SYLLABUS PART ONE[1]

COURSE TITLE AND COURSE NUMBER: **Computer Network Security ECE4490(1)/6490(1) Sections 1**

TERM: Fall 2022[2]

CLASS MEETING TIME AND PLACE: **4490/6490 lectures on Tues, 17:00 to 17:50** Section 1 – Riggs 223, Main Campus, Clemson . Online (If I am sick, or hhwatever) -- https://clemson.zoom.us/my/la.peste[4],

4491/6491 Labs – Lab space location will be provided to students on first day of class. Goal is to make the lab facilities open at most times for most students. Lab room is typically closed on football weekends. Lab machines might be made available for remote access, or other accommodations may be provided as necessary. If remote work is allowed, information regarding how to either access machines remotely or download virtual machines will be provided. Labs will possibly be in lab or on machines that can run more than 1 VM. Only use VMS for labs.

TIME TO WAIT: 15 minutes wait is preferred. Class attendance is not considered mandatory. If students are not available for class, they are still responsible for the material covered in class. Note that fee reimbursement may depend on the last date students attended class. Students are considered responsible for documenting when they stop attending class.

INFORMATION ON MODALITY: In person. The instructor may also use remote access when necessary (travel, illness, …) Some sessions will also be flipped classrooms where students are given media (readings, podcasts, videos, …) to absorb before class and lectures are devoted to discussions.

INSTRUCTOR NAME: R. R. Brooks
Professor

---

[1] Version 0.1 Aug 19, 2021—Course syllabus contents subject to change in response to changing circumstances. The most current syllabus version will be posted on Canvas.

[2] See https://www.clemson.edu/registrar/academic-calendars/calendars.html?year=2021&semester=fall for official university start date and end date and other major dates from the academic calendar (last day to drop without a W, fall break, etc.)

[3] We intend to post recorded lectures at: https://clemson.box.com/s/tc5f2u9rrdswsas8157iod6glz7ahmfk Lectures from previous years are there. It is not clear how long the university will maintain this service. If changes are made, students will be informed promptly.

[4] We intend to post recorded lectures at: https://clemson.box.com/s/tc5f2u9rrdswsas8157iod6glz7ahmfk Lectures from previous years are there. It is not clear how long the university will maintain this service. If changes are made, students will be informed promptly.

(He/Him/His)
College of Engineering Computing and Applied Science
https://www.clemson.edu/cecas
Clemson University
313-C Riggs Hall
PO Box 340915
Clemson, SC 29634-0915
USA
office: 864-656-0920
fax: 864-656-5910
voicemail: 864-986-0813
rrb@acm.org
www.clemson.edu
https://www.clemson.edu
PGP 1: 955B 3813 41C0 9101 3E6B CF05 02FB 29D6 8E1E 6137
PGP 2: FC15 BAF0 4296 B47E 932A 9DB3 D41B 81AF C6EA 90F6

Grader: Chunpeng Shao
Email: chunpes@g.clemson.edu
Office hours: TBD

DEPARTMENT AND COLLEGE OF INSTRUCTOR:

INSTRUCTOR EMAIL: rrb@acm.org I will attempt to respond to email inquiries within 36 hours, excluding weekends, university holidays, and travel.

UNIVERSITY OFFICE PHONE: 864-656-0920

OFFICE ADDRESS/OFFICE NUMBER: 313-C Riggs, Main Campus, Clemson, SC

Office Hours: 16:00 to 17:00 Tuesdays in Riggs 313-C. Maybe by zoom
https://clemson.zoom.us/my/la.peste
Or by individual arrangement. In person office hours will take place at the time and place we agree on (Preferably outdoors).

INSTRUCTOR PHOTO:

FIGURE 1PICTURE OF R. R. BROOKS

OFFICE AND/OR CLASSROOM MAP: https://www.campus-maps.com/clemson-university/riggs-hall/

COURSE DESCRIPTION Hands-on practicum in the administration and security of modern network service emphasizing intrusion prevention techniques, detection, and recovery. Preq: Senior standing in Computer Engineering or Electrical Engineering. Coreq: ECE 4491.

VALUE STATEMENT

Current laws make computer hardware, software and service providers not liable for security flaws in their systems. The Internet allows world-wide access to any machine, which means that it is difficult to establish the legal jurisdiction for any criminal behavior. World-wide access to computer nodes makes it difficult to determine the source of any attack. Many countries do not prosecute computer criminals as long as they only attack people outside of that country. Government interesting computer security is mainly limited to keeping the devices vulnerable to attack in order to ease surveillance on its own citizens and foreign opponents. Every piece of software and hardware that is currently in use relies on a global supply chain of companies/individuals for whom security is an expensive cost that provides no benefits to them.

Each individual and company is responsible for maintaining the security of their systems. Doing so requires an in depth knowledge of devices that most of their suppliers consider proprietary intellectual property that must be hidden from their customers. This course provides students with an initial introduction to the problem of maintaining secure computer nodes and networks. It looks largely at the most egregious flaws that exist in current systems and how they can be exploited. Exploration of these errors also provides students with a better view of the complexity of the systems they use and the basic principles of secure systems.

COURSE OVERVIEW

LEARNING OUTCOMES

At the completion of the course the student will:

- Understand prevalent computer and network security issues,

- Avoid common implementation mistakes,
- Be able to configure VPNs,
- Exploit memory configuration errors,
- Create self-replicating programs, and
- Explain the role of ethics in system design/implementation.

