ECE 4490 Section 1 ECE 6490 Sections 1, 843
Computer Network Security
Fall 2018

Instructor and contact information:
R. R. Brooks
313-C Riggs Hall
Tel: (864) 656-0920
Fax: (864) 656-1347
email: rrb@acm.org
PGP: 48EC1E30

Grader/Lab administrator:
You will receive their contact information once they are officially assigned.

Office hours:
Tuesday 4:00 PM – 5:00 PM, (16:00 to 16:50)
Or by appointment

Class meeting times and location:
Tues. 5:00PM – 5:50PM Watt Center 310
Charleston Zucker
Exam 7:00PM – 9:30PM Dec. 13 Watt Center 310
Charleston Zucker
Laboratory (Riggs 22-A, Charleston Zucker) access outside of class time. Laboratory access code given first day of class

Attendance policy: Course meetings mainly follow a seminar, rather than lecture, format. Attendance at course meetings is mandatory, since the seminar format includes in-class discussion. For the discussion, students are expected to have completed the reading assignments in advance. On days when presentations or demonstrations are due, students must be present and properly prepared. Students are expected to wait for 10 minutes, should the professor be late. Should students stop attending class, it is their responsibility to provide proof of the last day of attendance of class to the instructor.

Disability access policy: "It is University policy to provide, on a flexible and individualized basis, reasonable accommodations to students who have disabilities. Students are encouraged to contact Student Disability Services to discuss their individual needs for accommodation."

Academic integrity: This course follows Clemson University procedures. Students suspected of violating academic integrity will be reported. In particular, any form of plagiarism will result in no credit for the assignment and being reported for further disciplinary action.

"As members of the Clemson University community, we have inherited Thomas Green Clemson's "As members of the Clemson University community, we have inherited Thomas Green Clemson's vision of this institution as a 'high seminary of learning.' Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form. In instances where academic standards may have been compromised, Clemson University has a responsibility to respond appropriately and expeditiously to charges of violations of academic integrity."

"When, in the opinion of a faculty member, there is evidence that a student has committed an act of academic dishonesty, the faculty member shall make a formal written charge of academic dishonesty, including a description of the misconduct, to the Associate Dean for Curriculum in the Office of Undergraduate Studies. At the same time, the faculty member may, but is not required to, inform each involved student privately of the nature of the alleged charge."

Please refer to the graduate academic integrity policy, approved March 26, 2007 by the Provost's Advisory Council, at

http://gradspace.editme.com/AcademicGrievancePolicyandProcedures#integritypolicy

Each graduate student should read this policy annually to be apprised of this critical information.

Sexual harassment: Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran's status, genetic information or protected activity (e.g., opposition to prohibited discrimination or participation in any complaint process, etc.) in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This policy is located at:

http://www.clemson.edu/campus-life/campus-services/access/title-ix/.

Mr. Jerry Knighton is the Clemson University Title IX Coordinator. He also is the Director of Access and Equity. (for undergraduates) His office is located at 111 Holtzendorff Hall, 864.656.3181 (voice) or 864.565.0899 (TDD). (for graduate students) knightl@clemson.edu or 656-3181

Objectives and outcomes: This course is a project-oriented introduction to computer and network security. Security is a process that maintains well-defined system properties. Students will need to understand security threats and existing security countermeasures. Discussions will identify security

holes in current network implementations. A set of challenging assignments has been developed that provide students with the basic skill sets needed for work in network security. In class discussions will help students prepare their assignments. Ethical and legal aspects of computer security issues are introduced and discussed as a part of the course. The final includes essay questions on these topics. Assignments will include:

- Technical deliverables (system installation, implementation, test, and maintenance).
- Technical reports and design documents.
- Technical presentations.

Students are expected to create and deliver professional quality materials. Graduate students need to implement a security research project and present their results to the class. The security project should be at a level suitable for submission to a professional conference.

A note on ethics, legal issues and etiquette: In order to develop and maintain secure systems, it is necessary to fully understand system vulnerabilities. This understanding is best attained by mimicking the mindset of potential attackers. This course provides students with facilities and resources for exploring system vulnerabilities. It is expected that any exploits attempted will be carefully designed with a specific purpose in mind. Exploit designs will be documented and delivered to the instructor before implementation occurs. They will involve neither physical access to machines nor vandalism (including destruction of software or hardware infrastructure). Exploits will most often involve violating system confidentiality, consistency, and/or non-repudiation attributes. **Attack implementation and testing will be performed solely within the laboratory on the machines provided for that purpose. These machines will remain on an isolated network during this process. If non-laboratory machines are used, the student will receive no credit for the assignment.**

Attacks on operational networks potentially violate existing laws with severe consequences. Illegal activity is not condoned and will be dealt with severely. Red team analysis of systems should be performed with the informed consent of the owners of the system being analyzed and not in connection with this course.

Resources: This course is project oriented. Students are expected to independently find the resources needed to fulfill their assignments. They will also write a number of reports and present their results. Most lectures will be run as a seminar with the instructor questioning the students. The instructor is available to the students for discussion of design alternatives and as an information resource.

