The Economics of Cybersecurity — Lecture 4 Notes

Adam Hastings

January 23, 2024

1 Would You Rather

Would you rather:

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

Would you rather:

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

2 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.

3 Paper Discussion

Let's start today's class by framing this paper, since it's at the intersection of several fields:

3.1 Framing the paper

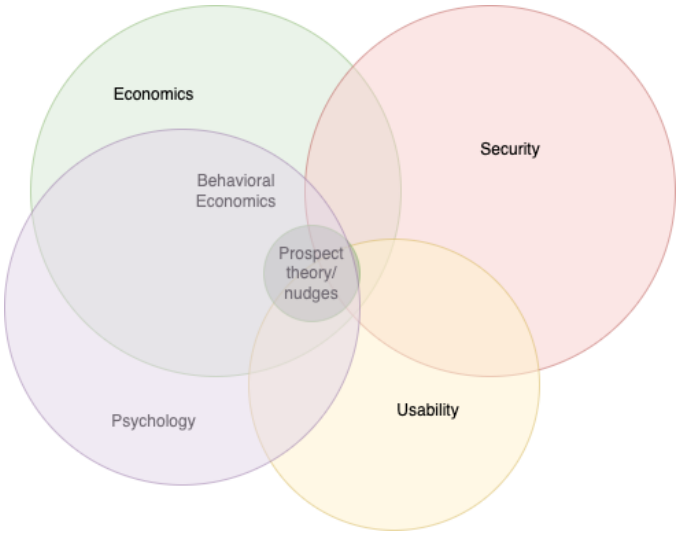

Figure 1: Propsect theory, behavioral economics, and security.

- **Economics and Security:** This intersection is the focus of this class
- **Psychology:** Study of the human mind
- The intersection of these two is **behavioral economics**, which is the study of how and make decisions and why they make the decisions they do. This overlaps with questions of security; this intersection is the topic of today's class.
- So where does this paper fit it? The authors of this paper come from the field of **Usability**, which is the study of how humans interact with systems and the task of designing ways to make interacting with systems and software an easier experience. This intersects with psychology, economics, and security.
- *This paper* is specifically focused on a the intersection of these fields, and in particular it's focused on two subsets of behavioral economics called **prospect theory** and **nudges**, which are closely related and maybe two sides of the same coin.

3.1.1 Prospect Theory

Propsect theory is an alternative to **expected utility theory**, which is the hypothesis used in much of economics that people are rational agents who maximize utility.

Let's try the would you rather questions again:

Would you rather:

- receive $900?
- take a 90% chance of winning $1001?

Would you rather:

- lose $900?
- take a 90% chance of losing $1001?

It's likely that your decisions do not align with classic utility theory! You may have chosen the option that has a lower expected value!

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/

Prospect theory is about capturing these quirks and biases of human cognition and incorporating them into our economic models, tied together by the theme that our decisions are largely driven by the way that our decisions will make us feel rather than strictly by the utility of our decisions. Prospect theory can be summarized using this following graph:

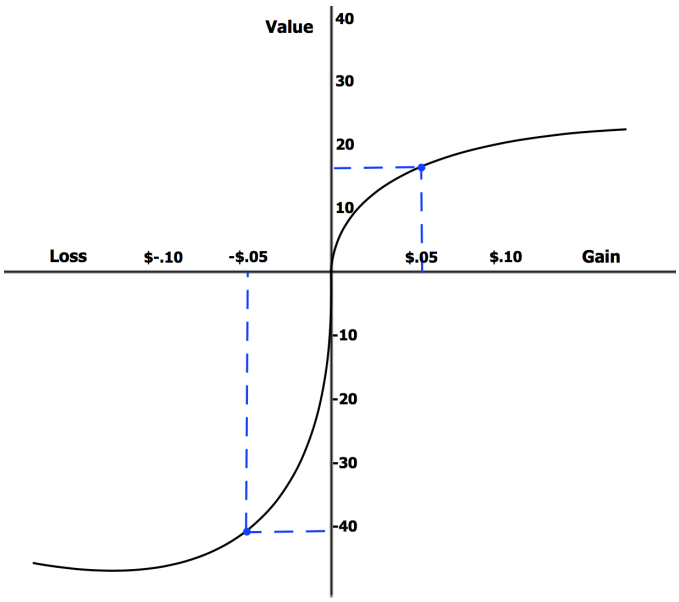

Figure 2: Propsect theory in a nutshell. Diminishing value of utility is expected by classical economics (convex slope). Propsect theory adds the lower portion of this chart. Two things to note: 1) It's asymmetric (loss aversion). 2) It's convex in lower portion (risk seeking instead of risk averse). This chart has been experimentally verified.

3.1.2 Nudges

Prospect theory supposes that humans are "predictably irrational" in quantifiable and expected ways. Nudges are a complement to this, particularly trying to harness or exploit the cognitive biases that we all have. A **nudge** is something that encourages someone to make some decision without either 1) constraining their behavior, or 2) even bringing the nudge to the subjects' attention.

One example: let's say you're in charge of the breakfast buffet at the student dorms. If you place healthy food right at the entrace to the buffet like fruits and vegtables you are likely going to nudge people into eating healthier food. If you place doughnuts right at the entrace, people might eat unhealthier food. If people were perfectly rational they would simply choose what they want regardless of where it's placed, but by exploiting human biases and cognition you can nudge people towards making certain decisions without them even realizing it.

This has lots of implications for security! We've covered that most users don't really understand security and don't know what the tradeoffs are. Yet we don't want to constrain people's behavior. *This paper is a survey of the body of research on how to nudge people towards making better security and privacy decisions.*

Any questions?

This is called "soft paternalism" in the paper. 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".

3.2 Important topics from the paper

3.2.1 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

4 Paper Presentations

What I want from these presentations:

- I want us to get a sense of the type of research in this subfield in cybersecurity economics.
- *But more importantly* I wanted you to dive in to the actual studies and get a sense of what researchers actually do to answer questions in this domain.

4.1 3.2.2 Education in Privacy and Security

4.2 3.2.3 Feedback for Privacy and Security

4.3 3.3.4 Presentation Nudges for Privacy and Security

4.4 3.4.2 Defaults in Privacy and Security

4.5 3.5.2 Costs of Privacy and Security

4.6 3.5.3 Incentives for Security

5 Danger Zone!

Behavioral Economics is having a bit of a reckoning at the moment: It seems to be a field that has a disproportionate share of academic misconduct in recent years.

- 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).
- Many studies do not replicate (replication crisis bleeding over from psychology)
- Signals that people are testing for are likely very weak (i.e. retracted honesty study w/ signature at top vs bottom).
- Small sample sizes (studies are expensive), pressure to publish –¿ p-hacking
- 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).