PREREQUISITES Senior standing in ECE, or equivalent, and/or instructor permission.

REQUIRED MATERIALS

- Introduction To Computer and Network Security: Navigating Shades of Gray, by R. R. Brooks, CRC Press
- Computer capable of running simultaneously at least 2 virtual machines,
- Webcamera
- Microphone
- Internet connections
- Cell phone

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.

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.

REQUIRED TECHNICAL SKILLS

For technical assistance with the course site, students should contact ithelp@clemson.edu, visit CCIT's website, or contact the grader.

LEARNING ENVIRONMENT

A basic understanding of Linux, computer architecture, TCP/IP, and programming is probably needed. Some understanding of how assembly and computer binary works would be useful. We have tried to make the course self-contained, but challenging. Creativity is required, as well as the ability to decipher how and why computers behave the way they do. It is hard to list prerequisites, since much of what I ask you to do is the opposite of accepted best practices. You have been taught for years to not do what I want you to do.

Major Assessment/Grading Activities and topical outline

Date	Due	Reading assignments	Lecture topic
8/29/2023		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
9/5/2023		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapter 3	Cryptography basics
9/12/2023	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
9/19/2023		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapters 4 and 11	Privacy
9/26/2023		Shashanna Zuboff *Surveillance Capitalism*	Surveillance capitalism, and social implications
10/3/2023	Buffer overflow assignment due	Introduction to Computer and Network Security: Navigating Shades of Gray: Chapter 9	Virus execution details
10/10/2023		External materials provided	How to survive under an authoritarian government
10/17/2023	Fall break		
10/24/2023		Signature assignment	War game planning: Network surveillance tools
10/31/2023		Signature assignment	War game planning: Online privacy toolkit
11/7/2023	Virus assignment due	*Privacy Protection and Computer Forensics*	Data forensics, data hygeine, and privacy
11/14/2023		Introduction to Computer and Network Security: Navigating Shades of Gray: Chapters 13 and 14	Digital Rights Management / Ethics
11/21/2023	Graduate research		Graduate student research presentations
11/28/2023	Graduate research		Graduate student research presentations
12/5/2023	In class war game exercise	Signature assignment	Class divided into teams executing role playing game
12/14/2023	Final at 7:00 PM		

Assignment	Group or Individual	Deliverable	Due	Points (and weighting) Undergraduate	Points for Graduate	Graduate weighting
VPN and sniffer installation, use, and analysis	Individual	Document and presentation	09/12/23	10	10	6.67
Graduate research topic	Individual (6490 only)	1 page abstract	09/19/23	0	5	3.33
Buffer overflow implementation	Individual	Report and demonstration	10/03/23	25	25	16.67
Polymorphic virus implementation	Individual	Report and demonstration	11/07/23	25	25	16.67
War game exercise	Group	Implementation and Role Playing Game	10/31/23	25	25	16.67
Graduate research project (6490 only)	Individual	Report and in-class presentation	11/21/23	0	45	30.00
Class participation	Individual	N/A		5	5	3.33
Final exam	Individual	Examination	12/14/2023	10	10	6.67
Total Undergrad				100		
Total Grad					150	100

Grading System

: (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

GRADING POLICIES

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 on the machines allocated for that purpose. If non-authorized 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.

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.

NOTIFICATION OF ABSENCE:

The **Notification of Absence module in Canvas** allows students to quickly notify instructors (via an email) of an absence from class and provides for the following categories: court attendance, death of immediate family member, illness, illness of family member, injury, military duty, religious observance, scheduled surgery, university function, unscheduled hospitalization, other anticipated absence, or other unanticipated absence. The notification form requires a brief explanation, dates and times. Based on the dates and times indicated, instructors are automatically selected, but students may decide which instructors will receive the notification. This does not serve as an "excuse" from class. It is a request for an excused absence and students are encouraged to discuss the absence with instructors, as the instructor

is the only person who can excuse an absence. If students are unable to report the absence by computer, they may reach the Office of Advocacy and Success via 864.656.0935. Students with excessive absences who need academic or medical assistance can also contact the Office of Advocacy and Success.

Any exam that was scheduled at the time of a class cancellation due to inclement weather will be given at the next class meeting unless contacted by the instructor. Any assignments due at the time of a class cancellation due to inclement weather will be due at the next class meeting unless contacted by the instructor. Any extension or postponement of assignments or exams must be granted by the instructor via email or Canvas within 24 hours of the weather-related cancellation.

COURSE FEEDBACK

Please feel free to provide feedback at any time. Requests for suggestions on how to improve the class will be provided.

How to be successful in this course

Honesty, openness, and respect are expected from everyone in the course. Feel free to be creative, experiment, and try new ideas. Do not damage the property, or privacy, of others. That is way too easy to do, and there can be legal consequences.

Student's Responsibility

- Be prepared for all classes
- Be respectful of others
- Actively contribute to the learning activities in class
- Abide by the University Academic Integrity Policy
- Do your own work
- Be creative
- Ask questions when you are confused, or reach a point where you do not know what your next wove will be. The course is designed to make that occur).

Instructor's Responsibility

- Be prepared for classes
- Evaluate all fairly and equally
- Be respectful of all students
- Create and facilitate meaningful learning activities
- Behave according to University codes of conduct
- Provide open and honest feedback to student work and questions.