# The Economics of Cybersecurity — Lecture 2 Notes

Adam Hastings

January 23, 2024

## Pre-Class

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

## 1 Homework Recap (6:10)

(Discuss agenda for the day. Write agenda on board)

(New Would-You-Rather question). The thing about Would-You-Rather questions is that that are perfectly suited for a class on economics. Why? Because economics is largely about quantifying and ranking *preferences*. A good would-you-rather question is about identifying interesting splits in peoples' preferences.

Getting to know each other through silly questions is a good way to feel more comfortable speaking up and making this a discussion-based class, which as a 6000-level seminar it should be discussion-based.

What makes a good would-you-rather?

- Splits responses roughly 50/50
- Exposes peoples values in a meaningful way (it's not very interesting to ask "what do you prefer—red or blue")
- Compares two very disparate things
- For this class — let's avoid gross topics

In fact, a big part of experimental economics research is clever ways of asking would-you-rather questions :)

I also want students to state their names again. In one seminar class I was in, we did names and introductions the first week but then I forgot everyone's names so it was awkward because when talking to people I had to say "hey you" instead of their names....

### 1.1 Systems diagrams review (6:15)

- I have made a slideshow of everyone's submissions, ready to be displayed on the screen.
- We're going to take a look at some examples of systems that we've identified, and then discuss, critique, and offer suggestions.
- *Does anyone want to volunteer to present what they have?*
- Let me just add that it is a privilege and an honor to have the opportunity to get time and attention of your peers to help you analyze and critique your work. Volunteering to have your work discussed is like free XP points :)
- Other benefits of sharing our work: It seems like there is a moderate amount of variance in the level of security background in the class. So by sharing work, we can not only practice the actual task at hand (thinking in systems) but also help teach other students about areas of security that perhaps they didn't know about beforehand.
- I want to be very clear about something here. We are not taking a "high level" view of security. I would argue that security is first and foremost a "high-level" problem. But because it's so high-level I think that computer scientists like to abstract away this view of security, or focus on a small subset of the problem. And that's OK! We can't solve every problem in every research project we do. But let's not forget that even though it's maybe fuzzy and nebulous, this is the *actual scope* of the problem of cybersecurity.
- **Big takeaway**: A common theme we're going to run into in this class, and a skill that we are going to develop, is the art of making something **defensible**. There's no right answer to any of these systems-level problems you've created. There's no such thing as an optimal systems understanding of something. You may be able to rank things in terms of better or worse, *if you're lucky*, but how "good" something is really depends on context, how it's being used, et cetera. So for better or for worse, in security economics, you're going to have to make the case that your interpretation and understanding is correct.
- Learning the art of what makes something defensible is an art, and hopefully by looking at examples of papers that the economics and security community have deemed to be worthwhile and important will help us develop an intuition for what a defensible set of assumptions are.

This brings up a few other questions:

- If someone presents a model of something (be it systems diagram), how do we know they're right? Peer review? Smell test? Predictive power + real-world validation? Combination of all the above? What else?
- I don't have good answers to this besides just the fact that the longer you work in this area the better you get.

- Keep in mind that we're talking about diagrams that we all drew for homework but this discussion will generalize to pretty much everything we're going to talk about in this class.
- Controversial question: Is economics a science? How is it different from other sciences? Is it just that the models are just less reliable than other hard sciences? Example: Newton's laws of physics are a really good model of the world. They describe most of the physical world that we interact with. But we know it doesn't explain everything, and Newton's laws become incorrect when things get very very small or very very large or start moving very very fast.

Conclusion: It's kind of messy! Good segue...

# 2 Big Ideas in Economics (6:30)

So far we've talked about security as a system and maybe talked about some open issues in security but up to this point we haven't really talked about security as an *economics* problem.

This class doesn't assume any economics knowledge. So we're going to establish a basic foundation. You may have seen some of this stuff before if you've ever taken an economics class before. But we need to establish a shared baseline. A lot of this (in my opinion) is just providing you with the *vocabulary* needed to discuss things like an economist would. Many of the ideas we're going to talk may sometimes feel obvious but that's because we're maybe taking for granted the mindset that economists have given the world. Maybe obvious in hindsight but highly non-obvious at the time they were formulated. Same thing in computer systems. The idea that code could be treated just like any other data is beyond obvious at this point but you just have to keep in mind that at one point things like this were revolutionary. Same with the "bit"—not coined until 1947! Let's give these maybe seemingly obvious ideas the respect they deserve.

