Jackson State University
Department of Computer Science
CSC 539-02 Advanced Information Security
Spring 2013

Instructor: Dr. Natarajan Meghanathan
Office: JAP 115 (near Lab 117)
Phone: 601-979-3661
Email: natarajan.meghanathan@jsums.edu

Class Room: ENB 104
Class Time: MW 7.30 PM to 8.50 PM
Office Hours: Mon, Wed 6.15 to 7.15 PM
Friday 2 PM to 3 PM

Course Description

CSC 439 (3) Advanced Information Security. This course discusses advanced topics in information security related to Cryptography, Steganography, Network security controls, Web and E-mail security, Wireless network security, Security in distributed systems and Database security. (D).

Course Outcomes

Each graduate student who successfully completes this course should be able to:
CO-1: Apply cryptography for data confidentiality, integrity, authentication as well as for key distribution and e-mail security
CO-2: Develop software programs that adhere to the secure coding standards and meet the specification.
CO-3: Analyze the working of various advanced security controls, techniques and standards to combat attacks on web, wired and wireless networks
CO-4: Describe the various access control models applicable for information security
CO-5: Apply emerging topics such as Steganography, Biometrics and Virtualization for information security
CO-6: Explain the different classes of malware, their propagation mechanisms and detection strategies.

Required Textbook

M. Stamp, "Information Security: Principles and Practice," 2nd Edition, Wiley, ISBN: 0470626399, May 2011.

Course Website

http://www.jsums.edu/cms/tues/html/CSC439-539-AIS-Spring2013.html
Students are required to attend every class and frequently check the course website for latest updates regarding the course. All announcements, lecture materials for all chapters, lab projects, reading assignments, sample questions and quiz solutions will be posted in the course website.
Note that the course website can also be accessed through two other ways: (i) by visiting the website http://www.jsums.edu/cms/tues and then clicking on the CSC 439/539 Advanced Information Security, Spring 2013 link in the list of TUES Courses at the right; (ii) by visiting the website http://www.jsums.edu/cms/nmeghanathan and then click on the CSC 439/539 course link in the list of courses for Spring 2013 posted at the right side.

Evaluation

Lab Projects (25%) - 5 projects, 5% each
Quizzes (30%): 7 Quizzes [Sum of all Quiz scores, each for 100%, and divide by 6]
Exams (45%): Exam 1, Exam 2 and Exam 3 (each 15%) [Sum of all Exam scores, each for 100%, and divide by 2.8.

Reference Books

No.	Book Title/ Edition, Year	Authors	Publisher	ISBN
1	Computer Networks: A Systems Approach, 4th Edition, March 2007	Peterson and Davie	Morgan Kaufmann	0123705487
2	Database and Applications Security: Integrating Information Security and Data Management, 1st Edition, 2005	B. Thuraisingham	Auerbach Publishers	0849322243
3	Cryptography and Network Security: Principles and Practice, 5th Edition, January 2010	W. Stallings	Prentice Hall	0136097049
4	Digital Watermarking and Steganography, 2nd Edition, November 2007	I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker	Morgan Kauffman	0123725852
5	Handbook of Information and Communication Security, 1st Edition, April 2010	P. Stavroulakis and M. Stamp (Eds.)	Springer	3642041167
6	Security in Computing, 4th Edition, October 2006	C. P. Pfleeger and S. L. Pfleeger	Prentice Hall	0132390779
7	CERT Oracle Secure Coding Standard for Java	F. Long, et. al	Addison-Wesley	0321803957
8	Mastering VMware Infrastructure 3, 1st Edition, May 2008	C. McCain	Sybex Publishers	0470183136
9	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, September 2009	M. Howard, D. LeBlanc, J. Viega	McGraw Hill	0071626751
10	Introduction to Computer Security, 1st Edition, October 2010.	M. Goodrich and R. Tamassia	Addison Wesley	0321512944

Online References

1. http://unixwiz.net/techtips/iguide-ipsec.html
2. http://www.codinghorror.com/blog/2008/09/cross-site-request-forgeries-and-you.html
3. http://freedom-to-tinker.com/blog/wzeller/popular-websites-vulnerable-cross-site-request-forgery-attacks
4. http://zone.ni.com/devzone/cda/tut/p/id/10588, http://zone.ni.com/devzone/cda/tut/p/id/8708

Research Papers as References

1. A. K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125 – 143, June 2006.
2. N. Ratha, J. Connell, R. M. Bolle and S. Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints," *Proceedings of the 18th Int'l Conf. on Pattern Recognition*, 2006.
3. N. Meghanathan, "Biometric Systems for User Authentication," *International Journal of Information Processing and Management* (IJIPM), vol. 2, no. 4, pp. 10-21, October, 2011.

