CSCI 307 Computer Networks and Security

Fall 2025

This course builds on the foundation established in CSCI 306 Computer Systems, leveraging your prior experience with **C programming**. We will build a foundation in computer and network security by introducing fundamental concepts and practical skills. A key focus will be on the interconnected nature of systems, starting with an exploration of the **ISO/OSI reference model** and essential networking protocols like **UDP, TCP, and HTTP**. You'll gain practical experience in **network programming** and learn how to write secure C code to mitigate common vulnerabilities.

Throughout the course, we will explore and apply core cybersecurity principles, including:

- **Availability:** Information and systems are accessible and usable by authorized users whenever needed.
- **Confidentiality:** Data is accessible only to those authorized to view it.
- **Integrity:** Data is protected from unauthorized modification or corruption.

By the end of the course, you will have a solid understanding of how these concepts are applied in real-world systems. This course serves as a vital bridge to more advanced topics in our core systems sequence, providing a strong foundation for CSCI 315 Operating Systems.

Class Schedule

Thursday, 10:00 AM – 11:20 AM, Academic East 116

Week	Day	Date	Topic	Concepts
1	Thu	Aug. 28, 2025	Introduction	Course overview, review of C programming. Introduction to the CIA triad (Confidentiality, Integrity, Availability). Discussion of the threat landscape and the importance of a systems-level approach to security.
2	Thu	Sep. 4, 2025	Network Models & Protocols	Introduce the ISO/OSI 7-layer reference and TCP/IP models. Focus on the purpose of each layer and how data is encapsulated as it moves down the stack. Detailed exploration of core protocols: TCP, UDP, and HTTP. Introduction to sockets and client-server communication in C. Hands-on lab to build a simple TCP client and server.
3	Thu	Sep. 11, 2025	Network Programming Fundamentals	Introduction to sockets and client-server communication in C. Hands-on lab to build a simple TCP client and server.
4	Thu	Sep. 18, 2025	Core Network Services & Analysis	In-depth look at essential protocols like DNS and DHCP. Use tools like Wireshark to capture and analyze network traffic.
5	Thu	Sep. 25, 2025	Secure Network Programming	Focus on writing robust C code for networking. Handling network errors, validating input from network streams, and preventing simple attacks. Use Valgrind.
6	Thu	Oct. 2, 2025	Introduction to C Vulnerabilities	Explore common vulnerabilities specific to C: buffer overflows, format string vulnerabilities, and integer overflows.
7	Thu	Oct. 9, 2025	Defensive Coding & Mitigation	Strategies for writing secure C code, including input sanitization, using safe string functions, and compiler-level protections like stack canaries.
8	Thu	Oct. 16, 2025	Cryptography Fundamentals	Core principles of cryptography. Introduction to symmetric and asymmetric encryption, hashing, and digital signatures. Discuss the role of these in ensuring confidentiality and integrity.
9	Thu	Oct. 23, 2025	Transport Layer Security (TLS)	How TLS secures internet communication. Explore the TLS handshake process, the role of certificates, and how it provides confidentiality and integrity for protocols like HTTPS.
10	Thu	Oct. 30, 2025		

11	Thu	Nov. 6, 2025	Authentication & Authorization	Differentiate between authentication ("who you are") and authorization ("what you can do"). Explore common authentication methods like passwords and multi-factor authentication (MFA).
12	Thu	Nov. 13, 2025	Access Control	Focus on the authorization aspect. Dive into different access control models, including Access Control Lists (ACLs) and Role-Based Access Control (RBAC), and discuss their real-world application.
13	Thu	Nov. 20, 2025	Availability & Denial of Service (DoS)	Focus on the principle of Availability. Learn about different types of DoS and DDoS attacks and the architectural strategies used to mitigate them.
14	Thu	Nov. 27, 2025	**THANKSGIVING**	
15	Thu	Dec. 4, 2025	Course Review	Bridge to CSCI 315 by discussing how operating systems enforce security principles, including file permissions, process isolation, and memory protection.

Instructor

Prof. Alan Marchiori

Office: Dana 335a

E-mail: amm042@bucknell.edu

Office hours: open door, MWF 10:00 AM - noon, TR 1:00 PM - 3:00 PM, appointments appreciated!

Web: burl.live /alan

Values and Commitments

Bucknell University steadfastly affirms our commitment to our students, staff, and faculty. Regardless of race, ethnicity, or nationality, gender, gender expression or sexual orientation, religion or belief system, economic status, or ability, you are a values, respected, and essential member of our community. We are all committed to welcoming others in this manner. We will not tolerate mistreatment or disrespect of persons for any reason by

members of our community. The College of Engineering strives to offer a safe environment for learning, growth, inquiry, and the respectful sharing of ideas for all.

We have a moral and professional obligation to share the responsibility of always treating each other with respect and dignity, even when we disagree. However, we will not question or leave room for disagreement about the value of different human beings. We investigate and solve problems, sometimes very challenging ones. An important method for such investigations and solutions is through the exploration of ideas in conjunction with the unquestioned support and value of individuals. We can all engage in such processes when we feel comfortable and safe as members of a community.

