Network Security and Privacy

UT CS361S

Spring 2021

Lecture Notes

About the Instructor

Brigham Young University
CS
Department
Provo, UT

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

RICE
Computer Science

CRIMSON VISTA
TECHNICAL CONSULTING & LITIGATION SUPPORT

What about You?

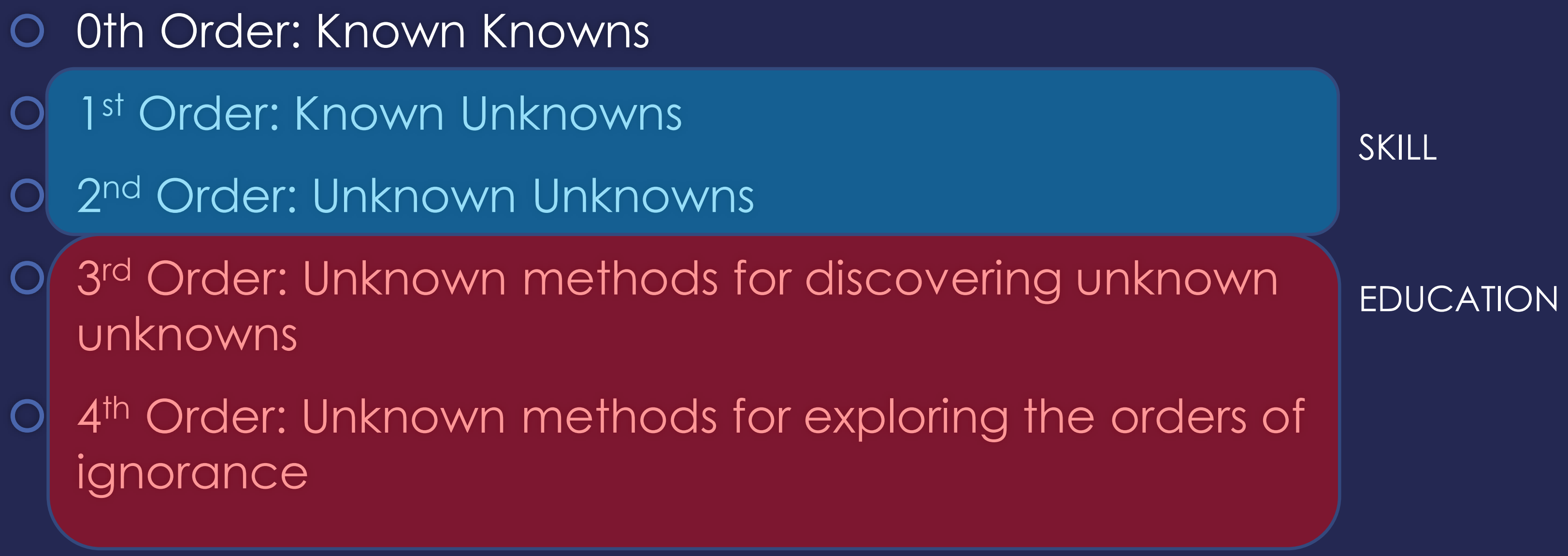
- Why did you take this course?
- What is your programming background like?
- What has been your favorite course so far? Why?
- What is your learning style?
- What is your favorite teaching style?

The 5 Orders of Ignorance

- 0th Order: Known Knowns
- 1st Order: Known Unknowns
- 2nd Order: Unknown Unknowns
- 3rd Order: Unknown methods for discovering unknown unknowns
- 4th Order: Unknown methods for exploring the orders of ignorance

(Adapted from Phillip Armour, “The Five Orders of Ignorance”)

The 5 Orders of Ignorance



- 0th Order: Known Knowns
- 1st Order: Known Unknowns
- 2nd Order: Unknown Unknowns
- 3rd Order: Unknown methods for discovering unknown unknowns
- 4th Order: Unknown methods for exploring the orders of ignorance

