Intro to Cybersecurity

UT LAW 379M

Spring 2022

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 technology 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

SKILL

- 3rd Order: Unknown methods for discovering unknown unknowns
- 4th Order: Unknown methods for exploring the orders of ignorance

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

Course Objectives

- Learn some basics about technology
- Learn about how technology protects systems
- Learn about how attackers get in anyway
- Learn ***principles*** that allow you to evaluate technology

Schedule And topics

PART 1 – Tech Background

- How Computers Work
- How Networks Work
- Network Lab

PART 2 – Core Security

- Psychology
- Authentication/Authorization
- Cryptography
- Password Lab

Schedule And topics

PART 3 – Protecting the Internet

- Protecting Computers
- Protecting Local Networks
- Protecting the Web
- Browser Security Lab

PART 4 – Contemporary Security

- Email and Social Media
- SOTA Technologies
- Phishing Competition

Technology Evaluation

- Forces behind design/development
- Intended Purpose
- Feature Set
- Strengths and Weaknesses
- Context and Requirements
- Deployment in Practice
- Lessons Learned

Evaluation of New Tech

- GOAL: You can evaluate tech at a basic level
- Especially cut through the vendor marketing
- No technology is “magic”
- Governed by principles
- Use the principles to understand the specifics

Peek Ahead Example

- Authentication is verifying an identity
- Three basic approaches
  - Something you know (passwords)
  - Something you have (phone or security token)
  - Something you are (biometrics)
- Knowing just this better enables you to evaluate

Team Presentations

- Every student assigned a team
- Teams discuss reading together
- Teams also do presentations on technology
    - First presentation: Survey of technologies
    - Second presentation: Evaluation of specific technology

Presentation Details

- I will provide a list of technologies to choose from
- Your team will sign up for a time in class to present
- Refer to the assignment page for more details.

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
- For each reading, discuss using canvas comments

Grading

- 40% labs (10% each)
- 10% participation
- 20% presentations (10% each)
- 30% Exams (15% each)
  - 1 Midterm (Mar 7 – 11)
  - 1 “floating” Final (Due May 12)

Readings

- I’m writing a book. I think it’s pretty good.
- Most readings come from preprints (drafts) of the book
- YOU MUST NOT SHARE OR DISTRIBUTE
- You can get a copy when it is published later this year
- Some additional online readings/videos

Labwork

- lab 1 - Wireshark and Browsing
- lab 2 - Password Cracking
- lab 3 - Certificates and Public Keys
- lab 4 - Phishing Contest

Labwork Policies

- **PASS/FAIL** – Not worth it to do part
- You may talk to other students about the labs
- But you must do your own work
- I also will provide help sections as needed

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 93%
- This semester, enforcing law school curve
- The curve must apply to law students
- Non-law students will be slotted into the curve as well

Introducing Cybersecurity

- This is a very broad concept
- Includes concepts of technology, psychology, etc etc
- Where to start?
- Let’s start with Ross Anderson’s “Security Engineering”

What is “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

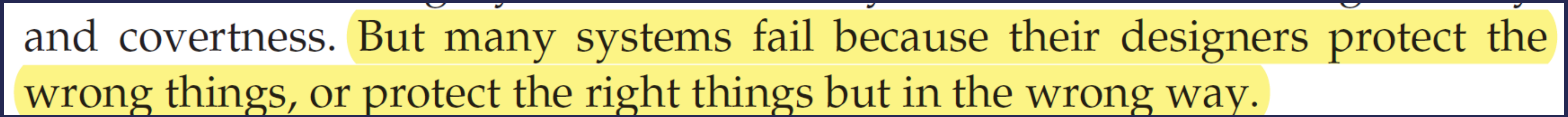
The Goal

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

“Having” Security

- Everyone wants “security”. But how?
- “***Whoever thinks his problem can be solved using cryptography, doesn’t understand his problem and doesn’t understand cryptography.***”
  - — Attributed by Roger Needham and Butler Lampson to Each Other