## 2.1 ~~Big Idea #1: Goods~~

Economics is fundamentally about the distribution of goods and services.

*Ask: What is a good?*

A **good** is an item that provides value or utility for someone. Something that someone wants. Something that someone is willing to sacrifice something to obtain. Example: A table, or a barrel of oil.

*Ask: What are some goods we deal with in security?* Hardware, obviously. Software can also be a good (even though it is sort of intangible).

*Ask: What about services? How are they different?*

A **service** is an act that someone performs because someone else values the act and is willing to pay for it. A good is transferrable. A service is not. Example: a haircut.

| | Excludable | Non-Excludable |
|---|---|---|
| **Rivarlrous** | private goods | common-pool resources |
| **Non-Rivalrous** | club goods | public goods |

Different from goods in that they are always **intangible** (whereas goods can be tangible or intangible). Another difference is that services are **non-transferrable**: Once a service is performed, it can't be transferred to someone else. If I can't a haircut I can't undo it and give it someone else. Different from a transferrable good like a chair.

*Ask: What are some services we deal with in security?* Penetration testing, incident response.

### 2.1.1 Types of Goods

We can taxonomize goods in a few ways. Two main ones are used: rivalrousness and exclusivity.

(Write out 2x2 grid)

**Rivalrous**: Consumption by one person → cannot be consumed by another. Example: If I eat an apple, you can't also eat it.

**Excludable**: Consumption can be restricted to certain people only. Example: Concerts. You physically cannot get access without buying a ticket.

*Ask: What's an example of a non-excludable good?* Air. A lighthouse (everyone can take advantage of it).

I'm writing these as binary categories but in reality they exist more on spectrums. Example: this class! Supposed to be available to those who pay tuition. But if someone wanted to audit, I wouldn't physically prevent them from entering the classroom (could even enhance if they contribute to the discussion!). So this class is semi-excludable.

1. Private goods: rivalrous + excludable. Examples: GPUs, firewalls. As opposed to...
2. Public goods: non-rivalrous, non-excludable. Examples: Air. Cybersecurity itself?
3. Club goods: excludable, non-rivalrous. Examples: Antivirus software? Since it is intangible.
4. Common-pool resources: rivalrous but non-excludable. Example: Fish in the sea. Internet traffic?

## 2.2 ~~Big Idea #2: We can model the value of goods~~

Some goods are more valuable to some people than to others.

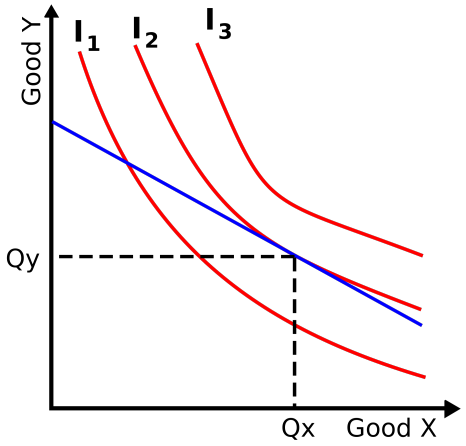
Some goods can even be more or less valuable to the same people depending on circumstances. E.g. if it's a sunny day, I might not care to have an umbrella; if it's raining really hard, I'm really going to want one.

Acquiring goods usually involves trading off something you want for something else you want more.

There are a few common methods that economists to capture how valuable things are to people.

### 2.2.1 Indifference curves

A typical way of expressing how much people value something is via indifference curves. This is a way of expressing how much someone values something in terms of something else.




- X: the good in question
- Y: could be another good. But typically is a composite of all other goods!

This is a 2D space of possible goods you can acquire. We're going to make some simplifying assumptions and say that we're dealing with "normal" goods (like e.g. more is better. May not be a realistic assumption! Economics can handle more advanced cases but take an econ class if you want to learn more about that).

Each point is a different combination of goods, like $Q_x$ of good X and $Q_y$ of good Y. (Draw $(Q_x, Q_y)$ on the board) We call this point a **bundle**.

An **indifference curve** is the line connecting all the bundles that someone finds to be equally attractive (draw a few indifference curves).

