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)

- Last class we started with an introduction round where we said our names and then answered a would-you-rather question about rats vs cockroaches
- There are some new faces in class today.
- I actually liked this quite a bit because 1) people could learn our names but 2) it forced everyone to speak.This a discussion-based class, which as a 6000-level seminar it should be discussion-based; the more discussion we can engender, the better the class will be.
- Knowing names is important (don't have to called everyone "hey you")
- The thing about Would You Rather questions is that they are a tiny little economic experiment. Economics is largely about quantifying and ranking *preferences*. A good would-you-rather question is about identifying interesting splits in peoples' preferences.

So here's today's: *Would you rather start each class with a quick would you rather question that is* **relevant** *to the class topic, or would your rather not, and presumably use our class time on other things?*

Go around the room, state your name (even though we did this last week), and tell me if you'd rather do a little would you rather question or not.

1.1 Systems diagrams review (6:15)

- I made a slideshow of submissions
- We're going to take a look at some examples of systems that you'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.

Discuss 3–4 students' diagrams Some questions to ask:

- *What was your process for creating this diagram?*
- *How did you decide what to include? How did you decide what to exclude?*

Ask: What are the takeaways from this exercise?

- I want to be very clear: I hesitate calling this taking a "high level" view of security. This is the *actual scope* of the problem 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! But as the saying goes, lets not miss the forest for the trees.
- **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.

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

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.

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.

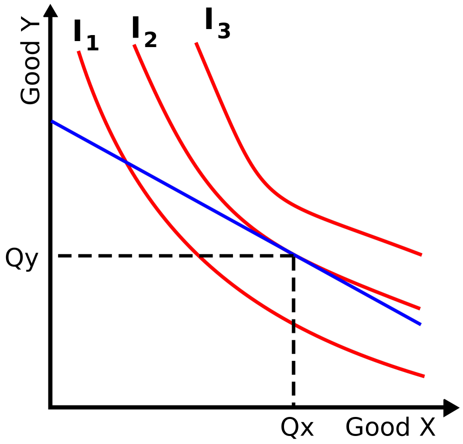
Some goods can even be more or less valuable to the same people depending on circumstances. E.g. if it's a sunny day, I might not care to have an umbrella; if it's raining really hard, I'm really going to want one.

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^*))*

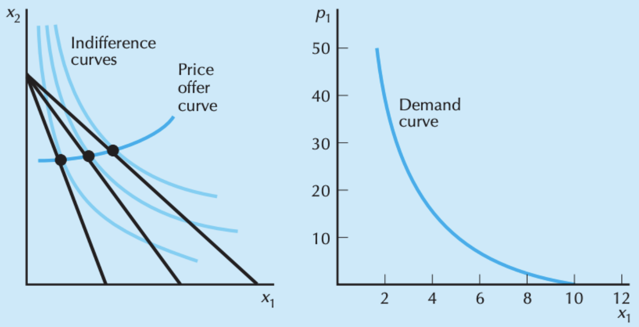
At this point the marginal rate of substitution is equal to the slope of the budget line.

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.)



A Price offer curve

B Demand curve

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.

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 more useful to present this material by building up *why* things are the way they are. Less of me *telling* and more of us *doing*.

3.1 Macroeconomics vs. Microeconomics (6:30)

Since this class assumes no background in economics whatsoever, we're first going to talk a little more about some really basic distinctions just to get a lay of the land.

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

Ask: Does anyone know the difference?

(Draw table on chalkboard)

Macroeconomics A large-scale view of how an economy works	**Microeconomics** 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).

You probably already knew that though if you read the assigned readings! Since Ross Anderson explicitly states in the first paper that is about taking a *microeconomic* view of security :)

3.2 Efficiency

What does it mean for an economic outcome to be efficient?

Hal Varian: ”One useful criterion for comparing the outcomes of different economic institutions is a concept known as Pareto efficiency or economic efficiency.1 We start with the following definition: if we can find a way to make some people better off without making anybody else worse off, we have a Pareto improvement. If an allocation allows for a Pareto improvement, it is called Pareto inefficient; if an allocation is such that no Pareto improvements are possible, it is called Pareto efficient”

How does this compare to Pareto efficiency in engineering?

3.3 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.
- Perfect information
- No barriers to entry
- Lots of buyers and sellers

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

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.

4 Paper Discussion + 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 much money Crowdstrike makes in a year?

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?
- What was interesting?
- Did this change anything in the way you view or think about security?