Course Modules

The entire course is divided into the following modules:

Module #	Module Name	Course Outcome	References
1	Number Theory and RSA Public-Key Encryption	CO-1	Req. Text (Ch. 4)
2	Key Distribution and Management	CO-1	Ref. Book # 3 (Ch. 14)
3	E-mail Security	CO-1	Ref. Book # 3 (Ch. 18); Online Ref # 2, 3
4	Virtualization	CO-5	Online Ref. # 4
5	Access Control Models	CO-4	Req. Text (Ch. 8) Ref. Books # 10 (Ch. 9), # 5
6	Web Security	CO-3	Ref. Book # 10 (Ch. 7)
7	Network Security	CO-3	Req. Text (Chaps. 8, 10); Ref. Book # 10 (Chaps. 5, 6); Online Ref # 1
8	Secure Programming	CO-2	Ref. # 7
9	Malware	CO-6	Ref. # 10
10	Steganography	CO-5	Ref. Book # 4
11	Biomterics	CO-5	Ref. Papers 1, 2, 3

Course Outline (Tentative)

Week #	Module Name/ Topics	Course Outcome
1	Syllabus introduction; **Module 1 – Number Theory and Public-Key Encryption (Lecture notes):** Modular arithmetic, Multiplicative inverse modulo *n*, Euclid's algorithm to find the GCD, Extended Euclid algorithm, RSA algorithm – derivation of public/private keys and examples, Diffie-Hellman key exchange	CO-1
2	**Module 2 – Key Distribution and Management (Lecture notes):** Needham Schroeder protocol; Public-key certificates – steps to generate, contents of a certificate, certificate revocation, classes of certificates, secure communication using certificates; Key distribution (public keys and secret keys) using public-key authority	CO-1
3	**Module 2 – Key Distribution and Management (Lecture notes):** Kerberos – protocol steps, advantages and weaknesses **Module 4 – Virtualization (Lecture notes):** Basics, Hosted vs. Bare-metal architecture; Virtualization techniques – Full virtualization (Binary translation), Para virtualization and Hardware assist; Memory virtualization, Networking issues with VMs.	CO-1 CO-5
4	**Module 6 – Web Security (Lecture notes):** Cookies, Applets vs. ActiveX; Cross-site Scripting (XSS) attacks – persistent and non-persistent XSS attacks and solutions	CO-3
5	**Module 6 – Web Security (Lecture notes):** Cross-site Request Forgery (XSRF) attacks and prevention strategies **Module 3 – Email Security (Lecture notes):** PGP for authentication, confidentiality and both; Use of Radix-64 format for PGP; PGP keys; S/MIME; DKIM standard	CO-3 CO-1

		CO-4
6	**Module 11 - Biometrics:** Biometric systems – identification vs. verification, performance metrics, basic blocks of a biometric system, Comparison of biometric systems; Multi-biometric systems and different levels of fusion; Cancelable biometrics	CO-5
7	**Module 9 – Malware (Lecture notes)**	CO-6
8	**Module 5 – Access Control Models (Lecture notes):** Mandatory access control model – Multi-level security in databases and the polyinstantiation (visible and invisible) problem; Biba integrity model; Bell LaPadula confidentiality model; Discretionary access control (DAC) – UNIX file permissions; weakness of DAC; Dynamic access control model – Chinese wall model: read and write rules; Role-based access control model (RBAC) and hierarchical RBAC **Module 7 – Network Security (Lecture notes):** Link encryption vs. end-to-end encryption	CO-4 CO-3
9	**Module 7 – Network Security (Lecture notes):** IPSec – Steps in forming security association, AH and ESP headers, Transport vs. Tunnel modes; Firewalls – Packet filter, Stateful, Application proxy firewalls, Personal firewall; Comparison of different categories of firewalls; SSH	CO-3
10	**Spring Break Holidays**	
11	**Module 7 – Network Security (Lecture notes):** Wireless Network security – WEP (Wired Equivalent Privacy) standard and its weakness; WPA (Wi-Fi Protected Access) standard; WAP protocol stack; WTLS; WAP gap problem and solution	CO-3
12	**Module 8 – Secure Programming Standards (Lecture notes)**	CO-2
13	**Module 8 – Secure Programming Standards (Lecture notes):** Arithmetic overflow attacks; Stack smashing attacks and solutions; Format string attacks and Time of Check to Time of Use attacks	CO-2
14	**Module 10 – Steganography (Lecture notes):** Steganography Models, types (secret key, public-key), LSB-based substitution, problem of collisions and solution; Information hiding in palette images, through quantization using predictive coding	CO-5
15	**Module 10 – Steganography (Lecture notes):** Information hiding through automated generation of English texts using Context-free grammar (CFG)	CO-5
	Final Exam on Wednesday, May 1, 2013: 6 PM to 7.50 PM	

Grading Scale

90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
Below 60	F

Course Policies

Note: The course policies will be discussed with students in the first meeting of the class. Students (including those who missed the first meeting of the class) are expected to be aware of these course policies for the rest of the semester. The instructor will not discuss these course policies after the first day of the class and will follow the policies as stated assuming the students are aware of them.

