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.

This is an OPEN BOOK examination.

Year 4 Courses
Convener: ITO-Will-Determine
External Examiners: ITO-Will-Determine

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY
1. (a) Explain Prospect Theory as it applies to decision-making. [6 marks]

(b) You are the operator of a scam designed to steal passwords for a popular online shopping website.
   
   i. How would you exploit attitudes to risk to maximise the number of victims? [4 marks]

   ii. How would you extract value from the scam? [4 marks]

   iii. How would you expect the shopping website’s operator to respond? [4 marks]

(c) Hal Varian described the software industry business model as being “bargains then ripoffs”: initial low-cost enticement, followed by rising prices once users are locked in. Describe how these dynamics impact security as well as cost. [7 marks]
2. You are working as a consultant for a small social-network company, who are worried about being fined in the event of a data breach, but are anxious to keep costs down. To cut costs, the company is thinking of moving its hosting from on-premises servers to a US cloud service.

(a) What attacks are made easier by the move to cloud hosting? [8 marks]

(b) What attacks are made harder by the move to cloud hosting? [8 marks]

(c) The company has listened to your concerns in part a, and suggests that they can be mitigated effectively using a variety of the latest technological mechanisms. What mechanisms may be relevant to such a discussion, and how might the system still be attacked? [9 marks]
3. (a) Access control is nominally a triple of \((user, program, file)\). Explain to what extent this manifests in
   
i. Windows [4 marks]
   ii. Android [4 marks]
   iii. Linux [6 marks]

(b) “If a process running at root-level privilege is compromised, the security of an Android phone is entirely defeated.” To what extent is this statement correct? [5 marks]

(c) Explain how a user may gain “root” access to an Android device, even without a software bug in the kernel. [6 marks]