SKILL

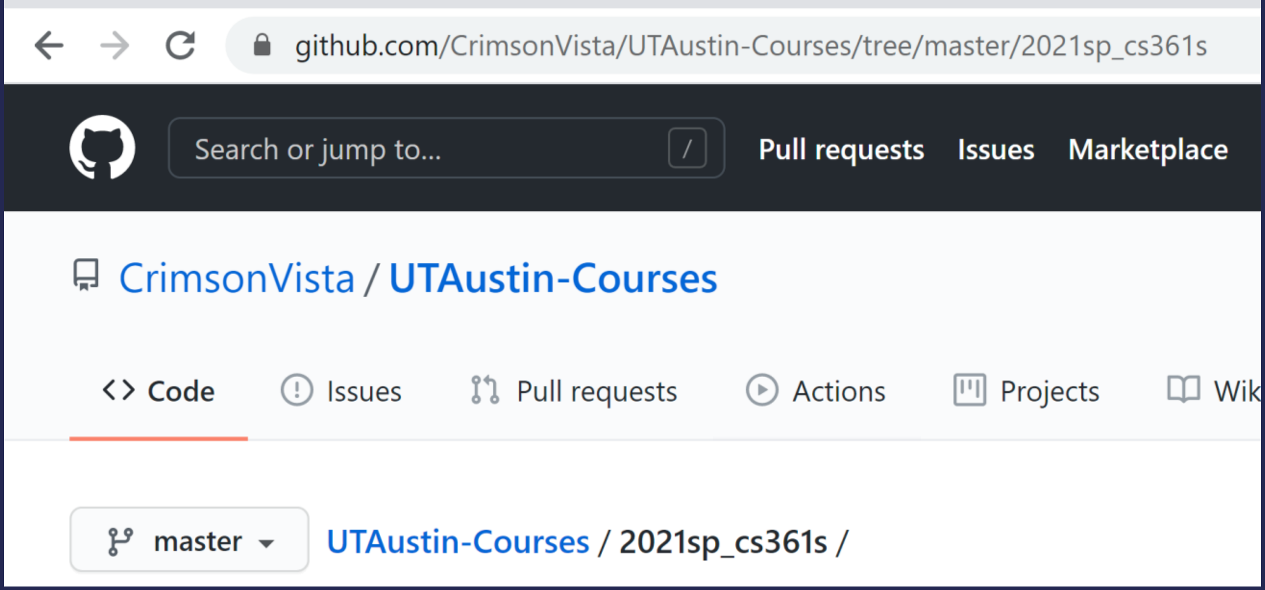
EDUCATION

(Adapted from Phillip Armour, “The Five Orders of Ignorance”)

A Few Introductory Notes

- This course is still a little new for me
- I’m still developing the materials
- Please feel free to make suggestions or raise concerns