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

A Framework

- Policy
- Mechanism
- Assurance
- Incentives

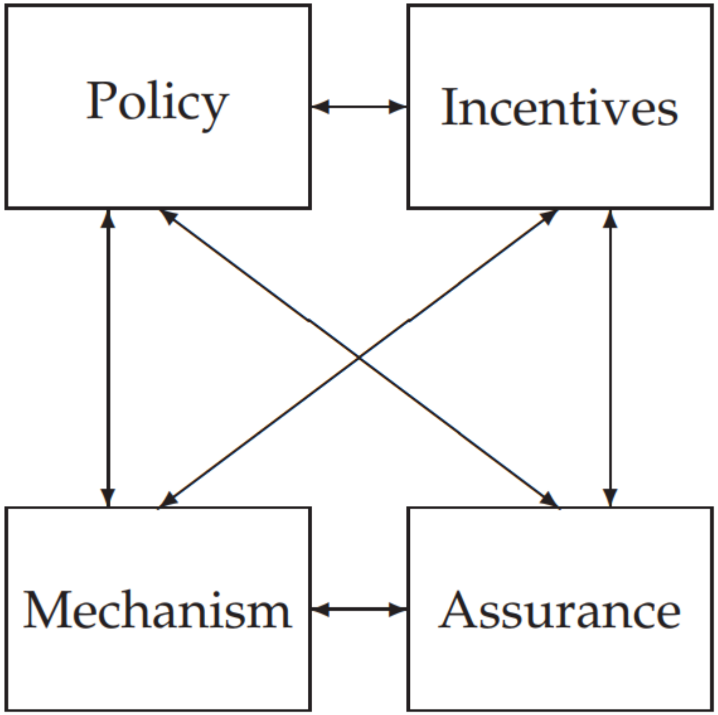


Figure 1.1: Security Engineering Analysis Framework

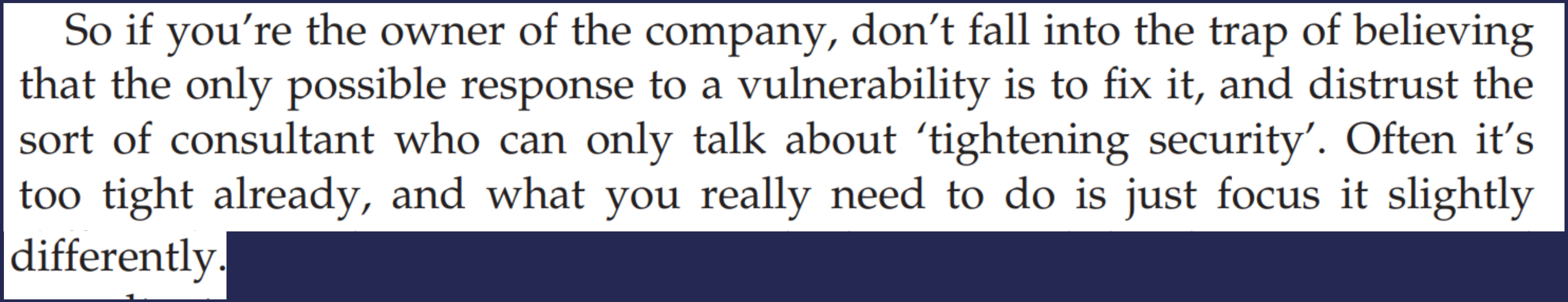
Some Definitions

- System – Tech + Auxiliary Tech + Staff + Users + etc.
- Subject – Physical “person”
- Principal – Entity in the system
- Identity – Unique label attached to a unique principal
- Trusted – Failure results in compromise
- Trustworthy – Failure is unlikely

CIA (Not the Spies)

- Confidentiality – Cannot be read
- Integrity – Cannot be altered
- Availability – Cannot be interrupted

Understand This



So if you’re the owner of the company, don’t fall into the trap of believing that the only possible response to a vulnerability is to fix it, and distrust the sort of consultant who can only talk about ‘tightening security’. Often it’s too tight already, and what you really need to do is just focus it slightly differently.

Anderson, Ch 25, p. 816

Anderson’s Examples

- Bank
- Military
- Hospital
- Home

IAAA

- Identity – Unique label for a unique principal
- Authentication – Validation of the principal's identity
- Authorization – Permissions granted the prinicpal
- Accountability – Metering and auditing of principal

- (Message Authenticity – Integrity + Freshness)

Grasp the Context

- SECURITY IS ABOUT CONTEXT (Repeat after me)
- What does it mean when you say "system *X* is secure"?
  - Secure against *whom*?
  - Secure under *what conditions*?
  - Are we even protecting what matters?!
- Take voting security
  - Who are the potential attackers?
  - How does the context change if a nation decides to be the attacker?

