The Technology of Cybersecurity

UT LAW 396V

Spring 2024

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?

A Few Introductory Notes

This course continues to develop and evolve

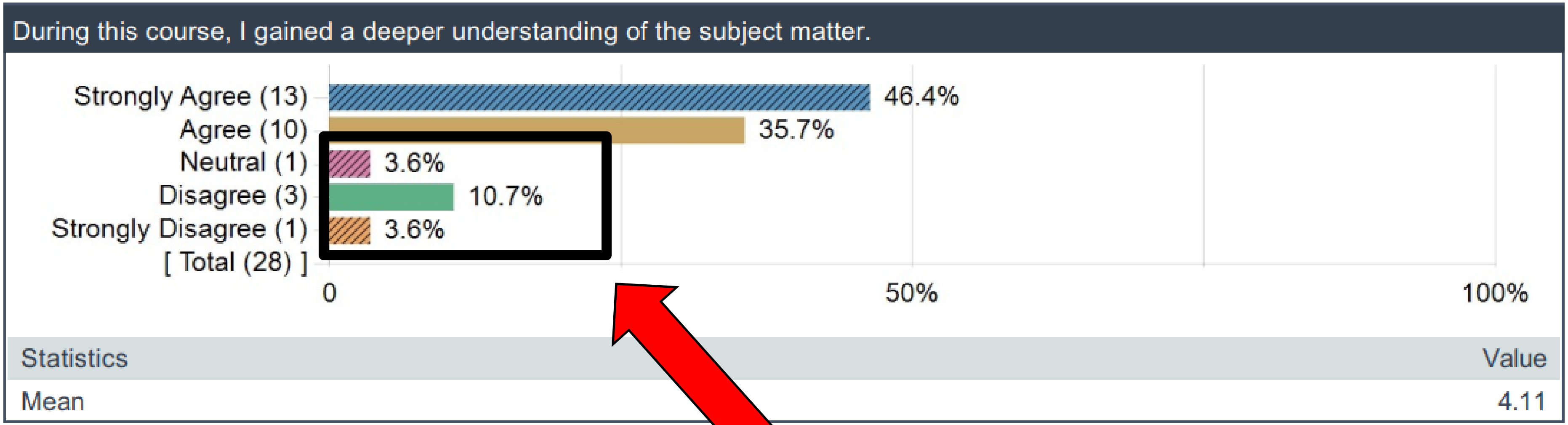
I make changes based on what works and what doesn’t

Every semester has new labs and assignments

Textbook is published! (***but it is not perfect***)