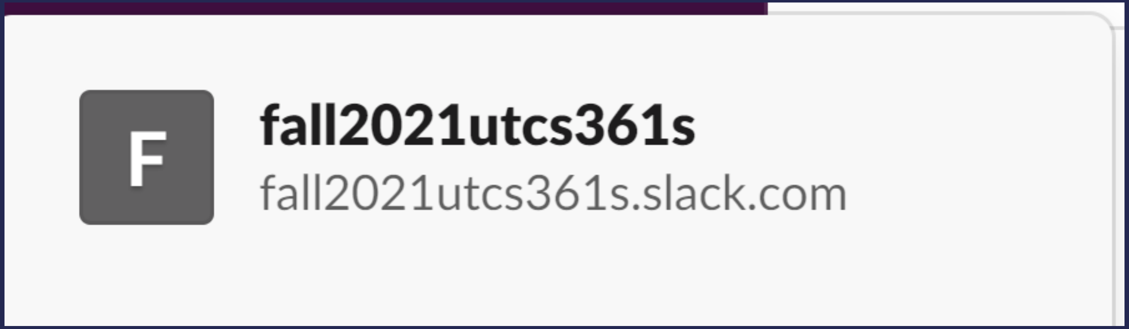
Two Resources



github.com/CrimsonVista/UTAustin-Courses/tree/master/2021sp_cs361s

CrimsonVista / UTAustin-Courses

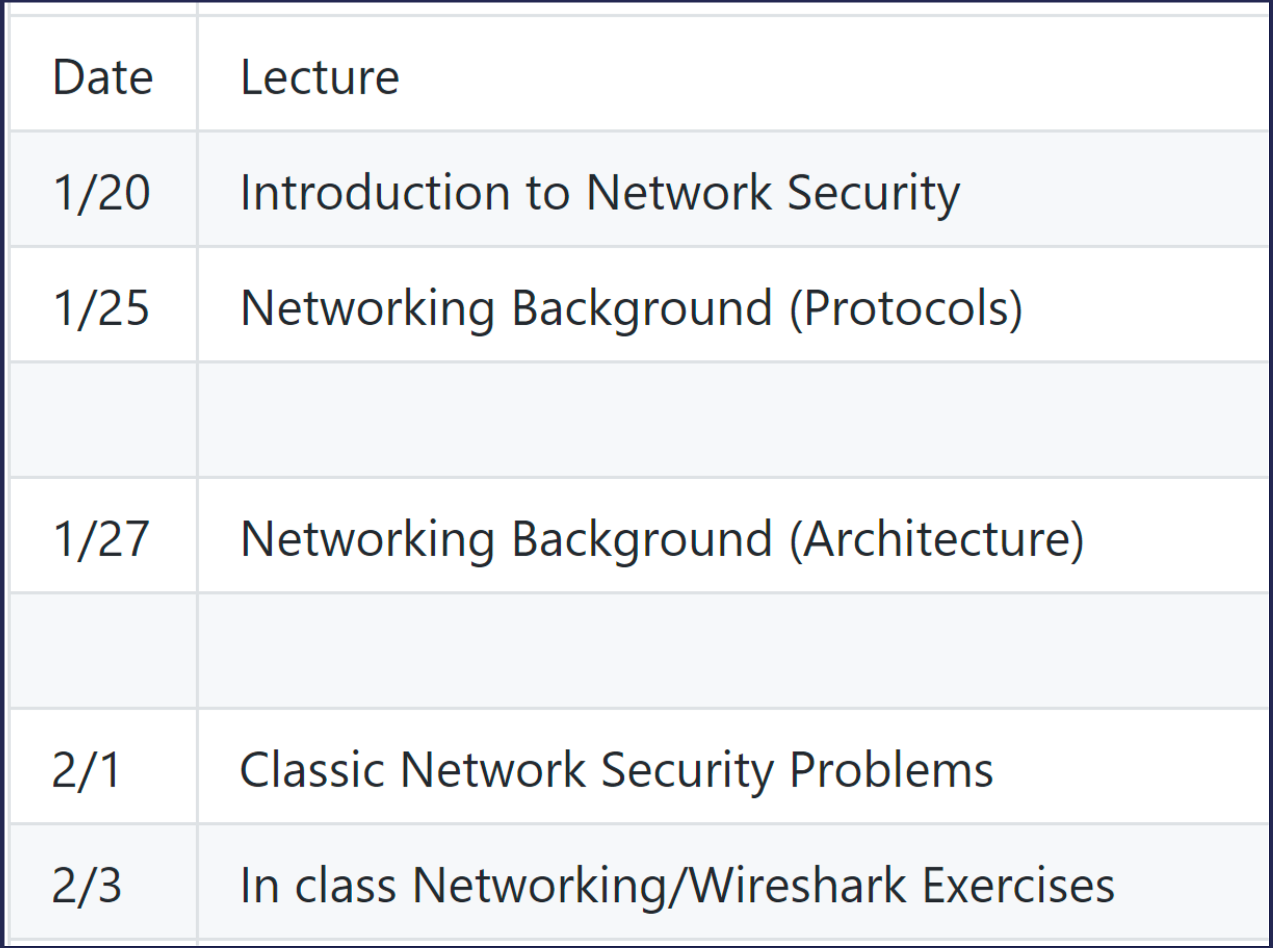
