COMP 116: Introduction to Computer Security

Tufts University Department of Computer Science, Fall 2016

Instructor

- Ming Chow, mchow@cs.tufts.edu
- Office Hours: Wednesdays from 1 - 4 PM, or by appointment, "in my usual spot". Hours are good until the last day of classes, December 8th.
- Please send all class questions via Piazza. DO NOT E-MAIL ME! Sign up at https://piazza.com/tufts/fall2016/comp116.
- For emergencies or private matters, please e-mail or see me directly.

Class Time

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

Teaching Assistant

- Maretta Morovitz

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

- None
- Here are some very good resources about security, in case you're interested:
  - ***Security Engineering*** by Ross J. Anderson

- ***Applied Cryptography*** by Bruce Schneier
- ***The Art of Deception: Controlling the Human Element of Security*** by Kevin Mitnick
- ***Building Secure Software*** by John Viega and Gary McGraw
- ***Software Security: Building Security In*** by Gary McGraw
- Phrack Magazine

Software Requirements (on your personal computer)

- Git
- A copy of the Kali Linux Live-CD ISO: Download at http://www.kali.org/downloads/
- One of the following to run the Kali Linux live-CD ISO:
  - VirtualBox (free)
  - VMware Fusion for Mac OS X or VMware Workstation for Windows or Linux (free one year license via Tufts CS)

Assessment

- Labs (45%)
- Final project (15%)
- 3 quizzes (30%)
- Subjective factors including attendance, class participation, and posting to Piazza (10%)

Syllabus

Schedule is subject to change.

Date	Agenda	Deliverables
Tuesday, September 6th	• Course Introduction • Read: A Disaster Foretold --and Ignored (Washington Post) • Read: Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say (NYT) • Read (classic):	• Lab 0: Course Roster. PLEASE COMPLETE ASAP! This lab is worth 1 point. • Please sign up for our Piazza group • Lab 1: Working

	Reflections on Trusting Trust by Ken Thompson • 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)	with a Hypervisor and a Virtual Machine, Due Wednesday, September 14th
Thursday, September 8th	• Social Engineering • Read: "Researchers dropped 297 USB keys on a University campus. 135 of them were inserted to an online computer" (by Elie Bursztein at Black Hat USA 2016; tweet by Mikko Hypponen https://twitter.com/mikko/status/761103606472781824) • Read: How to Dramatically Improve Corporate IT Security Without Spending Millions (Praetorian) • Watch: Tacoma Narrows Bridge Collapse	
Tuesday, September 13th	• Read: DEF CON: Why Conference Harassment	Lab 2: Packet Sleuth, Due on Tuesday,

	Matters • Read: Sexual Harassment at DefCon (and Other Hacker Cons) by Bruce Schneier • Read: DEF CON Conference Code of Conduct • Networking • Read: How The Web Works --In One Easy Lesson (mkcohen.com) • Tools and Techniques to Succeed at the Wall of Sheep (on wallofsheep.com) • Read: Welcome To Def Con — You've Already Been Hacked (on buzzfeed.com) • Cheat Sheet:TCP/IP and tcpdump (PDF; from SANS Institute)	September 27th
Thursday, September 15th	• Attacking Networks: Sniffing • Read: The Basics of Arpspoofing/Arppoisoning (Irongeek.com) • Read: Fun With Network Friends (2600 Magazine, Summer 2008) • Read: ARP Spoofing (Veracode)	
Tuesday, September 20th	• Attacking Networks: Scanning, Part I • Read (dated September 18, 2016): Mass-Analyzing a Chunk of the Internet • Read: Masscan: the	

	entire Internet in 3 minutes (Errata Security) • Read: We scanned the Internet for port 22 (Errata Security) • Read: Thousands of computers open to eavesdropping and hijacking (Sophos) • Cheat Sheet:Netcat Cheat Sheet (PDF; from SANS Institute) • Read: Remote Exploitation of an Unaltered Passenger Vehicle (PDF) by Charlie Miller and Chris Valasek	
Thursday, September 22nd	• Attacking Networks: Scanning, Part II • Read: Port Scanning Techniques (Chapter 15. Nmap Reference Guide) • Read: Firewall/IDS Evasion and Spoofing (Chapter 15. Nmap Reference Guide) • Read: Nmap Examples	• Lab 3: The Scanning Lab, Due on Wednesday, September 28th • The Final Project Assigned
Tuesday, September 27th	• Attacking Networks: Distributed Denial of Service Attacks • Read: Brian Krebs' Blog Hit by 665 Gbps DDoS Attack • Read: Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net (Ars Technica)	Lab 4: Scapy, Due on Friday, October 21st

