# CSC/ECE 574 Syllabus — Spring 2024

## Course Information

**Course** CSC/ECE 574 – Computer and Network Security Spring 2024

**Meeting Location** 1230 Engineering Building 2

**Meeting Times** 10:15 AM – 11:30 AM

**Credits** 3

**Instructor** Prof. Brad Reaves

**Email** bgreaves@ncsu.edu

**Office Hours** After class or by appointment. Book Here

**TA** Alex Ross

**TA Office Hours** By Appointment

**Class Forum** Piazza

**Lecture Recordings** Panopto

**Schedule** Available here

**Formal Prerequisites:** [CSC 316 or ECE309] and [CSC 401 or ECE407] or equivalent

**Informal Prerequisites:** I assume students have the equivalent of a comprehensive computer science or engineering bachelor's degrees that covered operating systems, networks, discrete mathematics, and programming in multiple languages. Students without prior classes on these topics have done well after increased individual study. Students without this background or a willingness to independently review it may struggle with course content.

---

# Course Overview

## Catalog Description

Fundamentals of computer security and privacy, including security models, policies, and mechanisms. Cryptography for secure systems, including symmetric and asymmetric ciphers, hash functions, and integrity mechanisms. Authentication of users and computers. Network attacks and defenses at the network and application layers. Common software vulnerabilities and mitigation strategies. Secure operating systems and seminal access control models and policies. Principles of intrusion detection. Privacy, including considerations of end-user technologies.

## Course Description

This course provides a graduate-level introduction to computer and network security and privacy. Students successfully completing this class will be able to evaluate works in academic and commercial security, and will have rudimentary skills in security research. The course covers four key topic areas: basics of cryptography and crypto protocols, network security, systems security, and privacy. Readings primarily come from the course textbook and seminal papers in the field. A detailed list of lecture by lecture contents, assignments, and due dates (subject to change as semester evolves) is available on the course schedule.

## Course Goals

The goal of CSC/ECE 574 is to provide students with a foundation of computer security fundamentals. It is the first of a set of courses security PhD students and MS students who pursue the MS Track in Security will take, and it serves as an introduction to material that will be covered in later security electives in cryptography, network security, software security, systems security, and privacy. It is also suitable as a single elective for MS students and PhD students who wish to enrich their education with an expanded base of computer security experience. After graduation, students can use the material of this course to design, analyze, and critique secure computing designs.

## Structure

This course meets in-person twice a week. Content is primarily delivered via lectures with integrated learning activities. The course will consist of a reading reports, a midterm, a final, and three mini-projects or a research project. A detailed list of lecture by lecture contents, assignments, and due dates (subject to change as semester evolves) is available on the course schedule.

## Learning Outcomes

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

- *Fundamentals:* Specify a security model for a given computer system
- *Crypto:* Explain and apply concepts related to applied cryptography, including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, digital signatures.

- *Authentication:* Outline the requirements and mechanisms for identification and authentication of users and computer systems, including authentication protocols and key management. Identify the possible threats to each mechanism and ways to protect against these threats.
- *Network:* Identify common network and application layer attacks and defense mechanisms.
- *Software:* Explain and identify instances of common software vulnerabilities and mitigations.
- *System:* Explain concepts related to access control and operating system security, including access control matrices, ACLs and capabilities, protection, reference monitors, least privilege, discretionary access control, mandatory access control.
- *Privacy:* Identify and explain common privacy definitions, techniques, and systems that preserve or reduce privacy.
- *Research:* Read and interpret bleeding-edge academic research papers on computer and network security and privacy, and describe how the results impact real systems and people.

---

## Course Structure

The course will consist of lectures, eading reports, a midterm exam, a final exam, and the student's choice of two project tracks.

**Project:** Students may choose either the [Research Project] track or the [Mini-Projects] track. The Research Project track will require the student to execute novel research in systems and network security or privacy. The result of the project will be a conference-quality paper. The Mini-projects track will provide a series of smaller projects that relate more directly to the course material. The projects require a range of programming as well as open-ended investigation.

