CS 182: Introduction to Computer Security, Spring 2014
Course Syllabus

Course Description

Instructor:	Steve Matsumoto
Email:	`smatsumoto@cmu.edu`
Meeting times:	MWF 10-11 AM
Location:	TBD
Units:	9 (CMU units)
TAs:	TBD

Course Overview

This course is an introduction to topics in computer security for undergraduate students in their third or fourth year. Through an in-depth look at three main areas of security (cryptography, system/software security, and network security), this course seeks to develop students' security mindsets. By taking part in a variety of analytical and hands-on activities, we will also discover the interaction of security with other disciplines and in turn reflect on how we should communicate with others about security topics.

Course Objectives

There are three primary objectives which run as common threads throughout the course:

1. **Development of a security mindset.**

> Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.
>
> I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to." (Bruce Schneier)

The craft of computer security is built upon the *security mindset*, a way of observing and questioning systems in the world around us. This mindset is an acquired skill honed through practice and vigilance. When security experts see a new system, they think about how it can be made to fail and what mistakes or faulty assumptions lead to these vulnerabilities.

This course is designed to help you sharpen your security mindset. You will learn how to reason about the security of computer systems in a variety of applications. You will also practice the skill of questioning and testing the security of systems through lab assignments and reflect on the assumptions that you and your classmates make about the way these systems work.

Students with a good security mindset should be able to:

- Identify the assumptions underlying a system.

- Determine the extent to which these assumptions reflect reality.
- Determine any mistakes that have been made in implementing the system.
- Propose an attack based on any mistakes or faulty assumptions that were made.

2. **Understanding the ethics of security.** Ethics plays a critical role in security. Knowing when and how to disclose vulnerabilities and exploits is of the utmost importance, particularly when attacks can leak sensitive personal information or cause millions of dollars in damage. Therefore, in this course we will frequently discuss the ethical aspects of security topics. Assignment writeups will require you to consider what information to disclose, and readings may examine the ethics of security practices that are common in the field.

   Students who understand the role of ethics in security should be able to:

   - Provide examples of white-hat, gray-hat, and black-hat activities.
   - Write a vulnerability report with an appropriate scope and audience.
   - Follow ethical practices when testing the security of a system.

3. **Engaging with security in its societal context.** Areas of security such as cryptography have rich theoretical underpinnings, but it is important to remember that security takes place in the real world. The best cryptography in the world cannot protect data from a user who can be easily fooled or coerced into giving up his or her password. Therefore, we will discuss interactions of security with the social sciences, such as digital currency, Internet governance, and usability in security.

   Students who can engage with security in its social context should be able to:

   - Identify the real-world aspects that may cause even a secure system to fail.
   - Understand adversarial motivations and how they make sense in the context of the social sciences.
   - Analyze the tradeoffs between usability, convenience, and security in a system.
   - Discuss how security and public policy affect each other.

Course Format

The course meets three times per week. Each week consists of one lecture, one lab session, and one group activity. My goal with this format is to maintain a steady, predictable workload (about 7-8 hours outside of class) during the semester, allowing you to budget a set amount of time each week for this course rather than working in bursts. I ask that you budget some time each week (and ideally each day) to spend on this course and stick to it – if you do so, the work for this course should be quite manageable.

Please see the schedule at the end of this syllabus for a list of topics.

Course Text

I try to keep my course self-sufficient; therefore, there are no required textbooks. I may assign papers as required reading, but I will provide electronic copies of these papers.

I draw some of my material from the following texts, which you may find useful references:

- Charles P. Pfleeger and Shari Lawrence Pfleeger. “Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach.” ISBN 978-0132789462.
- Bruce Schneier. “Applied Cryptography.” Second Edition. ISBN 978-0471117094.

Prerequisites

Students are expected to have a basic knowledge of competency in discrete math and programming. In particular, you should be familiar with basic number theory, programming in C/C++, and be comfortable working in a UNIX command-line environment. Knowledge of computer systems and networking, such as x86 assembly language, compilation, and TCP/IP is helpful, but not required.

Grading

Over the semester you will have the opportunity to demonstrate your learning through five types of assessments: quizzes, problem sets, group discussions, labs, and a final project. Each component counts for 20% of your final course grade. There will be approximately 40 quizzes, 12 problem sets, 6 discussions, 6 syntheses, and 12 labs, as well as a final project.

I expect this course to take approximately 7-8 hours per week outside of class meetings. If you find that you are putting in significantly more or less time for this class, please contact me, and I will try to provide additional help or adjust the workload.

Quizzes

This course will have a short, five-minute quiz at the beginning of each class meeting. The purpose of these quizzes are threefold: to reinforce long-term retention of the material, to ensure that students are keeping up with the pace of the course, and to indicate to me which concepts need to be clarified or reiterated. Each quiz may cover material from any previous class meeting, though generally concepts taught in a class will be tested in the next class’s quiz and retested less frequently as the course progresses. Questions will be brief and straightforward (e.g., definitions, simple calculations, etc). Quizzes will be graded, scanned, and returned to you by email within 24 hours of class.

