

2022-01-20

Network Security 2022

G. Kaptchuk. 2022. "Network Security 2022"

<https://hdl.handle.net/2144/46957>

"Downloaded from OpenBU. Boston University's institutional repository."

OLD SYLLABUS!

IF YOU ARE HERE FOR DEADLINES, THIS IS THE WRONG PLACE

Instructor Contact Information:

Gabriel Kaptchuk

Email: kaptchuk@bu.edu

Office: MCS 135

TF Contact Information:

Palak Jain

Email: palakj@bu.edu

Graders (Please contact me rather than the graders):

Amy Feng Chen

Eesha Gholap

Julie Ha

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. CS391, CS538, CS548, CS568 or equivalent recommended.
- 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) - 10% (Always Due Monday @9pm via Gradescope)
- Weekly Ask-A-Question (1 Per week) - 3% (Always Due Friday @9pm via Gradescope)
- Written Homeworks (3) - 30% (Always Due Mondays @9pm via Gradescope)
 - (1) Crypto Review (5%)
 - (2) Network Security Written Assignment (7.5%)
 - (4) TLS Homework (5%)
 - (3) Signal Written Homework(s) (12.5%)
- Programming Assignments (3) - 32% (Always Due Mondays @9pm via Gradescope)
 - (1) Heartbleed Assignment (12%)
 - (2) Tor Assignment (20%)
- Final Cumulative Exam - 25%

Schedule:

Colors link assignment date and due date for each assignment

<u>Week</u>	<u>Date</u>	<u>Topics</u>	<u>Homework</u>	<u>Readings</u>
W0 (Jan 25-29)	Jan 20	Introduction/Networks overview	Crypto Review Assigned (2wks)	NONE. It's the first day of class! There can't be readings!
W1 (Jan 24-28)	Jan 25	Networks overview/Crypto overview		Why Johnny Can't Encrypt Bruce Schneier Blog 1 Bruce Schneier Blog 2
	Jan 27	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 (Jan31-Feb 4)	Feb 1	ARP		ARP Poisoning Explainer Or https://www.varonis.com/blog/arp-poisoning Cloudflare Writeup of 2021 Facebook Downtime

	Feb 3	BGP	Crypto Review Due (Monday Feb7th)	Computerphile Explanation of 2021 Facebook Downtime Cloudflare explainer of BGP (Additional, Optional Reading/Watching:) What is DNS 2018 BGP Hijack To Steal Cryptocurrencies History of IPv4 AS Relationships
W3 (Feb 7-11)	Feb 8	BGP Hijacking Mitigation	Network Security Written Homework Assigned (2wks)	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?
	Feb 10	BGP Sec		
W4	Feb 15	DDOS		DNS Cache Poisoning

(Feb 14-18)	Feb 17	DNS	Network Security Written Homework Due (Monday Feb 21 @ 9pm)	<p>The DDOS that almost broke the internet</p> <p>Amplification Hell: Revisiting Network Protocols for DDoS Abuse</p> <p>(Additional, Optional Reading/Watching:)</p> <p>Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks</p> <p>TCP Amplification Attacks in depth</p> <p>DNSSec Root Signing Ceremony</p> <p>DNSSec Intro RFC (4033)</p>
W5 (Feb 21-25)	Feb 22	NO CLASS (Monday Schedule)		<p>Transport Layer Security</p> <p>A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)</p>
	Feb 24	DNSSec		<p>(Additional, Optional Reading/Watching:)</p> <p>The Illustrated TLS Connection</p> <p>Public key crypto in the wild, by Nadia Heninger</p> <p>TLS (Talk by Eric Rescorla) -- Discusses TLS1.3 Improvements on TLS1.2</p>
W6 (Feb 28 -Mar 4)	Mar 1	TLS pt1	Heartbleed Programming Assignment Assigned (2wk)	<p>RFC 5246 (Section 7.3 and 7.4) (The text sprinkled in between the structs and term definitions is the most important part)</p> <p>Smashing The Stack For Fun An Profit</p>
	Mar 3	TLS pt2		

W7	SPRING BREAK			
W8 (Mar 14-18)	Mar 15	TLS pt3		NO REQUIRED READING THIS WEEK (Additional, Optional Reading/Watching:) Tor Paper
	Mar 17	TLS pt4		
W9 (Mar 21-25)	Mar 22	TLS pt4	TLS Homework Assigned	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
	Mar 24	Tor Protocol	Heartbleed Programming Assignment (DNS due Mar 21st @9pm and Heartbleed due Mar 24th @9pm)	
W10 (Mar 28-Apr 1)	Mar 29	Tor Protocol		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)
	Mar 31	Tor Protocol	TLS Homework Due (Apr 4th @9PM)	
W11 (Apr 4-8)	Apr 5	Censorship Evasion: Tor bridges, Domain Fronting and	Tor Project Assignment	New America Summary of the 1990's Crypto Wars Matt Green's History of Backdoors

		Encrypted SNI, Protocol Obfuscation		Optional:
	Apr 7	Censorship Part 2		Riana Pfeffercorn “Whats new in the US Crypto Wars” (Very comprehensive, but also dense)
W12 (Apr 11-15)	Apr 12	iMessage and Goals for user friendly E2E encryption (Palak Lecturing)		Syniverse Hack Matt Green’s Blog on the EARN IT Act (Relevant to Apr 19 Class) Signal Blog on Async (The described fix is old, but the setup to the problem is key)
	Apr 14	Key Derivation Functions (Palak Lecturing)		Optional: NYTimes Article about CSAM (Content warning for child sexual abuse)
W13 (Apr 18-22)	Apr 19	Social Context for Encryption	Signal Homework Assigned	The Double Ratchet: Security Notions, Proof, and Modularization for the Signal Protocol (Abstract and Introduction) WhatsApp Signal and Privacy Labels
	Apr 21	Signal Protocol pt 1	Tor Project Due (April 25, midnight)	OPTIONAL READING Signal Documentation (Lots of colors!) (RECOMMENDED) New Yorker Profile of Marlinspike (Signal founder)
W14 (Apr 25-29)	Apr 26	Signal Protocol pt 2		Signal Sealed Sender
	Apr 28	Metadata Protection (Sealed Sender,		Secret Sharing Explainer Video (Should have been removed! – My bad!)

		Private information retrieval, private set intersection		<p>OPTIONAL READING</p> <p>Signal Initial Key Exchange</p> <p>Signal SGX Contact Discovery</p> <p>NDSS Paper on Crawling Contact Discovery</p>
W15 (May 2-6)	May 3	Course Review	<p>Signal Homework Due (Last day of class – MAY 4th)</p>	<p>NO REQUIRED READING THIS WEEK. (use that time to study!)</p> <p>You may be interested to look at the new bi-partisan piece of legislation that was proposed last week though!</p> <p>https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-</p> <p>https://www.wyden.senate.gov/imo/media/doc/The%20Fourth%20Amendment%20Is%20Not%20For%20Sale%20Act%20of%202021%20One%20Page.pdf</p>