Your suggestions to help the University meet this commitment are encouraged and appreciated. If something occurs in class that makes you feel uncomfortable, please talk to me about it. Other resources for you include your instructors, department chairs, and Associate Deans Terri Norton (trn005@bucknell.edu) and Rich Robbins (rlr024@bucknell.edu). Instead of or additionally, you may file a bias incident report using this link. This report may be filed anonymously if you so choose. The College of Engineering commits to working alongside students expressing concerns and/or making reports to empower them in any follow-up actions

and to ensure that they are protected from repercussions of any kind.

Professionally, we adhere to ACM's Code of Ethics. More broadly, a course like Operating Systems involves group and class discussion. Computer science has a checkered history with respect to inclusion – in corporate environments, in our classrooms, and in the products we create. We strive to promote characteristics of transparency and inclusivity that reflect what we hope our field becomes (and not necessarily what it has been or is now).

We reject behaviors that stray into discrimination, racism, or harassment. Such behavior (whether verbal, written, or through actions) may relate to others' race, gender, faith, or sexual orientation, among virtually innumerable *professionally irrelevant* characteristics (e.g., religion, [dis]ability, age, etc.); sexual images in public spaces; deliberate intimidation, stalking, following, harassing photography or recording, disruption of meetings, inappropriate physical contact, and unwelcome sexual attention.

If you believe someone is violating these principles (for example, with a joke that could be interpreted as sexist, racist, or exclusionary), **please feel empowered to speak up.** If the behavior persists, send a private email to your instructor to explain the situation. While we will preserve anonymity when

possible, also be aware that we are required by law to report incidents of sexual misconduct or relationship violence.

You may also contact Bias Incident Reporting at https://www.bucknell.edu/life-bucknell/health-wellness-safety/bias-incident-policy

We are here for you. Life can be full of uncertainties and hardships. You may find yourself in tough situations such as being sick, having to care for someone who is sick, having a hard time coping with a personal crisis, or even facing food insecurity. If you find yourself in a predicament that is weighing on you, please get in touch with us. We will work with you to make the accommodations necessary to help you out and we will try our best to help you. Please believe that we are invested in supporting you.

Course Objectives

This course will help students develop a broad understanding of the areas of computer networking and security. Our primary objectives are to:

1. Apply and expand on the knowledge gained in CSCI 306 Computer Systems, more specifically Unix systems programming in C,
2. Understand the architecture of computer networks software,

3. Understand how to develop networked applications using UDP and TCP sockets,
4. Understand the main principles of computer and network security.

Course Outcomes

By the end of the course, students will be able to:

- Understand a network protocol from documentation such as an RFC.
- Create networked applications that communicate using the UDP and TCP protocols (CAC 2).
- Create customized application-level protocols (CAC 2).
- Understand fundamental properties of computer security, such as authentication, authorization, data confidentiality, and data integrity (CAC 4).

Learning Materials

A variety of articles and other written materials will be shared through Google Classroom. No textbooks are required for this course.

Optional reading: Stallings & Brown, Computer Security Principles and Practice, 5th ed.
https://www.pearson.com/en-us/pearsonplus/p/9780138091712

Course Grade Distribution

Course grades will be assigned only at the end of the semester. Throughout the semester, you can monitor the grade book to track your progress.

- 60% Assignments (aka. Labs)
- 30% Quizzes
- 10% Engagement

Final letter grades will be assigned at the end of the semester according to the following scale:
A >= 93% [Superior achievement]
A- >= 90% [Outstanding]
B+ >= 87%, B >= 83%, B- >= 80% [High Pass; Above Average]
C+ >= 77%, C >= 73%, C- >= 70% [Average work; Satisfactory]
D >= 60% [Low Pass]
F < 60% [Unsatisfactory]

Attendance

Attendance is ***mandatory*** and will be taken ***at the start of the class period***. Unexcused absences will have an impact on the student's final grade. If you are experiencing health problems, please understand that you should not come to class: we all have a shared responsibility to each other to avoid the dissemination

of transmissible diseases. **Be sure to notify the instructor in advance if you must be absent for any reason.**

Late Work

Unless otherwise listed, assume that all assignments are to be submitted prior to the beginning of the lecture on the due date. Assignments turned in late will be reduced by 10% of the original assignment value per week late, up to a maximum of four weeks. After this time, the grade will be a zero.

Exceptions to the late policy can be requested with good reason from the instructor at least 24 hours before the due date (email is acceptable).

Use of Artificial Intelligence

Artificial intelligence (AI) tools may be used with appropriate attribution (example below) unless otherwise noted in the assignment. However, AI tools will not be available for classroom assessments (quizzes). You are responsible for fact checking statements composed by an AI as well as being sure it does not violate policies on intellectual property or unethical content. You are solely responsible for the work you submit based on an AI query.

Sample attribution: “The author(s) generated this text in part with GPT-3. Upon generating draft language, the author

reviewed, edited, and revised the language. I/We take ultimate responsibility for the content."

Access Statement

Any student who needs accommodation based on the impact of a disability should contact the Office of Accessibility Resources at oar@bucknell.edu, who will coordinate reasonable accommodations for students with documented disabilities.