COMP 116: Introduction to Computer Security

Tufts University Department of Computer Science, Fall 2019

NOTE: For the summer 2019 online course syllabus, go here

Instructor

- Ming Chow, mchow@cs.tufts.edu
- Office Hours: Wednesdays from 1 - 4 PM, or by appointment, "in my usual spot" (the collaboration area next to the CS Main Office in Halligan). Hours are good until the last day of classes, Thursday, December 5th.
- Please send all class questions (e.g., help labs) via Piazza. DO NOT E-MAIL ME ABOUT LABS AND ASSIGNMENTS! Sign up at https://piazza.com/tufts/fall2019/comp116.
- For emergencies or private matters, please e-mail or see me directly.

Class Time and Location

- Tuesdays and Thursdays, 4:30 - 5:45 PM in Nelson Auditorium

Prerequisites

- COMP 15. Strongly recommended that you have taken COMP 40. Please disregard prerequisites listed in the University's bulletin as they are incorrect!

Textbook

- No textbook. Don't make me laugh.

- Module 1: Networking and Attacking Networks
- Module 2: Cryptography
- Module 3: Web Security
- Module 4: Vulnerabilities, Static and Dynamic Analysis
- Module 5: Malware
- List of required readings for this class

Hardware and Software for This Class (on your personal computer)

Absolute Requirements

- A modern web browser (e.g., Firefox, Google Chrome, Chromium, Safari, Microsoft Edge)
- A command line interface to run Unix/Linux commands

Strongly Recommended Requirements

- A computer with at least 20 GB of hard disk space free and 4 GB of RAM
- Kali Linux and a Virtual Machine Hypervisor

Assessment

- Labs (55%)
- Final project (15%)
- 2 quizzes (25%)
- Subjective factors including readings, attendance, class participation, and posting to Piazza (5%)

Class participation encompasses a variety of activities, all with the same purpose. To earn high grades for class participation, you must show that you are actively engaged in managing your own learning, developing new skills, and developing new ways of programming and problem-solving. You can be engaged in a variety of ways:

- Asking appropriate questions in class

- Asking appropriate questions on Piazza
- Answering questions well on Piazza
- Going to cyber security events in the area
- Writing sane and sensible answers on quizzes
- Answering questions when called on in class
- Organizing study groups
- Interacting professionally with programming partners and course staff
- Working out ideas with teaching assistants

Nobody has to do all of these things; you can earn top grades for class participation by doing just a few things well. In particular, nobody is required to speak in class, but everybody should be prepared to answer questions if called upon.

Professional interactions with other students and with course staff are the same as those which are expected in any workplace. It is also professional for you to recognize that a member of the course staff may be present but not actually available to talk about COMP 116.

Syllabus

Schedule is subject to change. Given the nature of this subject, changes to schedule will happen.

All labs in this course are on Canvas, https://canvas.tufts.edu/.

My scripted class notes are available at https://github.com/tuftsdev/DefenseAgainstTheDarkArts/blob/gh-pages/class_outlines.md (added supplement to slide decks)

Date	Agenda	Deliverables
Tuesday, September 3th	• Course Introduction • READ FIRST: A Disaster Foretold --and Ignored (Washington Post) • READ SECOND: Reflections on Trusting Trust by Ken Thompson	• Lab 1 Assigned (available on Canvas), Due on Wednesday, September 11th at 11:59 PM: Working with the Command Line

	• READ THIRD: Every Computer Science Degree Should Require a Course in Cybersecurity (Harvard Business Review) • READ FOURTH: Programmers: Stop Calling Yourselves Engineers (The Atlantic) • Watch: Dr. Dan Geer's Black Hat 2014 Keynote. The text of his talk: http://geer.tinho.net/geer.blackhat.6viii14.txt • Watch: How to Prevent Security Afterthought Syndrome by Sarah Zatko (HOPE X, July 2014) • Watch: (continuing Sarah's work) The Cyber Security Education Gap - What Do We Do Now? (The Eleventh HOPE, July 2016) • Watch: Tacoma Narrows Bridge Collapse • Read: Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say (NYT) • Read: Cybersecurity: Time for a New Definition (Lawfare)	
Thursday, September 5th	• Networking • Video (YouTube): Basic Wireshark overview, PCAPs, reconstruction, extraction, filters • Video (YouTube): The OSI Model Demystified • Read: DEF CON: Why Conference Harassment Matters • Read: Sexual Harassment at DefCon (and Other Hacker Cons) by Bruce Schneier	

