Security Engineering Question Sheet 1: Lectures 1 and 2

Ross Anderson & Yuvraj Patel[*]

Here are a set of questions to help you think through the topics covered in our first two lectures on Opponents and Threat Models. We will consider these in the tutorials, so be prepared to discuss them.

1. All large software has bugs in it, and the most powerful nation-state actors will have a collection of zero-day attacks for all of the most popular systems. So why is installing the latest software updates still good security advice for most people in spite of this?
2. Suppose you run a web service that has become targeted by political activists. What sorts of attacks might they be able to launch at your system, and how might you defend against them?
3. Why would Google run a hacker team like Project Zero (`https://googleprojectzero.blogspot.com`)?
4. Microsoft describes the apps on its Windows Store as "trusted" (`https://support.microsoft.com/en-us/account-billing/get-trusted-apps-and-games-from-microsoft-store-on-windows-773745c0-e4e8-4f8e-b14f-6b7c2051cf9f`). Is this good news or bad?
5. When might it be desirable or even possible to implement a system with both BIBA and Bell-Lapadula guarantees simultaneously?
6. How might the concept of "Separation of Duty" as used in book-keeping systems also be applicable to writing secure code? In what ways might it be less applicable?
7. Why might the poor "Policy" ("This policy is approved by management...") pass as a valid security policy in many companies?

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