approach Featuring the Internet, 3rd Edition, James F. Kurose and Keith W. Ross, Addison Wesley, 2004.
- Network Security Essentials, Applications and Standards, 3rd Edition, by William Stallings, Prentice Hall, 2007.
- Ethics & Technology, 2nd Edition, by Herman T. Tavani, 2007.

Recommended Texts

- Computer Networks: A Systems Approach, 3rd Edition, Larry Peterson and Bruce Davie, Morgan Kaufmann, 2003.
- Principles of Information Security, M. C. Whitman and H. J. Mattord, 2nd Edition, 2005.

Other Resources: (Journal / Conference papers, websites, etc)

- http://authors.phptr.com/tanenbaumcn4/webResources/coverPageWebResources.html
- National Institute for Science and Technology (NIST) Computer Security Resource Clearinghouse
- TinyOS Tutorial: http://www.tinyos.net/tinyos-1.x/doc/tutorial/
- TinyOS Webpage: http://www.tinyos.net/
- TinyOS Programming by Phil Levis (online book)

Intended Outcomes:

- *Networking*:
    1. The student will be able to recall basic concepts underlying a computer network.
    2. The student will be able to list the protocol layers in a TCP/IP based network.
    3. The student will be able to list basic distinguishing characteristics of popular computer networks such as the Internet, Wireless Network, Wi-Fi, cellular phone based network, Personal Area Network, Mobile and Ad Hoc Networks, Wireless Sensor Networks, etc.
- *Information Assurance*:
    1. The student will be able to identify common vulnerabilities of a networked computer system.
    2. The student will be able to define basic concepts of information assurance.
    3. The student will be able to list basic tools commonly used to secure networked computer systems.
    4. The students will be able to inform their friends, peers, colleagues of the security vulnerabilities, common techniques for securing computer systems, and about the resources for gaining up-to-date knowledge on computer security.
- Programming Skills – *Wireless Sensor Network Platform (Mote)*:
    1. The student will be able to write simple NesC programs for the mote platform.
    2. The student will be able to write and test simple NesC programs for secure communication between mote units.

Class Format:

The class will involve lectures by the instructor, individual and team-based homework, paper presentations by students, and a team-based project. Basic concepts for each topic will first be introduced by the instructor in lectures. Homework will then be assigned to enhance the understanding of basic concepts.

Class Preparation:

Thorough preparation—by students *and* instructor—and active participation are essential to a successful course. Learning comes from struggling with the issues outside of class, then discussing them (and the struggle) in class. Unprepared students personally miss out on most of the learning and also cheat their classmates because they cannot contribute fully to the learning that occurs in class.

The instructor will assign readings from books and papers. Each student is expected to have read these before coming to class. This will enhance student learning as well as enhance other students' learning because more meaningful discussion can take place in the class. Class participation assessment will be done by the instructor as well as peer students in the class.

Teams:

Each student is expected to form/join a team for both homework and the project. The team composition for homework may be different than for the project. Team membership for homework will frequently be rotated to allow students to know and learn from different students in the class.

During the first week of class, students will form teams of 2-3 unless the instructor deems a different team size is warranted. Formation of teams will be left to your discretion, but I encourage you to include some variety in terms of gender, ethnicity, nationality, work experience, etc. If you need motivation beyond the opportunity to learn from classmates with different experiences, recognize that the teams you work with on the job usually include such diversity. It is wise to have at least one team member who is a fluent in English, to help ensure that your reports are written clearly.

Teams are to work *independently*. Reports, programs, or solutions from students who took the class in the past are strictly off limits.

The Project:

Each student team will do a programming project on the wireless sensor network mote platform. See the TinyOS webpages listed in "Other Resources" section for a tutorial on how to program the mote platform.

A list of options for the project will be provided. However, students are free to propose their own projects. No two teams will be working on the same project.

A series of programming assignments will prepare the students for their projects. Upon successful completion, the projects will be demonstrated to the public in the FIT building in the final exam week. Each project will be accompanied with a short presentation from student teams in the last class.

Evaluation:

Final Grades:
An individual's grade will be composed of his/her team's score as well as his/her individual score as described in the following table.

Team Evaluation		***Individual Evaluation***	
Homework	20%	Homework & Quizzes	15%
Survey Paper and Presentation (2)	10%	Midterm Exam 1	15%
Programming Assignments	10%	Midterm Exam 2	15%
Project Presentation and Demonstration	10%	Class Participation	5%

Assignment of letter grade will be determined based on performance of the entire class. Current plan is as follows:

A+: >= 95, A: >= 90, A-: >= 87.5, B+: >= 82.5, B: >= 80, B-: >= 77.5, C+: >= 72.5, C: >= 70, C-: >= 67.5, D+: >= 62.5, D: >= 60, F: < 60.

Course Policies:

Attendance

You are required to attend every class *unless there is a documented emergency*. The instructor may check attendance at the beginning of every class. If you miss a class, you will have to make your own arrangements to learn the materials covered in that class and to know of any announcements made in that class.

Late Policy

Homework and reports are due *before class on the due date*. For every 24 hours that an assignment is late, 20% of the total score will be deducted. For every day that an assignment is late, 10% of the total maximum credit will be deducted. For example, if an assignment is worth a maximum of 10 points, it will be worth only a maximum of 8 points if the assignment is late by one day.

Any homework or reports submitted 5 days after the due date and time will **NOT** be accepted (please submit all your homework on WebCT).

Testing Policy

There will **NOT** be any makeup quizzes or exams *unless there is a documented emergency*, so it is very important for you to attend every lecture and exam.

Plagiarism/Cheating Policy: (These paragraphs are mandatory.)

Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and ***will not be tolerated.*** All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student's own work. The plagiarism is incurred when any part of anybody else's work is passed as your own (no proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to discuss with each other and look up resources in the literature (including the internet) on their assignments, but ***appropriate references must be included for the materials consulted***, and appropriate citations made when the material is taken verbatim.

If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor's discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the University Judicial Affairs Office for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to: **http://www.people.memphis.edu/~jaffairs/**

Course Syllabus
List lecture topics or chapter sections by week or lecture meeting days.

Lecture	Date	Lecture Topics (Tentative)
1		Course Overview and Introduction to net-centric computing
2		Introduction to net-centric computing (TCP/IP layering)
3		Communication and networking (application layer)
4		Communication and networking (transport layer)
5		Communication and networking (network layer)
6		Network Addressing and Domain Name System
7		Communication and networking (link layer)
8		Communication and networking (physical layer)
9		Wireless Networks
10		Mobile and Ad Hoc Networks
11		Wireless Sensor Networks
12		Student Survey Presentations
13		Network management
14		Mid Term Exam 1 (Networking)
15		Review of IA Issues and Concepts
16		Security Principles
17		Threat Modeling
18		Threat Modeling (cont'd.)
19		Buffer Overflow and Input
20		Database / Web Specific Input
21		Cryptographic Issues / Protecting Data
22		Encryption Methods
23		Planning, Incidence response
24		Security Policy, Access Control / Least Privilege
25		Web Security
26		Student Survey Presentations
27		Cyber Ethics and Netiquette
28		Midterm Exam 2 (Information Assurance)
Finals Week		Project Presentation and Demonstration