Instructor Contact Information:
Gabriel Kaptchuk
Email: kaptchuk@bu.edu
Office: CSDS 1024

TF Contact Information:
Julie Ha
Email: hajulie@bu.edu

Logistics:
Class Piazza
Gradescope signup code pinned on piazza.

Summary:
This course will cover a wide variety of computer security topics, with a focus on real, deployed protocols. Our first unit will cover vulnerabilities in critical internet protocols that could be exploited by an attacker to redirect or decrypt internet traffic or launch denial of service attacks. Our second unit will focus on privacy on the web, including a deep dive into Tor and secure messaging protocols.

Why Take This Course:
This class will give you a good look at the state of network security today, covering both the challenges to and techniques for achieving a secure and private internet. Over the course of the class, students will gain a deep understanding of adversarial thinking and gain an intuition for how to both attack and secure protocols. If you like to break things or enjoy seeing what happens when expert protocol designers make mistakes, this course should be a lot of fun. Additionally, we will be spending significant time discussing censorship resistance and secure messaging, which are fundamental tools to protocol freedom of expression and promote human rights. If you are passionate about privacy as it relates to protecting human rights, you will find the techniques covered in this class to be well motivated.

Who should Take This Course:
- Upper level undergraduate students or graduate students passionate about security and privacy
- We will assume that students already have a working knowledge of the fundamentals of cryptography. This should include symmetric key cryptography, public key cryptography, digital signatures, pseudorandomness, and hash functions. Any one of CS357, CS571, CS538, CS548, CS568 **or** equivalent required.
- We will also assume that students have been exposed to thinking adversarially, for instance in one of the courses listed above

Grading (All time Eastern):
- Reading Responses (1 Per week) - 15% (Always Due Mondays @9pm via. Gradescope)

- Weekly Ask-A-Question (1 Per week) - 3% (Always Due Fridays @9pm via. Gradescope)
- Written Homeworks (3) - 25% (Always Due Mondays @9pm via Gradescope)
    - (1) Crypto Review (5%)
    - (2) Network Security Written Assignment (10%)
    - (3) TLS Homework (10%)
- Programming Assignments (3) - 32% (Always Due Mondays @9pm via Gradescope)
    - (1) Heartbleed Assignment (16%)
    - (2) Tor Assignment (16%)
- Final Cumulative Exam - 25%

Schedule:

Colors link assignment date and due date for each assignment

Week	**Date**	**Topics**	**Homework**	**Readings**
W0 (Jan 16-20)	Jan 19	Introduction/Networks overview	**Crypto Review Assigned (2wks)**	**NONE. It's the first day of class! There can't be readings!**
W1 (Jan 23-27)	Jan 24	Networks overview/Crypto overview		**Why Johnny Can't Encrypt** **Bruce Schneier Blog 1** **Bruce Schneier Blog 2**
	Jan 26	Usable Security		**(Additional, Optional Reading/Watching):** The Moral Character of Cryptographic Work Crypto for the People (Crypto 2020 Invited Talk, Seny Kamara) Crying Wolf: An Empirical Study of SSL Warning Effectiveness Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes
W2 (Jan30 -Feb 3)	Jan 31	ARP		**ARP Poisoning Explainer** **Or** **https://www.varonis.com/blog/arp-poisoning** **Cloudflare Writeup of 2021 Facebook Downtime**

	Feb 2	BGP	**Crypto Review Due (Monday Feb6th @9pm)**	**(Additional, optional Reading/Watching):** Kids Online Safety Act (Pro) (Anti)
W3 (Feb 6-10)	Feb 7	BGP Hijacking Mitigation	**Network Security Written Homework Assigned (3wks)**	**Cloudflare RPKI Writeup** **BGP Hijack Targeting Cryptocurrencies** **Google Going Offline** **AS7007 Incident** **One Year in BGP Security** **(Additional, Optional Reading/Watching:)** 2018 BGP Hijack To Steal Cryptocurrencies Is BGP Safe Yet? BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?
	Feb 9	BGP Sec		
W4 (Feb 13-17)	Feb 14	DDOS		**DNS Cache Poisoning** **The DDOS that almost broke the internet** **Amplification Hell: Revisiting Network Protocols for DDoS Abuse** **(Additional, Optional Reading/Watching:)** Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks TCP Amplification Attacks in depth DNSSec Root Signing Ceremony
	Feb 16	DNS		

