The University of Melbourne

SWEN90010: High Integrity Systems Engineering

Assignment 1

Due Date: 11:59pm (Melbourne time), Sunday 28 March, 2021

This assignment is worth 10% of your total mark.

You will work in pairs for the assignment. Each pair will submit only one solution, produced jointly by both partners. Working in pairs is important since a significant part of the assignment is brainstorming security threats to a system, using the STRIDE methodology discussed in lectures. As with other brainstorming activities, security threat enumeration is an inherently creative process that will benefit from being performed by a pair, rather than by a single individual.

Your assignment solution will consist of a written report that answers the questions, and carries out the tasks, listed below.

1 Background

A fictitious state government wants to deploy a *COVID check-in* system, called *COVIDSafer*. The system comprises an app that runs on users' mobile phones. Users use the app to "check-in" as they visit shops, restaurants, and other locations around their city, by scanning QR codes. For example, when a user visits a restaurant, the restaurant owner asks them to scan a QR code on their phone that causes the COVIDSafer app to be loaded. On the first use, the user enters their name and contact deatils (phone number, email address, etc.). This information is then uploaded to a central database creating a *record* that contains the user's information as well as the current date and time of day, and the location the user is visiting (e.g. the name and address of the restaurant that the user is visiting). This location information is encoded in the QR code. The phone app saves the user's information so that on subsequent check-ins the user does not need to re-enter it.

The COVIDSafer app uploads all records to a central database that is designed to be accessed by contact tracing employees, i.e. people employed by the government to carry out contact tracing in the event that a person returns a positive COVID test. Contact tracing staff access the central database via a web based *Contact Tracing Portal*, which they log-in to from a computing devices (e.g. desktop PC).

2 System overview

The system contains a number of distinct components.

User Devices, COVIDSafer app, and QR Codes Ordinary users access the system via the COVIDSafer app running on their mobile phone. The app is responsible for scanning QR codes: each QR code encodes the location that the user is checking into, plus any additional information needed to guard against security threats that you might identify during this assignment.

Genuine QR codes are printed by the government and supplied to business owners. The genuine

COVIDSafer app was written by the government and (perhaps surprisingly) can be assumed to be free of bugs for the purposes of this assignment.

Users' mobile phones are of course under their own control.

App Authenticity You might identify certain threats that arise when the user *mistakenly* runs a fake COVIDSafer app. For the purposes of this assignment you can assume that all users who think they are using the genuine COVIDSafer app really are using the genuine app, and that this application is trustworthy. Hence, threats in which the COVIDSafer app is spoofed or impersonated *to the user* can be ignored. This does not exclude, however, threats that might arise when a malicious user chooses to run an app that impersonates the COVIDSafer app *to the central database.*

Central Database The central database receives updates from user devices. Each update adds a new record to the database containing the information described above.

The central database is administered by a third-party (e.g. Amazon AWS) to whom its administration and management has been outsourced by the government.

Contact Tracing Portal The contact tracing portal is a web-site used by contact tracing staff to access the central database. The portal allows contact tracing staff to run certain queries on the central database, e.g. to find all users who were in a particular location at a particular date and time.

The contact-tracing portal is administered by the government.

Contact Tracing Devices Contact tracing staff access the contact-tracing portal via devices, e.g. desktop PCs. These devices are provided to contact-tracing staff by their employer (the government), who also administers them.

3 Your Tasks

1. [**(1 mark)**] Draw a block diagram of the architecture of the system, including its main components and the legitimate channels of communication between them.

   For each component, describe in no more than a few sentences:

   (a) Who has control over that component?

   (b) What is its role in the system and how is it intended to interact with the other components?

   On your diagram, indicate the trust boundaries that exist within the system. For each trust boundary, describe who controls the components within that boundary.

   Trust boundaries can only exist *between* components (not *within* them, i.e. a single component can live inside only one trust boundary).

2. [**(4 marks)**] Use the STRIDE methodology to enumerate potential security threats to the system. For each threat that you identify you should document:

(a) Who is the potential attacker that might try to exploit this threat?

