Syllabus

Handout 1
CSCI 331: Fall 2023

Introduction to Computer Security

Instructor	Prof. Daniel Barowy
Office	TPL 306
Email	dbarowy@cs.williams.edu
Lectures	Mon & Thu 2:35–3:50pm in Schow Science Library 30B
Web Page	`https://williams-cs.github.io/cs331-f23-www/`

Texts

Required readings are in the course packet.

The following books are optional, but recommended, readings on the C programming language. They are on reserve in the Schow Science Library. I personally prefer the book by Oualline.

- *The C Programming Language* , 2nd Edition, by Brian Kernighan and Dennis Ritchie (ISBN: 0131103628).
- *Practical C Programming: Why Does 2+2 = 5986?*, 3rd Edition, by Steve Oualline (ISBN: 1565923065).

Prerequisites

You should have taken and be comfortable with the material in the following two courses. We will be making extensive use of data structures and low-level computer architecture in this course.

- CSCI 136: Data Structures and Advanced Programming
- CSCI 237: Computer Organization

C Proficiency. All of the assignments in this course should be written in C or ARM assembly. C programs should be accompanied by a `Makefile`. You do not need to be an expert in C, but you should be comfortable writing simple programs, and you should know what a pointer is. Although you should have a basic understanding of computer architecture (e.g., registers, memory, instructions, etc.), you do not need to be familiar with ARM in particular.

Course Objectives

Knowledge of security is increasingly critical to be able to function as a competent software engineer. This course is intended to give you the skills needed to avoid common security pitfalls. We will explore common vulnerabilities in computer systems, how attackers exploit them, and how systems engineers design defenses to mitigate them.

Outcomes. By the end of the semester, you should be able to 1. understand the low-level operation of running programs, 2. recognize potential vulnerabilities in your own software, 3. practice defensive design, and 4. know how to keep your knowledge up-to-date in the computer security "arms race."

Computer Resources

Standard environment. All programming assignments in this course should be completed on the supplied Raspberry Pi computers, which will be distributed during our first lab meeting. Since these machines are "headless," meaning that they do not have displays or keyboards, you will connect to them using a serial console adapter. You can connect this adapter to your personal computer, or any of the CS department's Linux lab computers. Although it is possible to complete assignments on a non-lab computer, please keep in mind that all assignments will be graded in the standard environment. Therefore, it is essential that you ensure that your solutions function correctly in the standard environment before submitting your work.

Lab resources. You are encouraged but not required to use the Linux lab computers in TCL 312 or TBL 301. You will be given door codes to access these labs once the semester begins. This option is especially helpful if you do not have a personal computer or if your computer is unreliable. Remember that we do not have the resources to support your personal computer.

Course Activities

Workload. The work that you should expect to engage with, beyond the scheduled lectures, will involve

- reading assigned readings: one to two hours, on average, per week;
- completing the programming assignments: 10-20 hours, on average, every two weeks; and
- working on your final project: time may vary considerably, depending on what topic you choose.

Some students program quickly but read slowly, and some do the opposite. Think about your learning style and plan accordingly. You should expect to spend *at least 10 hours per week beyond the scheduled lecture* on this course. The schedule on the course website includes estimates of weekly time required based on feedback from students in prior semesters. If you find yourself spending substantially more time than that on a regular basis, *please talk to me*.

Weekly reading and discussion. One of the most important skills had by every good security practitioner is the ability to keep up with the latest security literature. We will develop this skill through weekly readings and class discussion. Every week, your written responses will be discussed in class. You should consider this to be one of the most important aspects of this course.

Programming assignments. Every other week you will hand in your solution to an assigned programming problem. All programs will be graded on the basis of design, documentation, style, correctness, and efficiency. As stated before, they will be evaluated using the standard computing environment for the course (Raspberry Pi). Programs should be turned in electronically by 10:00pm on the due date, typically Sunday evening by 10:00pm.

Midterm Exam. The midterm will be scheduled during your a class period sometime in October. Stay tuned for the precise date.

Final Project. Instead of a final exam, there will be a final project of your choosing, and you may work with a partner if you wish. There will be several project checkpoints and a final presentation.