**Project Grading Scale:** This class will not use a 100-point scale for Projects. In graduate courses, most grading is subjective based on the experience of the instructor, which is never precise to 2 decimal places. Instead, project deliverables will receive one of the following numerical grades:

- 95: Excellent work: Student demonstrates full mastery of all elements of an assignment, high-quality execution, and clear and professional presentation.
- 85: Standard work: Student demonstrates mastery of most elements of an assignment, with adequate execution and unremarkable presentation. **This is the "default" grade** – students must deviate significantly from the mean to go above this grade.
- 75: Substandard work: Student fails to demonstrate mastery of a significant portion of the assignment, executes some elements poorly or incorrectly, and/or presents portions of work in an unclear or inappropriate manner.
- 65: Unsatisfactory work: Student fails to address most key elements of the assignment, leaves significant portions of the assignment unattempted or incomplete, and/or fails to provide a comprehensible presentation of the work done.
- 0: Student fails to provide evidence of a good-faith attempt at the assignment.

**Reading Reports:** Students will read seminal research papers in computer security throughout the semester and submit very brief worksheets termed "reading reports" for each paper. There will generally be one paper per week, with occasional "bye weeks" without a paper assigned due to breaks or significant deadlines. Generally, students should budget a few hours per week for reading,

and 15-30 minutes to complete the report. **Up to 10% of exam points may cover key ideas from papers not discussed in class.**

**Reading Report Grading Scale:**

Each report will be evaluated for **earnest completion** on a "pass/fail" basis. The reading report component of the final grade will be the ratio of passed papers to the total. I anticipate each report will be worth approximately 1 point on the final average.

**Final Grade Breakdown:**

The final grade will be computed as follows: - 40% Projects - 25% Midterm - 25% Final Exam - 10% Reading Reports

For research project, the final paper submission will comprise half of the project portion of the final grade.

The final average will be converted to letter grade using the scale in NC State REG 02.50.03.

## Weekly Course Schedule

See the course schedule. Note that the schedule is subject to change as the semester evolves.

## Textbooks and Reading Material

This course will use the following textbook, along with readings from other informative sources. The text is strongly recommended, but not required.

- Network Security: Private Communication in a Public World by Kaufman, Perlman, Speciner, and Perlman. 3rd Edition only. ISBN: 978-0136643609.

Here are some useful online books that provide additional information:

- Ross Anderson. Security Engineering, 2nd Edition. Wiley. April 2008.
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. October 1996.
- Paul C. Van Oorschot. Computer Security and the Internet: Tools and Jewels. Springer. 2020. **Note:** Author's self-archived version is freely available.

## Resources for Support

The instructor's goal is to help students gain a clear understanding of the course material, to foster a deep interest in the topic of computer security, and develop the basic research skills essential to a career at the frontiers of technology. With security, the devil is often in the details, and crucial understanding often relies on subtleties. Accordingly, it is natural for students to struggle both with the content of this course and with requisite background material.

To this end, the instructional staff are providing a number of mechanisms for support. These include:

- **Piazza** The course will feature a Piazza message board. This should be your first go-to resource for any questions about course structure, deadlines, class material, or anything else that could possibly be relevant to other students. The instructional staff receives emails from Piazza, so any questions posted to Piazza will be addressed as fast or faster than those sent by email.
- **Panopto** I will make recorded lectures available to you to aid in studying or to help in catching up after absences. These will be available on Panopto.
- **Office Hours** Students are highly encouraged to come to office hours with the instructor or TAs to discuss doubts about course material, concerns about course performance, or to discuss computer security beyond what can be discussed in class.
- **Email** The instructional staff strongly discourages email communication. Emails will be posted anonymously to Piazza on a student's behalf and answered there. If it is possible to publish the question without revealing sensitive information, we will make the question public.

If at any time you have constructive suggestions about how to improve the course, feel free to share them with the instructor during office hours or via a private Piazza message.

## Ethics Statement

This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class. This is a very serious issue – violations may not just be immoral, they may violate federal laws.

When in doubt, please contact the course professor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from the instructor.

Students are also encouraged to read and adhere to the ACM Code of Ethics and Professional Conduct. Note that building secure and privacy-respecting systems is considered an *ethical obligation,* not merely a suggestion, by the ACM.