Please feel free to make suggestions or raise concerns

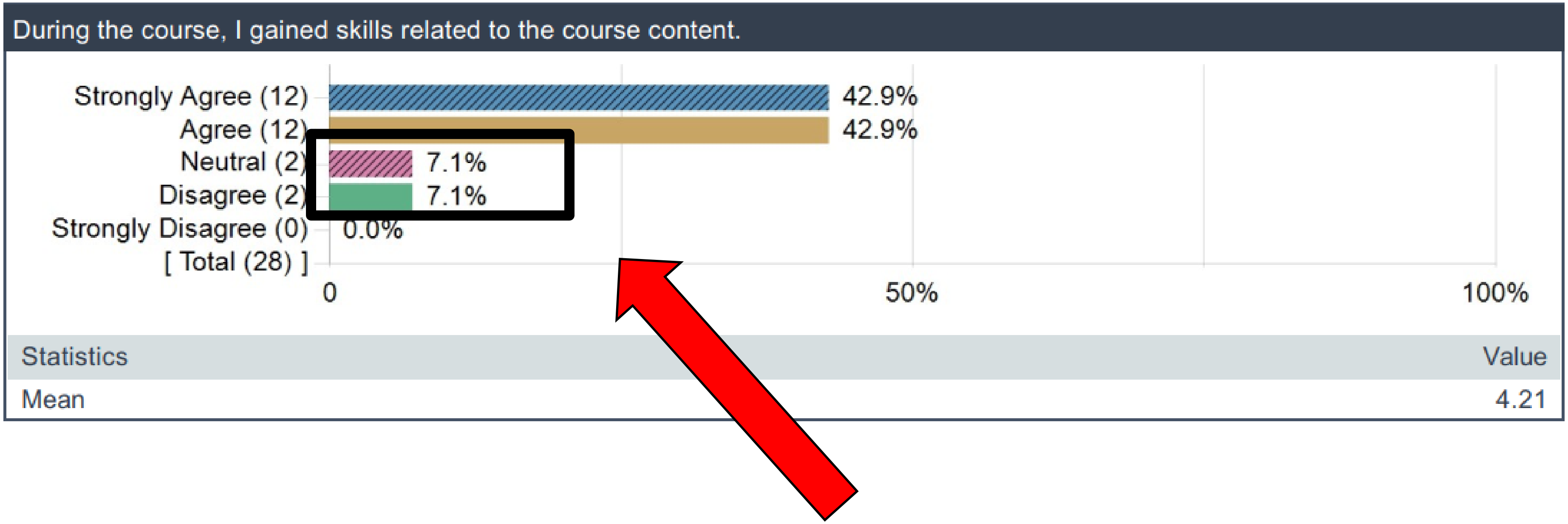
Review of Spring 2023 Feedback


During this course, I gained a deeper understanding of the subject matter.

Statistics	Value
Mean	4.11

This **really** surprised me.

Review of Spring 2023 Feedback

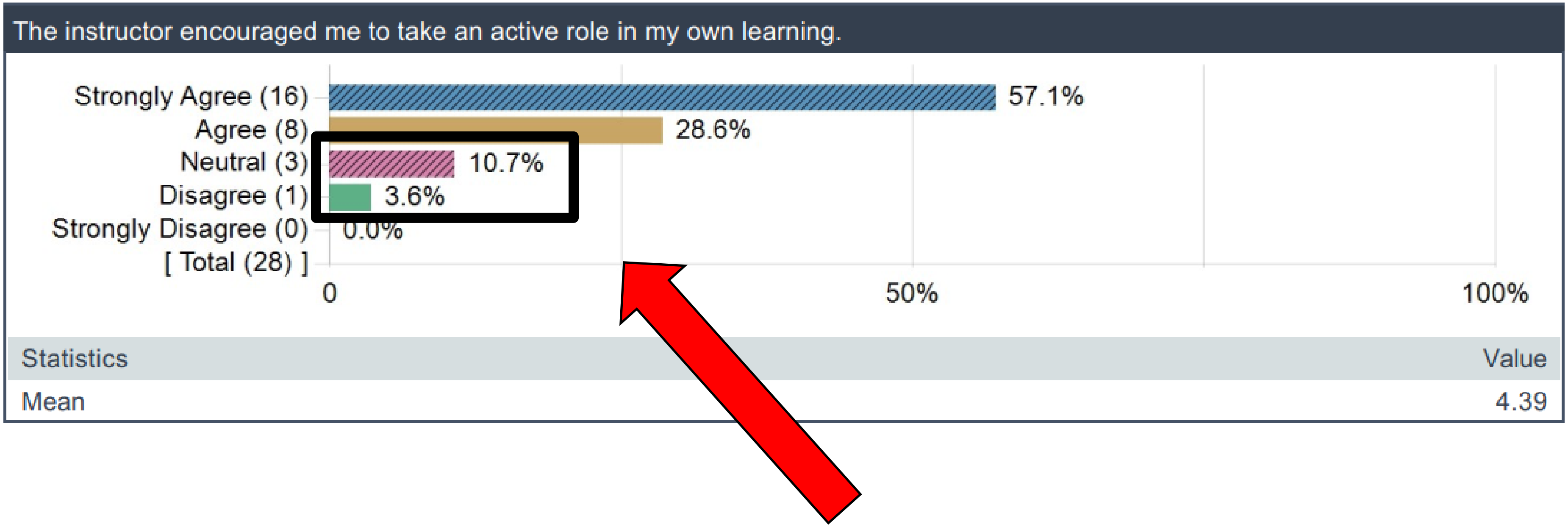


During the course, I gained skills related to the course content.

Statistics	Value
Mean	4.21

How is this possible?