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*

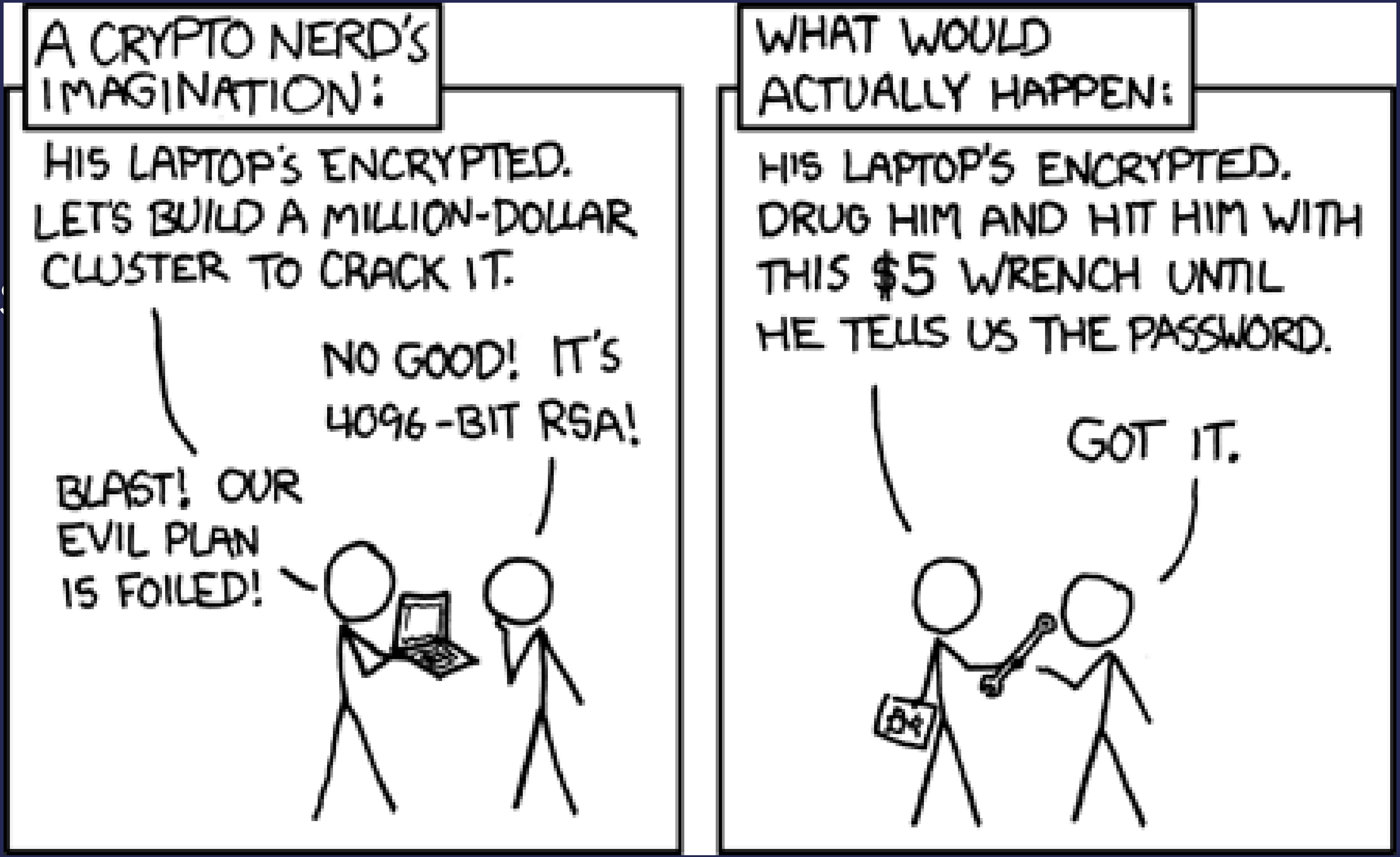
Assurance

- 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

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)

Illustrations


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.

Important Security Principles

- Least privilege
- Minimize attack surface
- Defense in depth
- Separation of duties and responsibilities
- Crowdsourcing
- Open systems
- Fail Safe/Fail Secure

Course Goals

- Understand how secure systems are constructed
  - Underlying concepts, such as policy and mechanism
  - Tools, such as cryptography
  - Systems, such as perimeter defense
- Understand how “secure” systems are deconstructed (attacked)
  - Underlying concepts, such as “halting problem”
  - Tools, such as vulnerabilities
  - “Systems” such as Advanced Persistent Threats