NETWORK SECURITY AND PRIVACY

UT CS361S

Fall 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?

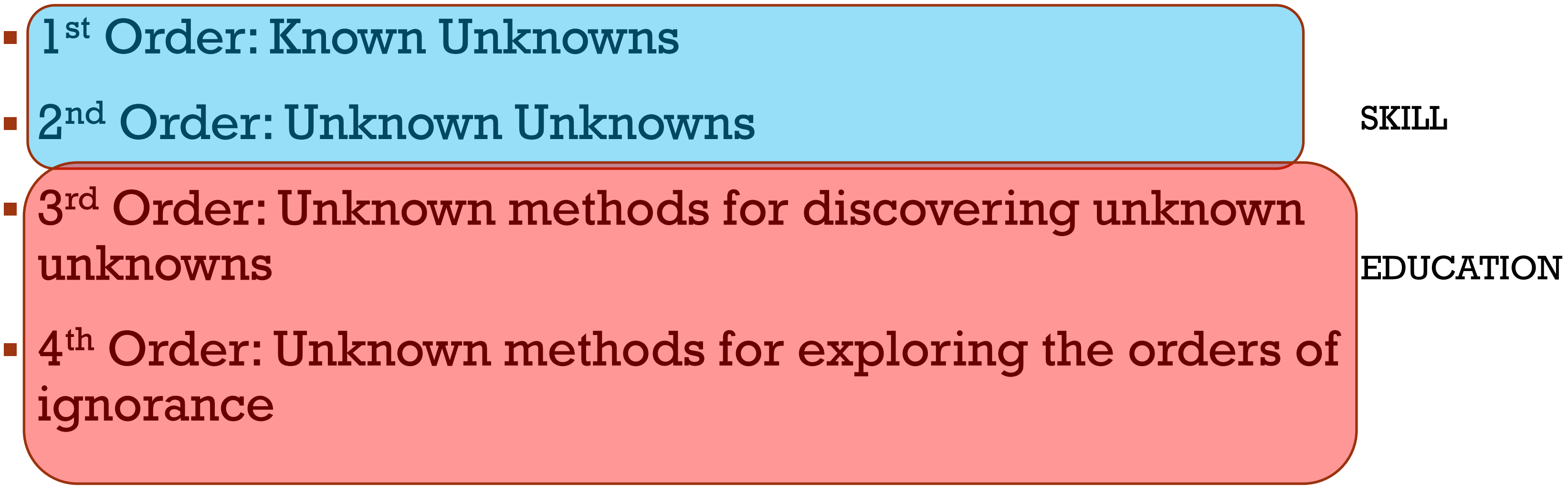
THE 5 ORDERS OF IGNORANCE

- 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

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…

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

GRADING

NO EXAMS!

- 60% labs
- 30% In-class Labs
  - We will do these together
  - Finish later if you miss class
  - (Class is Recorded)
- 10% Reading discussions

IN-CLASS MINI LABS (5% EACH)

- Lab 1 – Buffer Overflow and GDB
- Lab 2 – Networking and Wireshark
- Lab 3 – Cryptography 1
- Lab 4 – Cryptography 2
- Lab 5 – HTTP and Web
- Lab 6 – Cookies

LABWORK (10% EACH)

- Lab 1 – Return Oriented Programming
- Lab 2 – Authentication/Authorization
- Lab 3 – TLS 1.2 Server
- Lab 4 – TLS Visibility
- Lab 5 – Oauth SSO
- Lab 6 – CTF Exercises

LABWORK POLICIES

- Bare minimum requirements for each lab
- 80% score if minimum requirements reached
- ZERO POINTS if minimum requirements not met
- Code alone, debug in assigned groups
- 10% off per day late to a maximum of 50%
- Any one lab can be redone for no penalty by end of class

