

Syllabus

Course Title and Course Number: Include section number

**Distributed Denial of Service (DDoS) Attacks, ECE 8860 Sections 001, 843,
CPSC 8860 Sections 001,843**

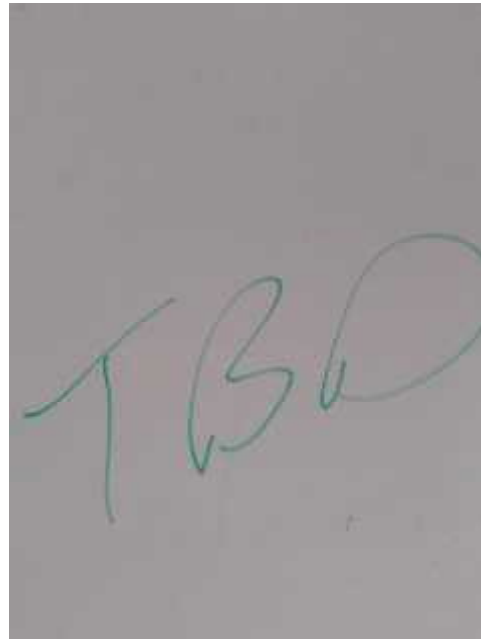
Term: Spring 2023

<https://www.clemson.edu/registrar/academic-calendars/calendars.html?year=2023&semester=spring>

Class Meeting Time and Place:

Monday and Wednesday 5:00 PM Eastern to 6:15 PM Eastern

Lectures: Riggs 226 (Main Campus) TBD Classroom (Charleston)



Online:

<https://clemson.zoom.us/my/la.pesto>

Most likely Charleston will access via this link, but there may be other options.) Will try (no promise) to make videos of lectures to put online. Lecture videos (together with lectures from previous years) will most likely (Not certain that the university is maintaining its agreement with box.com) be stored at:

<https://clemson.box.com/s/1ucccv08u1apth9gb3z4oa90gj3w9s0r>

Lab sessions:

Main Campus: Lab in basement of Riggs. We will explain on the first day of class.

Charleston Campus: Will be explained.

Time to Wait: Please wait 15 minutes in case we may be late.

Information on Modality: Mainly in person. Might change. Lab sessions, we will discuss

Instructor Name:



R. R. Brooks

Professor

<http://rrb.people.clemson.edu/>

(He/Him/His)

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 (Email is an asynchronous medium. Will attempt to respond.)

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

Ms. Winifried Aideyan

Student Assistant

Contact info to be provided

Office Hours: 4:00 PM Eastern time to 5:00 PM Wednesdays or as arranged.

Course Description:

Denial of Service (DoS) attacks are an important weakness of the current Internet. This course is meant to give the students understanding of how these attacks occur, they can be detected and to mitigate them. Students will be taught about normal Internet traffic time series and how difficult it is to create, model, and analyze Internet traffic. Students will use software defined networking primitives to set up experiments. Network attacks will be executed and mitigated..

Prerequisites: Permission of instructor.

Value Statement:

Learn about networks. Learn about security. Learn about how networks go bad. Learn how to avoid networks going bad. Learn how the Internet works, or does not.

Learning Objectives / Outcomes:

After completing this course, students will be able to:

- Explain vulnerabilities that enable DDoS.
- Tools and attacks used to launch DDoS.
- The history and evolution of DDoS.
- Understand what Internet traffic looks like and why it is hard to model.
- Approaches used to detect DDoS and why they fail.
- How to cause intrusion detection systems to detect attacks that are not there and not detect attacks that are ongoing.
- How to configure networks to mitigate DDoS.
- Understand prevalent computer and network security issues,
- Implement DDoS mitigation strategies,
- Be able to configure network services,
- Understand Internet traffic patterns,, and
- Avoid network bottlenecks.

Required Materials

- *Distributed Denial of Service Attacks*, by I. Ozcelik, and R. R. Brooks, CRC Press
- Computer capable of running simultaneously at least 2 virtual machines,
- Webcam
- Microphone
- Internet connections
- Cell phone.

