Computer Security

COMP 4290

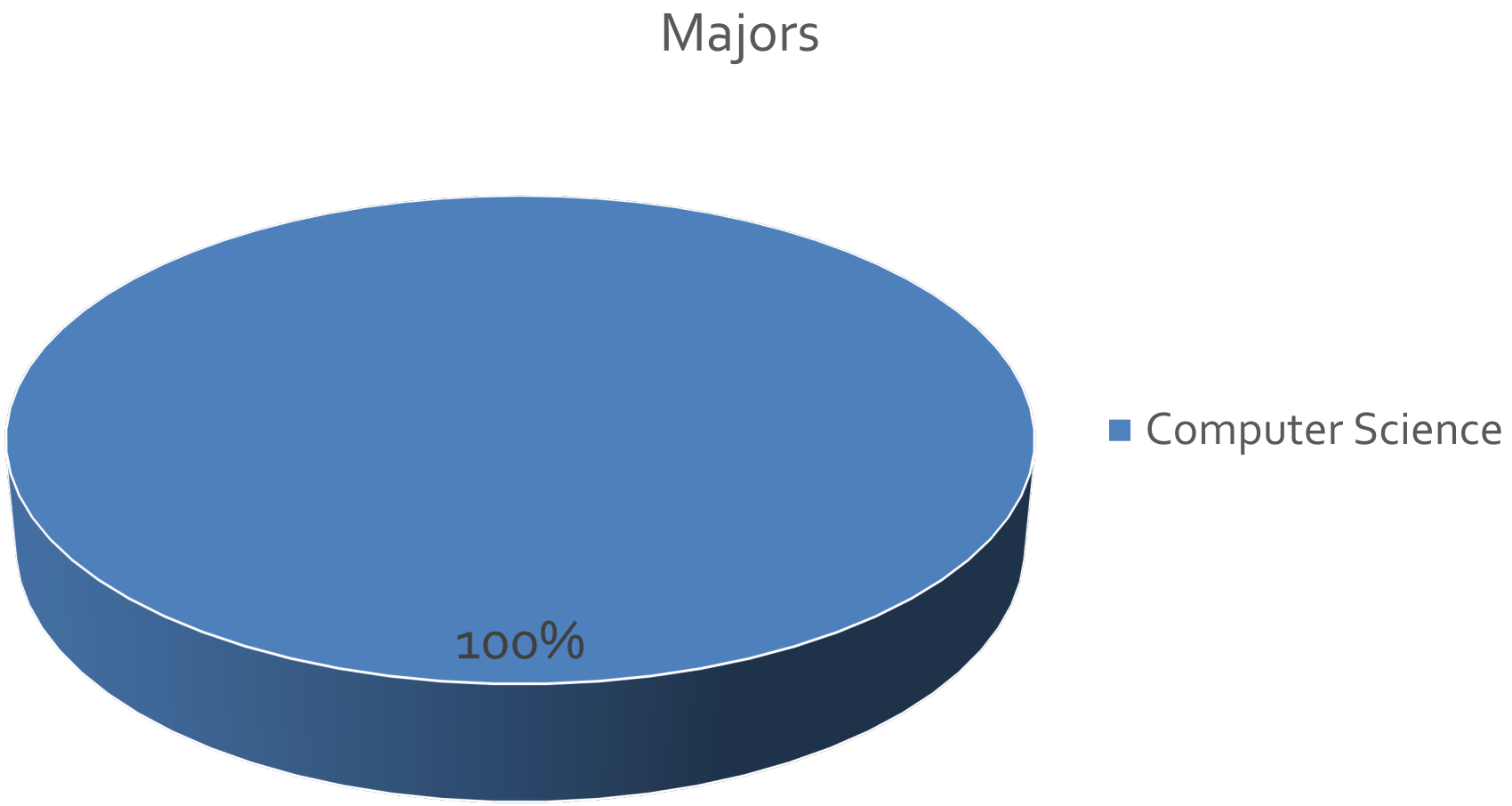
Who am I?

- Dr. Barry Wittman
- Not Dr. Barry Whitman
- Education:
  - PhD and MS in Computer Science, Purdue University
  - BS in Computer Science, Morehouse College
- Hobbies:
  - Reading, writing
  - Enjoying ethnic cuisine
  - DJing
  - Lockpicking
  - Stand-up comedy

How can you reach me?