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

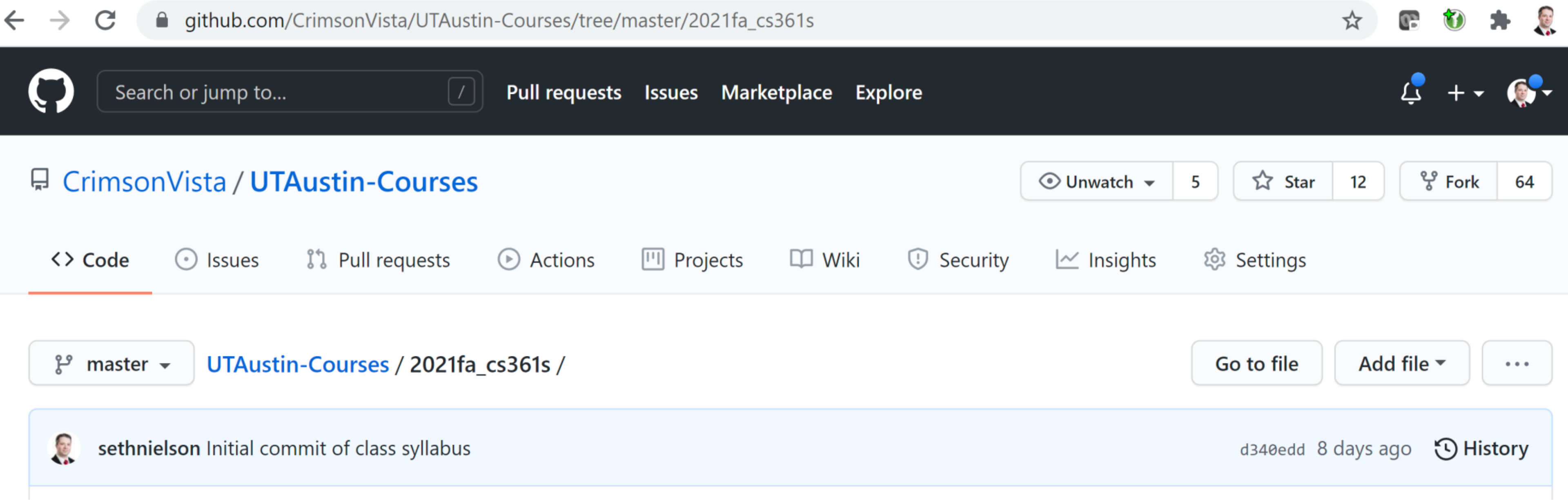
READING POLICIES

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

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

TWO RESOURCES

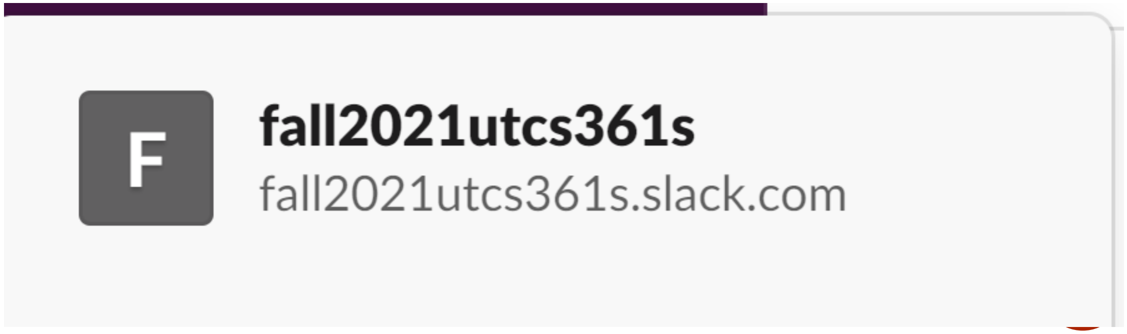


github.com/CrimsonVista/UTAustin-Courses/tree/master/2021fa_cs361s

CrimsonVista / UTAustin-Courses

UTAustin-Courses / 2021fa_cs361s /

sethnielson Initial commit of class syllabus d340edd 8 days ago



fall2021utcs361s

fall2021utcs361s.slack.com

TYPICAL SECURITY OBJECTIVES

- Confidentiality
- Integrity
- Availability

- (CIA Triad)
- (See, NIST 800-12)