Exam and Quiz Dates

- Unless otherwise notified, we will stick on to dates for the quizzes and exams listed in the calendar table in Page 2 of this syllabus. The exact date and the topics for a quiz will be announced 4-7 days before the actual day and time of the quiz/exam. A quiz/exam could be conducted any time during the class. So, students need to be present on-time at the beginning of the class and stay till the end of the class.
- Tentatively, the topics for the exam are those covered in the 4-5 week period preceding the exam. The exact exam/ quiz topics will be announced by the instructor, a week before the actual date and time of the test.
- The final exam will be on the day and time as specified by the university.

Lab Projects

- The due dates for the lab projects would be as listed in the Course Outline.
- All of the lab projects would be posted in the course website, well ahead of time and you are at your own pace to complete and submit the projects by the deadline. There would not be any extension of these deadlines.

- **Laboratory projects should be done independently**.
- **Late submission of homework assignments and Lab Projects will not be accepted.**
- It is the responsibility of the student to make sure he/she can print the lab reports before the due date /time. No excuse will be given for lack of computer access and printers to print the document.

Make-up Quizzes and Exams

- No Make-up Quizzes will be given. If a student misses a quiz for ANY reason, the student gets a score of 'zero' for the quiz and no make-up quiz will be given.
- **No make-up examinations will be given except for emergencies such as death in the family or serious illness. The instructor must be informed, through e-mail or a written request, BEFORE the time of the examination that is to be missed.** The instructor will make a decision on the make-up examination after verifying the appropriate written documentation. Failure to furnish, written, verifiable documentation will result in a grade of zero for the missed examination.
- **Any make-up exam for a missed exam has to be taken before the next class meeting time.**
- **A make-up exam will be different and will be relatively tough compared to the actual missed exam.**
- **NO MAKE-UP EXAM WILL BE GIVEN FOR THE FINAL EXAM. Students are required to take the final exam during the date and time specified by the university.**

Cheating

The instructor will be extremely strict with regards to this policy.

- **A student found to have copied in any lab project report will get a 0 for all of his/ her lab projects in the course.** If a student is found to have copied the lab project from some other student, both the students will get a 0 for all their lab projects in the course.
- **A student found to have plagiarized in the term-paper reports (proposal, mid-term, final) will get a 0 for the term-paper component of the course .**

Contesting Grades

- Grades for a particular exam can be contested only within a week after the grades for that exam are announced.
- Grades for the final exam will have to be contested within two days after the exam.
- The grade for the overall course will have to be also contested within two days after the final exam. Any change of grade requested by the student 48 hours after the completion of the final exam will not be considered.

Maintaining Registration Status

- It is the duty of the student to make sure that he/she stays registered in the course throughout the semester. If a student sees he/she is dropped from the course without his/her knowledge, the student should notify the instructor before the next meeting of the class.
- A student cannot attend a class or take an exam/quiz if the student is not registered for the course at that point of time.

Dropping the Course

- The last date to drop the course without any grade is January 25, 2013. The last date to drop the course with a "W" grade is March 25, 2013.
- The instructor will not assist in any way to get the student dropped with no grade or "W' grade after the above dates.

Anticipated Leave

- If a student is anticipating any medical emergency (like surgery, pregnancy, etc.), conference participation, game participation, etc. during the course of the semester, the student should furnish the appropriate medical documents, conference registration receipt, letter from the coach, etc, and discuss with the instructor within the first two weeks of the course on how to make up for the classes/exams/assignments that will be missed.
- The instructor will make a decision on the make-up examination after verifying the appropriate written documentation. Failure to furnish, written, verifiable documentation will result in a grade of zero for the missed examination.
- The instructor will give a different set of assignments, projects and make-up exams than the ones given in class.
- **The student is responsible for the materials covered in a class that he/she misses.**

Other Course Policies

- Turn off your cell phone in class. Use of a cell phone or a laptop computer is not allowed in class.
- If a student leaves the classroom during a quiz or exam for any reason, the student's exam paper will be collected, and thus he/she will not be able to resume the testing after coming back to the room. Inform the instructor if any health problem prevents you from remaining in the classroom until you complete the quiz or exam.
- Cell Phones, Tablets, Laptops, etc., will not be allowed for use during a quiz or exam. Any Math calculation, if needed, is supposed to be done using a calculator only. Students will not be allowed to borrow calculators from peer students during an exam/quiz.