	• Read: DEF CON Conference Code of Conduct • Read: The Trinity of Trouble: Why the Problem is Growing (Freedom to Tinker) • Read: Tools and Techniques to Succeed at the Wall of Sheep (on wallofsheep.com) • Read: Network Protocols (Destroy All Software) | Discussion on Hacker News: https://news.ycombinator.com/item?id=14468471	
Tuesday, September 10th	• Basic Packet Analysis and Sniffing • Video (YouTube): Address Resolution Protocol (ARP) Explained • Video (Asciinema): Identifying usernames and passwords in PCAPs using Ettercap • Read: The Basics of Arpspoofing/Arppoisoning (Irongeek.com) • Read: ARP Spoofing (Veracode) • Read: Fun With Network Friends (2600 Magazine, Summer 2008) • Read: A Bettercap Tutorial (Daniel Miessler)	• Lab 2 Assigned (available on Canvas), Due on Wednesday, September 18th at 11:59 PM: Packet Sleuth
Thursday, September 12th		
Tuesday, September 17th	• Attacking Networks: Scanning, Part I • Read: We scanned the Internet for port 22 (Errata Security) • Read: Thousands of computers open to eavesdropping and hijacking (Sophos)	

Thursday, September 19th	• Attacking Networks: Scanning, Part II	• Lab 3 Assigned (available on Canvas), Due on Wednesday, September 25th at 11:59 PM: Scanning and Reconnaissance
~~Tuesday, September 24th~~		
Thursday, September 26th	• Attacking Networks: Distributed Denial of Service Attacks • Read: Deep Inside a DNS Amplification DDoS Attack (Cloudflare) • Read: Brian Krebs' Blog Hit by 665 Gbps DDoS Attack (SecurityWeek) • Read: How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet (Motherboard) • Read: Dramatic Increase of DDoS Attack Sizes Attributed to IoT Devices (BleepingComputer)	• Tufts Fall 2019 Career Fair, Friday, September 27th, Gantcher Center, 11:30 AM - 2:30 PM • Reverse Career Fair (directly after the Career Fair), Halligan 102, 2:45 - 4 PM. RSVP
Tuesday, October 1st	• Cryptography: The Basics • Read: You Wouldn't Base64 a Password - Cryptography Decoded (Paragon Initiative)	• Lab 4 Assigned (available on Canvas), Due on Wednesday, October 23rd at 11:59 PM: Snake Oil, The Incident Alarm • Fall 2019 Password Cracking Contest Officially Announced (Lab 5), closes on Friday, November 1st at 11:59 PM ABSOLUTE DEADLINE. The hashes: crackme-fall2019.txt. Submission on Canvas.

		• Practice Quiz 1
Thursday, October 3rd	• Cryptography, Part II: Hash Functions and Password Cracking • Read: GitHub Security Update: Reused password attack (GitHub) • Read: Analyzing the Patterns of Numbers in 10M Passwords (2015) • Read: Salted Password Hashing - Doing it Right • Read: Hacker, Hack Thyself: Always assume that Internet Bad Guys will somehow get a copy of your database. Then what? (Coding Horror)	
Tuesday, October 8th	• Cryptography, Part III: Asymmetric Algorithms, Diffie Hellman Key Exchange, Transport Layer Security (TLS) • Read: Enterprise Security - SSL/TLS Primer Part 1 - Data Encryption (Akamai) • Read: Enterprise Security - SSL/TLS Primer Part 2 - Public Key Certificates (Akamai) • Read: Illustrated: How HTTPS Works (sudhakar.online)	• Final Project Announced ◦ Abstract Due on Thursday, October 17th ◦ Outline Due on Thursday, November 7th ◦ Absolute Deadline for Paper and Supporting Material Due on Wednesday, December 11th at 11:59 PM
Thursday, October 10th	• Vulnerabilities • Read: A Brief History of Software, Security, and Software Security: Bits, Bytes, Bugs,	Quiz 1

	and the BSIMM (Gary McGraw's talk to my class in fall 2013) • Read: Introduction to CVE, CWE, and the Top 25 (Steve Christey Coley's guest talk to this class back in fall 2015) • Read: Why Everything is Hackable: Computer Security is Broken From Top to Bottom (The Economist) • Read: The Difference Between CWE and CVE (Daniel Miessler) • Read: Web Applications Under Attack: Tenable.io and the 2017 Verizon DBIR (Tenable) • Read: The Language of AppSec (Veracode) • Read: Application Security Tools: Good or Bad? (Freedom-To-Tinker) • Read: Badness-meters Are Good. Do You Own One? (Synopsys)	
Thursday, October 17th	NO CLASS	
Tuesday, October 22nd	• Web Security: HTTP Review, OWASP, Web Proxy, Training Grounds, Cross-Site Scripting • Watch: Cross-Site Scripting (XSS) Tutorial by Chris Eng (Veracode) • READ FIRST: How The Web Works --In One Easy Lesson (mkcohen.com) • READ SECOND: Veracode's State of Software Security 2016	