Introduction to Computer and Network Security Navigating Shades of Gray is the required text.

A number of security-related URL's, videos and other information will be provided. Use of open source tools for system implementation is strongly encouraged. Books worth referring to: (The first 4 are on reserve)

- S. Young and Dave Aitel, *The Hacker's Handbook*
- Bob Toxen, *Real World Linux Security: Intrusion Prevention, Detection, and Recovery*
- Kolesnikov and Hatch, *Building Linux VPN's*
- Mike Schiffman, *Building Open source network security tools*, Wiley
- Michael Donahoo and Kenneth Calvert, *The Pocket Guide to TCP/IP Programming*
- Warren Gay, *Linux Socket Programming by Example*
- John Chirillo, *Hack Attacks Revealed (*lots of information, well-organized, poorly written)
- *Building Secure Software,* Addison-Wesley.

Assignments: Demonstrations and presentations will be done in the lab at times arranged with the instructor. They are a form of oral examination and should be treated accordingly. They will include either individuals or work groups and the instructor. Written assignments must be turned in before the start of class on the day they are due. No credit is given for late assignments.

For assignments with presentations, **students are given 10 minutes to present their work and convince the instructor that they fulfilled the assignment.** Students will be given credit for the intersection of the information in the written report and their demonstration. No credit will be given for functionality presented to the instructor that is not in the written report, nor will credit be given for written functionality that does not work during the demonstration.

The ECE6490 section is the same as ECE4490, except that the graduate students do an independent research project. The project topic is due on October 9. The project will be graded as if it were a conference paper. The last 2 class meetings are an in class seminar on these projects. The papers are due by Nov. 27. If students need guidance, they need to initiate contact with the instructor.

Grading: (Percentages. For undergraduates, points and percentages are identical. For graduate students, they are quite different.)

A – 90 or above
B – 80 to 89
C – 70 to 79
D – 60 to 69
F – Below 60

Deadlines are fixed. No extensions will be given. No late assignments will be accepted. This means that assignments are due at the start of class. No credit

will be given for a late assignment. Printers printing slowly are not an adequate excuse for a late assignment. Presentations are interactive. Students must be prepared to answer questions from the instructor and other students. Documents must be professionally prepared. Sloppy and poorly written documents will be graded harshly. Students may be asked to re-write the document to make it fulfill professional standards. The documentation is due at the start of class on the due date. Presentations will be given during the week. A sign up sheet will be circulated in class.

Schedule: (Subject to change)

Date	Due	Reading assignments	Lecture topic	On Travel
8/28/2018		Syllabus, IEEE Security and Privacy, Introduction to Computer and Network Security: Navigating Shades of Gray: Chapters 5 and 6	Introduction to course, history of security, discussion of first assignment	
9/4/2018		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapter 3	Cryptography basics	
9/11/2018	VPN and sniffer assignment, Graduate research topic due	Introduction to Computer and Network Security: Navigating Shades of Gray: Chapters 7 and 8	Buffer overflow details	
9/18/2018		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapters 4 and 11	Privacy	Kaspersky meeting in Sochi
9/25/2018		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapter 1 and 2	Survey of security issues - Ross Anderson	NSF PI meeting in DC
10/2/2018	Buffer overflow assignment due	Introduction to Computer and Network Security: Navigating Shades of Gray: Chapter 9	Virus execution details	
10/9/2018			Game console security	
10/16/2018	War Game in Class	External materials provided	How to survive under an authoritarian government	
10/23/2018		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapter 10 and 12	Automotive System Security	Malware Conference Nantucket Monetec Conference Moscow
10/30/2018	Virus assignment due		Wireless security / Ethical Hacker Presentation	
11/6/2018	Fall break			
11/13/2018		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapters 13 and 14	Digital Rights Management / Ethics	IEEE Blockchain for clinical trials, Scotland
11/20/2018	Graduate research		Graduate student research presentations	Thanksgiving
11/27/2018	Graduate research		Graduate student research presentations	IEEE Blockchain for Ag, Hawaii
12/4/2018	Wireless assignment due		Class has presentations of wireless assignment. Review during the week	
12/13/2018	Final at 7:00 PM			

Assignment	Group or Individual	Deliverable	2-Oct	Points
VPN and sniffer installation, use, and analysis	Individual (pair)	Document and presentation	09/11/18	15
Graduate research topic	Individual (6490 only)	1 page abstract	09/11/18	5
War game	Groups (dynamic)	In class competition	10/16/18	10 points extra credit for winners
Buffer overflow implementation	Individual	Report and demonstration	10/02/18	25
Polymorphic virus implementation	Individual	Report and demonstration	10/30/18	25
Wireless Security	Group	Report and Demonstration	12/04/18	15
Graduate research project (6490 only)	Individual	Report and in-class presentation	11/20/18	45
Class participation	Individual	N/A		10
Final exam	Individual	Examination	12/13/2018	10
Total Undergrad				100
Total Grad				150