Course Overview:

Date	Lecture topic	Reference	Assignment	Due
1/11/2023	Overview and syllabus	Chapter 1		
1/16/2023	MLK Day			
1/18/2023	SDN lecture and network topology	Chapters 6, 11, 14.1, 14.2, 14.3		
1/23/2023	Lab 1 – Part A. Traffic sniffing		Lab report 1	2/6/2023
1/25/2023	History and Motivation of DDoS	Last day to drop Chapters 2 and 3		
1/30/2023	Importance of background traffic / DDoS legal discussion	Chapters 4 and 5		
2/1/2023	Lab 1 -- Part B. spoofing		Lab Report 1	2/6/2023
2/6/2023	Botnet and IoT background	Chapters 2 and 3		
2/8/2023	Lab 2 – Part A. Background traffic generation	Chapter 6	Lab report 2	03/07/23
2/13/2023	Attack traffic tools	Chapter 5		
2/15/2023	Lab 2 - Part B. Attack generation	Chapter 5	Lab report 2	03/07/23
2/20/2023	Flooding attack traffic generation techniques and tools	Chapter 5		
2/22/2023	Lab 2 - Part B. Attack generation	Chapter 14	Lab Report 2	03/07/23
2/27/2023	In class test		Mid term	2/27/2023
3/1/2023	DDoS Amplification	Chapter 14		
3/3/2023	Lab 2 - Part B. Attack generation		Lab report 2	03/07/23
3/6/2023	Detection basics	Chapter 7		
3/8/2023	Attack detection lecture	Chapter 8		
3/13/2023	Lab 3 – Attack detection	Chapter 7,8,14	Lab report 3	04/03/23
3/15/2023	Lab 3 – Attack detection	Chapter 7,8,14	Lab report 3	04/03/23
3/20/2023	Spring Break			
3/22/2023	Spring Break			
3/29/2023	Traffic spoofing lecture	Chapter 9		
4/3/2023	Lab 4 – Deceiving DDoS Detection		Lab report 4	05/02/23
4/5/2023	Firewall/filtering lecture	Fu Yu Remote Lecture (To be confirmed)		
4/7/2023	Lab 4 – DDoS mitigation		Lab report 4	05/02/23
4/10/2023	Mitigation lecture	Chapter 10		
4/12/2023	Lab 4 – DDoS mitigation	Chapter 10, 14	Lab report 4	05/02/23
4/17/2023	Mitigation scaling			
4/19/2023	Lab 4 – DDoS mitigation		Lab report 4	05/02/23
4/24/2023	Review			
5/2/2023	Final exam	7:00 to 9:30 PM	Final	Take home final due at 7:00 PM

Learning Environment:

Instruction will be a combination of lectures and hands-on on-line labs. Lots of the work will be doing hands-on work configuring networks, collecting network traffic, staging attacks, and seeing what happens.

How to Be Successful in this Course

Be attentive and persistent. If you do not understand something, ask questions. Do not take no for an answer. Try to figure things out, but if it is not working, ask questions. I provide puzzles for you to solve.

Major Assessment/Grading Activities:

Assignment	Due	Percent grade
Lab report 1	2/6/2023	10%
Lab report 2	3/7/2023	15%
Midterm	2/22/2021	15%
Lab report 3	4/3/2023	15%
Lab report 4	5/2/2023	20%
Final	5/2/2023	25%
Total		100%

Course Feedback

Feedback is welcome.

