CSE 194: Cybersecurity History and Culture

This is the syllabus of CSE 194: a course on cybersecurity history and culture.

Course Number: CSE 194
Instructor: Pratham Gupta
Email: prathamgupta@asu.edu
Office: BYENG 460EF (desk)
Meeting Times: W 3:00pm - 6:00pm
Meeting Location: BYENG 361

Course Description

In the days of Marco Polo and Ferdinand Magellan, before we had satellite imagery and Google Earth, the world was a mystery too big to fit into the mind of the average person. Even those experts who knew all there was to know about the wide reaches of human civilization (and beyond) were forced, eventually, on some part of their maps, to write "Here Be Dragons."

The world has not only changed since those times; it has been *replaced*. We live in a digital reality, full of wonder unimaginable just a few short centuries ago. But a modern Marco Polo would find, once more, that there is no satellite imagery of this frontier. The maps are dangerously incomplete. Again, there are dragons, ominous whispers in the dark claiming network packets as krakens once claimed whole ships.

Hackers are the dragons of the digital world. They are shrouded in mystery, steeped in intrigue, and imbued with a sort of romance. But unlike the dragons of times long gone, these dragons are real. They lived, they breathed, they hacked. They have names, criminal records, autobiographies. And in order to truly know how to operate in the open seas of cyberspace, we must understand them.

This course will focus on learning about the history and culture of cybersecurity. We will do so through both theory and practice: over the course of the semester, we will learn about many prominent and important hackers from different periods of Computer Science. We will also learn about (and use!) historic hacker and hacker-adjacent tools and services.

Topics Covered

Module 0: The Beginning

Alan Turing, early cryptographer, father of computability

Reading: Alan Turing — a short biography https://www.turing.org.uk/publications/dnb.html

Ken Thompson, co-creator of C and Unix

Reading: Reflections on Trusting Trust https://dl.acm.org/doi/10.1145/358198.358210
Reading: Coding Machines https://www.teamten.com/lawrence/writings/coding-machines/

Module 1: Phone Phreaking:

Phreaking

📰 "Secrets of the Little Blue Box, Esquire", 1971
http://www.thestacksreader.com/secrets-of-the-blue-box-ron-rosenbaum-steve-jobs-influence/

Susan Thunder, late-era phreaker / early-era hacker

📰 "Searching for Susy Thunder", 2021
https://www.theverge.com/c/22889425/susy-thunder-headley-hackers-phone-phreakers-claire-evans

Module 2: Early Hackers

Bulletin Board Systems

📰 The Lost Civilization of Dial-Up Bulletin Board Systems
https://www.theatlantic.com/technology/archive/2016/11/the-lost-civilization-of-dial-up-bulletin-board-systems/506465/

Loyd Blankenship, early hacker

📰 The Hacker's Manifesto http://www.phrack.org/archives/issues/7/3.txt

Kevin Mitnick and Tsutomu Shimomura, early-era hackers

📰 Catching kevin https://www.wired.com/1996/02/catching/

Internet Relay Chat

📰: History of IRC http://www.irc.org/history.html
📰 History of IRC https://daniel.haxx.se/irchistory.html
📰 Fall of Freenode https://fuchsnet.ch/privat/fn-resign-letter.txt

USENET

📰 The Evolution of Usenet https://firstmonday.org/ojs/index.php/fm/article/view/608/529

Early Hacking Policy

📰 An Oral History of How the Movie 'WarGames' Inspired Ronald Reagan's Cybersecurity Policies https://melmagazine.com/en-us/story/wargames-ronald-reagan-cybersecurity

Module 3: Hackers and Hacktivists

Robert Tappan Morris Jr, early hacker, author of first wide-spread "worm"

📰 How a grad student trying to build the first botnet brought the Internet to its knees https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/

Dan Kaminsky, network hacker

📰 Secret Geek A-Team Hacks Back, Defends Worldwide Web https://www.wired.com/2008/11/ff-kaminsky/

Aaron Swartz, hacktivist

📰 The Brilliant Life and Tragic Death of Aaron Swartz https://www.rollingstone.com/culture/culture-news/the-brilliant-life-and-tragic-death-of-aaron-swartz-177191/

Phineas Fisher, hacktivist

📰 The Phineas Philes https://github.com/Alekseyyy/phineas-philes
Viewing: Interview with Phineas Fisher https://www.youtube.com/watch?v=BpyCl1Qm6Xs