Some things that stand out to me:

- How is this paper different from other academic papers you have read? (*Ask: Mix of undergrad and masters students. Who here reads papers?*).
- This is a seminal paper. So where are the experiments? Where are the graphs and tables? There are none. Mostly a constellation of anecdotes that point to some larger thing going on. How can this be?
- A big part of this class is going to be studying methods. *Ask: What methods does these papers use?* Do they even use methods?
- How do we evaluate the claims made in a paper like this? (If you're looking for a technical rigor to this class, we will get to that next week when we look at some classic economic models).

4.2 Types of Market Failures in Security

For me, the value of these papers is not so much in their technical rigor but in their ability to frame something in a new way (the new way being microeconomics, which is not new, but will be new to many programmers and cybersecurity people). The contribution is just pointing out, with many examples, of situations where the market mechanism doesn't work very well. We call these scenarios market failures:

Market failure: Situation where the market mechanism produces inefficient outcomes.

There are many cases where the market mechanism doesn't work or don't work well, meaning that the markets don't produce the most efficient outcome. This could be due to the nature of the goods in question, or due to a flaw or shortcoming in the way we've made our economic models and framed the problem.

In many of these cases there's a canonical "story" that goes along with the example, and I think as part of your education I have to give you the canonical story.

4.2.1 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)

You read the paper so this should be review. The canonical example comes from a 1968 paper in Science titled The Tragedy of the Commons, and this itself was a reference to a 1833 pamphlet, but the general principle has been known since antiquity. The tragedy is this: Suppose you are a dairy farmer in medieval village. In your village, there is a shared plot of landcalled the commons—that is used for cattle grazing. If each farmer puts, say, 10 cows onto the commons, then everybody has lots of milk and cheese to eat and everyone is happy. But you would be even happier if you could put 11 cows onto the commons, and sell the extra milk and cheese to the village down the road. So you add another cow to the commons. But your fellow farmers see this, and so they each put another cow on the commons. And so now you put 12 cows on the commons. And so on. And what happens? The commons has too many cows on it and becomes overgrazed and barren, and so all your cows starved and now you have 0 cows. The tragedy is that this is the outcome that occurs when each agent is individually acting rationally. If you can put 11 cows onto the commons, you should. But individual rational behavior can create outcomes that is to the detriment of all. That's the tragedy. Of course, there are ways to avoid this, but it comes requires that the individual farmers limit the number of cattle they have on the commons, and essentially self-impose an opportunity cost onto themselves

To summarize, commonly-held resources are rationally overused to the detriment of all. No farmer is being individually irrational by putting more and more livestock on the commons. This is the really important part.

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

1. DDoS attacks. *Ask: What's a DDoS attack?* Distributed denial of service?

Ask: In security, what might other examples be?

Ask: What are some possible solutions to tragedies of the commons? Generally speaking, you need to find some way to coerce people into cooperating with each other. In the case of farmers, maybe they can just work it out amongst themselves but in larger situations you usually need some degree of law and authority and government to manage common pool resource consumption.

Ask: Any questions before we move on?

4.2.2 The Market for Lemons

This one was in the second paper we read.

- Consider a used car lot with 50 good cars worth \$2000 and 50 bad cars (also known as lemons) worth \$1000
- Suppose that customers cannot tell the difference between a good car and a bad car. The seller knows the difference though. Since odds of a good car are 50/50, customers will pay \$1500
- Sellers will not sell a good car worth \$2000 for \$1500, and will leave the market Price collapses to \$1000 and only the "lemons" remain

This is a very famous example of an information asymmetry. An **information asymmetry** is exactly what it sounds like—it means that one party has more information than another. Usually implies important relevant information (like the quality of a used car).

Ask: What was the example given in the paper of the market for lemons? Software market (keep in mind this was 2006 when you would buy software in a box at Best Buy...business model for software companies has changed a bit but the principle is every bit as true today).

- It's really hard for users to be able to evaluate the security of a system or a piece of software. It's hard even for product vendors themselves!
- Consumers generally are not going to be willing to pay for something they can't appreciate or identify.
- A consequence of this is that consumers are not willing to pay extra for security if they don't understand or appreciate the difference
- *How does this change the incentives for product vendors?* They're probably not going to go out of their way as much to make their products secure if their customers can't tell the difference.

Ask: What might be one way we can reduce information asymmetry in the marketplace? Iot Security labels? We'll talk about what some of the proposed solutions are later in the semester.