Review of Spring 2023 Feedback



The instructor encouraged me to take an active role in my own learning.

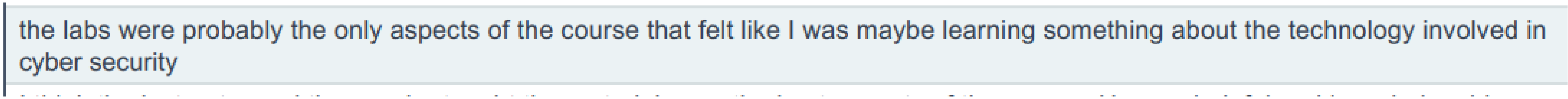
Statistics	Value
Mean	4.39

Ok, seriously?

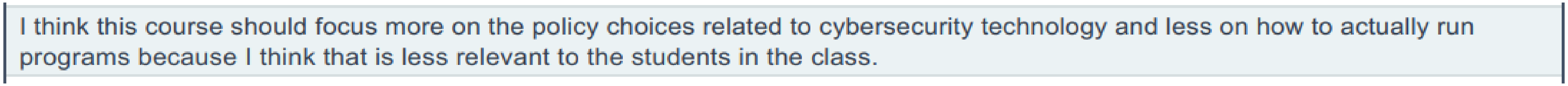
Your Responsibilities

1. If you don’t feel like you’re understanding, ***come talk to me***
2. If you don’t get new skills, ***come talk to me***
3. You will largely decide your outcomes in this class

More Interesting Feedback



the labs were probably the only aspects of the course that felt like I was maybe learning something about the technology involved in cyber security



I think this course should focus more on the policy choices related to cybersecurity technology and less on how to actually run programs because I think that is less relevant to the students in the class.

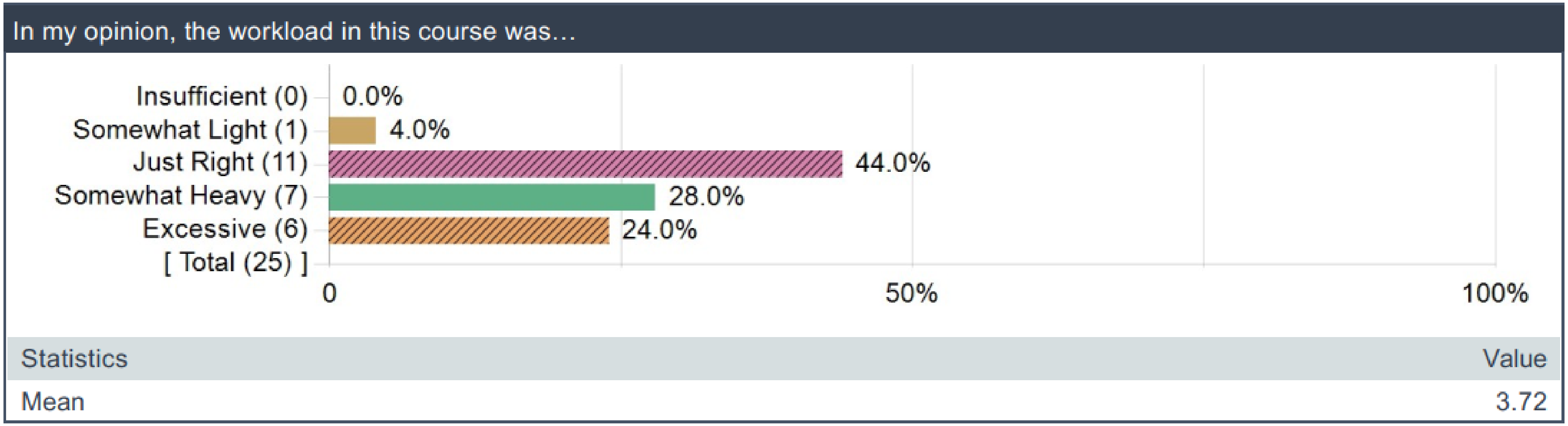
This is a Technical Class

1. If you don’t think it’s technical, ***you don’t understand***
2. There are other policy classes. ***This is not one of them***.
3. I was asked to teach at technical class.