UTAustin-Courses / 2021sp_cs361s /



fall2021utcs361s

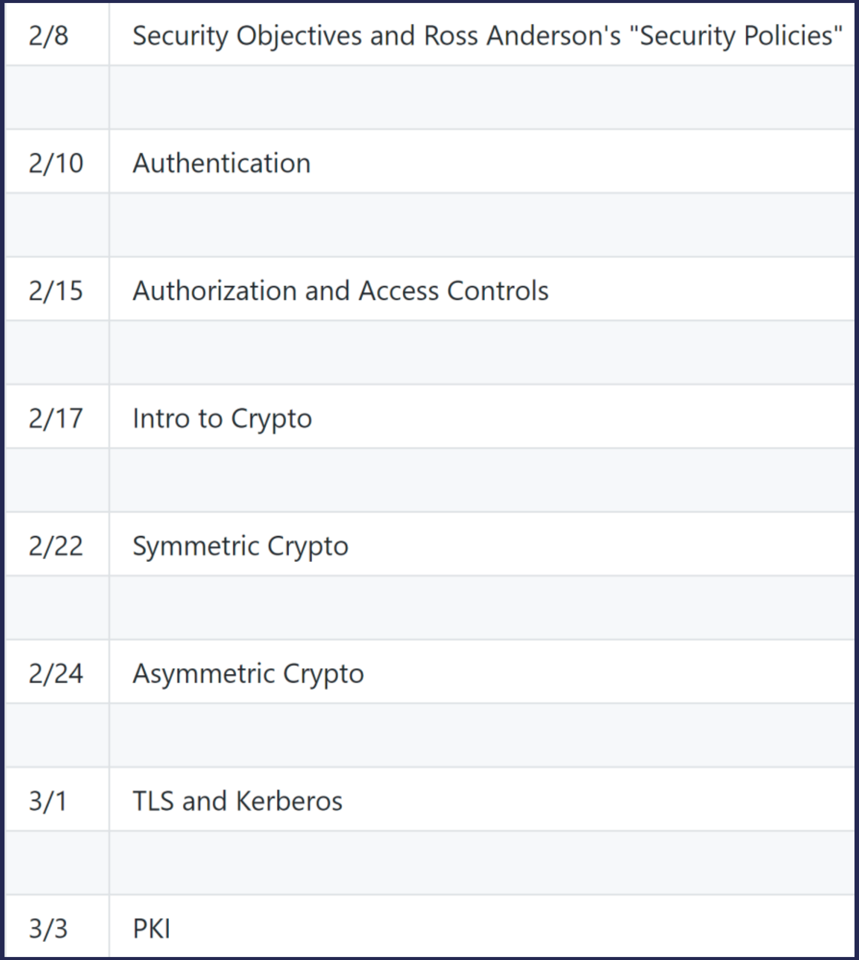
fall2021utcs361s.slack.com

Schedule Part 1
Network Background



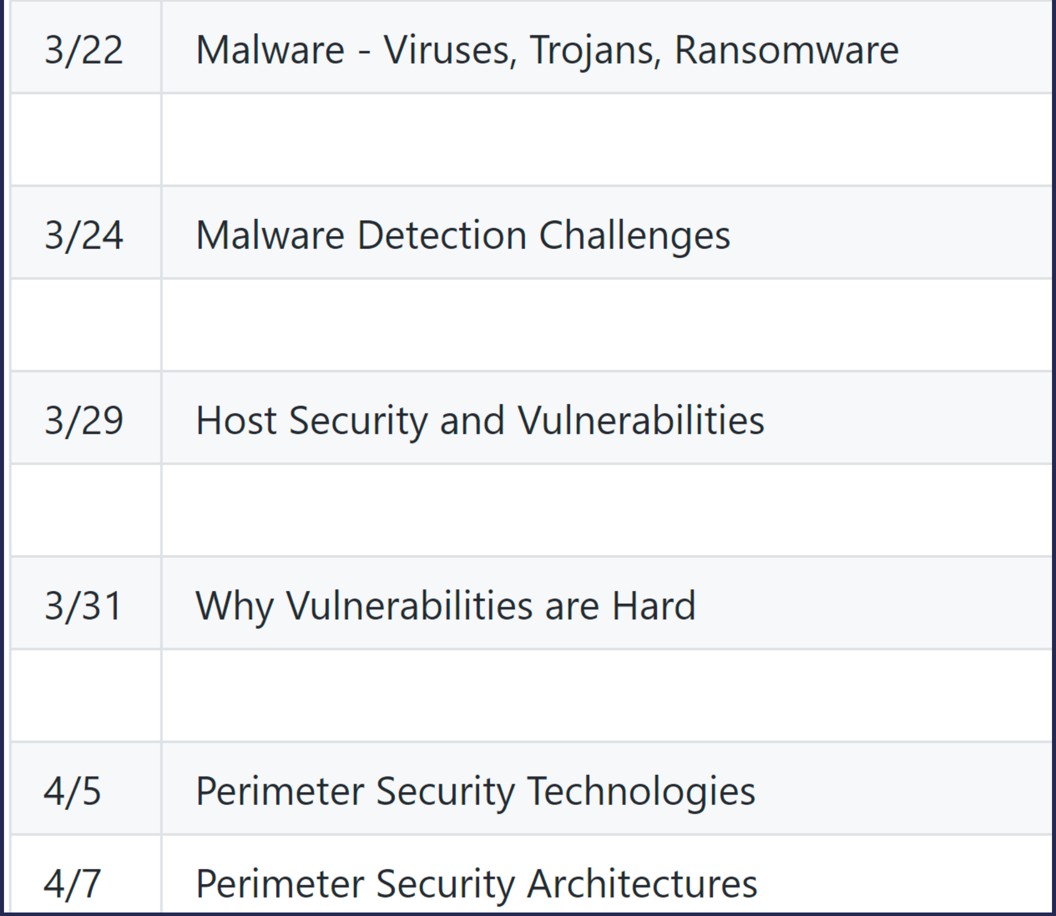
Date	Lecture
1/20	Introduction to Network Security
1/25	Networking Background (Protocols)
1/27	Networking Background (Architecture)
2/1	Classic Network Security Problems
2/3	In class Networking/Wireshark Exercises

