COMP0141 Security
Tutorial 1

Questions

1. Consider a student information system (SIS) in which students provide a university student number (SN) and a card for account access. Give examples of confidentiality, integrity and availability requirements associated with the system and indicate the degree of the importance of the requirement.
2. Which of the following attacks are attacks on (1) **confidentiality**, (2) **integrity**, (3) **availability**?
   (a) Opening my neighbour's letter without their consent
   (b) Installing malware on a data server that has private information in order to transmit the data to attackers
   (c) Conducting a ransomware attack that encrypts data on targeted computers so that the authorised parties cannot use it in order to compel them to pay a ransom to the attacker
   (d) Deliberately disrupting a server room's power supply in order to take those servers offline
   (e) An employee is putting sensitive data on a removable media device such as an SD card or an optical disc and giving it to unauthorised parties
   (f) Eavesdropping a phone conversation
   (g) Maliciously accessing a financial server in order to falsify financial records
   (h) Maliciously erasing disk containing important information
   (i) Pushing an update to an app that modifies its permissions without notifying the users
   (j) Showing different users different views of the same web page
   (k) Sharing a patient's medical record (or any sensitive data in other contexts) without their consent
   (l) Obtaining more data than necessary for the purpose of a task
3. Are these (1) **threats**, (2) **impact** (i.e, harm) or (3) **vulnerabilities**? (justify)
   (a) Thieves can enter the lab to steal equipment
   (b) Credit card numbers were stolen
   (c) Users choose weak passwords
   (d) A backup system stopped working
   (e) A hacker can install malware
   (f) Students can see the exam questions before the test
   (g) A machine learning algorithm that is used to make important decisions is biased, or has a significant error rate
   (h) I am staying at a hotel that gave me access to my room without verifying my identity
4. Is this a security problem? (justify)
   (a) I need to send a wireless signal in an environment where there may be obstacles (walls, rain, ...)
   (b) I need to keep my valuable laptop in my car to go shopping
   (c) I need to build a boat that floats under adverse conditions (storm)
   (d) I need to store the secret final exam on a server open to the internet

(e) I need to make sure I am talking with my lawyer over the phone

(f) I inadvertently added an infinite loop and took down my server

(g) My operating system offers full disk encryption, but really just uses the hard disk encryption mechanism

(h) I am connected to a public wireless network that does not seem to be encrypted

(i) I have sensitive information on my laptop/smartphone and have to go through strict border control

(j) I cannot verify that the downloaded software comes from the intended software distributor

(k) My hardware and/or software is manufactured in a country that is hostile to my country

(l) I have lost my phone and it suspiciously reappears after some time

(m) I am going to an event that has deployed facial recognition cameras

5. Consider the following situation: *Los Angeles Unified School District started issuing iPads to its students this school year, as part of a $30 million deal with Apple. Now Sam Sanders reports at NPR that less than a week after getting their iPads, high school students have found a way to bypass software blocks on the devices that limit what websites the students can use. The students are getting around software that lets school district officials know where the iPads are, what the students are doing with them at all times and lets the district block certain sites, such as social media favourites like Facebook. 'They were bound to fail,' says Renee Hobbs, who's been a sceptic of the iPad program from the start. 'There is a huge history in American education of being attracted to the new, shiny, hugely promising bauble and then watching the idea fizzle because teachers were not properly trained to use it and it just ended up in the closet.' The roll out of the iPads might have to be delayed as officials reassess access policies. Right now, the program is still in Phase 1, with fewer than 15,000 iPads distributed. 'I'm guessing this is just a sample of what will likely occur on other campuses once this hits Twitter, YouTube or other social media sites explaining to our students how to breach or compromise the security of these devices,' says Steven Zipperman. 'I want to prevent a "runaway train" scenario when we may have the ability to put a hold on the roll-out.' The incident has prompted questions about overall preparations for the $1-billion tablet initiative.*

   Discuss how would you define the (1) **threats**, (2) **vulnerabilities**, (3) **likelihood**, (4) **impact**, and (5) **protection** in the above case?

6. (Optional) Consider the following situation: *The national lottery is currently ran using paper tickets that are sold by a network of 3rd party retailers. Once a week a sequence of numbers is physically drawn at random using balls during a televised show. If a customer presents that ticket they win 1M. The national lottery wants to computerise the whole process. To save money, by reducing the need to produce and transport paper tickets, and maintaining the machine that mixes balls.*

   Discuss how would you define the (1) **threats**, (2) **vulnerabilities**, (3) **likelihood**, (4) **impact**, and (5) **protection** in the above case?

7. (Optional) This exercise looks at risk perception and the different layers at which failures can happen in practice. Consider a system that is intended to be designed with security as a high priority, for example an end-to-end encrypted messaging app. How would the following factors affect your trust in the system? Which factors (or combination of factors) would you require to trust a system? Do all the systems you use have all these factors?

   (a) A peer reviewed paper describing the system

   (b) The identity of the designers and/or developers of the system

   (c) An implementation of the system by some well-known company or person

   (d) An open source (i.e., public code) implementation of the system

   (e) The system properties and implementation have been widely studied and proved by security researchers to be secure

   (f) The system has been tested on machines (hardware and operating system) similar to mine

   (g) The system is centralised or decentralised

   (h) The system depends on a party that is under the jurisdiction of a specific country

8. (Optional) This exercise is aimed at considering how security failures in the real world can depend on many parties and policies. The point is that no system lives in isolation and decisions by one party may end up affecting another negatively even if their security goals should not conflict in principle. A good example of this

is the WannaCry's effect on the NHS, which can be viewed from the point of view of security policies. This exercise is a bit more involved so the answers are more about discussion than yes/no.

WannaCry affected (among other institutions, including UCL) the NHS for a few days in 2017, leading to a lot of media attention. The purpose of the malware (more specifically, ransomware as it asks for a ransom) was to encrypt the contents of a system, demanding a ransom (payable in Bitcoin) to decrypt the system. The attack is technical in nature, but the reasons that the attack was able to happen are policy related. In particular:

- The malware propagated through systems using code from another exploit name EternalBlue which was kept (and allegedly developed) by the NSA (and likely shared with GCHQ) until it ended up in the hands of the ShadowBrokers who released it.
- Microsoft was notified by the NSA that they had lost control of EternalBlue and patched systems that were still maintained, i.e., Windows 7, Windows Server 2008 and later.
- The NHS was reliant on Windows XP. Microsoft stopped maintaining Windows XP in 2014 except for paid customers, which the NHS was not after April 2015. The NHS also operated many Windows 7 machines that were affected.

(a) This case involves a few parties, the NHS and UK Government, Microsoft and the NSA/GCHQ. Is any one party responsible? How should the blame be shared?

(b) All of the parties above operate in distinct areas with different policies and goals. What are these goals? Do they clash in one way or another?

(c) What reasons are there, economic and otherwise, for the NHS to still rely on Windows XP? Why were many Windows 7 machines also affected? In March 2018, the UK Parliament published a report titled "Cyber-attack on the NHS" stating that none the of the 200 trusts evaluated had passed NHS Digitals cyber security assessment, how can this be?

(d) Is Microsoft's choice to discontinue support of old (but still used) operating systems reasonable?

(e) The NSA is tasked with both offensive and defensive operations (as is GCHQ). How is this relevant in this context?