…For Students with No Background

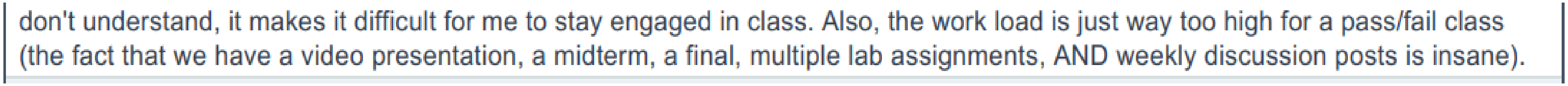
1. This is insanely hard to do
2. I have put in hundreds of hours trying to find ways to do it
3. *It works best when YOU work WITH me*

Workload Feedback

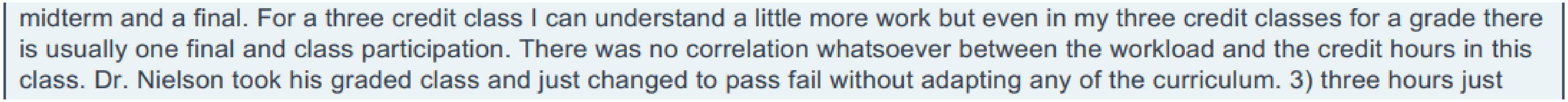


In my opinion, the workload in this course was…

Statistics	Value
Mean	3.72



don't understand, it makes it difficult for me to stay engaged in class. Also, the work load is just way too high for a pass/fail class (the fact that we have a video presentation, a midterm, a final, multiple lab assignments, AND weekly discussion posts is insane).



midterm and a final. For a three credit class I can understand a little more work but even in my three credit classes for a grade there is usually one final and class participation. There was no correlation whatsoever between the workload and the credit hours in this class. Dr. Nielson took his graded class and just changed to pass fail without adapting any of the curriculum. 3) three hours just

No Good Deed Goes Unpunished

This class was not originally pass/fail

But I felt the curve was unfair for material that was new

We switched to pass/fail to not mess with grades

But the workload remains the same

Any questions?

Please Don’t Whine at the End

I am very approachable

I never retaliate

I really want students to learn

I teach part time because I love teaching

Early, constructive feedback is better for me and you

The 5 Orders of Ignorance

0th Order: Known Knowns

1st Order: Known Unknowns

2nd Order: Unknown Unknowns

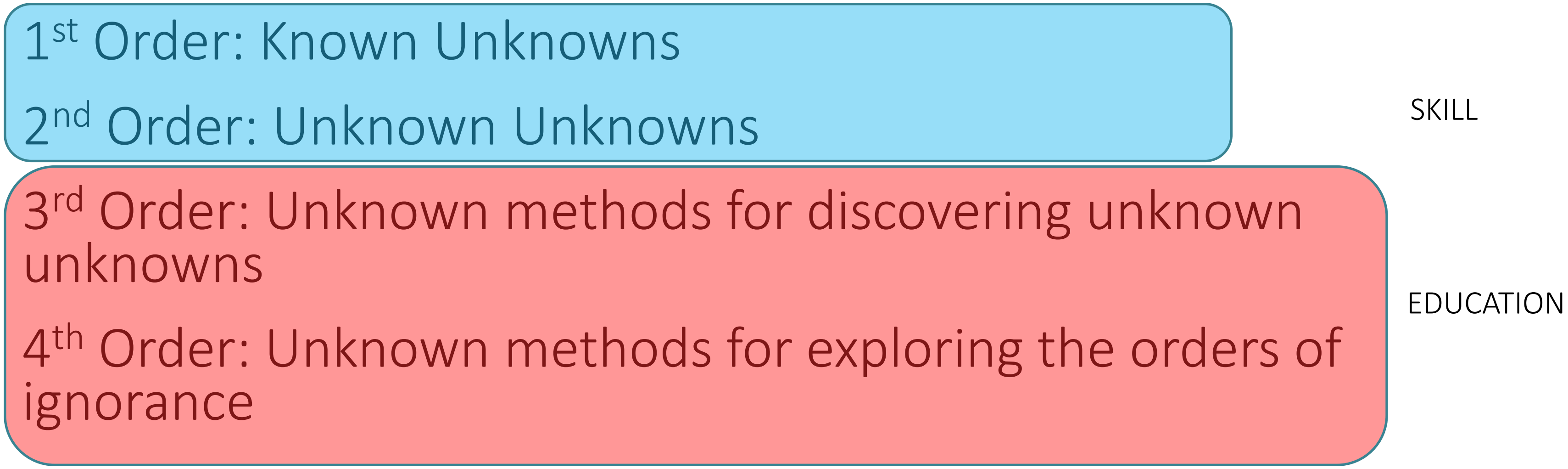
3rd Order: Unknown methods for discovering unknown unknowns