4.2.3 Moral Hazards

This one can be confusing to people because of its name. In fact, I did some researching and found that economists themselves are unclear on where the name came from. But the concept is simple: A **moral hazard** is a situation where someone is shielded from risk because the consequences will be borne by someone else.

- Does anyone else ski? Or snowboard?
- Do you have your own skis?
- I don't. So I have to rent.
- Usually as part of the rental you can buy insurance on the rentals for an extra $10 to cover any damages.
- Now lets suppose that I see a ski run and there's low snow coveage and it's covered in rocks, and I know that if I ski down it I'm going to scratch up my skis.
  - If I'm on my own personal skis that I've paid a lot for, maybe I would skip it.
  - But if I'm on rentals and I've paid for the insurance, why do I care?
- (I probably wouldn't actually do this because it's a bit unethical, but you could see how it could create problems)

Also an issue when it comes to things like hedge funds. If take a crazy risk and it really pays off, you get super rich. If your investment goes to zero, it's not your money anyway. So there's an incentive to take big risks becuase you're shielded from the consequences.

What was the example of this in the papers? ATM fraud. In several European banks, the burden of proving fraud was placed on the customers, whereas in American banks, the burden was on banks to prove fraud did not happen European banks didn't care if a customer was victim of fraud. The problem didn't affect them! So they were reckless with their security In the end, they ended up having to pay more for security and were less secure!

Ask: Does this problem exist anywhere else in security?

4.2.4 Misaligned Incentives

The general problem here is called **misaligned incentives**. If an IoT product vendor sells a horribly insecure product, or they don't bother issuing security patches once vulnerabilities are discovered, it's sort of not their problem, because the product vendor doesn't have to deal with the consequences of their own insecurity. They shift the cost onto their users.

4.2.5 Adverse Selection

- Classic example = buying insurance policies. Consider the era before the ACA
- If you're healthy, you don't need health insurance
- If you're sick with a chronic disease, you will need health insurance
- Result: Insurer's customers are a bunch of sick people who are going to be very costly to insure!
- There is not a pool of non-sick customers to distribute the risk of having to pay out to customers.
- Premiums become very high less people buy insurance more catastrophic events occur

This exact problem is happening with cyber insurance right now: Cyber insurance premiums have skyrocketed because the ones buying insurance are the ones who are really vulnerable to getting hit with expensive ransomware attacks

Ask: What example of this was given in the papers? Dubious companies buying web certificates.

Does this principle apply to areas of security outside of insurance?

4.2.6 Perverse Incentives

The canonical story/example comes from India during British rule. The story goes that the British, seeing the large number of venomous cobras in the city of Delhi, decided they wanted to reduce the number of deadly snakes by instituting a policy: The British started paying bounties for each cobra killed. And at first it worked. The number of cobras decreased. But then some people had an idea on how they could make some more money—*Ask: Anyone know?* They started breeding cobras! And, as the story goes, once the British realized what was going on, they shut down the program, and what did the cobra breeders do? They released them. And now there were more snakes than before!

The takeaway is that if you don't consider the full system that you're working with, your policy "solutions" may have the exact opposite effect of what you intend. We call this a **perverse incentive**.

Apparently this story may be merely anecdotal and may not have happened exactly like the story goes, but to be honest it doesn't really matter if the story is true or not because it gets the point across so clearly. If you'd like a historically-verified version of the principle, the same thing happened in Vietnam during French rule but with rats instead of cobras.

This principle comes up all the time in systems. Last week when I introduced systems and systems thinking, I gave the example of drug addiction, which as we talked about is a system with many different components in many different domains. One thing I *didn't* mention though was a well-known perverse incentive in the system. Like other any other "good", the price of drugs are subject to the laws of supply and demand.

(Draw supply and demand straightline curves on the board).

A government might decide that they don't want their citizens using harmful drugs, so they might make certain drugs illegal and arrest a bunch of drug dealers and destroy seized drugs. *Ask: What does this do to the market?* Answer—it reduces supply.

