Security Engineering Question Sheet 4: Lectures 7 and 8

Yuvraj Patel

Here are a set of questions to help you think through the topics covered in lectures 7 and 8, on Networks and Hardware Security 1.

1. “Deperimeterisation 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 I don’t have to worry anymore about malicious or out-of-date devices on my network anymore.”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 deperimeterisation?
2. Can we trust anything we do online, given the known weakness of protocols such as BGP, and the various limitations of Certificating Authorities?
3. The default settings used in VPNs are probably intentionally weak. So do VPNs have any value in any setting?
4. 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?
5. 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?
6. Why is MiFare Classic such a weak protocol? If you have a building using it, what steps might you take to improve assurance?
7. Explain how Deter-detect-alarm-delay-respond might be relevant in a home security environment.
8. Might an IoT device need some forms of tamper resistance? What about a video games console?
9. 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, which you have produced 3 million units of. 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?