- **E-mail:** wittman1@otterbein.edu
- **Office:** C123 (Art & Communication Building)
- **Phone:** (614) 823-2944
- **Office hours:** **MWF** 9:00 – 10:15 a.m.
  MF 1:45 – 4:00 p.m.
  W 1:45 – 3:30 p.m.
  R 10:00 – 11:15 a.m.
  TR 2:00 – 4:00 p.m.
  and by appointment
- **Website:**
  http://faculty.otterbein.edu/wittman1/

Who are you?



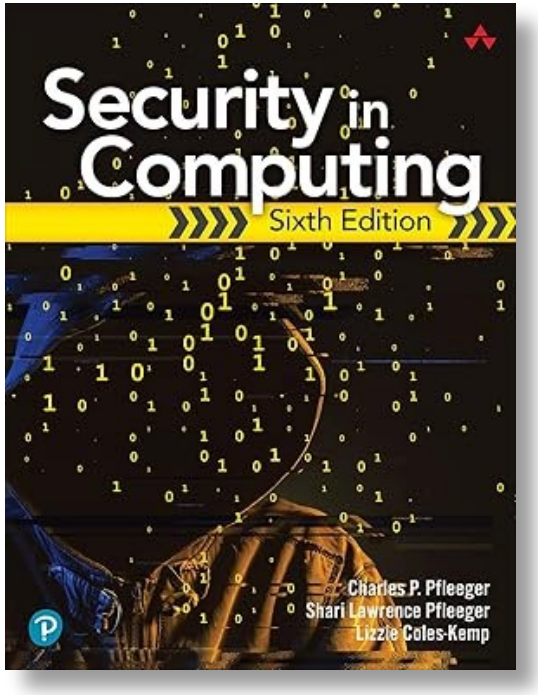
Why are we here?

- What's the purpose of this class?
- What do you want to get out of it?
- Do you want to be here?

Course Overview

Textbook

- Charles Pfleeger, Shari Pfleeger, and Lizzie Coles-Kemp
- ***Security in Computing***
- Sixth Edition, 2023, Addison-Wesley Professional
- ISBN-10: 0137891210
- ISBN-13: 978-0137891214



You have to read the book

- You are expected to read the material before class
- If you're not prepared, you may be asked to leave
  - You will forfeit the education you have paid around **$100 per class meeting** to get

This is a class about computer security

- It's more theory than practice
- This is not a class that will teach you how to hack a web server (at least not directly)
- Hacking systems depends on knowing about very specific vulnerabilities
  - Those vulnerabilities are constantly changing
  - Teaching the principles behind security is a much better investment

Cost

- Real security often boils down to cost:
  - How much does it cost to secure a system?
  - What is the value of the data or services to be secured?
  - Is it more cost effective to hire a computer security expert to break into a system or to bribe someone to give you their password?

Topics to be covered

- Security basics
- Authentication and access control
- Cryptography
  - Classical ciphers
  - Modern ciphers
  - Public key cryptography
  - Cryptographic hash functions
- Program security
- Web security
- OS security
- Network security
- Database security
- Privacy
- Risk management
- Legal and ethical issues

More information

For more information, visit the webpage:

`http://faculty.otterbein.edu/wittman1/comp4290`

- The webpage will contain:
  - The most current schedule
  - Notes available for download
  - Reminders about exams and homework
  - Detailed policies and guidelines

Projects

Three projects

- 30% of your grade will be three equally weighted projects
- Each will focus on a hands-on element of computer security
  - Cracking encryption
  - Using cryptography to communicate securely over a network
  - Designing a secure system
- You will work on each project in two-person teams

Teams

- All projects are done in teams of two
- You may pick your partners
  - But you have to have a different partner for each project!
  - Use Brightspace to form teams
- Projects must be uploaded to Brightspace: `https://otterbein.brightspace.com`

Turning in projects

- Projects must be uploaded to Brightspace **before** the deadline
- Late projects will not be accepted
  - Exception: Each person will have 3 grace days
  - You can use these grace days together or separately as extensions for your projects
  - You must inform me **before** the deadline that you are going to use grace days
  - If two people in a team don't have the same number of grace days, the number of days they will have available will be the **maximum** of those remaining for either teammate

