

CIS 490-01 Spring 2004
(In the new catalog this course will be listed as CIS 480)

Network Security

INSTRUCTOR : DR. S. SRINIVASAN, 380 COLLEGE OF BUSINESS, 852-4790
srini@ louisville.edu URL: [http:// blackboard.Louisville.edu](http://blackboard.Louisville.edu)

OFFICE HOURS : T, R 8 a.m. to 9:30 a.m., 11 a.m. to 12 noon and 1:30 to 2:30 p.m.
Other times by appointment.

COURSE OBJECTIVES : 1. Learn the fundamental concepts in network security.
2. Understand the types of attacks on a network.
3. Understand how to develop countermeasures to defend against an attack.
4. Be familiar with the laws governing computer security
5. Be familiar with disaster recovery and contingency planning methods.
6. Learn ethical and privacy aspects of network security.

COURSE: CIS 490-01 T, R 2:30 to 3:45 p.m. in Room BS 008

PRE-REQUISITE: CIS 360

COURSE DESCRIPTION : Basic concepts of networking, operations security, protocol features for security, transmission security, packet filtering, TCP wrappers, firewalls, computer viruses, physical protection, legal protection, liability issues, significance of National Security Directive 42, implications of Computer Security Act, CERT recommendations, assessment of threats and vulnerabilities of systems, security countermeasures, contingency planning, disaster recovery, risk management, and auditing and monitoring, policies and procedures dealing with storage and disposition of sensitive data.

TEXT : Network Security Fundamentals by P. Campbell, B. Calvert, S. Boswell, Course Technology, 2003, ISBN: 0-619-12017-7

REFERENCES:

1. Guide to Firewalls and Network Security: Intrusion Detection and VPNs by Greg Holden, Course Technology, 2003.
2. Network Security – A Hacker’s Perspective by Ankit Fadia, Premier Press, 2003, ISBN: 1-59200-045-2
3. Cryptography and Network Security: Principles and Practice, 2nd Edition by William Stallings, Prentice Hall, NJ, 1999, ISBN: 0-13-869017-0.
4. Internet Security and Firewalls by V. V. Preetham, Premier Press, 2002, ISBN: 1-931841-97-7

TESTING Class participation worth 75 points
PROCEDURE: Three research reports worth 25 points each
One individual project worth 50 points
Midterm and final examinations worth 100 points each.
The course grade will be based on these 400 points as follows:

The course grade will be based on these 400 points as follows:

A	360 - 400	C	280 - 319	F	0 - 239
B	320 - 359	D	240 - 279		

INSTRUCTIONS:

- Last date to withdraw is March 1, 2004.
- Everything submitted for grading must reflect your own work.
- Class participation will be assessed after each class period. This part will include the obvious aspects such as paying attention, answering questions as well as reporting on special features of network security and sharing with the rest of the class the resources that you find useful. I do not want the class session to be disrupted by students arriving late or leaving before the class ends, for whatever reason. You will automatically lose participation points for that class if you arrive late or leave while the class is in session. Also, if you fall asleep during class or if you are absent, then you automatically lose the participation point for that class. The instructor has the sole responsibility in making this assessment and will take into account the contributions you make in class. The participation point for each class period is approximately 5 points (for a total of 75 points), excluding some class sessions. The Blackboard site will have a cumulative score of class participation points posted regularly.
- All research reports will be due at the starting time of class. A five point penalty applies for late submission on the due date and additional five points for each succeeding day that the submission is late. Topics for the research reports will be provided in class, along with the due dates. The research report should follow the sample research report format posted in my Blackboard site.
- Each student must choose a topic for Individual Project and get it approved by **January 27, 2004**. This project could involve any one of the major topics of this course namely: security design, security protection, security policy, or legal aspects. You should develop something innovative to address a problem that you identify in a typical scenario. This scenario and the problem must be identified in an interim report due on **February 10, 2004**. The interim report (typed double spaced) is worth 5 points. You should make a presentation on your project on **April 22, 2004**. The presentation is worth 10 points. The project report is worth 35 points. The project report should include your solution to the problem in a report format (typed double spaced), any programming code that might be applicable to your project, any applicable diagrams, and a list of references. Be innovative in the presentation. The report could be a video, a simulation, a poster, or some creative website.
- The test format will be short answer questions, approximately one paragraph for each question. The questions will cover key terminologies, legal aspects, policies and procedures, problem solving for typical security vulnerabilities. I will provide you with a detailed set of questions to prepare for the closed book, closed notes tests.

- Academic dishonesty of any kind will result in F grade for all students involved. CBPA supports the University policy on academic dishonesty. Academic dishonesty includes: (a) cheating, (b) fabrications and falsification, (c) multiple submissions, (d) plagiarism, and (e) complicity in academic dishonesty. Proven cases of academic dishonesty will result in a grade of zero for the affected assignment(s) and/or test(s).
- Any student with a disability should note my commitment to work with you in facilitating your learning and testing by suitable means. In this regard, I would like to reaffirm the university's commitment to ADA as outlined on page 30 of the following link:
<http://www.louisville.edu/student/services/registrar/0304catalog.pdf>

SYLLABUS

CIS 490-01 Spring 2004 Network Security

TEXT: Network Security Fundamentals by P. Campbell, B. Calvert, S. Boswell

DAY	DATE	TOPIC
Tue	1/13	Review of Networking concepts
Thu	1/15	Security Overview
Tue	1/20	Authentication
Thu	1/22	Authentication
Tue	1/27	Attacks and Malicious code
Thu	1/29	Attacks and Malicious code
Tue	2/3	Attacks and Malicious code
Thu	2/5	Viruses
Tue	2/10	E-mail security
Thu	2/12	Instant Messaging security
Tue	2/17	Firewalls
Thu	2/19	Physical security
Tue	2/24	Perimeter security
Thu	2/26	Wireless security
Tue	3/2	Intrusion Detection and Prevention Systems
Thu	3/4	Virtual Private Networks
Tue	3/9	Review
Thu	3/11	Midterm Examination (All topics covered up to this point)
Tue	3/16	Spring Break
Thu	3/18	Spring Break
Tue	3/23	Computer Security Act
Thu	3/25	CERT
Tue	3/30	National Security Directive 42
Thu	4/1	Liabilities
Tue	4/6	Security policies and procedures
Thu	4/8	Security audit and monitoring
Tue	4/13	Disaster recovery and Contingency planning
Thu	4/15	Risk management
Tue	4/20	Privacy and ethics
Thu	4/22	Project Presentations
Wed	5/6	11:30 a.m. to 2 p.m. Final examination (All topics covered after Midterm)

Note: I have scheduled an Information Security Seminar Series for Spring 2004.
All seminars will be in CBPA Room 336 from 2:30 to 3:30 p.m. on Mondays.
Seminar dates are: January 26, February 23, March 22