The Economics of Cybersecurity — Lecture 4 Notes

Adam Hastings

January 23, 2024

1 Homework Review

I couldn't access the training since I'd already completed it.

- What did we think?
- How long did it take?
- Was anything surprising?

You now have the credentials needed to conduct studies on human subjects. But that doesn't mean you can actually go out and do it yet. Before you can actually begin, you need to submit a protocol to the IRB to be reviewed and approved. At Columbia they usually have a turnaround time of a few days, but it's highly unlikely that you're going to receive approval on your first try. Not because there's anything wrong or dangerous about your research plan, but because of bureaucratic things, small details, or they're picky with how things are worded. The full process will probably take about a week if you know what you're doing, probably longer if it's your first time.

2 In-Class Experiment

2.1 Loss Aversion

Imagine that you receive $1000. Would you rather:

2.2 Risk Seeking vs. Risk Aversion

Would you rather:

- receive $900?
- take a 90% chance of winning $1000?

Would you rather:

- lose $900?
- take a 90% chance of losing $1000?

What's going on?

- In the first case, people tend to want the sure bet and take the $900, even though the expected value of both options is the same. When dealing with gains, people are **risk averse**
- In the second case, people tend to take the risk, even though the expected value of both options is the same. When dealing with losses, people are **risk seeking**
- Conclusion: People tend to overweigh options that are certain, and are risk averse for gains. Source: https://www.nngroup.com/articles/prospect-theory/

2.3 Post-Experiment Discussion

What are the implications for security?

These are biases that affect human cognition. *Does this mean that humans are irrational?* Maybe it means that the standard definition of "rational" is too simple and too abstracted.

3 Paper Discussion

3.1 Framing the paper

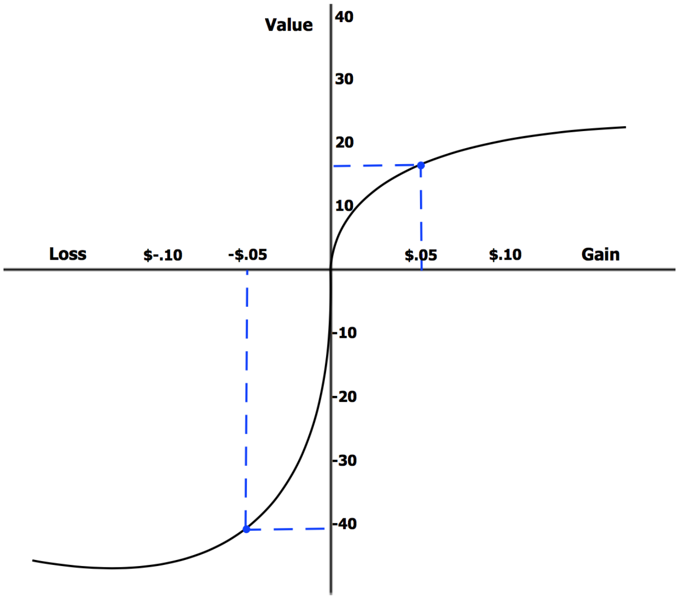

Figure 1: Propsect theory in a nutshell

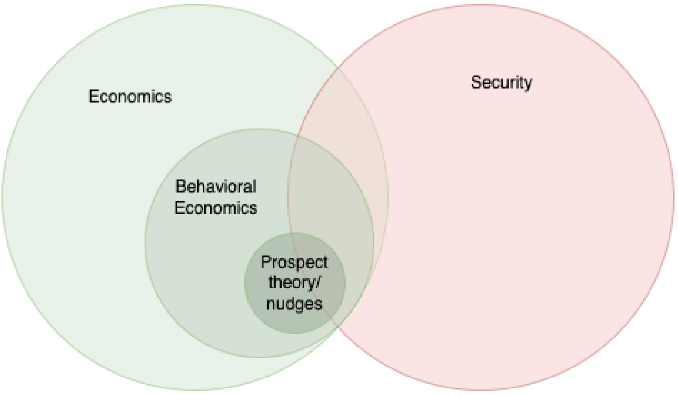

Figure 2: Propsect theory, behavioral economics, and security.

3.2 Intro

I think by this point in the class we have well an truly established that information asymmetry exists in computer security, and that this is a hindrance towards improving security. Whenever this topic comes up, I ask the class for suggestions on what to do about it.

This paper is all about "soft paternalism". Paternalism is when one party has a degree of control or responsibility over another party and makes decisions on their, typically under the guise of it being "for their own good". The word "paternalism" itself comes from the latin word *pater* for "father", so paternalism can be when a child wants to eat cookies for breakfast and their parent says no, because they know what's best for their child.

Can someone define what a "nudge" is for me?

3.3 Incomplete and Asymmetric Information

- A topic we have already covered many times
- One new example: Defenders don't know which vector attackers will use (i.e. not just consumers not being able to acertain quality)

3.4 What is Prospect Theory?

3.5 Heuristics and Bounded Rationality

- In CS we use heuristics to guide algorithms to compute more efficiently (e.g. A* vs Dijsktra's, or hillclimbing to find optima)
- In human cognition, we do the same thing, whether we recognize it or not.
- Just like in CS, cognitive heuristics can lead to traps in local optima
- This produces behavior that seems to conflict with the typical economists' assumption that humans are perfectly rational
  - Was your initial reaction to call B.S. on some of the assumptions economists makes? E.g. Akerlof's assumption that people want infinite cars according to the model.
  - How is it any different that when physicists say "assume a frictionless spherical cow a vacuum"?
  - The point is to abstract away things that have a negligible affect on outcomes when you can.
  - But the point of "bounded rationality" is that sometimes these mental shorcuts that we take *do* have an affect on our behavior and decisions, meaning that as humans we do often deviate from purely rational behavior.
  - You can measure and quantify how far off people are from purely rational behavior, and that you can use this to create more accurate models.
  - Similar to a physicist adding an additional term to an equation to represent friction in a physical model.

Some examples:

- **Availability heuristic:** Paper defines it loosely as "our estimates for event probabilities and likelihoods is shaped by examples we can

3.6 Not in paper? Experiments themselves interfering with results

TODO talk about this.

4 Paper Presentations

5 Danger Zone!

Behavioral Economics is having a bit of a reckoning at the moment:

- Many of the big names in the field have been called out for using questionable research practices or in some cases using outright faked data (Ariely, Gino, Wansink).
- There have been a lot of notable retractions (I don't know if any of the papers cited in our reading paper have been retracted, but there is a citation to a professor at Duke who has recently had several high-profile retractions).
- What can we do? What is the value of this line of research if everything is so questionable?
  - Much of issues of statistically low-powered studies can be fixed by enrolling more participants. In some cases though this is really hard to do and can be quite expensive. It's not obvious what the solution is.
  - Should we say that you can only publish study results if you have 100 participants? Does this mean that only research labs that have lots of money and are good at getting funding can do research?
- Regarding outright fraudulent data—sad but what can you do about it? Science is built on trust and cooperation, and for some there is an incentive to defect from the cooperation strategy (prisoner's dilemma).