UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFR11208 SECURITY ENGINEERING

Friday 13 th May 2022

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.

This is an OPEN BOOK examination.

Year 4 Courses

Convener: K.Etessami
External Examiners: J.Bowles, A.Pocklington, H.Vandierendonck

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

1. (a) Explain how the use of cryptography might differ between a messaging application (e.g. WhatsApp) and a social media network (e.g. Instagram). [*5 marks*]

   (b) Explain how the threats to the following actors might differ from each other on a messaging application such as that in part a). To what extent would end-to-end encryption improve their defences against their most likely adversaries? Explain in each case how the security of the application might be subverted despite the existence of end-to-end cryptography.

      i. A media celebrity, currently having an affair. [*5 marks*]

      ii. A high-ranking government officer. [*5 marks*]

      iii. A domestic abuse victim. [*5 marks*]

   (c) SpaceFace, a messaging app for children, has recently removed end-to-end cryptography from their service, citing both usability concerns and dangers to children. To what usability issues might they be referring, and to what extent are concerns of danger warranted? [*5 marks*]

2. (a) MegaCorp, a cloud operator, is currently offering heavily reduced rates if customers switch from using virtualisation to using containers. Why might they be offering such a discount, and what might the security implications be? [*6 marks*]

   (b) The CEO of MegaCorp has heard of the Spectre attack and side channels more generally, and sees an opportunity to sell a premium service to customers to mitigate the attack vector. What options are available to the CEO, what might the threats be, and how effective might any mitigation be from a security-engineering perspective? [*6 marks*]

   (c) i. On which of Windows and Linux is creating a file that can only be written as append-only more straightforward? [*4 marks*]

   ii. Explain how on each of Windows and Linux you would create such an append-only file. If it requires non-trivial engineering in either case, sketch a design and extend your answer to consider how you might make the file append-only on Wednesdays, and writable otherwise. *Note: Assume no access to any features not covered in the course, such as chattr, and that SELinux is not available.* [*9 marks*]

3. (a) From 2012 onwards, Microsoft has given away upgrades to its latest versions of its operating systems for free, whereas previously (before Windows 8) it used to charge for each new release. This means that an existing user of Windows 10 can upgrade to Windows 11 at no cost, or stay on Windows 10 and still receive security updates until 2025. In terms of security economics, what might motivate such a change in policy? [*5 marks*]

   (b) With Android 4.0 in 2012, Google changed strategy with its web browser. Previously, this was called "Browser" and was updated with the operating system. Following this date, it was switched to "Chrome", which was updated using the Google Play infrastructure. What might motivate such a change, and would we expect an improvement in security as a result? [*5 marks*]

   (c) A purchaser of second-hand devices has a choice between four different systems to use to connect to the internet. Place them in order with, in your opinion, the level of security you would expect them to provide, from weakest to strongest, giving justification. What would you expect the weakest part of each system would be? State any assumptions you make in your answer.

      i. An Android phone running Android version 9 (release date 2018).
      ii. A four-year-old iPhone X.
      iii. A Chromebook with Auto Update Expiry date 20th December 2020
      iv. A Windows Laptop, purchased in 2012.

   [*10 marks*]

   (d) You are the owner of a nuclear reactor. How might your security concerns differ from those of the purchaser in part c), how might you achieve assurance of security, and what issues might you face in doing so? [*5 marks*]