ADA Statement

Compliance with the Americans with Disabilities Act: "It is the university policy to provide, on a flexible and individualized basis, reasonable accommodations to students who have disabilities that may affect their ability to participate in course activities or to meet course requirements. Students with disabilities are encouraged to contact their instructors to discuss their individual needs for accommodations."

If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and ADA Coordinator (as early as possible in the term) located in the Jacob L. Reddix Building (old student union), rooms 101 and 102. The office hours are: 8:00 a. m. to 5:00 p.m., Monday through Friday. The telephone number is (601) 979-3704 or (601) 979-6919 (TTY) and the facsimile number is (601) 979-6918. The mailing address is: Office of Support Services for Students and Employees with Disabilities, P.O. Box 17156, Jackson State University, Jackson MS 39217.

Diversity Statement

Jackson State University is committed to creating a community that affirms and welcomes persons from diverse backgrounds and experiences and support the realization of their potential. We recognize that there are differences among groups of people and individuals based on ethnicity, race, socioeconomic status, gender, exceptionalities, language religion, sexual orientation, and geographical area. All persons are encouraged to respect the individual difference of others.

Collegiate Code of Conduct

Jackson State University students are expected to dress in a manner representative of higher education institution. More information on Dress Code; Verbal and/or Physical Harassment; Indecent, Obscene, Immoral Behavior and/or Profanity is available in the JSU Student Handbook. The JSU Student Handbook is available at http://www.jsums.edu/~studentlife/handbook.pdf

Dropping a course

The last day to drop a course with no grade:	01/25/2013
The last day to drop a course with "W" grade:	03/23/2013

Student Conduct and Class Attendance Policy

Students at Jackson State University must fully commit themselves to their program of study. One hundred percent (100%) punctual class attendance is expected from each student for all the scheduled classes and activities. The instructor will be maintaining the attendance record and any absence of a student without providing any written official excuse, is counted as an unexcused absence. Irrespective of the type of excuse (i.e., official or unofficial), the student is responsible for the work required during their absences.

The instructor will call the roll at the beginning of the class. Also, the instructor will pass an attendance sign-up sheet to each student. Students coming late to the class by more than 10 minutes will be marked "Absent". Students may be officially excused from class for attendance at University approved functions provided the sponsor properly executes a Student Affairs Leave Form. The instructor shall accept such excuses. The Dean of the School or the Vice President for Academic Affairs may also officially excuse students for certain campus activities. Students must submit written documentation to Student Affairs to obtain official excuses for absences due to illness or other emergency situations. Students who willfully miss class face serious consequences. After being absent four times in a 80-minute class, one time immediately before or after a scheduled recess/holiday, the instructor shall report the next unexcused absence to the Dean of University College for freshmen and sophomores and to the School Dean and Department Chair for Juniors and Seniors. The Dean/Chair or designee will counsel with the student and in concert with the instructor, may require the student complete complimentary course assignments. If a student does not respond well to the counsel or with the assignments, the instructor may impose a grade penalty on the student. Unexcused absences that exceed the equivalency of four 80-minute sessions may lead to an "F" for the course.

Academic Honesty

All acts of academic dishonesty (e.g., cheating on exams, plagiarizing – presenting another person's work as one's own, having another person write one's paper, making up research data, presenting excuses which are untrue for failing to meet academic and professional standards) are a violation of engineering values, ethics, and University policy, which will entail appropriate penalties.

Policy Regarding Course Incompleteness

Incomplete is the designation used to indicate failure to complete assignments or other course work including final or other examinations, by the end of the term in which the student is enrolled. The grade of incomplete "I" is recorded when the student has not completed the course due to some unavoidable reason that is acceptable by the instructor. An incomplete grade "I" is to be considered only when the majority of the course requirements and the assignments have been successfully completed and there is a documented crisis situation of illness, accident, or other occurrence which prevents a student from completing the remaining requirements before the school term ends. The incomplete grade "I" is not a substitute for the failure grade "F".

The instructor is required to indicate on the grade sheet the grade the student should receive if the incomplete is not removed within the prescribed time. If the student fails to complete the course requirements satisfactorily within the specified time, the alternate grade will be recorded as the grade of record.

Computer Network Lab Hours

All of the lab projects given in the course may require the use of the Computer Networks Lab (AT&T lab) at the J. Y. Woodard Building in the Main Campus. There will be a lab assistant who would keep the lab opened for at least 15 hours per week. M-F: 9.30 AM to 12 Noon; 2 PM to 5 PM