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”)

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

Syllabus Review

Review Schedule

Review Topics

Review Reading

Review Labs

Review Midterms

Why These Topics?

Cybersecurity is broader than you can imagine

I had to pick a small subset of topics

And I had to include enough background for these topics

This is my best effort to pick the right set of topics

If you have other interests, please send me requests by email

Class Discussions

I hate slides and I hate “lectures”

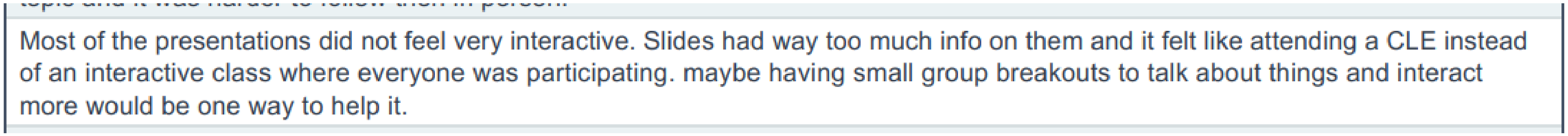
I only use them because I haven’t found something better

Please read before class, ***come prepared to discuss***

In an effort to make this easier, you can text me questions:

410-497-7384

More Feedback



topic and it was harder to follow then in person.

Most of the presentations did not feel very interactive. Slides had way too much info on them and it felt like attending a CLE instead of an interactive class where everyone was participating. maybe having small group breakouts to talk about things and interact more would be one way to help it.

This one actually made me really frustrated

I added in all the in-class labs to make it better

Also, ***I practically beg you students to participate***

You want it more interactive? ***COME PREPARED TO DISCUSS***

Readings

I wrote the textbook for this class

Previous classes got the preprints

You are the first class to get a published version

It can still improve; please be willing to help future students

ASSIGNMENT: Post a discussion/comment for each reading

Labwork

lab 1 - Class contract, binary numbers, learning about your computer

lab 2 - Password Cracking

lab 3 - Ransomware Lab

lab 4 - Phishing Contest

(Note, this last lab is easy and fun)

In-class Experiences (ICX)

lab 1 - Binary, Mini Processor Demo

lab 2 - Symmetric/Asymmetric Cryptography

lab 3 - Wireshark, Creating a Secure Authenticated Channel

lab 4 - Website Cookie Demo

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

Individual Presentations

Students will record themselves teaching a lecture

You will pick the class topic you wish to teach

You will share a YouTube video with me

I request them to be public (private if you must)

They do need to be visible to other classmates

Presentation Details

Your video is due by the last day of class (2024-04-29)

You will also watch 2 videos of classmates

Please submit a brief 1 paragraph review for each

Due by the end of finals

Grading

Ha Ha, Just kidding. It’s Pass/Fail

You must complete all labs and in-class experiences (ICXs)

10/12 readings

Pass on both midterms

Submit your video and watch/review 2 others

Midterm Exams

Essay based thought questions

Open book, open note

I hate memorization/regurgitation

Usually involve a hypothetical

REQUIRED CHAT-GPT

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

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.

