COMP-4721 Course Syllabus

March 26, 2026

1 Course Information

Course Name	COMP-4721: Computer Security
Prerequisites	None
Required Textbook	No textbook required

2 Course Description

This course provides an introduction and overview of computer security. This course gives you an overview of the essential components of computer security along with basic cryptography and some concepts from network security.

Specific topics include:

- Assets, risks and vulnerabilities
- The CIA triad
- Cryptography basics (asymmetric vs. symmetric, block vs. stream, etc.), old-school cryptosystems (substitution, rotation, transposition)
- Cryptanalysis (frequency analysis, brute force, general weaknesses)
- Cryptography details (RSA, DSA, DH, EC)
- Security policies, access controls and protection methods
- Role-based access controls
- Database security
- Authentication technologies
- Host-based and network-based security issues and defensive technology and techniques
- Software vulnerability exploitation and prevention (buffer over/underflows, untrusted input, numerical errors, ROP chains, etc.)
- Threat modeling and attack surface

3 Textbook and Materials

For lectures, we will use the following textbook:

Computer Security: Principles and Practice (3rd Edition), by William Stallings and Lawrie Brown

The following optional textbooks are also useful, but are not required materials:

Computer Security, by Dieter Gollmann. Dieter Gollmann, ISBN 978-0-470-74115-3, Publisher John Wiley & Sons, Incorporated, Publication Date February 28, 2011.

Computer Security Fundamentals (Fourth Edition), by Chuck Easttom, ISBN-13 978-0135774779, ISBN-10 0135774772, Publisher Pearson, Publication Date November, 2019

You will need a good internet connection and a laptop that meets DU specifications. (See `https://www.du.edu/it/support/how-to/students/laptops`). For technical support in using Canvas, please go to `http://otl.du.edu/knowledgebase/canvas`

3.1 Other Stuff

- Reliable access to a computer and the Internet. If you are online you can turn your homework in from wherever in the world you are!
- Wireshark, which is freely available. You will need to install this and make sure it's working on your computer. I'm assuming as computer science or computer engineering majors, you will have the ability to download software and install it without the need for technical support. Seriously, if you can't get the software installed, you're not ready for this course, it's far more advanced than that!
- git: We will be using git, a source code version control system. You will be required to set up and use a git repository to turn in the programming assignments.
- Canvas: We will be using the Canvas platform for most of the course, including course material and communication. Be sure you are able to access Canvas.
- CLion/PyCharm: This is not a requirement, but I will generally be programming in-class examples in the CLion IDE from JetBrains OR the PyCharm IDE from JetBrains. I like the JetBrains IDEs and they are free for you to use if you sign up with your du.edu email address.

4 Course Learning Objectives

By the end of this course, you should be able to:

- Assess risks, threats and vulnerabilities
- Develop a threat model
- Write a proposal to fortify the network against a given threat model
- Understand the details of a given intrusion

- Identify general principles that underlie different intrusions
- Learn vocabulary common to information security
- Understand the mathematical foundations on which the modern cryptography is built
- Detailed understanding of database SQL injection attacks
- In-depth knowledge of common types of software attacks, vulnerabilities and exploits
- Understand the trade offs offered different security models to enforce policies
- Use off the shelf software for encryption/decryption, key management
- Write code that utilizes crypto libraries for encryption/decryption/signing
- Use security controls in modern operating systems (Unixes/Windows) and understand the access control policies and implementation

5 Course Outcomes

The high level objectives of this course are as follows:

1. Give students a general overview of the most important aspects of computer security. This course is broad due to the wide range of topics that need to be covered.
2. Students should exit this course with the ability to converse intelligently about computer security and understand common nomenclature related to the field.
3. Students should exit the course with hands-on, technical and programming experience with cybersecurity subjects. Projects/assignments covering programming with cryptographic libraries, cyber attacks and defenses for vulnerabilities, and web applications are potential topics covered in detail.

6 Program Level Goals

Courses in the cyber security MS program, including this one, should contribute to overall program level outcomes for students. This course contributes to the following program level goals:

1. **Understand how modern operating systems work (with a leaning towards Unix style OSes).** Be familiar with their security components (identification, authentication, access controls, auditing) and how to configure them.
2. Understand common cyber security vocabulary, and understand and intelligently discuss cyber security topics (incidents, advisories, etc.)

3. Comprehend core computer security concepts from a theoretical standpoint. Components such as the CIA triad, security models, threat modeling, risk assessment, etc. are some examples of these topics.

4. Explain the legal and ethical ramifications of malicious cyber activities, and have an awareness of their responsibilities when working in this field.

5. Demonstrate a **foundational understanding of** networking and **network security**. Networking concepts like the 5-layer Internet protocol stack and their components, and **network security concepts including the purposes of firewalls, IDSes and SIEMs are deeply understood.**

7 Knowledge Units

This course covers the following NSA cybersecurity Knowledge Units:

1. IT Systems Components (ISC, Foundational CDE)

2. Basic Networking (BNW, Core Technical CDE)

3. Network Defense (NDF, Core Technical CDE)

4. Cybersecurity Ethics (CSE, Optional KU)

5. Systems Programming (SPG, Optional KU)

8 Attendance Policy

Regular attendance is expected. Students are responsible for all material covered in class, including announcements and handouts.

9 Academic Integrity

All work submitted for this course must be the student's own original work. Any instance of plagiarism or cheating will be dealt with according to the university's academic integrity policy. Refer to the Student Rights and Responsiblities, as well as the University of Denver Student Honor code, here: `https://studentaffairs.du.edu/student-rights-responsibilities`

10 Disability Services

If you have a disability that may affect your ability to complete the work for this course, please contact the Disability Services office at: `https://studentaffairs.du.edu/disability-services-progr`