Module 4: Hacking Collectives

📰 Phrack Pro-phile on Groups: http://phrack.org/issues/6/2.html

Legion of Doom

📰 The History of the Legion of Doom http://phrack.org/issues/31/5.html

Masters of Deception

📰 The History of MoD

- http://www.textfiles.com/hacking/modbook1.txt
- http://www.textfiles.com/hacking/modbook2.txt
- http://www.textfiles.com/hacking/modbook3.txt
- http://www.textfiles.com/hacking/modbook4.txt
- http://www.textfiles.com/hacking/modbook5.txt

The Great Hacker War

📰 Gang War in Cyberspace https://www.wired.com/1994/12/hacker-4/
📰 No Time for Goodbyes http://phrack.org/issues/45/9.html#article

Cult of the Dead Cow

📰 TBD
Viewing: How The Cult of The Dead Cow Helped Shape Modern Cybersecurity
https://www.youtube.com/watch?v=QvZuAwLIsEo

l0pht

📰 HacK, CouNterHaCk https://www.nytimes.com/1999/10/03/magazine/hack-counterhack.html

Shellphish

📰 Cyber Grand Shellphish http://www.phrack.org/issues/70/4.html
Viewing: History of Shellphish https://www.youtube.com/watch?v=jbZit5VFcOU

Module 5: The Hacker Aesthetic

📺 Sneakers https://en.wikipedia.org/wiki/Sneakers_(1992_film)
📺 Hackers https://en.wikipedia.org/wiki/Hackers_(film)
📺 Mr. Robot https://en.wikipedia.org/wiki/Mr._Robot

pwning noobs

📰 How “PWNED” went from hacker slang to the internet’s favorite taunt https://www.inverse.com/gaming/pwned-meaning-definition-origins-video-games-internet-hackers
📰 OWNED (PWNED) https://knowyourmeme.com/memes/owned-pwned

Module 6: Hacking the Planet

TBD

Module 7: The Dark Side

Early Viruses

📺 Malicious Life: The Dark Avenger https://malicious.life/episode/episode-2/

Albert Gonzales, organized cybercriminal

📰 "The Great Cyberheist" https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html
📰 "Sex, Drugs, and the Biggest Cybercrime of All Time" https://www.rollingstone.com/culture/culture-news/sex-drugs-and-the-biggest-cybercrime-of-all-time-241836/

Ross Ulbricht, cybercrime kingpin

📰 "Sunk: How Ross Ulbricht ended up in prison for life", 2015 https://arstechnica.com/tech-policy/2015/05/sunk-how-ross-ulbricht-ended-up-in-prison-for-life/
📰 "The Unsung Tax Agent Who Put a Face on the Silk Road", 2015 https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html

Assessment and Grading Policy

Assessment will be based on class attendance (1% for each class, up to 15%), participation (1% for each class, up to 15%), and the completion of assignments (cumulatively, 70%). These assignments will be assessed on a pass/fail basis, at 12% per assignment (resulting in a 2% forgiveness for missing one of the assignments).

1. Phreaking Long Distance. In Module 1, students will carry out classical attacks against legacy telephone systems against an approximated telephone system.

2. Mastering Locks. We will explore several physical attacks by learning how to break combo locks and pick real locks.
3. Netsplits! In Module 2, students will hack channels on an IRC server by inducing netsplits, mirroring hallowed hackers of the 1990s.
4. Dumpster Dive. Students will simulate a dumpster diving expedition by diving into pre-built
5. Destroy The Internet. In Module 3, students will unleash an approximation of the Morris Worm onto an approximation of the early internet. The successful students will take down the early internet, following in Morris' footsteps.
6. The Modern Hacker. In Module 5, students will create and present a modern hacker avatar, complete with a handle and an aesthetic design.
7. The Common Thread. Each student will be required to evaluate two hackers, groups, or technologies across two different modules, identify common threads between them, and present these in class. Depending on the number of students, this may become a group assignment.
8. Some modules may have Response Paper assignments: short papers to organize your thoughts on the assigned reading.

No programming knowledge will be needed to complete any of the assignments! Students will be able to complete these assignments through point-and-click interfaces.

Grades will be assigned on the typical A-E scale, without plusses or minuses, at standard cutoffs (90/80/70/60/50 for A/B/C/D/E).

Learning Outcomes

The successful student will finish the course with a deep understanding of:

1. The context in which modern cybersecurity (and Computer Science) operates. This will be conveyed through reading and viewing assignments.
2. Historically-relevant technologies that were, in their time, crucial cybersecurity battlefields. This will be conveyed through hands-on practice challenges using historic technology.
3. A common thread underpinning cybersecurity practice throughout the information era. This will be developed through assignments of analyzing not just the differences, but the similarities between non contemporaneous approaches to cybersecurity.