These quizzes are designed to assess your learning over the course of the semester, rather than assessing your learning through your performance in a single sitting as an exam would. Therefore, you should consider each quiz a daily opportunity to demonstrate your learning. My hope is that over the semester, the quiz material becomes common knowledge that we can use as the foundation of our class discussions.

There are no makeup quizzes, but the lowest two quiz scores will be dropped in calculating your final grade.

Problem Sets

The problem sets in this course facilitate deeper exploration of the material we discuss in class. Problems will be assigned each week and will cover both theoretical and practical elements of the course. Problems may ask you to do things such as:

- analyze a proposed solution to a security vulnerability

- prove the security of a cryptographic protocol
- calculate the complexity of an attack or defense
- discuss the ethical implications of a defense

Problem sets are due on Mondays at the beginning of class, and should take 2-3 hours to complete. They will not be assigned in the last weeks of the course. You are, however, expected to use this time to instead work on your final project.

Group Discussions

Over the semester we will frequently interact as a class or in small groups. The purpose of these interactions is to practice the art of communication in security-related topics and to examine the role of security in its societal contexts. To accomplish these goals, we will participate in several activities:

- **Engaging with security literature.** We will be reading a series of articles and papers in the field, which will serve as the basis for our group interactions. You are expected to analyze the readings, considering their main points and claims with a healthy dose of scientific skepticism. It is important that you consider the evidence at hand when analyzing the literature, since you will need to bring up such evidence (or lack thereof) when defending discussion points with your classmates. These readings will form the basis for the syntheses and discussions (described below). While you are not directly graded for completing the readings, doing so is essential for successfully completing the syntheses and discussions.
- **Literature syntheses.** At times you will be assigned to groups of 3 or 4 and given a series of readings. The group is responsible for dividing these readings amongst the members when they are assigned. Each member will then read his or her assigned reading and prepare a short, 1-page handout that summarizes the main points of the reading and provides a brief analysis of its arguments. On synthesis days, you should bring one copy of the handout for each member in your group, plus an additional copy for me.

  On the specified day, these groups will meet with one another and be given a brief, specific prompt. Each member will share their findings with the other members, using the handout as a reference. The group will then use the class time to synthesize their findings into a brief essay of about 500 words. Your handouts and group essays count for half of your grade in this component, or 10% of the total course grade.
- **Class discussions.** We will also discuss some topics as a whole class. You are expected to take part in these discussions, offering thoughtful perspectives and insightful questions. Your grade for these discussions will be based on the quality, not the quantity, of your contributions. Quality talking points should align with the course objectives and demonstrate that you have deeply thought about the discussion topics. Your participation in these discussions is also worth 10% of the total course grade.

Labs

To facilitate hands-on learning and to impart a deeper understanding of the concepts we discuss in class, you will complete a series of lab assignments throughout this course. Examples of lab activities include:

- Implementing a password cracker
- Gaining administrative access to a website using SQL injection
- Reading encrypted web traffic by forging an SSL certificate

These lab assignments can be completed individually or in pairs. I have allocated the class time on Wednesdays as a chance for you to get started on the lab with the help of the course staff. Each lab will have a pre-lab exercise to be completed before the in-class session. While these exercises are not graded, if you understand the concepts in the exercise, then the lab activity should not take more than two hours to complete. You will then complete a short writeup detailing your findings which should take no more than an hour.

Final Project

This course is designed to expose you to a breadth of topics in computer and information security. The final project is an opportunity for you to take a topic that particularly interests you and explore it in greater depth. I expect the project to strike a reasonable balance between theory and hands-on work, and scoped appropriately to the allotted time period.

Projects can be completed in teams of two to four students, and you are responsible for choosing your own teams. When the project period begins, you should come up with several ideas for your project. I will then meet with each team individually to help you refine and scope these ideas. You will then have several weeks to carry out your project and design some sort of exhibition for your results (e.g. a presentation, poster, or website). You will be graded on the quality of your analysis, your communication skills, and *the degree to which you demonstrate your security mindset and understanding of security in its ethical and societal contexts.*

Policies

Special Accommodations

If you have a physical or learning disability and would like to request a special accommodation in this course, please contact me as soon as possible. I will do my best to provide you with an effective learning environment. You can also coordinate this through the Office of Disability Resources, but in any case please come speak to me so that I am aware of any special needs you may have.

Classroom Behavior

Regarding aspects of classroom behavior and etiquette, I have one fundamental policy: I will do my best to provide a beneficial, enjoyable learning environment, and I ask that you in turn do your best to promote and enhance that environment for yourself and your classmates. That is, be mindful of the class, our time, and our attention, and please keep distractions to an absolute minimum.

