CS 88S: SAFETY IN THE CLOUD

INTRODUCTION TO CYBERSECURITY

UCLA's Beat 'SC Bonfire. Notice the sheer number of students recording the event and sharing with their friends in real time. In our current world, the internet has connected everyone, but this also introduces new problems regarding online safety.

Course Description

This course is an preliminary introduction to the field of cybersecurity. We will study a variety of topics that are important for a regular consumer of technology. This course has great relevance in our current society: cyber attacks and data leaks are becoming more mainstream. A shared belief in the journalism field is that "nothing is more important to democracy than an educated electorate"; the same can be said for education in cybersecurity. It is more important than ever for everyone to be *cybersecurity-aware.*

Frank Chen
frank.chen@ucla.edu

Location: Boelter 5419

Time: Tuesdays 11-11:50am

Faculty Mentor:
Peter Reiher

Office Hours: TBA

Course Website:
http://kfrankc.me/cs88s

Learning Objectives

Students will:

- Explore cybersecurity and its cultural influences
- Learn the vulnerabilities of their everyday online services
- Practice effective methods to protect themselves online
- Analyze how their online data is used to generate industry revenue
- Understand the role cybersecurity plays in our country
- Submit a final project/reflection about their thoughts on cybersecurity and internet safety after finishing the class

Google Authenticator, an app that provides two-factor authentication (2FA) to your online accounts. 2FA is one of the many topics we will cover in this class.

Course Requirements

This is a 1-unit P/NP seminar that meets 1 hour per week. Students are expected to attend each seminar, but given one absence; additional missed classes are a case-by-case basis. Small interactive assignments may be given some weeks that are designed to further understanding or provide additional insight. **Note:** No prior knowledge in computer science or programming is needed for this class! I encourage everyone interested in becoming cybersecurity-aware to take the course!

Course Expectations

Students are expected to actively participate in classroom discussions. In addition, students are encouraged to ask questions, as well as promote a positive, healthy atmosphere for discussion of ideas. Brief articles or videos will be given to students to familiarize themselves with each week's topic before and after each class. Students are not necessarily expected to fully understand the reading, but will be expected to get a general introduction.

Schedule

Week 1: Introduction & Motivations for the Class

We begin this course by exploring the impact cybersecurity has on our society, overviewing the topics we will cover throughout the quarter, and introducing the paradigms of cybersecurity: Confidentiality, Integrity, and Accessibility.

Week 2: Hacking in Popular Culture

In recent months, there have been some accurate portrayals of cybersecurity and hacking, but we'll revisit some of the more embarrassing examples, and discuss the issue of 'implicit bias' in cybersecurity.

Week 3: Phishing, Social Engineering, Various malwares

We start our study of various vulnerabilities in our online services at phishing, social engineering, and various malwares. We'll discuss why these attacks happen, their prevalence in our everyday lives, and how to watch out for them.

Week 4: Passwords, Authentication, & Password Managers

What does it mean to have a strong password? How long does it take to crack an easy password? How does password authentication work in a service? What are password managers? These are some of the questions we hope to answer this week.

Week 5: Web Browsing, Encryptions, VPNs

How can we tell if a website is safe to access? What is a Virtual Private Network (VPN), and how does it allow a user to have privacy when browsing on the Internet?

Week 6: Protecting Yourself: apps, methods, practices

We'll explore 2FA, encrypted emails, encrypted SMS, PGP, and various apps and services that you can use to protect your privacy online and strengthen your protection against attacks.

Week 7: Your data & how it's used to make money

Ever wonder how a website such as *Amazon.com* recommends items that you may like? We'll explore the ethical dilemmas that sometimes results from technology companies using your personal data for profit.

Week 8: Cybersecurity, Privacy, & US Government

Remember Apple vs. FBI a year ago? We'll explore what cybersecurity means in a government context, and how that sometimes clashes with the cybersecurity goals of the tech industry.

Week 9: Cybersecurity and Internet of Things (IoT)

From smart transportation to smart home assistance, we analyze how cybersecurity plays into various IoT devices via potential vulnerabilities, rules and regulations, as well as preventative measures

Week 10: Future Topics in Cybersecurity

Will we be using passwords for the rest of our lives? What other kinds of authentication systems are out there? How can we all contribute to a world more educated in cybersecurity?