Textbook and Reading

There is no textbook for this course. Reading materials will be linked from every module. That being said, the following resources are highly recommended to dive deeper into the material!

📘 A People's History of Computing in the United States by Joy Lisi Rankin

- 📘 All the Rave: The Rise and Fall of Shawn Fanning's Napster by Joseph Menn
- 📘 Broad Band: The Untold Story of the Women Who Made the Internet by Claire L. Evans
- 📘 Code Girls The Untold Story of the American Women Code Breakers of World War II by Liza Mundy
- 📘 Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon by Kim Zetter
- 📘 Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World by Joseph Menn
- 📘 Cyberpunk: Outlaws and Hackers on the Computer Frontier by Katie Hafner
- 📘 Dark Territory: The Secret History of Cyber War by Fred Kaplan
- 📘 Ghost In The Wires: My Adventures as the World's Most Wanted Hacker by Kevin Mitnick and William L. Simon
- 📘 Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground by Kevin Poulsen
- 📘 Masters of Deception: The Gang That Ruled Cyberspace by Michele Slatalla
- 📘 Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers by Andy Greenberg
- 📘 Space Rogue: How the Hackers Known As L0pht Changed the World by Cris Thomas
- 📘 Spam Nation: The Inside Story of Organized Cybercrime — from Global Epidemic to Your Front Door by Brian Krebs
- 📘 The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage by Clifford Stoll
- 📘 The Dark Net: Inside the Digital Underworld by Jamie Bartlett
- 📘 The Friendly Orange Glow: The Untold Story of the PLATO System and the Dawn of Cyberculture by Brian Dear
- 📘 The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics by Ben Buchanan
- 📘 The Hacker Crackdown: Law and Disorder on the Electronic Frontier by Bruce Sterling
- 📘 The Lazarus Heist: From Hollywood to High Finance: Inside North Korea's Global Cyber War by Geoff White
- 📘 The Modem World: A Prehistory of Social Media by Kevin Driscoll
- 📘 Underground: Tales of Hacking, Madness, and Obsession on the Electronic Frontier by Suelette Dreyfus
- 📘 Warez: The Infrastructure and Aesthetics of Piracy by Martin Paul Eve
- 📘 We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency by Parmy Olson
- 📘 Hack History: https://realhackhistory.org/

Academic Integrity

Students in this class must adhere to ASU's academic integrity policy, which can be found

at https://provost.asu.edu/academic-integrity/policy). Students are responsible for reviewing this policy and understanding each of the areas in which academic dishonesty can occur. In addition, all engineering students are expected to adhere to both the ASU Academic Integrity Honor Code and the Fulton Schools of Engineering Honor Code. All academic integrity violations will be reported to the Fulton Schools of Engineering Academic Integrity Office (AIO). The AIO maintains records of all violations and has access to academic integrity violations committed in all other ASU colleges/schools.

Copyright

Course content, including lectures, are copyrighted materials and students may not share outside the class, upload to online websites not approved by the instructor, sell, or distribute course content or notes taken during the conduct of the course (see ACD 304–06, "Commercial Note Taking Services" and ABOR Policy 5-308 F.14 for more information).

You must refrain from uploading to any course shell, discussion board, or website used by the course instructor or other course forum, material that is not the student's original work, unless the students first comply with all applicable copyright laws; faculty members reserve the right to delete materials on the grounds of suspected copyright infringement.

Disability Policy

Suitable accommodations will be made for students having disabilities. Students needing accommodations must register with the ASU Disabilities Resource Center and provide documentation of that registration to the instructor. Students should communicate the need for an accommodation in sufficient time for it to be properly arranged. See ACD 304-08 Classroom and Testing Accommodations for Students with Disabilities.

Harassment and Sexual Discrimination

Arizona State University is committed to providing an environment free of discrimination, harassment, or retaliation for the entire university community, including all students, faculty members, staff employees and guests. ASU expressly prohibits discrimination, harassment, and retaliation by employees, students, contractors, or agents of the university based on any protected status: race, color, religion, sex, national origin, age, disability, veteran status, sexual orientation, gender identity, and genetic information.

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to

sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at https://sexualviolenceprevention.asu.edu/faqs.

Mandated sexual harassment reporter: As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, https://eoss.asu.edu/counseling, is available if you wish discuss any concerns confidentially and privately.