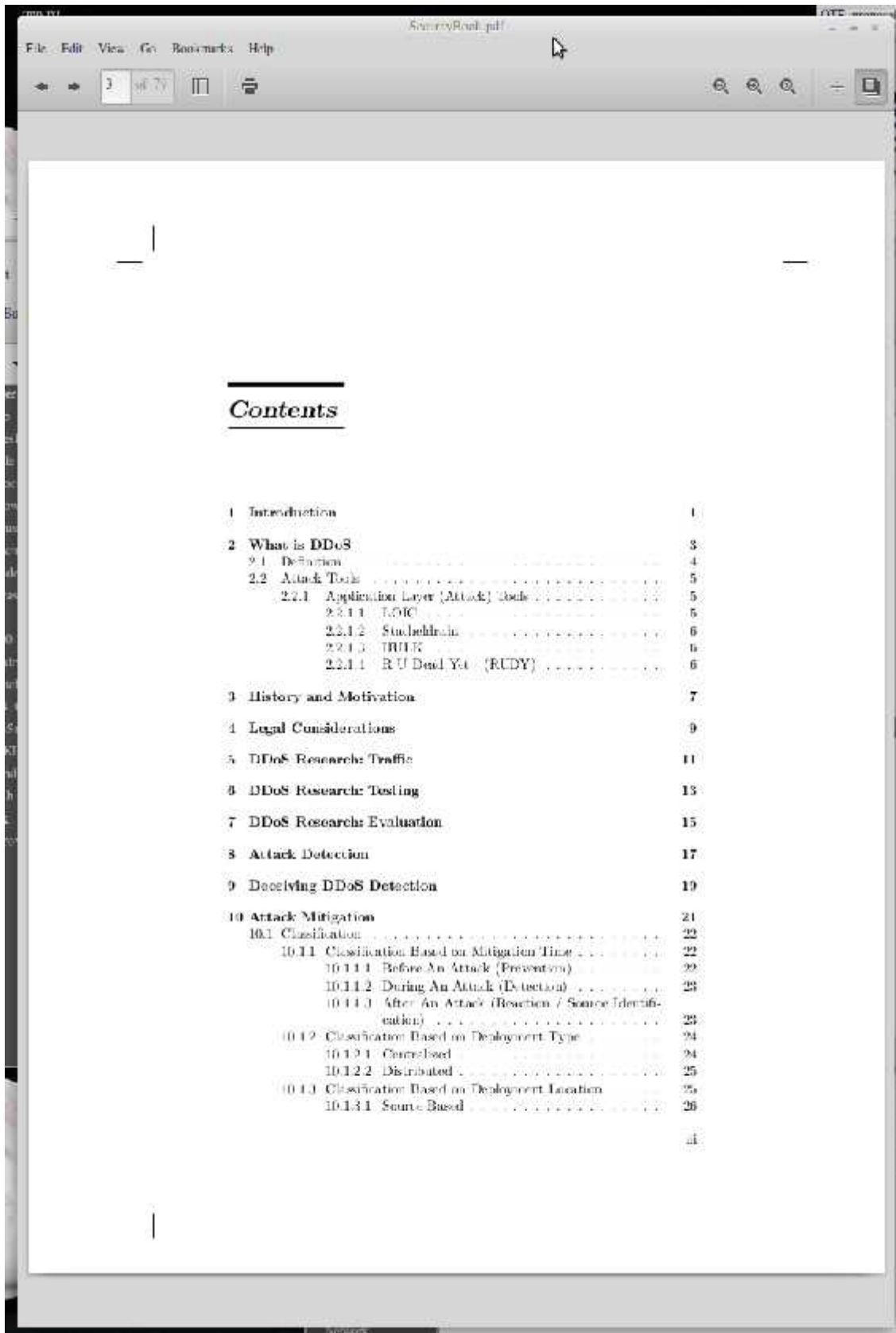
Grading System:

Letter	Points/Percentages
A	90%
B	80%
C	70%
D	60%
F	Below

Grading Policies:

Grades are rounded down. No penalties for absences, but you are responsible for your work. In case of illness, disability, or natural disaster, accommodations will be allowed as appropriate. Late Work: Does not count. You can turn it in for grading and feedback but you will receive no credit for that work. You are responsible for turning it in on time.

Topical Outline:



The image shows a screenshot of a PDF viewer window titled "SecurityRead.pdf". The window has a menu bar with "File", "Edit", "View", "Go", "Bookmarks", and "Help". Below the menu bar is a toolbar with navigation icons. The main content area displays the "Contents" page of the document. The table of contents lists chapters 1 through 10, with sub-chapters under chapters 2, 10.1, and 10.1.1. The page number "ii" is at the bottom right of the table of contents.

1	Introduction	1
2	What is DDoS	3
2.1	Definition	4
2.2	Attack Tools	5
2.2.1	Application Layer (Attack) Tools	5
2.2.1.1	LOIC	5
2.2.1.2	Stacheldraht	6
2.2.1.3	TRIFLE	6
2.2.1.4	R U Dead Yet (RUDY)	6
3	History and Motivation	7
4	Legal Considerations	9
5	DDoS Research: Traffic	11
6	DDoS Research: Testing	13
7	DDoS Research: Evaluation	15
8	Attack Detection	17
9	Deceiving DDoS Detection	19
10	Attack Mitigation	21
10.1	Classification	22
10.1.1	Classification Based on Mitigation Time	22
10.1.1.1	Before An Attack (Prevention)	22
10.1.1.2	During An Attack (Detection)	23
10.1.1.3	After An Attack (Reaction / Source Identification)	23
10.1.2	Classification Based on Deployment Type	24
10.1.2.1	Centralized	24
10.1.2.2	Distributed	25
10.1.3	Classification Based on Deployment Location	25
10.1.3.1	Source Based	26
		ii