*Ask: I drew it convex. Why?* Diminishing marginal utility. Lets use a computer systems analogy. Let's say I have a system where X is my CPU clock frequency (it's something we want! It's a good!) and Y is all other system design constraints. If my goal is to make a fast system, and my clock frequency is very low, this could be the bottleneck in system performance

Normal goods are usually convex like this. There are of course some exceptions.

*Ask: What does it mean if I draw the indifference curve as a straight line?* It means that X and Y are perfect substitutes—I don't care if I have one or the other.

Another variation is indifference curves with a "bliss point" i.e. an optimum. single point w/ surrounding lines. Looks like a topographic map!

One important element of an indifference curve is that the slope at each point is equal to the **marginal rate of substitution (MRS)**, which is the rate at which the consumer is wiling to substitute good $X$ for good $Y$. This is the "exchange rate" between the two goods.

### 2.2.2 The budget line

Recall that we usually deal with normal goods, so more = better. In this case people would always want to maximize $(q_x, q_y)$, i.e. the top-rightmost possible point. But people don't have unlimited budgets so we have to make some constraints.

A common assumption in many econ problems is that people are working with a fixed budget of money they have to spend. We can call this amount $m$. Then it necessarily follows that

$$p_X q_X + p_Y q_Y = m$$

This is just the formula of a straight line *(draw negative sloped line).*

### 2.2.3 Composite goods

One thing about this arrangement (indifference curves) is that it expresses how much someone values one good in terms of another. This might be useful if there were only two things people want. But if we want to know how much someone values apples, does this mean we need to make a new set of indifference curves for every possible other good out there? Apples vs pears? Apples vs corn? Apples vs iron ore? Apples vs movie theater tickets? No, there's a better solution. We can instead just let the other variable $Y$ be a **composite good**, which represents "everything else the consumer might want to consume" (Varian). In this case we can just write $p_Y = 1$ since the price of one dollar is one dollar.

### 2.2.4 Optimal Choice

The **optimal choice** is the point where the the budget line is tanget to the indifference curve. This is the most preferrable bundle of goods. We can call this bundle $(q_x^*, q_y^*)$ *(draw dashed lines connecting to tangent point $(q_x^*, q_y^*)$)*

At this point the marginal rate of substitution is equal to the slope of the budget line.

### 2.2.5 Changing prices

As prices change, the budget line and indifference curves intersect at different points *(draw 1-A)*. As the price decreases, the budget line pivots outwards.

## 2.3 The Demand Curve

Another important way of expressing peoples wants is through demand curves. A **demand curve** is the optimum quantity of a good as a function of its price. For reasons I'm not entirely clear on this is typically drawn with the *price on the Y axis even though demand is a function of price!* (I think this might be because when economists talk about supply, it's the opposite where they view price as a function of demand, so putting both on the same graph means one gets stuck with the unconventional plotting.)

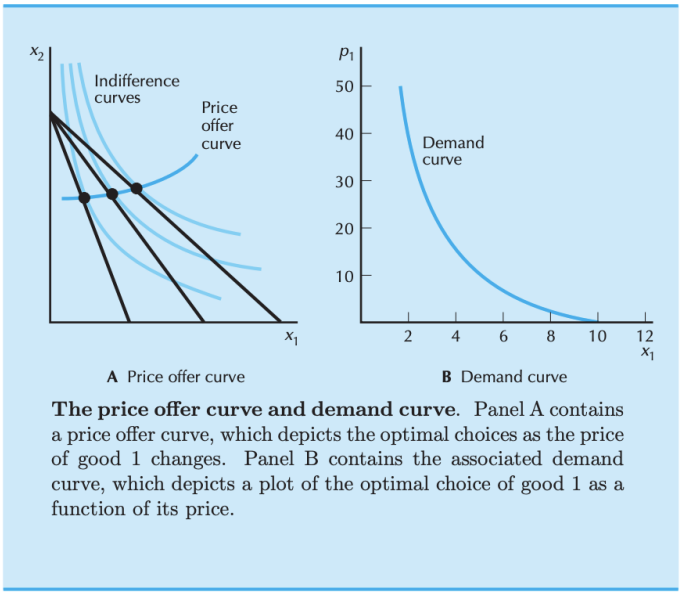



**Figure 6.11** **The price offer curve and demand curve.** Panel A contains a price offer curve, which depicts the optimal choices as the price of good 1 changes. Panel B contains the associated demand curve, which depicts a plot of the optimal choice of good 1 as a function of its price.

