Introduction to Computer Security

RICE UNIVERSITY

"Security engineering is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves." – Ross J. Anderson in Security Engineering.

Instructor

Instructor:	Nathan Dautenhahn
Office:	Duncan Hall 3028
Office Hours:	Wednesdays 11a-12a OR by Appt OR Chat
Phone:	713-348-4781
Email:	ndd@rice.edu

Course Information

Website:	`https://nathandautenhahn.com/comp427`
Communications:	`https://campuswire.com` (invite will be direct)
Lecture Time:	T/R 10:50a - 12:05p
Lecture Location	Duncan Hall 1076
Credits:	3
Prequisites:	Comp310 and Comp321, or consent of the instructor.
Education Requirement:	This course may serve as an elective.
Syllabus Flexibility:	This syllabus may change throughout the semester, notably topics and lecture sequences.
Survey:	Background Survey: ungraded, **but won't be added to campuswire without**.

Overview and Purpose

This elective course covers a wide variety of topics in computer security, including hands-on experience with breaking software and engineering software to be harder to break. For example, students will perform buffer overflow attacks and exploit web application vulnerabilities, while also learning how to defend against them. Grades will be based on homework, projects, and a final exam.

Themes, Objectives, and Learning Outcomes

The primary objective of this course is to learn to think like an attacker and to apply general principles of secure system design as well as common attack patterns to diverse systems. The goal is not to learn a few hacks but rather learn methods that can be applied to analyze, attack, and secure any system. Specifically, you will have the opportunity to learn how to:

- Distinguish between security and reliability
- Describe a threat model and analyze real systems, putting security in context
- Describe and apply security design principles
- Use common exploitation techniques to compromise (example) real software artifacts
- Understand, describe, and be able to examine process anatomy
- Understand basic motivation for cryptography and choose appropriate solutions
- Understand, attack, and protect unsafe software, web browsers, networks, and operating systems
- Characterize classes of attacks and access control models

At the end of the course you should expect a keen awareness of the security implications of the software you build, as well as general knowledge of basic tools, attack methods, and defense techniques.

Required Texts and Materials

No textbook is required, but if you would like additional references, we recommend:

- The Craft of System Security by Smith and Marchesini
- Hacking: The Art of Exploitation by Jon Erickson
- Security Engineering by Ross Anderson
- Cryptography Engineering by Ferguson, Schneier, and Kohno
- Introduction to Computer Security by Matt Bishop
- Computer Security: Principles and Practice by William Stallings
- Computer Security: Art and Science by Matt Bishop
- Security in Computing by Charles P. Pfleeger
- Introduction to Computer Security by Michael Goodrich and Roberto Tamassia

Our favorites are Smith, Erickson, Anderson, and Bishop. We will rely heavily on online postings to track and evaluate reading and participation. You must participate and will be held responsible for all communications made through the platform. The online communication platform is TBD. In addition, each lecture will reference related materials including original scientific results and documentation for the various tools we use throughout the course.

Course Sessions

You are responsible for knowing about all announcements made in lecture. We will discuss project expectations, suggestions for how to succeed, and grading guidelines in class, and general class policy issues, so make sure you don't miss any lectures. Each session will include a presentation on the particular topic, which may or may not include any lecture slides. We will perform hacking while in class, which will be invaluable for you to observe and participate in. There will be a few guest lectures and a few videos to be watched outside of class and discussed on communications platform.

Coursework

The coursework will consist of graded homeworks, machine problems, and a final exam. There will be one homework and machine problem for each of the following topics: 1) exploiting memory unsafe

applications, 2) exploiting web applications, 3) exploiting cryptographic applications, 4) penetration testing, and 5) performing a computer crime forensics investigation.

Exams and Papers

There will be a final exam but no midterm.

Grading

There are three things in Comp427 that will contribute to your final grade: homeworks, projects, and a final exam. (There will be no midterm exam.)

There will be five homeworks during the semester that will count for 30% of your course grade. Unless otherwise noted, you are free to discuss the problems and your general approach with other students in the class. However, the answers you turn in must be your own original work, and you are bound by the Honor Code. Please start early and attend your lab section for important instructions and extra help.

There will be five projects during the semester that will count for 40% of your course grade. Unless otherwise indicated, you must work in a team of two. (Teams of three will not be accepted. If you want to work solo, we strongly discourage you, but we'll allow it if necessary.) You may consult general reference material, but you may not collaborate outside your team . The material you turn in must be entirely your team's work, and you are bound by the Honor Code (see also "honor code issues", below). Please start early and attend office hours, as necessary, for assistance.