SecurityBook.pdf	
File Edit View Go Bookmarks Help	
4 of 70	Q Q Q + []
iv	
10.1.3.2 Destination Based	26
10.1.3.3 Network Based	26
10.1.3.4 Hybrid	26
10.1.4 Classification Based on Reaction Place	27
10.1.4.1 On The Premises	27
10.1.4.2 In The Cloud	28
10.1.5 Classification Based on Reaction Type	28
10.1.5.1 Filtering Based	29
11 DDoS in Software Defined Networks	31
12 DoS in Control Theory	33
13 Smart Grid DoS Attacks	35
14 DDoS Lab	37
14.1 Toolbox	38
14.1.1 Wireshark / tshark	38
14.1.2 Scapy	39
14.1.3 JMeter	40
14.1.4 Popular DDoS Attack Tools	41
14.1.4.1 DDoSsim	41
14.1.4.2 Tar's Hammer	41
14.1.4.3 SlowLoris/PyLoris	41
14.1.4.4 Saddam	41
14.1.5 Apache Traffic Server (ATS)	42
14.1.6 Apache HTTP Server	42
14.1.7 BIND Domain Name Server	42
14.1.8 Virtualbox	43
14.1.9 Defect	45
14.1.10 Distributed DDoS Mitigation Tool (DDM)	45
14.1.11 Attack	46
14.1.11.1 Sniffing Network	46
14.1.11.2 Man in the Middle	48
14.1.11.3 Network Background Traffic Generation	50
14.1.11.4 DDoS Simulation	53
14.1.11.5 Syn Flood	54
14.1.11.6 Bandwidth Starvation Attack	57
14.1.11.7 Amplification / Reflection	60
14.1.11.8 HTTP GET / POST	62
14.1.11.9 Packet Spoof	65
14.1.11.10 Meter Stress Testing	67
15 Conclusion	69
Bibliography	71

Absences:

Student attendance will not be tracked by the instructor. In some cases, the university requests the instructor to state the last date of attendance in the class. This information is typically related to student billing. It may be in the student's best interest to document, in a form that is not easily forged, when lengthy interruptions in class participation start.

Notification of Absence:

I suggest using the **Notification of Absence module in Canvas** to 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. It keeps a record of such things.

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.

STANDARD ACADEMIC POLICIES

Academic Integrity

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.

All infractions of academic dishonesty by undergraduates must be reported to Undergraduate Studies for resolution through that office. In cases of plagiarism instructors may use the Plagiarism Resolution Form.

See the [Undergraduate Academic Integrity Policy](#) website for additional information and [the current catalogue](#) for the policy. For graduate students, see the current [Graduate School Handbook](#) for all policies and procedures.

Accessibility

Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should let the instructor know and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible. You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged – drop-ins will be seen, if at all possible, but there could be a significant wait due to scheduled appointments. Students who have accommodations are strongly encouraged to request, obtain and send these to their instructors [through the AIM portal](#) as early in the semester as possible so that accommodations can be made in a timely manner. It is the student's responsibility to follow this process each semester.

You can access further information at the [Student Accessibility website](#). Other information is at the university's [Accessibility Portal](#).

The Clemson University Title IX Statement Regarding Non-Discrimination

The Clemson University Title IX statement: 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 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 [Title IX policy](#) is located on the Campus Life website. Ms. Alesia Smith is the Clemson University Title IX Coordinator, and the Executive Director of Equity Compliance. Her office is located at 223 Brackett Hall, 864-656-0620. Remember, email is not a fully secured method of communication and should not be used to discuss Title IX issues.

Clemson University aspires to create a diverse community that welcomes people of different races, cultures, ages, genders, sexual orientation, religions, socioeconomic levels, political perspectives, abilities, opinions, values and experiences.

Emergency Preparation

Emergency procedures have been posted in all buildings and on all elevators. Students should be reminded to review these procedures for their own safety. All students and employees

should be familiar with guidelines from the Clemson University Police Department. [Visit here for information about safety.](#)

Clemson University is committed to providing a safe campus environment for students, faculty, staff, and visitors. As members of the community, we encourage you to take the following actions to be better prepared in case of an emergency:

1. Ensure you are signed up for [emergency alerts](#)
2. Download the [Rave Guardian app](#) to your phone (<https://www.clemson.edu/cusafety/cupd/rave-guardian/>)
3. Learn what you can do to [prepare yourself](#) in the event of an active threat (<http://www.clemson.edu/cusafety/EmergencyManagement/>)