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, 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

2.1 Topics

- Market forces that affect security

- Analyzing security via economic models
- Behavioral economics + security
- Contemporary security problems (memory safety, speculation security, password weakness, patching issues, many more!)
- Cybercrime
- Hacker economics
- Game theory approaches to security
- Systems control + mechanism design
- Cyber insurance
- Economics of bug bounties
- Approaches to security regulation

2.2 Prerequisites

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

- 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. A good understanding of statistics if helpful.
- 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
- 20% homework (weekly presentation/analysis)
- 20% in-class presentations
- 10% in-class participation (may include quizzes). Come prepared to class having read papers!

Late policy: Lowest homework assignment will be dropped.

3 Get-to-Know-You Round

This class will be very discussion-based. Has anyone 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

This class will approach security using a very different set of tools than computer scientists are used to. I want to start by talking about security as a systems problem.

It's probably unclear what I mean by this.This is *not* the same thing as systems engineering!

- Systems engineering with similar problems, but systems engineering is about how to manage the integration of technical components towards some high level goal, like e.g. someone making an airplane has to have some role be the glue between aerospace engineers, mechanical engineers, software engineers, manage the intergration, deal with concerns like product lifecycle, et cetera.
- On the other hand, systems thinking is a kind of interdisciplinary quasi-field of study.
- More of an academic study of how systems in general are structured and how they behave
- For example how can we understand something like drug addiction when this is a problem that overlaps and combines with many other components, things like the physiology of addition, but also mental health, homelessness, pain medication prescriptions, drug smuggling, public attitudes to drugs, all they way to things like a drought in Afghanistan affecting the poppy plant yield.
- Systems thinking is figuring out how these components fit together and the structure between the components.

Very similar but certainly different from systems engineering, a term you may have heard of before.

It's a good way to introduce the types of problems we're going to deal with in this class and the types of *messiness* we're going to have to get accustomed to.

4.1 Computer Science Systems vs real-world systems

Let's talk about the types of systems we are going to deal with in this class.

In CS:

- The systems are ones that **we design** (or ones that others have designed)
- Systems have finite **boundaries**
- Underlying functions and interactions are known (**known underlying function**)
- Quantities are **measurable**
- The pieces and structure of the system are generally **under our control** (or under someone's control)

- Tradeoffs can be made **quantitatively**

In real-world systems (like security):

- The systems are ones we **inherit**
- **Unclear boundaries**
- Underlying functions and interactions are unknown (**unknown underlying function**)
- Quantities are often **not measurable**
- Many pieces/structure of system itself may be **out of our control**
- Tradeoffs often must be made **qualitatively**. Many cases impossible to decide tradeoffs quantitatively.

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. Thats what this class is for!

4.2 Illustrated Example

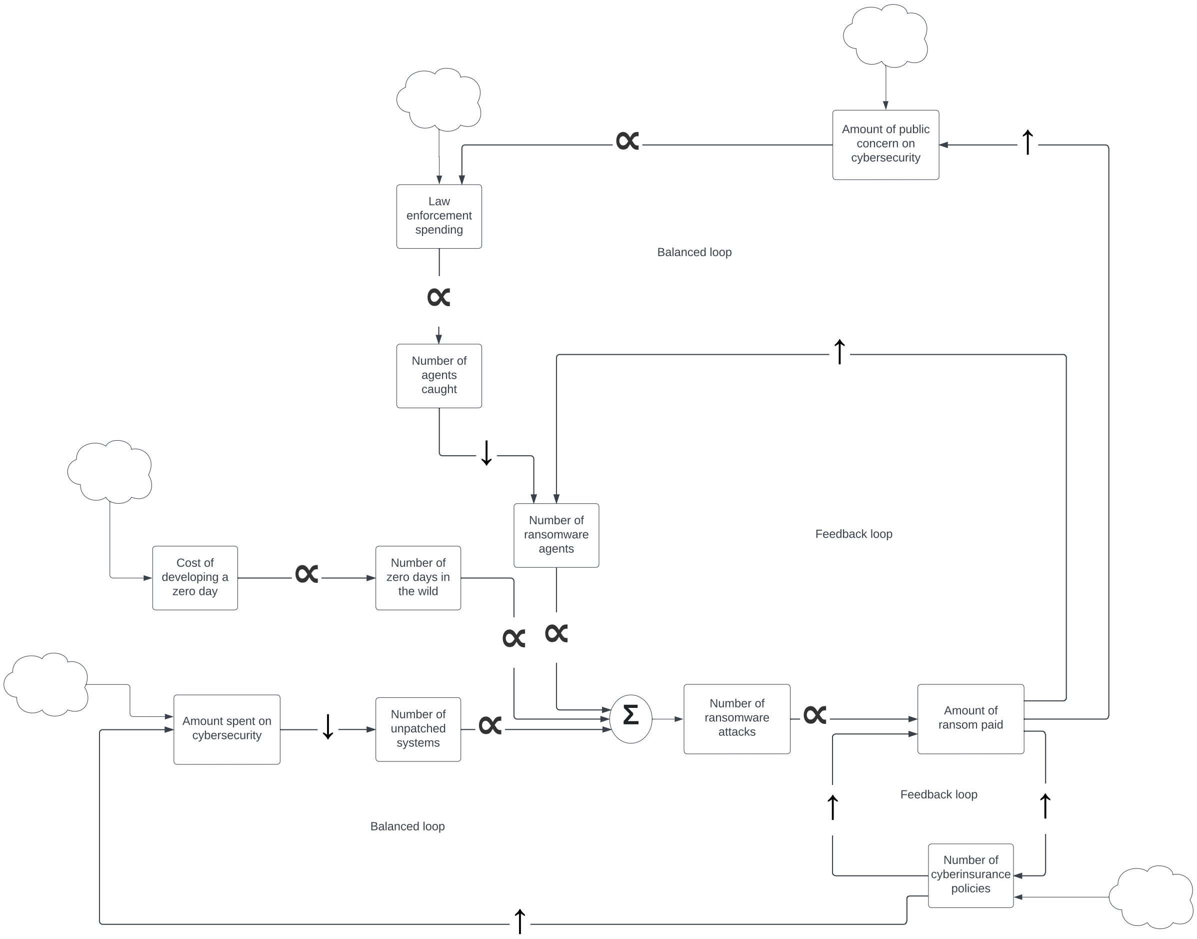
Dealing with real-world systems involves a bit of wading through the chaos. Trying to even define the problems we're working on is a bit like trying to nail jello to a wall. But not all hope is lost! One way we can try to bring order to the chaos is through systems diagrams.