Schedule Part 2
Security Foundation



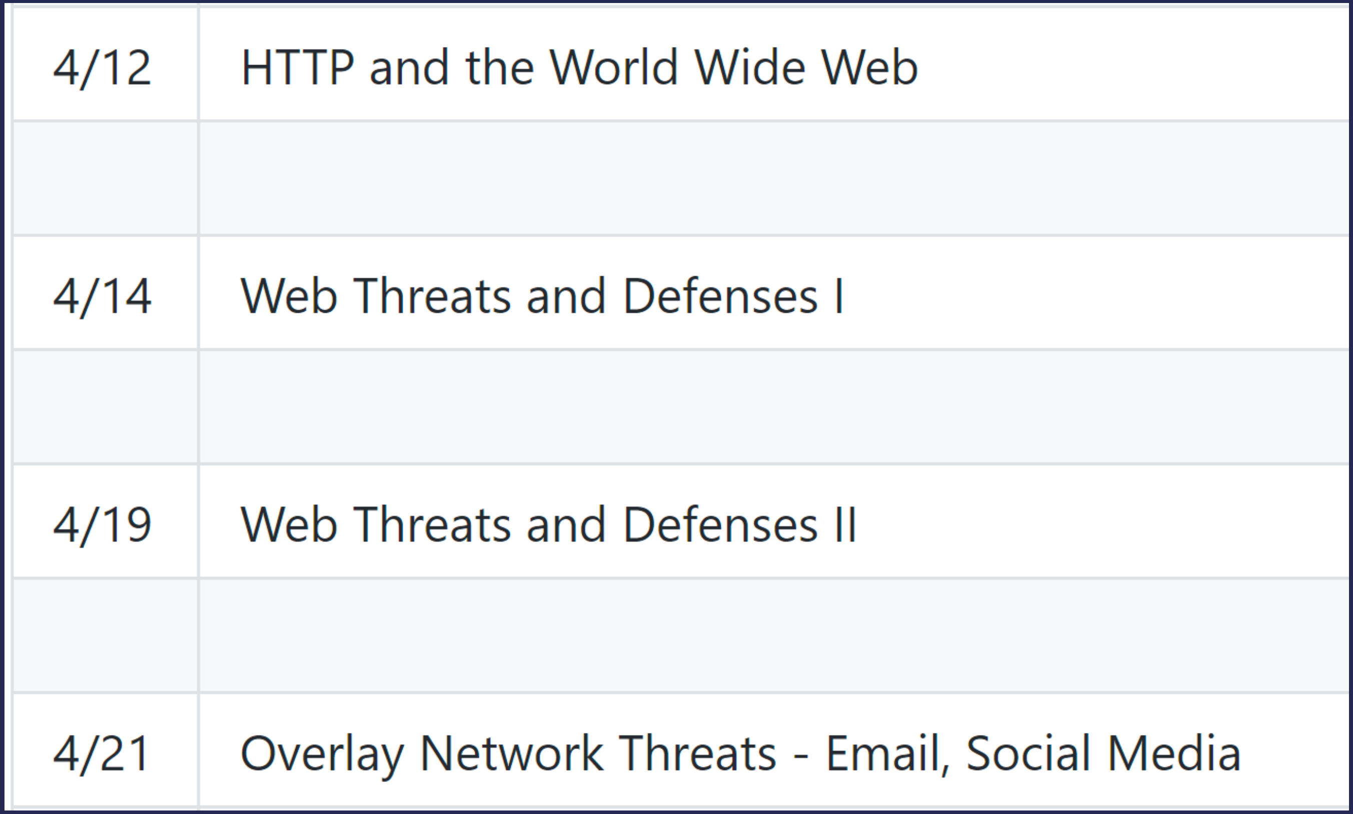
2/8	Security Objectives and Ross Anderson's "Security Policies"
2/10	Authentication
2/15	Authorization and Access Controls
2/17	Intro to Crypto
2/22	Symmetric Crypto
2/24	Asymmetric Crypto
3/1	TLS and Kerberos
3/3	PKI