Assignments

Five homework assignments

- 15% of your grade will be five equally weighted homework assignments
- Each will focus on a different set of topics from the course
- All homework is to be done individually
- I am available for assistance during office hours and through e-mail

Turning in homework

- Homework assignments must be uploaded to Brightspace **before** the deadline
- Late homework will not be accepted
- Each homework done in LaTeX will earn 1% extra credit toward the **final semester grade**
- Doing *every* homework in LaTeX will raise your final grade by 5% (one half of a letter grade)

Presentations

Presentations

- 5% of your grade will be based around two individual presentations given during the semester
- These presentations can be about anything related to computer security or privacy
- Choose topics you find interesting
- Part of your grade will be determined by your involvement in discussions of other students' presentations
- **Sign up on Friday for the date of your presentations**

Grading presentations

1. **Quality of content**

   Material is relevant to some aspect of computer security and is of interest to a classroom of computer science majors; content has not been covered in class and reflects current trends

2. **Factual accuracy**

   Material presented is free from major errors or inconsistencies

3. **Clear and concise communication of content**

   Talk has a defined beginning, middle, and end; a clear thesis statement emerges from the presentation; level of discussion is appropriate to the audience

4. **Polished presentation**

   Visually appealing presentation; use of images or animations when appropriate; spelling and grammatical mistakes are avoided

Tickets out the Door

Tickets out the door

- 5% of your grade will be tickets out the door
- These tickets will be based on material covered in the previous one or two lectures
- They will be graded leniently
- They are useful for these reasons:
  1. Informing me of your understanding
  2. Feedback to you about your understanding
  3. Easy points for you
  4. Attendance

Exams

Exams

- There will be two equally weighted in-class exams totaling 30% of your final grade
  - **Exam 1:** 09/22/2025
  - **Exam 2:** 11/03/2025
- The final exam will be worth 15% of your grade
  - **Final:** 12:30 – 2:30 p.m.
    12/10/2025

Course Schedule

Tentative schedule

Week	Starting	Topics	Chapters	Notes
1	08/18/25	Computer security overview	1 and 2	
2	08/25/25	Authentication and access control	2	
3	09/01/25	Cryptography basics	2 and 12	Labor Day
4	09/08/25	Public key cryptography	2 and 12	Project 1
5	09/15/25	Cryptographic hash functions	2 and 12	
6	09/22/25	Quantum cryptography	13	Exam 1
7	09/29/25	Program security	3	
8	10/06/25	Web security	4	
9	10/13/25	OS security	5	Project 2
10	10/20/25	Network security	6	
11	10/27/25	Database security	7 and 8	
12	11/03/25	Privacy	9	Exam 2
13	11/10/25	Management	10	Project 3 (Phase 1)
14	11/17/25	Legal and ethical issues	11 and 13	
15	11/24/25	Review	All	Thanksgiving
16	12/01/25	More review	All	Project 3 (Phase 2)

Project schedule

- **Project 1:** **10%** Tentatively due **09/12/2025**
- **Project 2:** **10%** Tentatively due **10/17/2025**
- **Project 3:** **10%**
  - **Phase 1:** Tentatively due **11/10/2025**
  - **Phase 2:** Tentatively due **12/03/2025**

Policies

Grading breakdown

- 30% • Three team projects
- 15% • Homework assignments
- 5% • Tickets out the door
- 5% • Individual presentations
- 30% • Two equally weighted midterm exams
- 15% • Final exam

Grading scale

A	93-100	B-	80-82	D+	67-69
A-	90-92	C+	77-79	D	60-66
B+	87-89	C	73-76	F	60-62
B	83-86	C-	70-72		

Attendance

- You are expected to attend class
- You are expected to have read the material we are going to cover **before** class
- Missed tickets out the door cannot be made up
- Exams must be made up **before** the scheduled time, for excused absences

R-E-S-P-E-C-T

- I hate having a slide like this
- I ask for respect for your classmates and for me
- You are smart enough to figure out what that means
- A few specific points:
  - Silence communication devices
  - Don't play with your phones
  - **Don't use computers in class unless specifically told to**
  - No food or drink in the lab

Computer usage

- We will be doing a lot of work on the computers together
- However, students are always tempted to surf the Internet, etc.
- Research shows that it is nearly impossible to do two things at the same time (e.g. watch TikTok and listen to a lecture)
- For your own good, I will enforce this by taking 1% of your final grade every time I catch you playing on your phones or using your computer for anything other than course exercises