				DNSSec Intro RFC (4033)
W5 (Feb 21-25)	Feb 21	**NO CLASS (Monday Schedule)**		**DNS Sec Overview** **DNSSec Root Signing Ceremony** **DNSSec Intro RFC (4033)**
	Feb 23	DNSSec	**Network Security Written Homework Due (Monday Feb 27 @ 9pm)**	
W6 (Feb 27 -Mar 3)	Feb 28	**<CLASS IS CANCELLED>**	**Heartbleed Programming Assignment Assigned (3wk)**	**Understanding the SSH Encryption and Connection Process** **A brief history of SSH and remote access** **RFC 4251, Sections 9.3.3, 9.3.4, 9.3.7, 9.3.9** **(The submission portal open until the monday after spring break so that you dont have to turn in the needed during spring break)**
	Mar 2	SSH/SFTP		
W7	**SPRING BREAK**			
W8 (Mar 13-17)	Mar 14	TLS pt1		**Transport Layer Security** **Smashing The Stack For Fun An Profit**
	Mar 16	TLS pt2		
W9 (Mar 20-24)	Mar 21	TLS pt3		**A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)** **AND READ THE INTRODUCTION SECTION AND BACKGROUND SECTIONS FOR ONE OF THE FOLLOWING PAPERS:** Drown Attack (S1 and S2) Logjam Attack (S1 and S2)
	Mar 23	TLS pt4	**Heartbleed Programming Assignment (Mar 27th @9pm)**	

				FREAK Attack (Just S1) POODLE Attack (Full paper) ROBOT Attack (S1 and S3) BEAST Attack (S1, S2, and, S3) Small Subgroup Attacks (just S1 – good paper if you are math inclined) **(Additional, Optional Reading/Watching:)** The Illustrated TLS Connection Public key crypto in the wild, by Nadia Heninger TLS (Talk by Eric Rescorla) -- Discusses TLS1.3 Improvements on TLS1.2
W10 (Mar 27-Mar31)	Mar 28	Tor Protocol	**TLS Homework Assigned (2wk)**	**Tor Abuse FAQ** **Tor Paper (**Section 4 through the end for 4.3. Section 7 Passive Attacks and Active Attacks) **(Additional, Optional Reading/Watching:)** RightsCon: "The Case for Privacy By Design - Privacy Law Shortcomings and the Role of Privacy Tools" Hidden Services Specification Brian Levine's Talk about Hidden Services
	Mar 30	Tor Protocol		
W11 (Apr	Apr 4	Tor Protocol		**Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market**

3-7)	Apr 6	**CLASS CANCELLED**		**Optional reading (please be warned, these readings discuss child abuse material):** **FBI on Playpen** **EFF on Playpen**
W12 (Apr 10-14)	Apr 11	Censorship Evasion: Tor bridges, Domain Fronting and Encrypted SNI, Protocol Obfuscation	**TLS Homework Due (Apr 12th @9PM)**	**Tor Onion Services Overview** **AND EITHER** **GFW Scanning and Tor Reachability in 2018** **OR (choose whichever seems more interesting to you)** **Domain Fronting Paper (Skip Background and Related Work and Fronting-capable web services, Deployment on Lantern and Psiphon) (Weirdly I'm getting a reset on chrome, but firefox can open it)**
	Apr 13	Snowflake, Steganography	**Tor Project Assignment (3wk)**	
W13 (Apr 17-21)	Apr 18	Future of Web Access: OPAQUE		**Cloudflare Writeup of OPAQUE** **Matt Green's History of Backdoors** **Optional:** **New America Summary of the 1990's Crypto Wars** **Riana Pfeffercorn "Whats new in the US Crypto Wars" (Very comprehensive, but also dense)**
	Apr 20	Social Context for Encryption		
W14 (Apr 24-28)	Apr 25	Blockchain Class with Guest Lecturer Nicolas Alhaddad		**NO READINGS THIS WEEK**

	Apr 27	iMessage and Goals for user friendly E2E encryption with Guest Lecturer Palak Jain	**Tor Project Due (May 3 @9pm)**	
W15 (May 1-5)	May 2	Course Review		