CSC 116 – Cybersecurity: An Introduction to Security and Privacy
Spring Semester 2025

Classroom: **Dooly Memorial 318.**
Lecture Hours: Monday/Wednesday**, 3:35PM-4:50PM**
Instructor: **Yusen Wu**; Email: **yxw1259@miami.edu**; Office: Ungar Building, 103E, Coral Gables.
Teaching Assistant: **Caden Radojevich Headrick**; Email: **crh873@miami.edu**
Office hours: by appointment

1 Course Goals:

The goal of this course is to develop a basic understanding of cybersecurity systematically.

2 Learning Objectives:

- Understand the cyberspace, threats, and vulnerabilities.
- Understand threats to the hardware, software, and network components of mobile devices.
- Understand various types of malwares --- Viruses, etc.
- Understand the methods of how to secure and prevent malware attacks.
- Understanding the vulnerability of human factors in Social Engineering attacks.
- Evaluate the workings, strengths, weaknesses, and applicability of existing systems.
- Exposure to the latest IT Security trends and awareness initiatives.
- Demonstrate innovative critical thinking from an information security perspective.

3 Attendance Policy:

Attendance is not mandatory but encouraged, because materials presented in the classes are drawn from diverse sources.

4 Grading Policy:

I will grade based on straight percentages, while also considering adjustments to the class distribution to ensure that everyone has a fair chance to achieve an ideal score. Any distribution adjustments, such as curving, will always be in favor of the class.

5 Honor Code:

Please be aware of and abide by the University of Miami Honor Code. All violations of the Honor Code will be dealt with through the University's Honor Council. Students should not seek external assistance with individual assignments/projects. If any clarification is needed, please consult with me.

6 Disability Accommodation:

- Accommodation for disabilities will be given only to students who have secured the proper documentation from UM's Office of Student Disabilities. Such documentation must be provided to the instructor within the first week of the start of class. Students should contact the Office of Disabilities to secure appropriate accommodation.
- Instead of extra time for quizzes, the students with disabilities will answer proportionately fewer questions.

7 Online discussions and announcements

Relevant course materials will be posted via ED (https://edstem.org/us/join/qDqqRw). Other relevant reading materials will be also uploaded prior to the class session. I encourage you to read the materials before joining the class.
Discussions in ED are highly encouraged. Please post your questions and concerns there so that your classmates can also assist you. ED is also a great platform to find team members or share new findings with your classmates. You can also share anonymous comments in ED with me if you have any other concerns. We will do our best to answer your questions and foster active participation, helping everyone engage in our class.

8 Textbook: William Stallings, Computer Security: Principles and Practice 3th Edition

After 02/17/2025, all the topics are from online resources and my past research.

9 Grades composition:

Exercises	Grade %	Comments
Assignments	50%	Starting from 4nd lecture and due in a week.
Quizzes	50%	15-minute quizzes, starting from 5th lecture
Project report	5% (optional)	Submit one report with your team members
Project Presentation	5%	**Top 3 in presentation will get 5% extra grade**

Course Schedule

Class	Date	Day	HW	Quiz	Topics
1	13-Jan	Monday			Introduction to this course, Importance of Cybersecurity. Case study
2	15-Jan	Wednesday			Overview. (**1.1, 1.2, 1.3**)
3	22-Jan	Wednesday			Symmetric encryption (**2.1**)
4	27-Jan	Monday	**HW1**		Authentication (**2.2**)
5	29-Jan	Wednesday		**Quiz 1**	Hash functions, Digital signatures (**2.3, 2.4**)
6	3-Feb	Monday			Access control, Role-based AC, Attribute AC (**4.1-4.7**)
7	5-Feb	Wednesday			Database, Cloud security (**5.1-5.11**)
8	10-Feb	Monday	**HW2**		Malicious mobile software (**Chapter 6**)
9	12-Feb	Wednesday		**Quiz 2**	DDoS attack (**Chapter 7**)
10	17-Feb	Monday			Single point of failure, Byzantine fault tolerance (BFT)
11	19-Feb	Wednesday			Blockchain 1
12	24-Feb	Monday	**HW3**		Blockchain 2
13	26-Feb	Wednesday		**Quiz 3**	Blockchain 3
14	3-Mar	Monday			Data Privacy overview
15	5-Mar	Wednesday			Differential Privacy **Presentation topic releasing**
16	17-Mar	Monday	**HW4**		Homomorphic Encryption
17	19-Mar	Wednesday		**Quiz 4**	Secure Multi-Party Computation
18	24-Mar	Monday			Zero-Knowledge Proof
19	26-Mar	Wednesday			Federated Learning and Privacy Preservation
20	31-Mar	Monday	**HW5**		Case Study: Secure gradient aggregation
21	2-Apr	Wednesday		**Quiz 5**	Case study: Cybersecurity for Medical Devices
22	7-Apr	Monday			Case study: Secure Data Sharing and Privacy Protection
23	9-Apr	Wednesday			Case study: Medical Data Privacy and Regulatory Compliance： Data anonymization
24	14-Apr	Monday			Case study: Blockchain-based IRB
25	16-Apr	Wednesday			Presentation
26	21-Apr	Monday			Presentation
27	23-Apr	Wednesday			Presentation
28	28-Apr	Monday			**Celebrating Your Security Journey!**

Notes:

1. Discuss your homework with your team members and the group leader needs to submit a final version of your homework to **Caden** (crh873@miami.edu) with your group name.
2. **The Quiz questions are from slides, you need to complete it individually in the class.**
3. Make a group with a maximum of 3 team members. Post group information: Book.xlsx
4. The final report is optional. If you're not satisfied with your quiz and homework scores, you can complete it for extra credit.
5. Slides will be posted before the class: https://anonymoususer08.github.io/csc116/

Grading Policy

Letter Grade	Numeric Grade Range
A+	>= 100

A	[90, 100)
A-	[85, 90)
B+	[82, 85)
B	[79, 82)
B-	[75, 79)
C+	[70, 75)
C	[65, 70)
C-	[60, 65)
D+	[55, 60)
D	[50, 55)
F	< 50