	• Read: How The Web Works --In One Easy Lesson (mkcohen.com) • Read: What happens when you type Google.com into your browser and press enter? (on GitHub) • Read: OWASP Top 10 • CWE/SANS TOP 25 Most Dangerous Software Errors • Read: AdiOS: Say Goodbye to Nosy iPhone Apps (Veracode) • Read: Mitmproxy: Your D.I.Y. Private Eye (Medium) • Read: Reverse-Engineering the Kayak App with mitmproxy (shubhro.com) • Read: Metasploitable 2 Exploitability Guide (Rapid7) • Read: Blind SQL Injection: What is it? (Acuenix) • Read: XKCD: Exploits of a Mom • Read: The History of SQL Injection, the Hack That Will Never Go Away (Vice) • Read: Anonymous Leaks Paris Climate Summit Officials' Private Data (Wired) • Read: Why Even Google Is Susceptible to the Most Basic Website Vulnerabilities (Veracode) • Read: Paypal 2FA Bypass (henryhoggard.co.uk) • Read: 10 Scariest Vulnerabilities (Veracode)	
Thursday, October 24th	We have our own homecoming	

Tuesday, October 29th	• Web Security, Part II: SQL Injection, Cross-Site Request Forgery, Directory Traversal, Command Execution, Local and Remote File Inclusion • Read: Cross-Site Request Forgery Guide: Learn All About CSRF Attacks and CSRF Protection (Veracode) • Read: Cross-Site Request Forgeries and You (Coding Horror) • Read: CSRF Attacks - What They Are and How to Defend Against Them (Acunetix) • Read: Cross-Site Request Forgery (OWASP) • Read: Cross-Site Request Forgeries: Exploitation and Prevention (Zeller, Felten)	• Lab 6 Assigned, Due on Halloween: The XSS Game • Lab 7 Assigned, Due on Halloween: Gain Access to Website
Thursday, October 31st		• Lab 8: The CTF Write Up (one per team)
Tuesday, November 5th	The Annual Capture The Flags (CTF) Game at 574 Boston Avenue, Room 401	• Lab 9 Assigned (available on Canvas), Due on Wednesday, November 13th: Technical Risk Analysis and Static Analysis
Thursday, November 7th	• Static and Dynamic Analysis • Read: Binary Static Analysis (Chris Wysopal's talk to this class back in spring 2012)	

	• Read: We See the Future and It's Not Pretty: Predicting the Future Using Vulnerability Data (Chris Wysopal's talk to this class back in fall 2013)	
Tuesday, November 12th	• Malware • Tutorial: Malware Unicorn's Reverse Engineering Malware 101 (GitHub) • Read: The Internet Worm Program: An Analysis (http://spaf.cerias.purdue.edu) • Read: Reverse Engineering Malware (Alien Vault) • Read: CryptoLocker Ransomware (Sophos) • Read: SMB Exploited: WannaCry Use of "EternalBlue" (FireEye) • Read: Viking Horde: A New Type of Android Malware on Google Play (Check Point) • Read: Attacking Malicious Code: A Report to the Infosec Research Council (McGraw, Morrisett; IEEE 2000)	
Thursday, November 14th		• Lab 10 Assigned (available on Canvas), Due on Wednesday, November 20th: Malware Analysis • Practice Quiz 2
Tuesday, November 19th	• Incident Handling and Forensics	
Thursday, November 21st		Quiz 2
Tuesday, December 3rd		
Thursday, December 5th	The Future (Still) Does Not Look Very Bright	

Course Policies

Student Accessibility Services (SAS)

If you have a disability that requires reasonable accommodations, please contact the Student Accessibility Services office at Accessibility@tufts.edu or 617-627-4539 to make an appointment with an SAS representative to determine appropriate accommodations. Please be aware that accommodations cannot be enacted retroactively, making timeliness a critical aspect for their provision. Please note that accommodation letters will no longer be on Trunk. Rather it is your responsibility to hand deliver them to me. For more details, see https://students.tufts.edu/student-accessibility-services/faculty-members.

Electronic Devices

Phones must be silent. You are allowed to politely step outside of the class to take phone calls (e.g., for emergencies, job offers).

Late Policy

We will grant an automatic extension of 24 hours to you at no cost (i.e., grace period). A lab submitted after the grace period will not be accepted.

An lab is expected to be submitted on time. However, we recognize that the exigencies of college life occasionally interfere with on-time submission. If you have difficulty getting the lab in on time, you have two options:

1. For ordinary difficulties, each student is automatically issued three (3) "extension tokens." By expending an extension token, you can get an automatic 24-hour extension on all deadlines associated with a single lab. To use an extension token, you must e-mail me at **`mchow@cs.tufts.edu`**. Thus must be sent before the lab is due and not during the grace period. At most two extension tokens may be expended on any single lab. When you are out of tokens, late labs will no longer be accepted: it will be returned ungraded, and you will receive no credit for the work.
2. If a serious illness affects your ability to complete the lab on time, your first step is to report the illness using the "Illness Notification Form" that is available in WebCenter for Students. We will make suitable arrangements. For extraordinary difficulties, such as bereavement, family emergencies, or other extraordinary unpleasant events, your first step should be to make contact with your associate dean for undergraduate education. You must take

this step before the lab is due. Ask your dean to drop me an email or give me a call, and we will make special arrangements that are suited to your circumstances.

Please understand that extension tokens are meant to be used. That is, you will not receive any special bonus at the end of the course if you do not use any of your extension tokens.

Solutions to Labs and Examinations

Some solutions to labs and examinations may be posted on Piazza.