Figure 1: Source: Intermediate Microeconomics by Hal Varian, 8th ed.

## 2.4 The Supply Curve

Supply side economics is equally important—to economists. We won't focus on it so much in this class. In classical microeconomics it suffices to say that those who produce goods are incentivized to produce more when prices are higher. The amount that acutally gets produced is the point where the supply curves and demand curves intersect. This is called the **market clearing price**. Of course this is a huge simplification and there are lots of caveats so go read an econ book if you want to learn more.

### 2.5 Assumptions built into the above models

The above is a model of the world that has proven itself to have remarkable predictive power. But it doesn't solve every problem. (?) For the above model to work it assumes that a number of conditions are being met. For example:

- Rationality: Assumes that peoples' preferences are rational. E.g. if I prefer good A to good B, and prefer good B to good C, then if I were being rational I would prefer good A to good C (this particular property is called **transitivity**). But in the real world people don't always behave like that.
- Others?

So does that mean that the above is doomed to fail? No, definitely not, just means that our models need to maybe take into account more information.

## 3 Intro to Microeconomics Redux (6:30)

Last week I did some very introductory microeconomics on the board. We talked about types of goods—*Ask: What were the four types of goods? Along what axes did we categorize them?*. I sort of just put a bunch on information on the board but I think it's useful to finish our introduction of microeconomic theory by making this a bit more engaging and hands-on.

### 3.1 Macroeconomics vs. Microeconomics (6:30)

Since this class assumes no background in economics whatsoever, we're going to talk a little more about the lay of the land.

There are two main branches of economics: Macroeconomics and microeconomics. Very good chance you've heard these terms before. Totally OK if you haven't.

*Ask: Does anyone know the difference*

*(Draw table on chalkboard)*

| **Macroeconomics** | **Microeconomics** |
|---|---|
| A large-scale view of how an economy works | How goods + services are allocated |
| GDP (Gross Domestic Product) | Individuals' preferences |
| Inflation | Supply and demand |
| Interest rates | Modeling behavior and choices |
| Unemployment | Markets |
| Economic growth | Utility functions |
| Business cycles | Prices (and where they come from) |

*Ask: Which one of these do you think computer scientists and security people are usually more interested in? (Answer — microeconomics. To me (and others), an economic understanding of security is an understanding of the incentives that underlie security and the decisions that people make and the types of tradeoffs they prefer. So when we talk about economics things in this class, keep in mind we'll mostly be talking about microeconomics).*

# 4 Market Failures in Security (7:00)

## 4.1 Preface

The main point of this lecture: Why is security an economics problem? Are we here because we want to learn how big the market for firewalls is? Are we here because we love xxxx?

No. We are here because security itself is an economics problem. Perhaps before *anything else* it is an economics problem. More than being a problem of software, or hardware, or usability, it is an economics problem.

And the implication here is that to really understand security, and to really understand how to *improve* security, we need to be able to have an economic understanding of security.

For homework I had you read a couple of papers. They were pretty straightforward I think.

### 4.1.1 Initial thoughts

*Ask: What did we think of these papers?*

- What stood out to everyone?
- How is this paper different from other academic papers you have read? (*Ask: Mix of undergrad and masters students. Who here reads papers?*).
- How do we evaluate the claims made in a paper like this?

Some things that stand out to me:

- There are no figures! No charts! Very little data. Mostly a constellation of anecdotes that point to some larger thing going on.

*Ask: What kinds of assumptions are needed to make markets efficient?*

This section is really the "why" this subject needs to exist. Markets are wonderful and they solve many problems of the allocation of goods and services. But let's review some of the required assumptions needed for efficient markets.

*Ask: Which of the above requirements might be violated in the world of security?*

Some suggested answers:

1. Perfect information

# 5 Paper Discussion: Why Information Security is Hard (7:00)

Introductory discussion things to note:

1. This is a seminal paper. So where are the experiments? Where are the graphs and tables? There are none. How can this be? (If you're looking for a technical rigor to this class, we will make sure we cover that too).
2. A big part of this class is going to be studying methods. This paper has no methods! But in future papers we will highlight methods used.