Academic dishonesty

- Don't cheat
- **First offense:**
  - I will try to give you a zero for the assignment, then try to lower your final letter grade for the course by one full grade
- **Second offense:**
  - I will try to fail you for the course and try to kick you out of Otterbein
- Refer to the syllabus for the school's policy
- Ask me if you have questions or concerns
- **You are not allowed to look at another student's code, except for group members in group projects (and after the project is turned in)**
- **Don't use AI tools like ChatGPT to write *any* code you turn in**
- **I will use tools that automatically test code for similarity**

Disability Services

The University has a continuing commitment to disability inclusion (e.g., learning disabilities, mental health diagnoses, and chronic or temporary medical conditions). Disability Services (DS) helps to facilitate reasonable accommodations, provides referrals to students interested in exploring a potential diagnosis, and assists students and faculty to minimize barriers for an accessible educational experience. If you need accommodations or guidance, please contact DS at DisabilityServices@otterbein.edu as soon as possible or visit www.otterbein.edu/ods for more information. While we strive to meet your needs within the parameters of our course requirements and learning objectives, accommodations are not typically retroactive and late requests may not be guaranteed. Please let us know how we can best support you. Your instructor is happy to discuss this privately with you as well.

What does security mean?

Computer systems

Computer systems

- We will be specifically discussing the security of **computer systems**
  - Hardware
  - Software
  - Data
- Attacks can focus on the theft, alteration, or disruption of any one of the three
- The **Principle of Easiest Penetration** states that an attacker can try anything and will gravitate toward the easiest option