New This Semester

Stories, stories, stories

Marketing literature from current technology

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

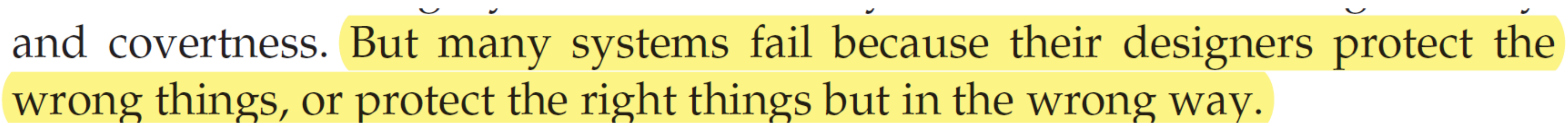
“Having” Security

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

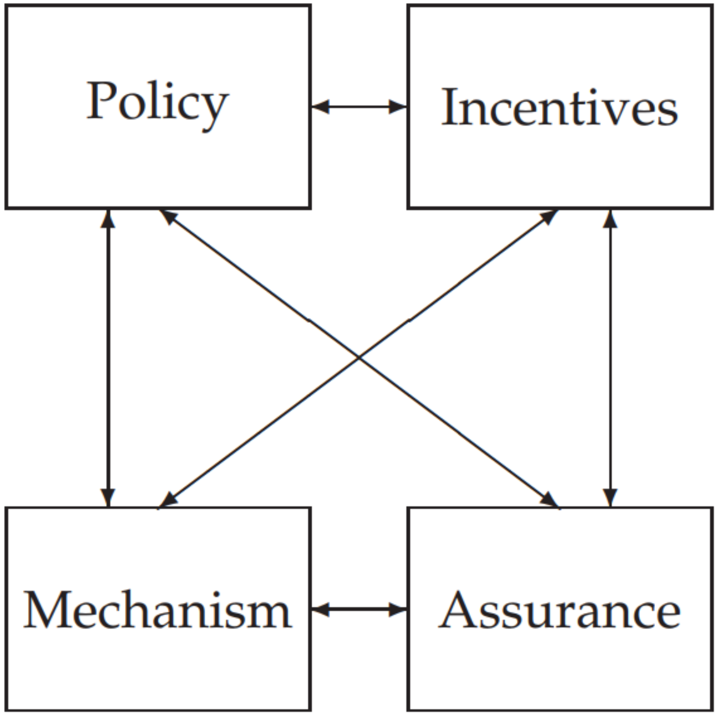


Figure 1.1: Security Engineering Analysis Framework

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

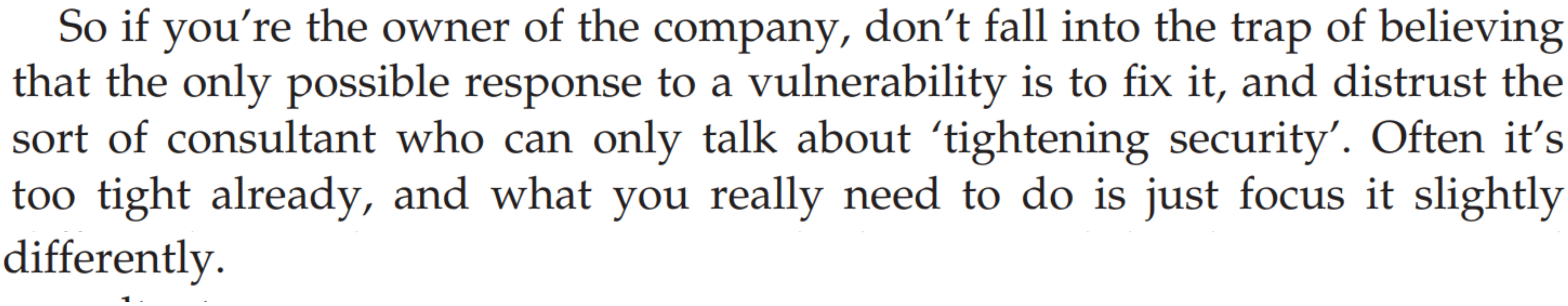
CIA (Not the Spies)

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?