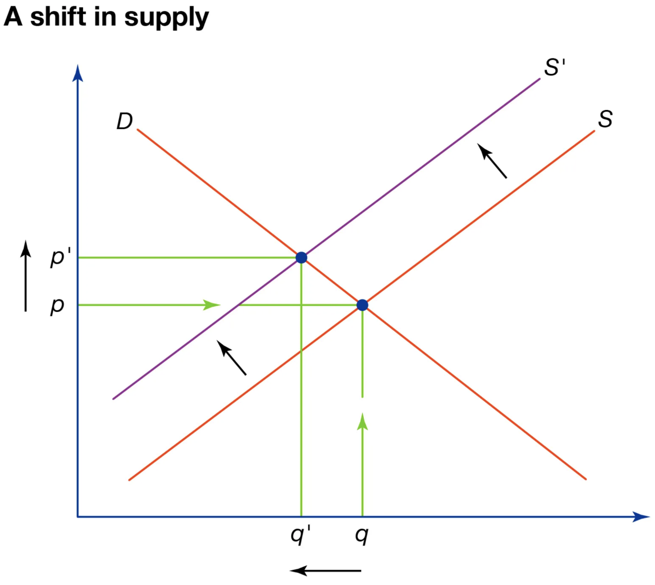
A reduction in supply means less quantity, so in classical microeconomics we represent this as a shift of the supply curve to the left. Let's make this even worse and make assume inelastic demand (vertical demand line). What happens to the equilibrium price when we shift the supply curve to the left? The equilibrium price goes up. What is the effect? The better the police are at getting drugs off the streets, the more valuable it becomes to *sell* drugs, which in turn might incentivize more people to produce and sell drugs. It can be a perverse incentive.

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

Ask: What was an example of a perverse incentive in the papers we read?

In the paper, this principle was observed with Common Criteria evaluations. For anyone who doesnt know, CC is an international standard for security certification. The way it works is you have a product with some security features and want to prove to people (or the government) that the security features work as advertised, so you come up with a test plan and have a certified laboratory perform tests according to your test plan to verify that your product meets the requirements. Then your product is CC certified and you can sell it to governments and boast about how secure your product is. And whos going to pay for this certification? Well naturally the vendor will.

But the problem, as pointed out in the paper, is that the certification is paid for by the vendors themselves. So the incentive for vendors is to find the worst-quality certification lab you can, who charges next to nothing and certifies your product on a shoestring budget and probably misses a bunch of vulnerabilities along the way.



© 2013 Encyclopædia Britannica, Inc.

Figure 2: When supply is constrained, prices go up. With a "good" like an addictive drug, we might see something called **inelasticity**. If you are addicted to a drug, you might pay any price to obtain it. Inelastic goods have steeper demand curves. In the most extreme case, the demand curve is a vertical line. This means that consumption of the good is completely independent of price. Presumably this *doesn't* mean that the price *will* be infinitely high, since there will still be multiple producers competing each other and trying to undercut each others' prices (assumes no monopolies...). This is the opposite of a **elastic** good, which is when the quantity of a good's consumption is highly dependent on its price (in the extreme case, this would be a horizontal demand curve). Usually you see this in cases where the good in question has a good number of substitutes available (e.g. gala apples in place of fuji apples).

Ask: What are some other scenarios in security where there are perverse incentives? If I could put on my conspiracy theory hat for a minute, you could say that cybersecurity companies—the ones who you pay to due audits, penetration tests, consulting, triaging, incident response—companies pay them to improve their security, but are these companies actually interested in reducing the amount of cybercrime that happens in the world? No, not necessarily! The more cybercrime that happens, the better for them. Sort of like the adage "no company will ever want to invent a pen that never runs out of ink"—I don't think I believe this (or my conspiracy theory above) but it's worth thinking about.

Ask: What can be done about fixing something like a CC perverse incentive?

4.2.7 Monopolies

This is another very famous market failure that you probably already know about (although maybe not in terms of it being a market failure). A **monopoly** is when a single seller dominates the market. In classical microeconomics, this is a problem becuase if you have a monopoly you can charge whatever you want. You can also have what's called a **discriminating monopolist** can charge people the most that they personally would be willing to pay (e.g. by holding an auction).

In the papers, the monopoly problems weren't so much about monopolies in this sense. They were more about network effects and Metcalfe's Law (Number of edges = $n(n-1)/2$, i.e. grows quadratically). In things like social networking, value of the network scales quadratically with the number of users.

What are the consequences?

- Race to market. May be winner-take-all situations. If you're a product vendor, and you have the option of either A) spending a bunch of time and money on making your product more secure, or B) just getting it to the market as soon as possible, which one might you choose?
- Technological lock-in compounds this.

