UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR11208 SECURITY ENGINEERING PG AND INFR11228 UG

Wednesday 24th May 2023

13:00 to 15:00

INSTRUCTIONS TO CANDIDATES

Answer any TWO of the three questions. If more than two questions are answered, only QUESTION 1 and QUESTION 2 will be marked.

All questions carry equal weight.

CALCULATORS MAY NOT BE USED IN THIS EXAMINATION.

Year 4 Courses

Convener: K.Etessami
External Examiners: J.Bowles, A.Pocklington, R.Mullins

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. **Cloud Environments**

You are the chief architect of a new cloud service that will let users run their virtual machines and containers in your data centers.

(a) What threat model will you consider for your data centers, and for your service more generally? [*10 marks*]

(b) What mechanisms will you employ to ensure that your data centers are dependable and secure? [*5 marks*]

(c) What assurances would you ask from customers to ensure that their applications and data pose no threat to you or to other customers. [*5 marks*]

(d) Can you provide a list of extra assurance mechanisms that you as a cloud service provider can offer the customers? [*5 marks*]

2. **Operating Systems for Mobile Phones**

You have joined a startup that is designing a new class of consumer device and the group you have joined is developing an OS and an app ecosystem to support the new product.

(a) What would be safer from the ecosystem security viewpoint – an open system like the Android Play Store where the developers sign the binaries or a closed system like Apple where you sign the binaries? Explain the reasons behind your choice. [*5 marks*]

(b) One of the founders is arguing in favor of an open ecosystem and making the OS source code open source too, on the grounds that the priority should be getting the network effects going; if you win the race to market you can lock things down later. But you feel uneasy about open sourcing the code. How might you argue this point with colleagues from a security perspective? [*10 marks*]

(c) What testing strategy will be employed to test the OS? [*5 marks*]

(d) What strategy would you use to monitor the ecosystem as it develops? [*5 marks*]

3. **Protecting against adversaries**

Suppose a medium-sized country A is attacked by a large neighbour B.

If both civilian and military organisations in A are using end-to-end encrypted messenger systems like WhatsApp and Signal, what interception options does B have against these systems:

(a) By exploiting the handsets? [*5 marks*]

(b) By exploiting the end users? [*5 marks*]

(c) By exploiting the network? [*5 marks*]

Furthermore,

(d). What extra exploitation options might B's intelligence agency have if B is a major power? [*5 marks*]

(e). If you're advising a company in country A that might be a target of action by B, what defensive measures would you tell them to prioritize? [*5 marks*]