Security Engineering Question Sheet 3: Lectures 5 and 6

Ross Anderson & Yuvraj Patel*

Here are a set of questions to help you think through the topics covered in lectures 5 and 6, on Economics and Psychology. We will consider these in the tutorials, so be prepared to discuss them.

1. a) Explain in terms of Game Theory why people are often nastier on the internet than in real life.

   b) "*A Hawk-Dove model is really just a Prisoner's Dilemma in disguise. They have the same dominant strategy, and that dominant strategy is Pareto-suboptimal.*" Is this statement ever true?

   c) Do the circumstances in which is it not true indicate any strategy for mitigating unpleasant behaviour online?

2. To what extent is the considerable damage caused by the Mirai botnet down to negative externalities?

3. In the US, monopolies have traditionally been measured by their effect on consumer surplus: i.e. whether customers pay vastly more than the supply cost. Google search is free, and holds over 90% of the market. So is there any negative effect on the consumer from this lack of competition in the search market?

4. Antivirus software is sometimes considered a "market for lemons". To what extent is this true, and is it down to hidden information, hidden action, or both?

5. Social media networks already spend significant effort on removing some forms of content, e.g. child sex abuse material, and yet they are less willing/able to deal with other forms of abusive content from "the swamp". Is this purely an issue of incentives, and if so might the right legal intervention be able to solve the issue?

6. Imagine that you are designing a spearphishing attack designed to scam Edinburgh students out of money. How would you do it, who (or what) would you impersonate, how would you extract the money, and could you use Prospect Theory to increase your chances? Are there any other social-psychology tricks that might help?

7. Do passwords have a compliance-budget issue? Does this have anything to do with the "Tragedy of the Commons"? Is this made better or worse by 2FA?

8. How do we know that "blame and train" isn't the right approach? Why might some companies try it anyway?

*Material adopted from the class taught by Prof. Ross Anderson & Dr. Sam Ainsworth in 2022.