Ask: What was the example of this given in the paper? "We'll ship it on Tuesday and get it right by Version 3" approach that Microsoft and others took in the 90s and early 2000s

4.2.8 Externalities

This is a great example of how an overly-simple model of microeconomic transactions can exclude pieces of a system and hide some of the true costs of things.

We are in New York City, where many people do *not* have cars, but let's assume for this example that we drive cars. One of the most common purchase that anyone with a car makes is the purchase of gasoline. There's supply from oil companies, demand from drivers, they settle on an equilibrium price that best satisfies everyone's preferences and we're all perfectly happy with the trade, right?

What's missing? Does the price of a gallon of gas reflect *all* of the costs associated with burning a gallon of gasoline? No. The price of a gallon of gas does not include the preferences of all the people who have to breathe in my car exhaust and live with the consequences of the pollution. These peoples' preferences are external to the price I pay at the gas pump. In other words I've *externalized* part of the true cost of a gallon of gas onto other people.

An **externality** is a cost or benefit imposed on someone other than the producer or consumer as a result of economic activity.

Side note: I'm being a little bit misleading here, because in many places there are policies in place to explicitly include these externalities and add the costs of pollution into the system. Anyone know one way that governments do this? Gas taxes. One of the ways governments try to internalize th externality is by taxing consumption. This does two things:

1. Taxes essentially just make things more expensive—what does that do to demand? It lowers demand. So raising taxes makes things cost more and as a result people may buy less of it. Generally this an undesireable downside of taxes, but for certain types of goods this may be a

desired outcome. This is why many governments put such high taxes on gasoline and tobacco products, since they produce negative externalities. A tax on market activities that generate negative externalities is called a **Pigouvian Tax**.

2. In the case of gasoline taxes, where does this money actually go? In many places, gasoline taxes fund public transportation. Most public transportation systems do not make enough money on fares alone to remain profitable, so they rely on money from taxes to keep the trains running. This is sort of but not entirely taking into account the externality. It doesn't remove pollution from the air but it does help produce less of it by giving people a viable alternative to driving everywhere.

Ask: Are externalities all bad? No (recall: externality == something that is influenced by a trade but not included in the price).

Ask: What would be an example of a positive externality? If a restaurant puts plants + flowers outside its front door to entice cusomters to come in, the trade is strictly between the restaurant and the flower shop where they bought their flowers. But there is a *positive* externality: The restaurant is more appealing, the neighborhood looks nicer, property values go up, et cetera. When the restaurant bought the flowers do you think they were doing it because they were going to be able to make money off of increased property values? No. It's an externality. But generally seen as a good one! So we call it a positive externality.

Ask: What are some positive externalities in cybersecurity? Example: If I keep my software up to date, I personally benefit from this but I also produce a positive externality because now my device can't be as easily compromised and integrated into some malicious botnet used to DDoS a website.

4.2.9 Free Riding

1. Free riding: very similar problem to the tragedy of the commons
2. Don't know if the term was originally coined regarding public transportation but it's a perfect illustration. If goods are non-excludable, and you can get the benefit of the consuming the good without having to pay for it, what's going to happen? People are going to rationally not pay for it. If the fare gates on the subway are easy enough to hop over, people are going to do it.

Ask: What are the consequences of free riding when dealing with rivalrous goods? In the case of rivalrous goods, it means that whoever is producing the good is getting paid less for it, so it's less enticing to produce the good, so they're going to produce less of it. A shift up in the supply curve. This raises costs for everyone else.

Ask: is this a problem with non-rivalrous goods as well? Yes. Can anyone think of examples?

Ask: What can be done about the free rider problem? Usually the goal is to find some way to make goods more excludable (i.e. full-body fare gates). Also lets not ignore the role that social norms play here, and the ability to shame people who free ride (since a lot of people feel like it's stealing from them in a way).

		Prisoner 1	
		Confess	Do not confess
Prisoner 2	Confess	(5, 5)	(10, 0)
	Do not confess	(0,10)	(1, 1)

Ask: What are some examples from the papers of free riding? It's a problem when security has positive externalities! This might be counterintuitive. If your network being more secure makes your neighbor's network, your neighbhor may try to free ride off of your security investments. Any other examples?

The free rider problem is very closely related to another very famous coordination problem, the Prisoner's Dilemma

4.2.10 Prisoner's Dilemma

This is very famous among not just economists but also policy people, social scientists, mathematicians, computer scientists, et cetera. Who has heard of it before?

This is, in some ways, a game theory version of the free rider problem.