There are lots of ways you can draw out a system but in my personal experience these are some good guidelines to follow:

- Quantities as boxes
- Things that can change the quantities as arrows.
- Direction of change written as part of arrow (increase? decrease? stay proportional?)

Draw out systems diagram one step at a time, starting with number of ransomware attacks per year. Ask students to help build out diagram. OK if it looks different than diagram in notes.

Discuss the diagram. What do students think about this? Is this a useful way of understanding security problems?


Amount of public concern on cybersecurity
Law enforcement spending
∝
↑
Balanced loop
∝
Number of agents caught
↑
↓
Number of ransomware agents
Feedback loop
Cost of developing a zero day
∝
Number of zero days in the wild
∝
∝
Amount spent on cybersecurity
↓
Number of unpatched systems
∝
Σ
Number of ransomware attacks
∝
Amount of ransom paid
↑
Feedback loop
↑
Balanced loop
Number of cyberinsurance policies
↑

Some possible takeaways:

1. "All models are wrong, but some are useful" — George Box
2. "The map is not the territory" (obvious in this case)
3. 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!
4. "When we draw structural diagrams and then write equations, we are forced to make our assumptions visible and to express them with rigor. We have to put every one of our assumptions about the system out where others (and we ourselves) can see them...Getting models out into the light of day, making them as rigorous as possible, testing them against the evidence, and being willing to scuttle them if they are no longer supported is nothing more than practicing the scientific method" — Donella Meadows
5. 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.

6. 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.
7. 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? Necessarily leaves out critical details. Hard to know when you’ve written out the “right” model. E.g. why not include number of cyber insurance companies?

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. You will also likely have to make subjective decisions and defend them more than you are used to. This is part of the subject! You need to practice these skills

(Review Homework 1 together)

At the beginning of next class, you will be asked to present your solution to the rest of the class! Submit on Courseworks. Due at **5:00 pm** the day of class. This is so I can compile into a slideshow so that we don’t have to deal with the hassle of everyone plugging in and unplugging laptops. You can also use the blackboard to explain your work if you’d prefer (but you still have to submit your work on Courseworks by 5:00pm).

Then at start of next class, we’ll spend probably 5 minutes on each of your submissions. Discuss choices, defend choices, suggest improvements. Depending on time we may have only a subset of students do this. Perhaps called upon at random.

The other two parts of the homework are two assigned papers. They are both classic papers. The first is not a computer science paper or even an econ paper, but is a paper from written by two urban planners on the nature of problems they call “wicked” problems. *Ask: Has anyone heard of a wicked problem before?* If not, you’ll find out soon enough. In the homework you’ll read the paper and then write a little bit about how, if at all, it applies to security.

A note on writing: don’t BS it! I’ll be able to tell. I’m not asking you to write a lot. Treat this like an exercise in compressing your writing. I will be reading and critically evaluating your writing! Don’t try to slip BS past me.

The second paper you will read starts getting closer to the topics this course is actually intended to cover, namely the economics of security. It is a seminal paper in the field.