In particular, I ask that you adhere to the following policies:

- **Attendance:** Please be on time for class. If you must arrive late or leave early, please let me know in advance and sit in a location that minimizes distraction, such as near the door.

- **Electronic devices:** I hand out course notes at the beginning of each lecture. Therefore, please do not use phones, tablets, or laptops during class. If this presents a serious problem to your learning during lectures, please come speak to me and we can make appropriate arrangements.
- **Cell phones:** Noises such as those made by cell phones can draw the attention of others and affect your classmates' learning. Therefore, please remember to silence your phones and other devices which may make noise.

  However, life goes on outside of the classroom. It is completely acceptable to step outside of the class to handle emergency situations that may arise during class time. If you know in advance that such a situation may happen during class (e.g., a loved one is in critical condition, getting an important job-related call, etc.), please inform me by email and sit near the door to keep distractions to a minimum.

Academic Integrity and Collaboration Policy

We highly encourage collaboration with your classmates in the form of discussion. You are free to discuss approaches to problems with your classmates, the graders, and instructor. However, copying solutions, whether code or prose, is strictly prohibited unless explicitly stated otherwise. In the event that a collaborative discussion involves writing of any kind, each person must complete their own write-up and all writing that took place during the discussion must be thrown away or erased prior to each person beginning their write-up.

If you are unsure of whether a specific type of collaboration is allowed, ask a grader or the instructor first. Please also look at the official university policy on academic integrity for further details. Penalties for academic dishonesty in this course may range from failure of the assignment to failure of the course, and any cases of academic dishonesty will be reported to the Dean of Student Affairs.

Security Techniques

In this course you will gain a deeper understanding of some security attacks by carrying them out firsthand against our test machines. This experience is intended to highlight the nuances of a security vulnerabilities so that you can avoid them in your future coding practices. While some of these techniques are sometimes in a legal gray area, they can be annoying or damaging if you apply them without being authorized to do so. Do not "test the security" of systems without obtaining prior permission from the owner, or you may be subject to criminal sanctions.

Late Homework

In general, late homework is not accepted. However, recognizing that life goes on outside the classroom and that urgent matters can come up unexpectedly, I will accept one problem set or lab, no questions asked, up to 24 hours late without any penalty. Labs completed in pairs may require both students to use their late days, but this will be handled on a case-by-case basis. Think of this provision as an emergency aid; you should have a very good reason for using it. Because of this, I cannot guarantee that I will accept any additional late assignments beyond the one you are given. However, if your request is reasonable then I will give it serious consideration.

Changes to this Syllabus

This syllabus is subject to change based on circumstances that may arise during the course. In the event that I make changes to the syllabus, I will inform you by email and post an updated version of the syllabus.

Tentative Schedule

	Date	Activity	Topic
			Foundations
W	1/22	Lecture	Syllabus, Security Mindset, Ethics
F	1/24	Lecture	Adversary Models, Definitions
			Cryptography
M	1/27	Lecture	Mathematical Foundations
W	1/29	Lab	Fast Modular Arithmetic
F	1/31	Discussion	“Hard” Problems in Number Theory
M	2/3	Lecture	Symmetric Key Cryptography
W	2/5	Lab	Decrypting Secret Messages
F	2/7	Synthesis	Encryption Models
M	2/10	Lecture	Public Key Cryptography
W	2/12	Lab	Forging Messages
F	2/14	Discussion	Real-World Implementations
M	2/17	Lecture	Hashes and MACs
W	2/19	Lab	Password Cracking
F	2/21	Synthesis	Hashing Vulnerabilities
			System and Software Security
M	2/24	Lecture	Assembly Language, Program Compilation
W	2/26	Lab	Reverse Engineering Tools
F	2/28	Discussion	Ethics of Reverse Engineering
M	3/3	Lecture	Program Analysis
W	3/5	Lab	Bug Hunting
F	3/7	Synthesis	Limitations of Analysis
M	3/10	Lecture	Buffer Overflow
W	3/12	Lab	Stack Smashing
F	3/14	Discussion	Stack Defenses
M	3/17	Lecture	Input Filtering
W	3/19	Lab	SQL Injection
F	3/21	Synthesis	Input Rectification
			Network Security
M	3/24	Lecture	Web Security
W	3/26	Lab	Cookie Attacks
F	3/28	Discussion	Vulnerability Disclosure
M	3/31	Lecture	SSL/TLS
W	4/2	Lab	Man-in-the-Middle Attacks
F	4/4	Synthesis	Public Key Infrastructures
M	4/7	Lecture	Routing Security
W	4/9	Lab	Traffic Hijacking
F	4/11	Discussion	Internet Governance
M	4/14	Lecture	TCP/IP Security
W	4/16	Lab	Denial of Service (DoS)
F	4/18	Synthesis	Computational Puzzles

The remainder of the semester will consist of special topics lectures and project exhibitions.