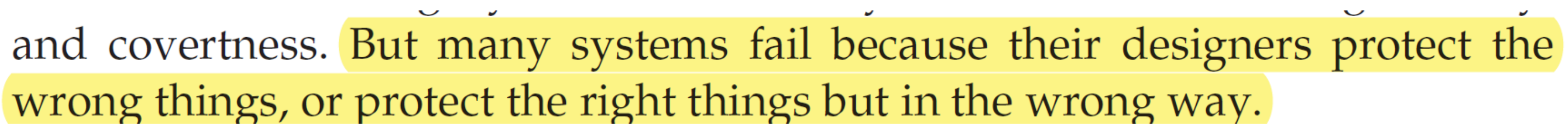
SECURITY ENGINEERING

- “[It] is about building systems to remain dependable in the face of …”
  - Malice
  - Error
  - Mischance.
- “As a discipline, it focuses on the…”
  - Tools
  - Processes
  - Methods

APPLICATION

- Confidentiality, Integrity, Availability
- For new systems:
  - Design security
  - Implement security
  - Test security
- For existing systems:
  - Adapt them for increased security
  - Adapt them as their *environment* evolves

KEY OBSERVATION

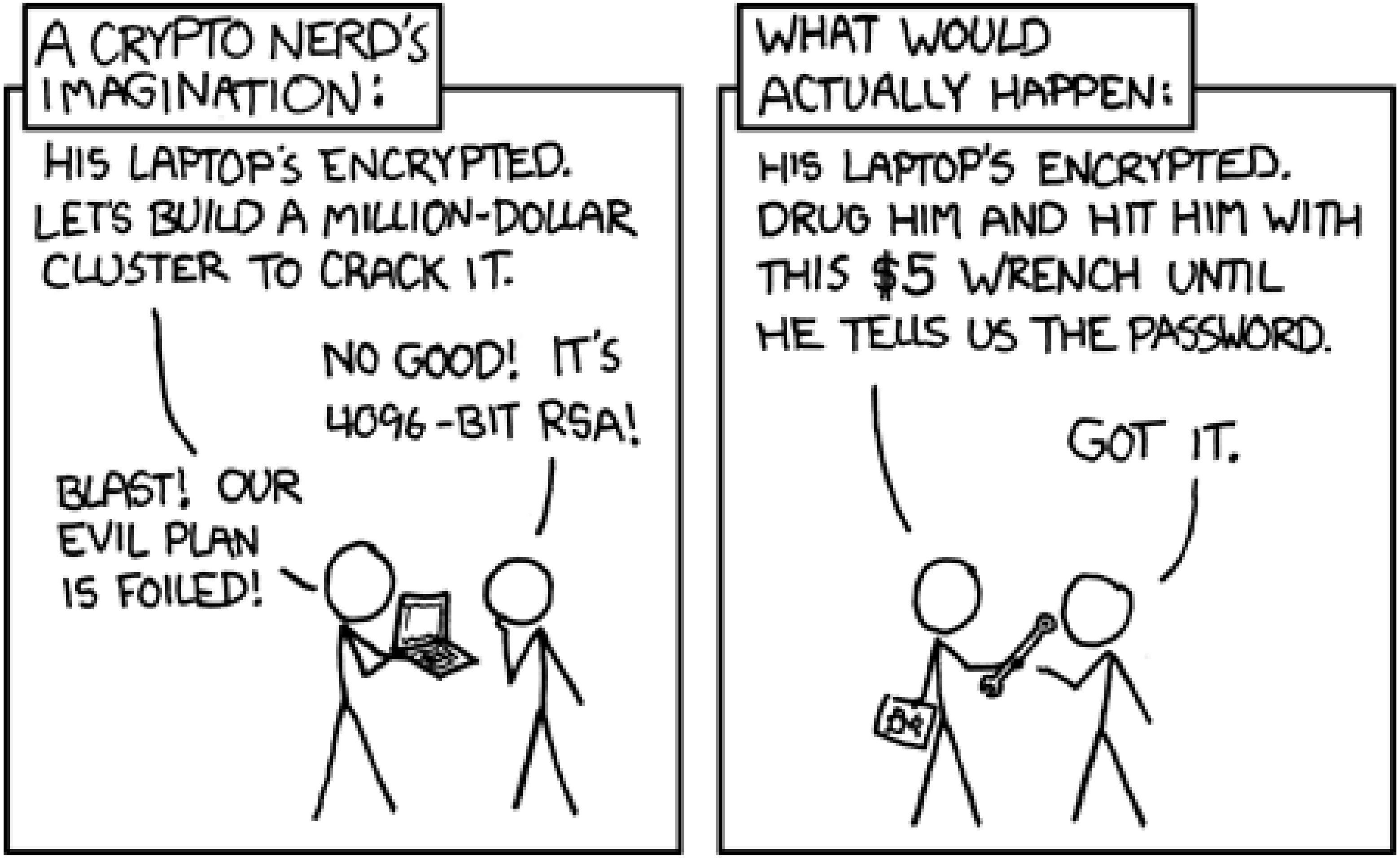


and covertness. But many systems fail because their designers protect the wrong things, or protect the right things but in the wrong way.

Anderson, Ch 1, p. 4

ILLUSTRATIONS

- See http://xkcd.com/538/


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

A FRAMEWORK

- Policy
- Mechanism
- Assurance
- Incentives

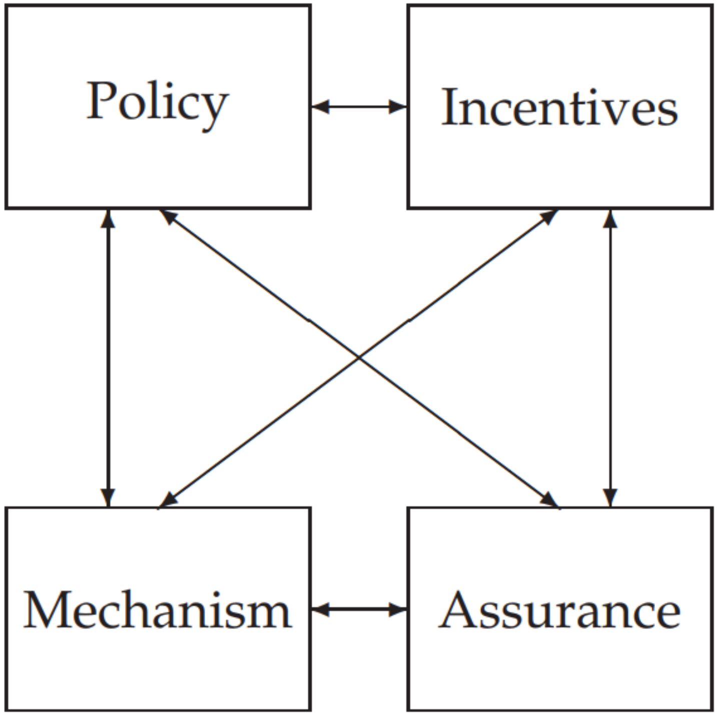


Figure 1.1: Security Engineering Analysis Framework

START WITH POLICY

- "…a succinct statement of a system's protection strategy" (Anderson ch1 p. 15)
- Examples:
  - Each credit must be matched by an equal and opposite debit
  - All transactions over $1,000 must be authorized by two managers
- Practice:
  - What are the security policies for TLS?

THEN FIGURE OUT MECHANISM

- This is where most security people like to start
- But really we only need mechanism to enforce policy
- Some mechanisms aren’t even technical (e.g., legal)
- MUST understand *threat model*

INCENTIVES

- Anderson’s example of airport security
- What motivates the behavior?
- What is “Security Theater?”
- Everyone should learn a little game theory
  - Read up on Prisoner’s dilemma
  - Understand “mechanism design”
  - Anderson’s “Moral Hazard” (Chapter 25)

ASSURANCE

- Just how strong/resilient/comprehensive is the mechanism?
- Requires a solid understanding of the threat model
- Applications at every stage!
  - Design – solid security engineering principles
  - Implementation – coding practices, development processes
  - Testing – adversarial, comprehensive assessment

IN THIS CLASS

- Focus on **POLICY and MECHANISM**
- In **NETWORK SECURITY**
- Much of our focus will be on network protocols/systems
  - Cryptographic protocols like TLS
  - Authentication/Authorization protocols like OAuth/OIDC
  - Web security mechanisms
- Touch on other elements:
  - Host security
  - Incentives
  - Assurance