Thursday, September 29th	• Vulnerabilities • Read: Verizon's 2016 Data Breach Investigations Report (DBIR)	• Tufts Career Fair on Friday, September 30th 11:30 AM - 2:30 PM at Gantcher Center • Event RSVP: Tufts Reverse Career Fair after the Tufts Career Fair, 3 - 4 PM in Halligan 102
Tuesday, October 4th	• Cryptography, Part I • Salted Password Hashing - Doing it Right	• Practice Quiz 1 • Lab 5: Crack Me If You Can - The 2016 Password Cracking Contest. Deadline: End of October
Thursday, October 6th	Cryptography, Part II	
Tuesday, October 11th	Cryptography, Part III	Quiz 1
Thursday, October 13th	• Web Security, Part I. Guest Speakers: Christine Cunningham and Doug Stetson (Tufts CS alumnus), MIT Lincoln Lab • Read: OWASP Top 10 • Read: CWE/SANS TOP 25 Most Dangerous Software Errors • Read: Cross-Site Request Forgery Guide: Learn All About CSRF Attacks and CSRF	Tufts Polyhack 2016: Friday, October 14th to Saturday, October 15th

	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)	
Tuesday, October 18th	• Web Security, Part II: XSS, SQL Injection • Watch: Cross-Site Scripting (XSS) Tutorial by Chris Eng (Veracode) • Tutorial and Reference: SQLZoo • 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) • Tool: Burp Suite (requires Java). Burp is included in Kali.	Details on the 2016 Capture The Flags Game (Lab 6)
Thursday, October 20th	• Web Security, Part III: Cookie Tampering,	

	Remote Code Execution • Is MitM a Good Thing? Auditing Mobile Apps • Read: AdiOS: Say Goodbye to Nosy iPhone Apps (Veracode)	
Tuesday, October 25th	Guest Speaker: Nick Davis (E'14, Course Alumnus Fall 2013), Software Engineer at Rapid7	
Thursday, October 27th	Guest Speaker: Sandy Carielli, Security Technologies Director at Entrust Datacard	
Tuesday, November 1st	The Annual Capture The Flags (CTF) Game. Location: Halligan 102	
Thursday, November 3rd	HOLD	
Thursday, November 10th	• 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)	• Lab 7: Technical Risk Analysis and Static Analysis, Due on Monday, November 21st • Practice Quiz 2
Tuesday, November 15th		Quiz 2
Thursday, November 17th	• Malware • Read: The Internet Worm Program: An Analysis by Gene Spafford • Read: **`tini.exe`** (via	

	ntsecurity) • Read: Bypass modern anti virus with an 8 year old backdoor • Forensics, Anti-Forensics, Incident Handling • Read: Making Sense of Digital Forensics and Incident Response Disciplines by Lenny Zeltser • My Old Presentation: Investigations and Incident Response Using BackTrack	
Tuesday, November 22nd	NO CLASS	Lab 8 Assigned: Forensics, Due on Tuesday, December 6th
Tuesday, November 29th	• Anti-Forensics, Privacy • Read: Panel: The Politicization of Security; Panel: Wireless Devices and Consumer Privacy (From USENIX '04) • Watch: Ordering Pizza (ACLU) • Read: Privacy and Free Speech: It's Good For Business (ACLU --thanks to Nicole Ozer)	Practice Quiz 3
Thursday, December 1st	• Read: Boston Loves One-Night Stands: Uber Data Reveals the Hub Has the Highest Number of Walks of Shame (BostInno) • Read: Creepy insurance company pulls coverage due to Facebook pics	

	(ArsTechnica)	
Tuesday, December 6th	• What's The Point? • Read: "Strike Back" by Jennifer Granick (;login: volume 29, number 6, 2004) • Read: "CyberInsecurity: The Cost of Monopoly" by Dan Geer (2004)	Quiz 3
Thursday, December 8th		

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.

Late Policy

A lab (to be known therefore an assignment) that is submitted electronically (most homework) will typically be due at 11:59 PM on a Tuesday or Thursday. We will grant an automatic extension of ten minutes at no cost to you. If you plan on submitting your work at midnight or at six, you will have nine minutes for last-minute changes.

An assignment 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 assignment 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

assignment. To use an extension token, you must e-mail me at **mchow@cs.tufts.edu**. Thus must be sent before the assignment is due. At most two extension tokens may be expended on any single assignment. When you are out of tokens, late assignments 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 assignment 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 assignment 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

Solutions to labs and examinations will not be posted for this course.