(b) What is the security goal that the attack or threat would violate if it were successful?

Importantly, your report should *document and justify any assumptions you make while carrying out your analysis.* The system description provided above is intentionally ambiguous. You might therefore need to make certain assumptions when carrying out your analysis. You should make sure that your assumptions are reasonable, by including with each a brief justification.

Try to make each of your threats specific. For example, the threat that an attacker might try to impersonate a contact tracing staff member is a bit vague. How might they try to impersonate the contact tracing staff member and for what purpose? You should be more specific, e.g.: "an attacker might pretend to be a contact tracing staff member when logging in to the contact-tracing portal. That could allow them to learn information including ....".

3. [**(2 marks)**] For each of the threats that you identified, which are the most serious? To work this out, for each threat you should think about what are its potential consequences. Use the IEC 61508 Consequence Classes (which range from Negligible to Catastrophic) discussed in lectures to rate the severity of each threat, including a brief justification for each.

4. [**(3 marks)**] Based on the assessment of the severity of each threat, derive a corresponding set of security requirements for the system that would address or mitigate that threat.

   List for each threat the requirements that are needed to mitigate it. If a threat cannot be reasonably mitigated, you should say why (including any assumptions you are making that lead you to believe the threat cannot be mitigated).

   Number each of your security requirements that you derive. That way, if one security requirement helps to address multiple threats, you don't need to repeat it.

   As an example, if you decided that one threat was that an attacker might try to impersonate a contact tracing staff member to the contact tracing portal, then a corresponding security requirement for the system would be that the contact-tracing portal needs to properly authenticate contact-tracing staff members, e.g. via a username and password.

   Of course, you might then worry that the password could be stolen by the attacker while in transit on the network from the contact-tracing staff member's device to the contact-tracing portal. So you might decide that the network connection between the contact-tracing device and the contact-tracing portal needs to be encrypted.

   Note: this is not a subject about encryption. You don't need to specify the precise encryption scheme or protocol to be used. However it may help to have a high-level understanding of basic cryptographic techniques like public key encryption, digital signatures, symmetric key encryption, message authentication codes, as covered in a subject like COMP90043 - Cryptography and Security or basic overview references like `http://ccss.usc.edu/499/lecture2.html`.

4 Marking Criteria

There is not a set of right or wrong answers for this assignment. Instead, it is testing your ability to understand and apply the concepts presented in lectures about security and safety engineering.

If you think that some of the requirements are ambiguous, then you should decide on an appropriate interpretation and, very importantly, you should document what your interpretation was. That way, you cannot be penalised for making an assumption that is different to what I or the markers had in mind.

You are also free to discuss the requirements on the LMS, especially where you think they are ambiguous, to help clarify them.

5 Submission

One of your pair should create a pdf file called *your_username*`.pdf`, containing your joint answers to the questions. Submit it via the LMS.

6 Communication Rules

You may discuss the questions freely within your pair, and write up your joint answers together. You may also consult any other materials you find on the Internet (or in the library), as long as you give proper references in your report. You may *not* discuss this with anyone other than your project partner. In particular, cross-pair collaboration is not allowed. However, you may ask or answer any question you like on the LMS discussion board—this is up to you. You may share answers or raise interesting questions if you like, for the benefit of all. This allows ideas to be shared but mitigates the (unfair) advantage of having clever friends.

7 Late submissions

Please submit on time. It's much better to submit a not-quite-finished version on time than a perfect version late. 1 mark will be deducted each day (or part thereof) after the submission deadline. If you have a real reason for needing an extension, please ask permission in advance. I will usually ask to see some form of evidence, e.g. a medical certificate.

8 Academic Misconduct

The University misconduct policy applies to this assignment.

The subject staff take plagiarism very seriously. In the past, we have successfully prosecuted several students that have breached the university policy. Often this results in receiving 0 marks for the assessment, and in some cases, has resulted in failure of the subject.