Problem Class 2 (Security Engineering 25/26)

Network Security (Lecture 8)

1. "De-perimeterization is great. I don't have to worry anymore about malicious or out-of-date devices on my network anymore." To what extent is this statement true? Does the Mirai Botnet tell us anything about de-perimeterization?
2. How comfortable would you be logging into your bank account on a public airport WiFi? Would a VPN offer you additional protection in this scenario?
3. The default settings used in VPNs are probably intentionally weak. So, do VPNs have any value in any setting?

Hardware Security 1 (Lecture 9)

4. What's the point of locks, if they can be so easily bumped? Why even bother breaking a lock if you can just smash a window?
5. Might an IoT device need some forms of tamper resistance? What about a video games console?
6. Differential Power and Fault analysis are really complicated. You are a CISO trying to explain to your CEO the possible attacks that may occur on your new IoT device, of which you have produced 3 million units. How far up the list of risks should these attacks be, and how would you explain their potential for damage and the circumstances under which this damage could occur?

Hardware Security 2 (Lecture 10)

7. A Rowhammer attack requires the rapid access of rows within the CPU's Random Access Memory. However, all modern systems have caches that act as a fast buffer for frequently accessed memory. Does such a cache make a Rowhammer attack impossible, given that it typically reduces the rate of access to main memory?
8. To eliminate Spectre attacks, your boss suggests you buy a processor without a cache. How effective do you think this might be, how feasible, and would there be any disadvantage?
9. Does Intel Software Guard Extensions (SGX) eliminate Spectre attacks? If so, how? If not, what does SGX achieve? Is SGX only beneficial in a data centre, rather than on end-consumer hardware?
10. Why do we need remote attestation? Can't we just trust that a good data centre will be running the right thing? Are there any parts of the system for which the guarantees on attestation provided by e.g. a TPM or SGX are insufficient?

OS Security (Lecture 11)

11. “All access control is just a matrix matching users to files, so capabilities and access control lists are exactly equivalent.” How accurate is this statement?
12. “The mandatory access control mechanisms in Android just serve to take control away from the user and place it in the platform holder’s hands. Any benefit to the consumer is just an illusion.” How accurate is this statement?
13. Why would Apple only store biometrics in their own proprietary Secure Enclave, rather than using TrustZone and/or allowing access to the iOS kernel more generally? Does this really improve security?
14. “The comparison between containers and virtualization shows that all new, under-tested technology is bad for security.” Do you agree with this statement?
15. “Isolation costs money, and so there will inevitably be a race-to-the-bottom on security technologies in the cloud.” What might this statement be referring to, and to what extent is it true?