Syllabus

Handout 1
CSCI 331: Fall 2021

Introduction to Computer Security

Instructor	Prof. Daniel Barowy
Office	TCL 307
Email	dbarowy@cs.williams.edu

Lectures	Mon & Thu 2:35–3:50pm in Schow Science Library 30A
Web Page	`https://williams-cs.github.io/cs331-f21-www/`

Texts

Required readings will be drawn from the following sources:

- *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, by Clifford Stoll (ISBN: 1416507787).
- Course readings posted on the course website.

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;
- writing weekly reading responses: one hour, 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 writing. 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 response papers. 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.

Most written paper responses will be in the form of *technical paper reviews*. All responses must be at least 500 words in length. You *must* use the LaTeX markup language to prepare your response, and your submission should include both your `.tex` file and a `.pdf` file. A LaTeX template will be provided to make this easier. Written work should be turned in electronically by 11:59pm on the due date, every Wednesday evening by 11:59pm.

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 11:59pm on the due date, typically Sunday evening by 11:59pm.

Midterm Exam. The midterm will be scheduled during your class period on **Monday, October 18**.

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 four project checkpoints, including a final presentation.

Github

All assignments in this course will be submitted using Github. When an assignment is posted, a Github repository will be created for you. Repository names generally conform to the following pattern: `https://github.com/williams-cs/cs331_lab<n>_<your github username>`. You will be notified by email when your Github repository is created.

Late days

You may use a maximum of **three** *late days* during the course of the semester. A late day permits you to hand in any assignment (except the final project presentation) up to 24 hours late, without penalty. You must notify me that you intend to use a late day prior to the due date. Late days are provided to help you deal with unforeseen circumstances and to allow some balancing of occasional uneven work demands due to other courses. They should be used judiciously; if you find yourself struggling with the workload of this course, I encourage you to reach out to me.

You may use **all** of your late days for any one assignment. Once late days are exhausted, late work will not be accepted. Using a late day requires that you

1. commit a `late.txt` file to your repository before the regular deadline that
   (a) contains the number of late days you plan to take, and
   (b) the date of the expected final submission; and
2. email me before the regular deadline to inform me when I can expect your complete work;

Any late assignment that does not follow this procedure will be graded using the last commit before the deadline.

Resubmissions

Every student occasionally struggles with course material. Occasionally, students even "bomb" an assignment. Good courses push your boundaries, and so this might very well happen to you. Such an outcome can only be considered a failing if you do not learn from the experience. To incentivize you to reflect on and correct inadequacies, you may resubmit **up to two** assignments during the semester. This policy includes all of the labs, and the midterm, but **none of the final project checkpoints**.

A resubmission will be accepted at the discretion of the course instructor and 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 within three weeks of the graded feedback.
2. They must include both the original work and the new submission.
3. They must be accompanied with a PDF text document, written in plain English, that explains
   (a) what the mistake was in the original work,
   (b) how you fixed the mistake, and
   (c) why the new version is correct.

Grades

Grades will be determined as follows:

Final project:	20%
Midterm exam:	20%
Programs/Labs:	30%
Writing assignments:	20%
Attendance and class discussion:	10%

Help!!!

There are many resources available to help you in this course. You are encouraged to discuss any questions, concerns, difficulties, or thoughts about the course with me. In addition, I am 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 of the assignments, and to discuss your problem-solving process. You do not need to wait until you are stuck and frustrated to speak with me!

If you find yourself facing challenges beyond the typical, please do not suffer silently. Talk to me, 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 your privacy in educational matters. We understand that difficulties sometimes arise. If you stay silent about your problems we definitely cannot help you!

Contrary to popular belief, the most successful students are not "effortlessly successful." Instead, they get to know course staff early on and they familiarize themselves with an institution's academic support resources. Williams has ample support resources, including

- Accessible Education and Disability Support Center: Students with documented disabilities may request accommodation. If you fall into that category, please take advantage of the options available.

  `https://academic-resources.williams.edu/disabilities/`

- The Health Center: Sometimes your challenges are not course-related. The Health Center provides a range of medical, psychological, and health/wellness services. `https://health.williams.edu`

COVID-19

In order to keep our classroom environment as healthy as possible, you will be required to wear a mask at all times while in the classroom. If you feel ill, please do not come to class. There will be absolutely no penalty for missing a class due to illness or even suspicion of illness.

Please let me know if you are unable to attend class due to COVID restrictions. I will work with you to develop a plan that allows you to continue making progress in the course during your time in isolation/quarantine.

Inclusion

The Williams community embraces diversity of age, background, beliefs, ethnicity, gender, gender identity, gender expression, national origin, religious affiliation, sexual orientation, and other visible and non-visible categories. I welcome all students in this course and expect that all students contribute to a respectful, welcoming and inclusive environment. If you have any concerns about the classroom climate, please come to me to share your concern.