Security Engineering Question Sheet 6: Lectures 11 and 12

Prof. Ross Anderson & Yuvraj Patel

Here are a set of questions to help you think through the topics covered in lectures 11 and 12, on Operating Systems 2 and Ecosystems Security.

1. *"The comparison between containers and virtualization shows that all new, under-tested technology is bad for security."* Do you agree with this statement?

2. *"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?

3. Compare the isolation features between processes in Android to the isolation features provided by a virtualization environment such as VirtualBox.

4. 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 for?

5. Why would you bother attacking the supply chain, when most systems use large amount of software that are buggy and/or out-of-date, and spearphishing attacks are so easy to pull off?

6. Why is a Mobile Network Operator less incentivised to patch your phone than Google or Apple? Why does Apple update for longer than Google?

7. How does the existence of App stores alter ecosystem-wide security on mobile phones?

8. Is Apple's IDFA (ID for Advertisers) good or bad?

9. *"Open-source code should be used wherever possible. It has more eyes on it than closed-source applications, so is less likely to be buggy or malicious."* To what extent do you agree?

10. On the Steam website (`https://partner.steamgames.com/doc/features/drm`), Valve has this to say about its DRM mechanisms for its video game store.

    "The Steam DRM wrapper by itself is not an anti-piracy solution. The Steam DRM wrapper protects against extremely casual piracy (i.e. copying all game files to another computer) and has some obfuscation, but it is easily removed by a motivated attacker.

    We suggest enhancing the value of legitimate copies of your game by using Steamworks features which won't work on non-legitimate copies (e.g. online multiplayer, achievements, leaderboards, trading cards, etc.)."

    How might Valve improve the level of assurance given by their anti-piracy solutions, and why might they choose not to do so?