*(Discussion)*

## 5.1 Types of Market Failures in Security

### 5.1.1 Tragedy of the Commons

*Poll: Before reading this paper, who knew what the tragedy of the commons was?*

A bit of etymology first: The word "common" is most often used today as an adjective, for example "sneakers are a common type of shoe". But "common" is also a noun, like Carleton Commons in Mudd, denoting a place with resources that is shared by many. In medeival Europe, the "commons" were the plots of land that were "owned" by a Lord but available for use by the "commoners"

Remember the 2x2 grid of types of goods from last week? Remember "common pool resources"?

*Ask: What is a common pool resource? Specifically, what are the two critera?* (Rivalrous and non-excludable)

*Ask: Can someone give an example of a common pool resource?* (Example: fish in the sea)

Ask: So does this mean that every time there is a common pool resource, we need outside government influence? No, probably not. Economist Elinor Ostrom wrote a book called "Managing the

Commons" on situations where those dependent on the commons are able to manage its consumption.

Ask: So in the two papers we read, what were some of the examples of tragedies of the commons?

Ask: In security, what might other examples be?

#### 5.1.2 Free Riding

(description)

#### 5.1.3 The Market for Lemons

#### 5.1.4 Moral Hazards

#### 5.1.5 Perverse Incentives

The canonical story

This is a case where I think a systems diagram would have been helpful!

### 5.2 Conclusion

"In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected."

## 6 Research Methodologies Used in Economics

The papers we read so far were a bit light on methodology—mostly they were just the author telling the audience the world as he sees it. Which may be suitable in some cases but a big portion of this class will be understanding and applying economics' attempts to apply rigor through various methodologies so that we don't just rely on vibes. There's a big range of methodologies that are available, and they each can be useful in cybersecurity. Each one is like a different tool that can solve a different problem.

I'm now going to go through what some of these available tools are and when you might use them. This is one of those things that may be very obvious, and you probably already know what most of these are, but I never had anyone really sit me down and tell me that this is the lay of the land, so as your kind-hearted instructor who wants the best for you, that is exactly what I'm going to do.

I'm using a taxonomy that I found in a paper by an econ professor. He breaks economics research methodologies into three main groups: Theory, Experiments, and Empirics.

(Source: "Methods Used in Economic Research: An Empirical Study of Trends and Levels" by Paldam)

- Theory
  - Economic theory
  - Statistical methods
  - Surveys
    - Assessed Surveys
    - Meta-studies
- Experiments
  - Lab experiments
  - Event studies
    - Field experiments
    - Natural experiments
- Empirics
  - Descriptive studies
  - Classical empirics
  - Newer empirics

This taxonomy is probably not exhaustive. In fact, I borrowed this taxonomy from an econ professor who of course was specifically talking about economics research. *Ask: What are the research methodologies used in computer science and security? (My response: They look remarkably similar.).*

*A task for the class: Can we think of any fields of security or research topics in security that are examples of the above taxonomy? How can we taxonomize research papers in computer science and security?*

- Theory — not much theory in security! Seems to actively *defy* security in many cases. One notable exception may be cryptography.

*Ask: Is anyone aware of any classes of research methodologies that might be missing?*

*Ask: How do you know which methodology to pick? (Possible answer: A lot of times, you don't exactly have the opportunity to choose.)*

# 7 The Tragedy of the Commons — Modeling Techniques

## 7.1 How to Read a Paper

*Ask: Remind me (by raise of hands)—who here is an undergrad? MS? PhD?*

*Ask: How much exposure do you have to reading papers? By raise of hands does anyone here think they've read over 20 papers top-to-bottom?* (Some students like will not have).

Before we go into discussing this paper, it might be useful to talk about *how* to read a paper. Reading a paper is not like reading a book or a newspaper. It is a distinct skill that requires practice.

Some good questions to ask yourself when reading a paper:

- What year did this paper come out? What do we know about what was happening in the rest of the world at this point? (Why Information Security is Hard — 2001. A lot of the topics in that paper had been observed before, but this was around the time that most of the rest of the world was getting online for the first time, and probably around the time that cybersecurity started to become a concern in the average persons' life.)
- Follow up question—what is the timeliness of the paper?
- Why did the author or authors write this paper? Are they trying to open up a dialogue? More common in the humanities.
- What are the claims they are making in the paper?
- Do they support their claims with evidence? If so, how good is the evidence?
-

# 8 Gordon-Loeb — Modeling Techniques