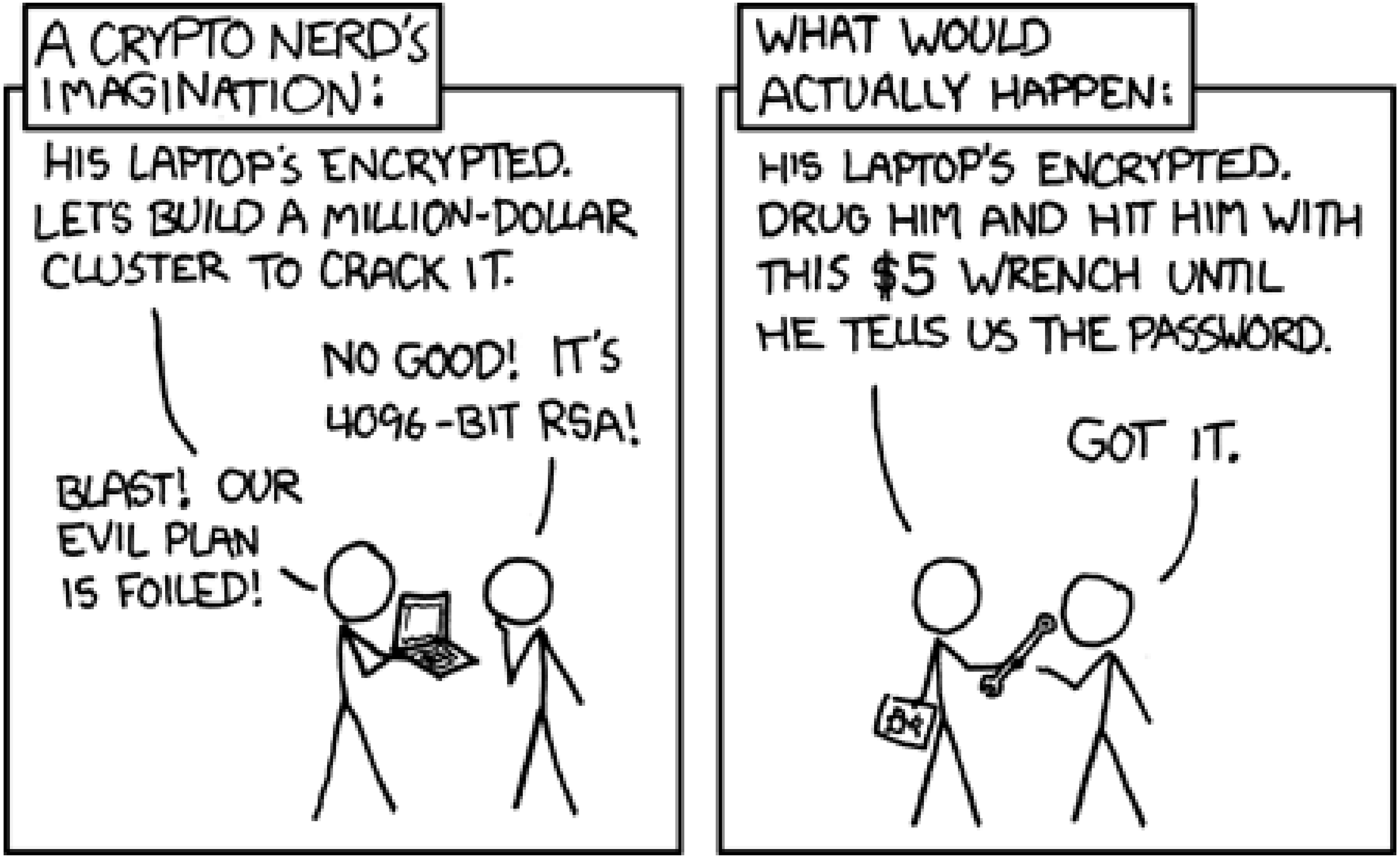
What is “Security Theater?”

Everyone should learn a little game theory

- Read up on Prisoner’s dilemma
- Understand “mechanism design”
- Anderson’s “Moral Hazard” (Chapter 25)

Illustrations

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.

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

Learn basics of how computer systems work

Learn about ***some*** of the current security technology

More importantly, the principles behind the technology

Know how to think and evaluate technology

It will change; be ready to change with it

Testing for Class Software

This semester is much easier

Install Wireshark

Test JavaScript