- Imagine youve done some crime with a buddy of yours, and you've both been arrested and put jail in separate cells and can't communicate with each other
- The police don't have enough evidence to convict you both on the principal charge. They plan to sentence both of you to a year in prison for a lesser charge
- But the police offer a bargain:
  - If you confess, and testify against your partner, you go free while your partner gets 10 years in prison.
  - But if you both confess and testify against each other, you will be sentenced for 5 years.
- Both of your are concerned only for your own welfare and although you can't communicate are informed that you've both been given the same deal.
- *What is the rational choice if you are the prisoner?* The best outcome for you and your partner is if you both stay quiet and serve 1 year each. Collectively you serve 2 years of prison time.
- But if you defect from this strategy, you can go free while your partner serves 10 years
- And if you don't defect but your partner does, you are sentenced to 10 years in prison
- The rational strategy is for you to testify against your partner, even though this means you both serve 5 years whereas if you'd just cooperated you'd serve only 1 year each.

Ask: Do any examples in the papers follow this pattern?

One area where this may be happening is in CPU patches for common weaknesses like speculative execution vulnerabilities. Generally agreed upon that customers don't know what is secure and what is insecure but they do know what is fast and what is not fast. Perhaps the best outcome is for all CPU vendors to issue patches and make everyone secure against attacks. This would be the "cooperate" strategy But if you defect (the equivalent of ratting out your partner), your product is fast and your competitors products are slow, so you may gain a market advantage. So the rational strategy is to not issue patches, to the detriment of everyone.

Other examples?

4.3 Conclusion

Conclusions:

- The rational outcome is not the optimal one! Seems to be a common theme here (after all, that is the very definition of a market failure—situations where people following their true incentives lead to suboptimal outcomes).
- There are incentives for people and product vendors to *not* invest in security. No wonder the state of security is so bad!
- It's not just about software engineers writing bad exploitable code. It's part of a whole system and the outcomes are generally not determined by technical factors. But it still is partially due to technical factors! There are very few people in this world who really understand both, but in my opinion this is what is needed if we want to improve security.

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.

5 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.
- 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 – Papers are where the main content is the development of a theoretical model. The ideal theory paper presents a (simple) new model that recasts the way we look at something important.
  - Statistical methods — Theoretical econometrics, e.g. research into statistical methodologies themselves. E.g. coming up with new ways of doing regression.
  - Surveys — not the same as "surveying" people! A review of the literature.
    - Assessed Surveys — just reading and assessing what the most reliable results are. Lots of judgement involved.
    - Meta-studies — attempts to quantify and integrate the results of work in the literature.
- Experiments
  - Lab experiments — you bring in study participants, subject them to some lab condition, observe the result. Controlled, but artificial.
  - Event studies — real world experiments.
    - Field experiments — some people get a treatment while others do not. Expensive! May involve ethical implications. UBI is an example
    - Natural experiments — Taking advantage of some event and studing the effect of it. E.g. two identical towns, one implements a minimum wage, one does not, study what happens.
- Empirics — making inferences from "real" data. Researcher chooses the sample but does not have control over the data generating process
  - Descriptive studies — Trying to find the distribution of one or more variables (e.g. my WTA work). Not trying to test out a hypothesis
  - Classical empirics — Start with a theory, turn into a model. Find supporting data, run regressions. Hypothesis testing
  - Newer empirics — Bayesian techniques, tests of causality, Kalman filters. I don't think any of the papers we'll read rely on too fancy of methodologies, but maybe we'll see some of these.

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.
- A lot of computer systems research is combined with engineering. E.g. "we designed something and then evaluated it". Is that an experiment or empirics? It seems to be more experimental. But subject to same biases!
- Some security papers are empirical.
- Classical empirics seems to have a lot to do with model fitting, which is a domain of machine learning! Anyone here have a good machine learning background might want to try out something along these lines for their course project. What are the issues? Choice of model can give different results....

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.)

6 The Tragedy of the Commons — Modeling Techniques

6.1 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.)

- Why did the author or authors write this paper?
  - Are they trying to open up a dialogue?
  - Are they trying to prove some point that they are going to defend?
  - Are they trying to refute a point someone else made?
- What are the claims they are making in the paper?
  - Do they support their claims with evidence? If so, how good is the evidence?
  - What methods do they use to support their claims? Does it fit into the above taxonomy?

7 Gordon-Loeb — Modeling Techniques

8 Killing Time activity — Look for market failures in homework submissions.