The final exam will cover the remaining 30% of your grade for the class.

Grades will be posted to Canvas as soon as they're available. If you see a problem with your grade, here's the process for resolving it.

If there's a minor issue that requires correction (e.g., the grader failed to notice a second page of your submission, or clearly gave you somebody else's grade), then you may contact your grader. If you disagree with your grader's interpretation of your work in any substantive way, then you may dispute your grade to Prof. Dautenhahn. The window for protesting a grade is precisely seven days from when you receive that grade. Your protest must be sent as an email to Prof. Dautenhahn include all necessary materials for him to resolve your grade. If inadequate information is present in the email to convince Prof. Dautenhahn, then your protest will be declined. The email subject line must start with "Comp427 grade dispute, " followed by the homework or project number (e.g., "Comp427 grade dispute, project 3"). Any disputes sent to the graders will be ignored. Any disputes without the required subject line might be missed or forgotten. Based on your final weighted average, we will assign letter grades as follows:

[80,83) is a B-, [83,87) is a B, [87,90) is a B+, [90,93) is an A-, etc. We might curve up. We won't curve down.

Course Policies

Professional Etiquette

We expect all of your interactions to be positive and never derogatory to anyone. We anticipate personal differences, but as you interact with others on the discussion boards, and in-class, we expect common courtesy and never condone offensive behaviors.

Attendance and Online Interaction

You and your peers will benefit from your presence at discussions. Lectures anticipate heavy interaction from students both in class and through the online communications platform.

Partnering Policies

For your projects, you will work with a partner. We will allow you to pick anybody in the class to be your partner. You may wish to use the communications platform to help you if you cannot find somebody. We encourage you to find partners who work on a time schedule that's compatible with your own. We have no problem when one partner is an undergraduate and another is a masters student. In the event that we have an odd number of students, we're willing to have a single grouping of three students, where the last person unpartnered tells us as much as we'll help them join a group. You may not unilaterally declare yourself to operate in groups larger than two.

The "You Flake, You Fail" Policy: Mostly, when two students agree to work as partners, everything works great. Occasionally, partners become unresponsive. Emails aren't returned. Schedules are slipped. Promised work isn't delivered. If your partner is flaking on you, please let us know ASAP. We'll email them and try to resolve the situation. If we conclude that they're not behaving responsibly, we will give them an immediate F in the course. We may also, on occasion, offer a non-equal assignment of points, where the "non-flaking" partner earns a higher score and the "flaking" partner earns a lower score, commensurate with their respective efforts.

Late Policy

Due to the tight scheduling of this class, there is truly no room for slack. Late work is simply not accepted. Period. In some cases, we will ask you to submit materials to Canvas. In other cases, we will ask you to submit materials through GitHub. Email attachments, zip files, and so forth are not accepted.

If you see a looming time conflict, such as a job interview or other off-campus activity, and you tell us in advance, we'll do our best to accommodate you. We will deny all extension requests made after the submission deadline.

Note that the Rice General Announcements state: "No student should be given an extension of time or opportunity to improve a grade that is not available to all members of the class, except for verified illness or justified absence from campus." They don't give a hard a fast definition of a "verified illness or justified absence", but we interpret this to mean that you provide a written note from a doctor, nurse, or other medical provider.

Ethics, Law, and University Policies Warning

To defend a system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in Comp427 is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what the law prohibits — you don't want to end up like this guy. If in doubt, we can refer you to an attorney.

Please review the university's policy on Responsible Use of Information Resources for guidelines concerning proper use of information technology at Rice. As members of the university, you are required to abide by these policies.

Rice Honor Code

In this course, all students will be held to the standards of the Rice Honor Code, a code that you pledged to honor when you matriculated at this institution. If you are unfamiliar with the details of this code and how it is administered, you should consult the Honor System Handbook at `http://honor.rice.edu/honor-system-handbook/`. This handbook outlines the University's expectations for the integrity of your academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process.

Disability Resource Center

If you have a documented disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with the Disability Resource Center (Allen Center, Room 111 / `adarice@rice.edu` / x5841) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs.

Syllabus Change Policy

This syllabus is only a guide for the course and is subject to change with advanced notice.