Schedule Part 3
Hosts and LANs



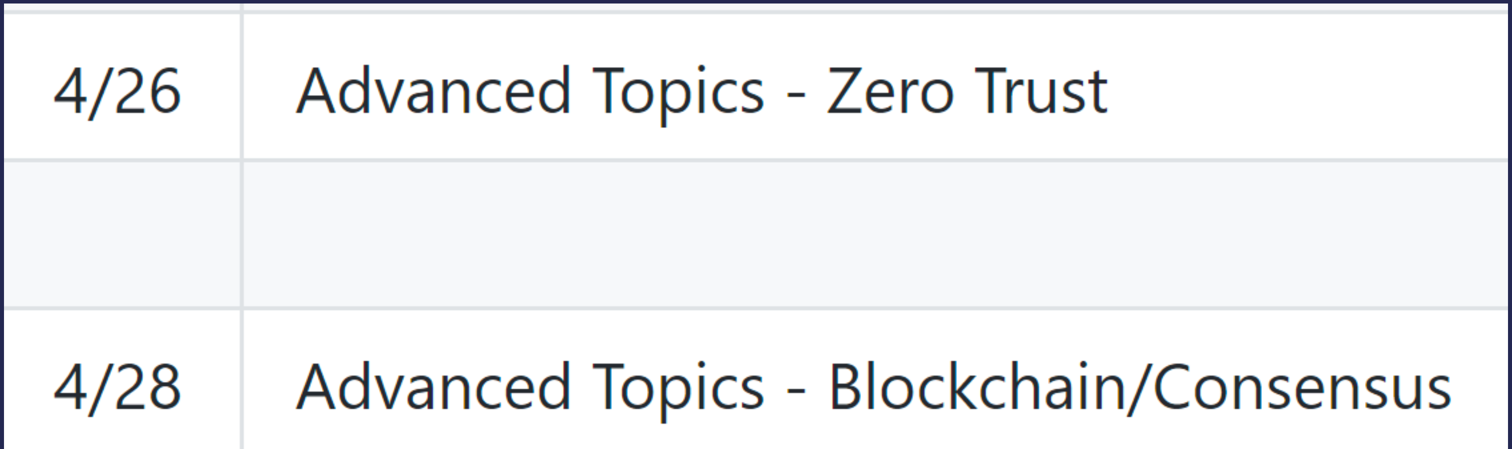
3/22	Malware - Viruses, Trojans, Ransomware
3/24	Malware Detection Challenges
3/29	Host Security and Vulnerabilities
3/31	Why Vulnerabilities are Hard
4/5	Perimeter Security Technologies
4/7	Perimeter Security Architectures

Schedule Part 4
The Wider Internet



4/12	HTTP and the World Wide Web
4/14	Web Threats and Defenses I
4/19	Web Threats and Defenses II
4/21	Overlay Network Threats - Email, Social Media

Schedule Part 5
Advanced Topics



4/26	Advanced Topics - Zero Trust
4/28	Advanced Topics - Blockchain/Consensus

Class Discussions

- I hate slides and I hate “lectures”
- I only use them because I haven’t found something better
- Please read before class, come prepared to discuss
- You will be assigned to discuss out-of-class as well

Grading

- 60% labs
- 10% participation
- 30% Exams
  - 2 Midterms
  - No Final
  - 15% each

Readings

- I’ve tried a bunch of books. I hate them all
- All free materials available online
- Ross Anderson’s “Security Engineering”
  - This IS a great book
  - Second edition is free online

Reading Policies

- Read before class for class discussion
- Each week, in groups, discuss previous week’s reading
- Discuss via text-based system and submit transcript

Labwork

- Lab 1 – In class networking. Almost a freebie
- Lab 2 – Authentication/Authorization
- Lab 3 – TLS
- Lab 4 – Return Oriented Programming
- Lab 5 – Web-based CTF exercises

Labwork Policies

- **PASS/FAIL** – Not worth it to do part
- Code alone, debug in assigned groups
- 10% off per day late
- Any one lab can be redone for no penalty

Exams

- Essay based thought questions
- Open book, open note
- I hate memorization/regurgitation
- Usually involve a hypothetical

Exam Sample Question

Every one complains about passwords and that they need to be replaced. Although every now and then someone comes up with a new replacement but they never seem to get much traction, so the search continues. Regardless of whatever new technology comes along to replace passwords, there are certain fundamental problems that will have to be solved. Write an essay explaining what kinds of evaluations YOU would do for a password-replacement technology.

Do not speculate about how this imaginary technology works, just imagine it to be some kind of “black box” authentication mechanism. Instead, focus your essay on the psychological, technical, and perhaps even mathematical problems that you would require it to solve or address before you believed it to be a “good” replacement. Because this is hypothetical, you can address this from a number of different angles. Your score for this essay will be based on how well you understand user authentication including principles related to “something you know”, “something you have”, and “something you are.” You may also get score for applying Anderson’s concepts on user psychology and security engineering.