Github

All assignments in this course will be submitted using Gitea. When an assignment is posted, a git repository will be created for you. Repository names generally conform to the following pattern: `https://aslan.barowy.net/[your-login-id]/cs331_lab<n>`. You will be notified by email when your git repository is created.

Late Work

You are expected to turn in all assignments in a timely manner to receive full credit. Nevertheless, I understand that sometimes events conspire to make on-time homework assignment a challenge. Each student may use a maximum of **three free late days** during the course of the semester. A late day permits you to hand in a lab up to 24 hours late, without penalty, no questions asked. **You may use at most one late day on a given assignment.**

To take a late day, be sure to fill out the late day form (`https://forms.gle/Q82Vnus4t4okEQQ38`). Without prior arrangement, late assignments will be penalized at a rate of **20% per day**.

Resubmissions

You may find that occasionally, you do not do as well on an assignment as you had hoped. That's OK! Revisiting a mistake is one of the best ways to learn. To encourage you to engage in this practice, you are permitted to resubmit two assignments during the semester. This policy includes labs 1–9 and the midterm exam, but not the final lab or the final project.

A resubmission allows you to earn back **up to 50% of the missing points**. For example, if you received a 75% on an assignment, you may earn up to 87.5% upon resubmission.

Resubmissions must be submitted in the following manner:

1. They must be submitted before the end of the final exam reading period.
2. They must include both the original work and the new submission.
3. They must be accompanied with a typed document, written in plain language, that explains, for every correction:
   (a) what the error was in the original work,
   (b) how you fixed the error, and
   (c) why the new version is correct.

Please note that resubmissions must be typed or they will not be accepted. Detailed instructions for submitting a resubmission will be distributed via a separate handout.

Grading

Your final grade will be determined according to the following formula:

Midterm:	25%
Final Project:	25%
Lab assignments:	35%
Class participation:	15%

$$\text{final grade} = \text{midterm exam} \times 0.25 + \text{final project} \times 0.25 + \text{lab mean} \times 0.35 + \text{participation} \times 0.15$$

If you are spending lots of mental energy worrying about grades, please see me and we can discuss your worries in private. I try to give you a great deal of control over your final grade, and while I can't promise you an A, any student who earnestly applies themselves to the challenges in this course and learns from their mistakes has little to worry about.

Lab letter grades are converted as follows:

A	95%
B	85%
C	75%
D	65%
F	0%

Numeric scores are converted as follows:

$\geq 93\%$	A
$\geq 90\%$ and $< 93\%$	A-
$\geq 87\%$ and $< 90\%$	B+
$\geq 83\%$ and $< 87\%$	B
$\geq 80\%$ and $< 83\%$	B-
$\geq 77\%$ and $< 80\%$	C+
$\geq 73\%$ and $< 77\%$	C
$\geq 70\%$ and $< 73\%$	C-
$\geq 67\%$ and $< 70\%$	D+
$\geq 63\%$ and $< 67\%$	D
$\geq 60\%$ and $< 63\%$	D-
$< 60\%$	F

Illness

As much as we would all like to put COVID-19 behind us, sadly, it is still a serious concern. I consider **your health to be your top priority**. Falling ill is not your fault, and your grade should not suffer as a result. If you become ill, whether it is COVID-19 or not, I ask that you inform me as soon as possible and **please refrain from attending class**. Consider your semester “on hold” with no negative consequences until you recover. We will negotiate adjusted due dates once you are feeling better.

On the prevention side of things, you are welcome to wear a mask as your comfort level dictates. Whether you wear a mask or not, please respect the choices made by your peers.

Help!!!

There are many resources available when you need them. You are encouraged to discuss any questions, concerns, difficulties, or thoughts about the course with me. In addition, TAs are available to help you with challenges you face as you work through the course material and lab assignments. You are welcome at any time to approach me to ask for clarification on assignments or to discuss your problem-solving process. Don’t wait until you are stuck and frustrated to speak with one of us!

If you find yourself facing challenges beyond the typical, please do not stay silent. Talk to your instructor, a friendly face from the Dean’s Office, or one of the many professionals across campus who stand ready to help. All faculty and staff at Williams are bound by the Family Educational Rights and Privacy Act (FERPA) to maintain the privacy of your educational records. We understand that difficulties arise, and we are prepared to help you.

You will never be penalized for seeking help!