Information About the Course

Course Title and Course Number: **Distributed Denial of Service (DDoS) Attacks, ECE 8860 Sections 001, 843, CPSC 8860 Sections 001,843**

Term: Spring 2024: https://www.clemson.edu/registrar/academic-calendars/calendars.html?year=2024&semester=spring

Class Meeting Time and Place: MW 17:30 – 18:45 in Humanities Hall 358

Time to Wait: Please wait up to around 15 minutes should I be delayed.

Information on Modality: Mainly in person, but you can use this zoom link if you desire (or if you are quarantined, having a bad day, etc.):

https://clemson.zoom.us/my/la.peste

Zooms of lectures will (probably) be recorded. Remind me if I forget to hit "record." The lectures (old and new) will probably be available in (remind me if not done) :

https://clemson.box.com/s/1ucccvo8u1apth9gb3z4oa90gj3w9s0r

Instructor Name: **Richard R Brooks (May provide graduate assistants to aid as needed.)**

Department and College of Instructor:

Instructor Email: rrb@g.clemson.

PGP 1: 955B 3813 41C0 9101 3E6B CF05 02FB 29D6 8E1E 6137

PGP 2: FC15 BAF0 4296 B47E 932A 9DB3 D41B 81AF C6EA 90F6

You can expect a response to your email inquiries within 48 hours, excluding weekends and university holidays.

University Office Phone: **864-656-0920 Voicemail: 864-986-0813**

Office Address/Office Number: ***313-C Riggs Hall]***

Office Hours:

3:00 to 4:00 PM on Tuesdays (or by arrangement)

Riggs 313-C or https://clemson.zoom.us/my/la.peste

Instructor Photo:

Office and/or Classroom Map:

https://www.google.com/maps/@34.6772221,-82.8377646,2a,75y,185.77h,77.43t/data=!3m7!1e1!3m5!1susix0lABLxRZzFTQbdzMRA!2e0!6shttps:%2F%2Fstreetviewpixels-pa.googleapis.com%2Fv1%2Fthumbnail%3Fpanoid%3Dusix0lABLxRZzFTQbdzMRA%26cb_client%3Dmaps_sv.tactile.gps%26w%3D203%26h%3D100%26yaw%3D158.54337%26pitch%3D0%26thumbfov%3D100!7i13312!8i6656

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..

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.

Course Overview

Date	Lecture topic	Reference	Assignment	Due
1/10/2024	Overview and syllabus	Chapter 1		
1/15/2024	MLK Day			
1/17/2024	SDN lecture and network topology	Chapters 6, 11, 14.1, 14.2,14.3		
1/22/2023	Lab 1 – Part A. Traffic sniffing		Lab report 1	2/12/2024
1/24/2024	History and Motivation of DDoS	Last day to drop Chapters 2 and 3		
1/29/2024	Importance of background traffic / DDoS legal discussion	Chapters 4 and 5		
1/31/2024	Lab 1 -- Part B. spoofing		Lab Report 1	2/12/2024
2/5/2024	Botnet and IoT background	Chapters 2 and 3		
2/7/2024	Lab 2 – Part A. Background traffic generation	Chapter 6	Lab report 2	03/13/24
2/12/2024	Attack traffic tools	Chapter 5		
2/14/2024	Lab 2 - Part B. Attack generation	Chapter 5	Lab report 2	03/13/24
2/19/2024	Flooding attack traffic generation techniques and tools	Chapter 5		
2/21/2024	Lab 2 - Part B. Attack generation	Chapter 14	Lab Report 2	03/13/24
2/26/2024	**In class test**		**Mid term**	2/26/2024
2/28/2024	DDoS Amplification	Chapter 14		
3/4/2024	Detection basics	Chapter 7		
3/6/2024	Lab 2 - Part B. Attack generation		Lab report 2	03/13/24
3/11/2024	Attack detection lecture	Chapter 8		
3/13/2024	Lab 3 – Attack detection	Chapter 7,8,14	Lab report 3	04/01/24
3/18/2024	Spring Break			
3/20/2024	Spring Break			
3/15/2023	Lab 3 – Attack detection	Chapter 7,8,14	Lab report 3	04/01/24
3/25/2024	Traffic spoofing lecture	Chapter 9		
3/27/2024	Lab 4 – Deceiving DDoS Detection		Lab report 4	04/24/24
4/1/2024	Firewall/filtering lecture	Fu Yu Remote Lecture (To be confirmed)		
4/3/2024	Lab 4 – DDoS mitigation		Lab report 4	04/24/24
4/8/2024	Mitigation lecture	Chapter 10		
4/10/2024	Lab 4 – DDoS mitigation	Chapter 10, 14	Lab report 4	04/24/24
4/15/2024	Mitigation scaling			
4/17/2024	Lab 4 – DDoS mitigation		Lab report 4	04/24/24
4/22/2024	Lab 4 – DDoS mitigation		Lab report 4	04/24/24
4/24/2024	Review			
4/29/2024	Final exam	7:00 to 9:30 PM	Final	In Class, Open Book, Handwritten on

Learning Outcomes *[Required]*

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.

Prerequisites *[Required]*

Permission of instructor.

Required Materials *[Required]*

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

Required Technical Skills

Programmnig. Statistics. Understanding of Internet. Math.

Learning Environment

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

Major Assessment/Grading Activities

Assignment	Due	Percent grade
Lab report 1	2/12/2024	10%
Lab report 2	3/13/2024	15%
Midterm	2/26/2024	15%
Lab report 3	4/1/2024	15%
Lab report 4	4/24/2024	20%
Final	4/29/2024	25%
Total		100%

Grading System

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

Grading Policies ***[REQUIRED]***

Grades are rounded down.

No penalties for absences, but you are responsible for your work. In case of illness or disability, accommodations will be allowed.

Written assignments will be subject to spot checks using generative AI text checkers. If your text scores greater then 50% on two randomly chosen checkers, it will get a zero. Since these checkers have frequent false positives, it is worth checking your text before turning it in, even if you do not use generative AI.

Written assignments that score high on a plagiarism checker (I submit all assignments from the class at once) get no credit. With one exception, if you signal to me that a colleague's paper will be similar to yours before I run it through the checker, you get double credit for the assignment (twice a perfect score) and your colleague will get zero. Only the first student that signals this cheating will get credit. If this text scores high on a generative AI checker, you both get minus credit.

The final had been take home with open Internet access in the past. Due to rampant cheating last year, the final is in class, handwritten on paper, and open book. No other aids will be allowed.

Late Work: Does not count.

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.

COURSE FEEDBACK

Feedback is welcome.