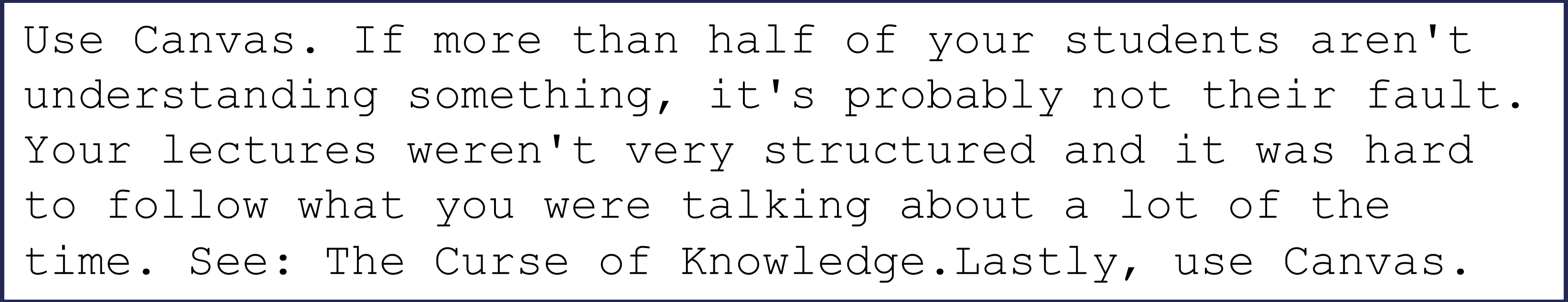
Grading

- Standard Scale
- Last semester, average was about 91%
- This semester, targeting 87%

Past Student Comment - #1

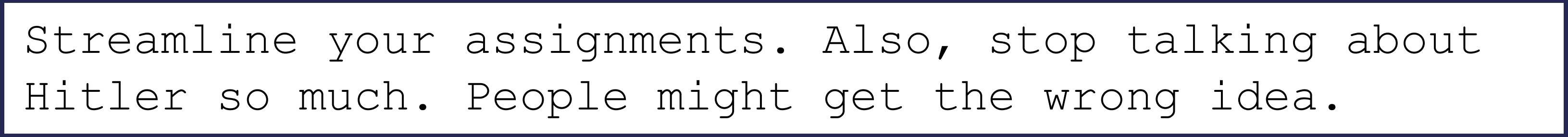
While the course material covered was interesting, I felt that we skimmed over many advanced concepts. Too much of the course was focused on obvious security considerations rather than the backing theory. The professor seemed to not always have a great grasp over the concepts, which made some explanations hard to grasp. Despite this, the professor made himself available a great deal to the class, and he was an enthusiastic lecturer. I think this course would be great with just a few tweaks.

Past Student Comment - #2



Use Canvas. If more than half of your students aren't understanding something, it's probably not their fault. Your lectures weren't very structured and it was hard to follow what you were talking about a lot of the time. See: The Curse of Knowledge.Lastly, use Canvas.

Past Student Comment - #3



Streamline your assignments. Also, stop talking about Hitler so much. People might get the wrong idea.

Past Student Comment - #4

I almost dropped the course because the first two labs were incredibly difficult for me and I wouldn't even know where to begin. Especially for the first lab. I've never cried because of a lab, but lab 1 made me cry due to the amount of frustration I had. The lectures were more theory based, so when it came to actually practicing this I didn't know where to begin, and the instructions were not very helpful and assumed a lot of prior knowledge…

Constructive Criticism

- Please let me know when you don't understand something
- Please let me know when you think I don't understand
- Please let me know when I offend you
- Please be specific

Early Criticism

- I would prefer criticism *before* the class reviews
- It gives me a chance to improve before being evaluated
- You may send anonymous emails if you need anonymity

Evaluation Policy

- Evaluation will now be mandatory and in-class
- Proof of submission required
- Factored into participation grade (3%)
- Reminder: comments are part of my ***permanent record***