UNIVERSITY OF WATERLOO
Cheriton School of Computer Science

CS 458/658 **Computer Security and Privacy** **Spring 2018**
Hassan Khan

ASSIGNMENT 1

Blog Task signup due date: **Mon, May 14, 2018 *3*:00pm (no extension)**
Milestone due date: **Fri, May 25, 2018 *3*:00pm**
Assignment due date: **Mon, June 4, 2018 *3*:00 pm**

Total Marks: 52 (+10 bonus)
Blog Task TA: Masoumeh Shafieinejad
Written Response TA: Pierfrancesco Cervellini
Programming TA: Sung-Shine Lee and Navid Esfahani

Please use Piazza for all communication. Ask a private question if necessary. The TAs' office hours are posted to Piazza.

Blog Task

0. [0 marks, but -2 if you do not sign up by the due date] Sign up for a blog task timeslot by the due date above. The 48 hour late policy, as described in the course syllabus, does not apply to this signup due date. Look at the blog task in the Course Materials, Content section of the course website to learn how to sign up.

   Please visit https://crysp.uwaterloo.ca/courses/cs458/infodist/blogtask.php to sign-up.

Written Response Questions [22 marks]

Note: Please ensure that written questions are answered using complete and grammatically correct sentences. You will be marked on the presentation and clarity of your answers as well as on the correctness of your answers.

Your mission, should you choose to accept it…

You are an employee of a well-known-for-being-shady political consulting firm Oxford Analytica (OA). Over the last month, things have become murkier than usual and allegations have surfaced

that the company has been misappropriating people's data in an effort to influence the presidential election. OA is a large company so when by pure happenstance you catch an UberPool with two members of the data harvesting team, they don't recognize you. They are talking about their work, and what you hear makes it clear—it is time to blow the whistle.

1. For each of the following, please:

   - identify the scenario as a compromise of Confidentiality, Integrity, Availability, and/or Privacy,
   - and, briefly explain your choice of compromise.

   (a) (2 marks) You discover that a few years back Oxford Analytica used a mobile application to harvest a few hundred thousand Facebook profiles, but it turns out that due to loose restrictions by the Facebook's API they were able to download the full profiles of close to 52 million unsuspecting users who were friends of the mobile application users.

   (b) (2 marks) Fortunately, so many access attempts from the mobile application is detected by Facebook. However, the defense strategy of Facebook prevents all further incoming requests from the IP that is used by the mobile application.

   (c) (2 marks) Unfortunately, though 52 million data points are a lot, they are not enough to create an accurate model for the election that the company is trying to influence. One of them recommends adding a few million fake profiles to the data. After all, who would know.

   (d) (2 marks) The other seems to think this is a good idea. He adds that OA's Chief Security Officer has privately revealed to him the existence of a company owned, secret server farm that does not track any usage metadata. If they dumped the fake data there, truly no one would know they made it all up.

   a. Confidentiality: profiles of friends of users should not have been reachable.
   b. Availability: The user is not longer able to access Facebook.
   c. Integrity: the additional needed profiles are made up.
   d. Confidentiality: the existence of the secret servers should not have been divulged. Also, integrity since they are also talking about dumping data

The whistleblower

You are unsettled by the conversation you overheard, but if you are going to blow the whistle, you need more information, and hard facts to prove Oxford Analytica is up to no good. You

start doing some old fashioned detective work, and soon people start realizing your questions might be just a little too specific. You start getting clues that you may have overplayed your hand.

2. For each of the following, please:

   - answer which of interception, modification, interruption, and/or fabrication, threats are represented in each of the following scenarios
   - and, give a brief explanation for each of your answers.

   (a) (2 marks) Looking through your company repository commit history you notice strange commits you do not recognize and do not remember doing.

   (b) (2 marks) After taking a closer look you discover some of the commits are changes to an authentication protocol for access to secret client files.

   (c) (2 marks) On a hunch you decide to check the internet packet routing from your work terminal and discover that your data is going through a hop that should not be there.

   (d) (2 marks) The most obvious hint that something is very wrong is that you seem to have lost access to the more sensitive company files.

   a. Fabrication: someone manufactured those commits and posted them under your name
   b. Modification: some of your previous code was modified.
   c. Interception: someone is intercepting your data.
   d. Interruption: your access has been interrupted

Running for cover

You made up your mind about exposing Oxford Analytica and are considering contingencies to minimize your own risks.

3. For each of the following, please:

   - explain how you could use the defense to your advantage
   - try to provide context that fits the narrative of your Oxford Analytica assignment.
   - The first one has been done for you.

(a) Deflecting.
Place some incriminating documents on the desk of a co-worker with a history of misbehaviour.

(b) (2 marks) Preventing.

(c) (2 marks) Detecting.

(d) (2 marks) Recovering.

There are many options here. A few examples below:

b. Preventing: check the validity of the certificates of the websites you browse to. Make sure they come from a trusted CA.

c. Detecting: have your version control software send you a confirmation email when you send in a commit.

d. Recovering: backup data in secure locations that OA may not be able to reach.