

Isaac Benioff
CSCI 331

Technical Review of “The Psychology of Security” by Bruce Schneier

“The Psychology of Security” seeks to explain the difference between people’s perception of how secure they are versus how secure they actually are. The paper draws from three major fields of research: behavioral economics, psychology, and neuroscience. The beginning of the paper explains that technological evolution has outpaced biological evolution, and it is our brain’s outdated neural circuitry that is to blame for people’s inability to accurately assess security in the modern age. The rest of the paper focuses on existing research that examines the various heuristics humans use when assessing security. These heuristics are further split into four categories: risk heuristics, probability heuristics, cost heuristics, and decision-making heuristics. For each category, the paper discusses how and why these heuristics lead humans astray so frequently. The paper then concludes by suggesting that further research into the psychology of security would advance humans’ ability to get security trade-offs right, and it would allow us to better unify our perception of security with the reality of security.

Pros of the paper:

- Focusing on security as a trade-off allows for greater insight than examining security solely through its efficacy.
- Multiple studies are mentioned for each heuristic, and the variety provides greater understanding without weighing down the paper in unnecessary detail.
- Convincingly relates discussed research back to security and problems specific to the modern age.

Cons:

- Never addresses the potential methodological issue facing many of the cited studies: the most common test subject is college students.
- Cost discounting research was interesting but it was unclear how it related back to security and whether the described behavior was positive or negative.
- Time discounting research faced similar issues, and the studies presented were too similar and specific to money to convincingly relate back to security.

Overall, I would say the paper is a good one, and most importantly a self-aware one. Early on in the paper, we find the following passage:

“And if this paper feels haphazard, it’s because I am just starting to scratch the surface...much of this essay is me saying: ‘Look at this! Isn’t it fascinating? Now look at this other thing! Isn’t that amazing too?’ Somewhere amidst all of this, there are threads that tie together, lessons we can learn...”

Indeed, the paper is more of a public service announcement than anything else, and in that capacity, it performs very well. It does not tie the threads for you nor pinpoint the lessons. What it does do, however, is grab your attention. It forces you to take seriously the psychology of security, and it alerts you to the fact that data and technical prudence have their own (often subtle) limitations.

In particular, I think the decision to conceptualize security as a trade-off with five components (risk severity, risk probability, cost magnitude, countermeasure efficacy, ability to compare disparate risks and costs) made it easier to both organize and understand the mass of research that the paper references. None of the research discussed in the paper deals directly with security, only the components of the security trade-off. This relieves the paper from a research burden—there is limited research that deals with the psychology of security specifically—but it also relieves the paper from the rhetorical burden of explicitly linking each and every discussed study back to the topic of security. Instead, the paper is free to, for example, explore the ramification of a given heuristic in the context of the modern age, such as when the paper details the dangers of the availability heuristic being coupled with the modern mainstream media.

However, this strength is also the paper's biggest weakness. Not having to explicitly link research back to security means that sometimes the link stays murky. For example, most sections on heuristics cited multiple studies, and each new study mentioned involved participants making different types of choices. However, in the cost heuristic section, every study involves monetary choices. Because of this, it is harder to discern whether the implications of the study generalize to other types of decision making, or if they simply represent a misunderstanding of basic economic principles (e.g. the "\$250 today or \$350 in twelve months....\$3,000 today or \$4,000 in twelve months" study strikes me as mostly representative of the fact that most people are not cognizant of the effect inflation has on the real value of money over extended periods of time).

Additionally, sometimes links stay murky because of methodological issues in the cited studies. Admittedly, the paper often uses collections of studies to prove its point instead of one specific study, so the integrity of one study does not necessarily call into the question the integrity of the whole paper. Still, the paper does itself no favors by saying something like, "If you read enough of these studies, you'll notice...college students are the most common test subject." Considering that the paper places such a heavy emphasis on neuroscience and brain development as an explanation for our false "feeling" of security, it is dubious to use mostly studies whose subjects are known to have only partially developed brains. Moreover, the area of the college student brain that is usually still under the most development is the neocortex (it generally takes 25 years before the neocortex is fully developed). Seeing how the paper spends most of its time detailing "examples of these newer parts of the brain [the neocortex] getting things wrong," it strikes me as a glaring omission to not mention that most of the participants in these studies do not have fully developed neocortices.