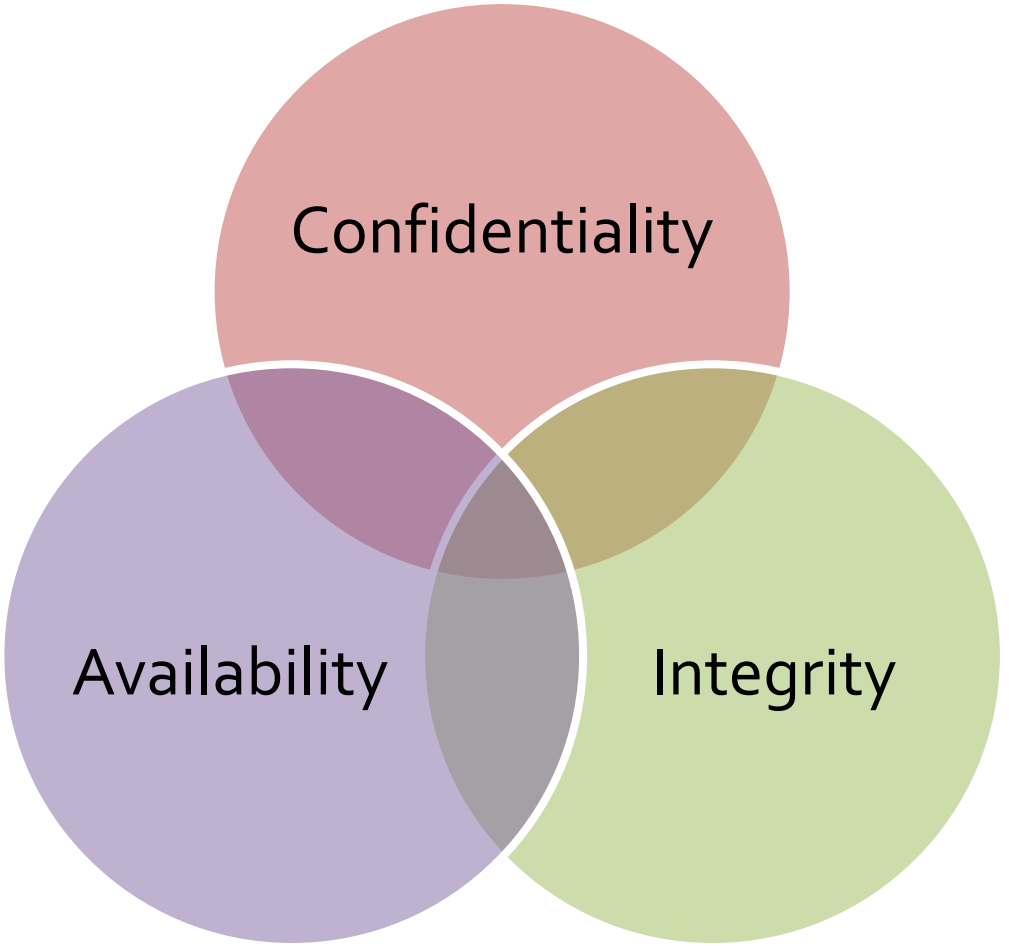
Terminology

- A **vulnerability** is a weakness in a security system
- A **threat** is a set of circumstances that can cause loss or harm
- Performing an **attack** is exploiting a vulnerability
- A **control** is a protection against an attack by reducing a vulnerability

"A **threat** is blocked by **control** of a **vulnerability**."

CIA

The basics of computer security:



Confidentiality

- You don't want other people to be able to read your stuff
  - Some of your stuff, anyway
- Cryptography, the art of encoding information so that it is only readable by those knowing a secret (key or password), is a principle tool used here
- Confidentiality is also called **secrecy** or **privacy**

Integrity

- You don't want people to mess up your stuff
- You want to know:
  - That your important data cannot be easily changed
  - That outside data you consider trustworthy cannot be easily changed either
- There are many different ways that data can be messed up, and every application has different priorities

Availability

- You want to be able to use your stuff
- Many attacks are based on **denial of service**, simply stopping a system from functioning correctly
- Availability can mean any of the following:
  - The service is present in usable form
  - There is enough capacity for authorized users
  - The service is making reasonable progress
  - The service completes in an acceptable period of time

Two other useful properties

- CIA covers a huge amount of ground, but there are other properties that are not directly under that umbrella:
  - **Authentication** is being able to confirm the identity of a sender
  - **Nonrepudiation** is the flip side: being unable to deny that you sent something

Threats

- There are many ways to classify threats
- **Nonhuman threats:** natural disasters, hardware failures, etc.
- **Human threats:** spilling a soft drink, entering the wrong data by mistake, intentionally hacking a system
- **Malicious** vs. **non-malicious**
- **Random** vs. **directed**

Harm

Malicious, human-caused threats often involve one or more of the following kind of harm:

Interception	• Someone read something they weren't supposed to
Interruption	• Something became unavailable or unusable
Modification	• Someone changed something they weren't supposed to
Fabrication	• Someone created fake things

Advanced persistent threat

- An **advanced persistent threat** is one that is organized, well-funded, and calculated to do maximum damage
- These threats are getting more media coverage today as possibilities for terrorism or cyber warfare
- Attacks on these threats come from governments, terrorist groups, and organized crime

Vulnerabilities

Hardware vulnerabilities

- Adding or removing devices
- Intercepting the traffic to devices or flooding them with too much traffic
- Physical attacks such as water, fire, electricity, food particles, mice chewing through cables, dust, and blunt force trauma
- These vulnerabilities can be exploited intentionally or unintentionally

Software vulnerabilities

- Software deletion
  - Accidental or otherwise
- Software modification
  - Accidental software changes due to hardware errors or software bugs
  - Trojan horses
  - Viruses
  - Trapdoors
  - Information leaks
- Software theft

Data vulnerabilities

- Data confidentiality
  - Wire tapping
  - Van Eck phreaking
  - Shoulder surfing
  - Looking through trash
- Data integrity
  - Intercepting data and passing it along with parts changed

Goals

- Mechanisms are intended to accomplish one or more goals:
  - Prevent an attack
  - Detect an attack
  - Recover from an attack

Other issues

- Networks can multiply the problems of computer security by making data easy to intercept and change
- Physical access to computer systems can allow people to use hardware and software for unauthorized benign or malignant purposes
- People are problematic
  - Someone has to design security systems, and they can't always be trusted
  - Sometimes people are needed but unavailable
  - People leave (or are fired) with valuable information
  - People behave unpredictably
  - People can be bribed

Upcoming

Next time…

- Attackers
- Harm
- Risk
- Method-opportunity-motive
- Controls

Reminders

- Read Chapter 1
- Form your teams for Project 1
- Decide when you want to give your presentations on security
  - Sign up on Friday!