The Economics of Cybersecurity — Lecture 1 Notes

Adam Hastings

January 16, 2024

Pre-Class

- Write title, course number, hours, on blackboard
- Write out sections of discussion

1 Introduction

- Adam Hastings, 6th and final year PhD student
- Advised by Simha Sethumadhavan
- My area of research: this class!
- Background: Computer engineering at BYU, digital design, FPGAs
- Added on a Masters degree where I started to get into security w/ FPGAs
- Decided to do PhD in hardware security, came to Columbia
- Started out wanting to build defenses and discover new attacks
- Kind of got started doing that at first. Came to realization that TODO
- Conclusion: What matters is studying what actually produces security *outcomes*. Was (and remains) a lack of this in the field.
- PhD since then has been on understanding the economic side of security, particularly hardware security.

2 Syllabus

An economics class for computer scientists/people interested in computer security, not a computer security class for economists (but economists are welcome to join!).

2.1 Topics

- Market forces in security

2.2 Prerequisites

- Economics—no experience required or expected
- COMS 4181 (Security I) or equivalent. Some exposure to security. Basic understanding of security goals like confidentiality, integrity, and availability. Basic understanding of how attacks are carried out. Basic understanding of various security primitives like isolation, privileges, cryptography, et cetera.
- 2 COMS/CSEE 41xx or equivalent. Some exposure to the technical elements of how systems are built. You should know how a computer works, meaning some level of technical exposure to software, operating systems, compilers, hardware, et cetera. We are going to discuss security failures at a technical level and you should be able keep up and contribute to these conversations.
- Some level of mathematical maturity. Economics is a field that likes to be quantitative about things and this class will be no exception. Some readings will be on topics of economic modeling and game theory, plus we will likely discuss various statistical methods by economists, and you should be able to read and understand these types of works. Nothing advanced! But you should have used math in some form or another between now and high school.
- Ability to try something new! This is a rather interdisciplinary topic, and whatever background you come from, at some point in this class you will use part of your brain you have ever used before (?)

Not meant to be exclusionary. Meant to ensure a sufficiently high level of discussion in the class. A lack of technical skills may be compensated by students who have a sufficiently strong security background.

2.3 Grading

- 50% final project
- 10% in-class participation (may include quizzes). Come prepared to class having read papers!
- 15% homework (weekly presentation/analysis)
- 15% in-class presentations

3 Get-to-Know-You Round

This class will be very discussion-based. Who has taken a 6000-level class before?

We should know each other, our backgrounds, etc. to facilitate discussions. You have to feel comfortable speaking up. (Anecdote about being shy in Hardware Security class — didn't feel like I knew enough to contribute much to discussion! If this is you, my recommendation is to *ask questions!*)

Please state:

- Name
- Degree type, year in school
- Any relevant background in systems design, security, or economics
- I sort of hate the "fun fact" question because panic and can never think of anything fun about myself and I end up saying something like "I like peanut butter", which interests nobody and causes me lots of anxiety. But I still want to get to know you so I'll ask a very New York-themed "Would You Rather" question–Would you rather have a rat scurry across your feet wearing close-toed shoes, or have a cockroach land your head? Give your answer and your best attempt to intellectualize which one is worse.
- (I have experienced both! For me the cockroach was twice as bad! Exposure to bare skin! No way to know when it's over!)

4 Security as a Systems-Level Problem

4.1 Computer Science Systems vs real-world systems

Make a table comparing the two.

In CS:

- The systems are ones that **we design** (or ones that others have designed)
- The systems are **understandable** and comprise of deliberate abstractions
- Quantities are **measurable**

In real-world systems:

- The systems are ones we **inherit**

- There is often **no agreed-upon definition** of what the system is and is not
- Quantities are often **not measurable**

Ask: Are there any other dimensions that we can use to delineate computer systems from real-world systems?

Ask: Where does security fit into this categorization? Answer: both. But computer scientists are trained to work with computer systems, whereas the economists/policy people can only work with the other. I'm a bit of an engineering chauvinist so I think that because security is a "both" type of problem, the people who are best situated to solve security problems are engineers who learn the economics since it's very hard for economists to learn the engineering.

4.2 Illustrated Example

Some guidelines:

- Quantities as boxes
- Things that can change the quantities as arrows.

Discuss the diagram

Some possible takeaways:

1. There are a LOT of assumptions built in here! It might just be a neat way of organizing our assumptions! But this itself is useful!
2. You are necessarily going to have to leave things out! You can't fit everything into a diagram! Key is to fit in the parts that are most relevant and the parts that will be the most informative.
3. Feels "messy" compared to what technical people are used to. "Amount of public concern on cybersecurity"??? "Law enforcement spending" somehow appearing in a diagram in a computer science class? How is this a science? It's the best we can do.
4. Probably every box deserves its own cloud for all the "other" things that can influence the quantities. Should this be included? Or is this just noise?

Ask: What else can go into this model? What is it missing?

Ask: What's wrong with this model? Answer:

Ask: Anything come to mind when looking at this? (Might remind students of dynamic systems and control engineering. Why don't we apply control engineering theory to security? Probably because things like "amount of public concern on cybersecurity" is not a very good signal!)

5 Homework

This course will require much more writing and *arguing* than perhaps you are likely used to.