

# COMP0141 Security Tutorial 1 Solutions

January 2023

## 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.

**Answer:** As a reminder about C-I-A terms, you can think about the example we discussed during the lecture – a message in the envelope.

**Confidentiality** of information means protecting the information from disclosure to unauthorised parties. For example, confidentiality means that if Alice is sending a letter to Bob, only they can read the message hidden in the envelope. Meaning that the message in the envelope is not disclosed to unauthorised parties. Examples of information that could be considered confidential are health records, financial account information, criminal records, trade secrets, and military tactical plans.

**Integrity** means that the message in the envelope is **not modified/alterd by anyone unauthorised**. For example, if you were sending a hand-written cheque in the envelope for a money transfer for \$100, you don't want the information to have been tampered in such a way that you actually sent \$1,000,000.

**Availability** refers to ensuring that authorised parties are **able to access the information** when needed. In the example with the letter, we want to make sure that Alice's letter is indeed successfully sent to Bob, and no one unauthorised can steal or destroy the letter.

**Confidentiality:**

- (1) Only a student with a valid student number and card can access their student records in the system,
- (2) The student's personal information and marks should be restricted by access controls and not available for unauthorised users,
- (3) No one should be able to intercept student's login details or requested data etc.

**Integrity:**

- (1) The system should guarantee that the student's marks and personal information visible on the website are valid and the same as the ones stored on the server
- (2) The student's information is not changed without their authorisation etc.

**Availability:**

- (1) The student should be able to (given they have valid credentials) access the SIS,
- (2) There should be a system for backing up the students' record, etc.

2. Which of the following attacks are attacks on (1) **confidentiality**, (2) **integrity**, (3) **availability**?

- (a) Opening my neighbour's letter without their consent

**Answer:** Confidentiality

- (b) Installing malware on a data server that has private information in order to transmit the data to attackers

**Answer:** Confidentiality

- (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

**Answer:** Availability

- (d) Deliberately disrupting a server room's power supply in order to take those servers offline  
**Answer:** Availability
  - (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  
**Answer:** Confidentiality
  - (f) Eavesdropping a phone conversation  
**Answer:** Confidentiality
  - (g) Maliciously accessing a financial server in order to falsify financial records  
**Answer:** Integrity
  - (h) Maliciously erasing disk containing important information  
**Answer:** Availability
  - (i) Pushing an update to an app that modifies its permissions without notifying the users  
**Answer:** Integrity
  - (j) Showing different users different views of the same web page  
**Answer:** Integrity
  - (k) Sharing a patient's medical record (or any sensitive data in other contexts) without their consent  
**Answer:** Confidentiality
  - (l) Obtaining more data than necessary for the purpose of a task  
**Answer:** Confidentiality
3. Are these (1) **threats**, (2) **impact** (i.e, harm) or (3) **vulnerabilities**? (justify)
- (a) Thieves can enter the lab to steal equipment  
**Answer:** **Threat** – this sentence expresses **something that can happen to the system**: who can attack it and with what goal. It is a feared event.  
Additionally, you can also think about this as **Impact**, if this sentence describes the result of the thieves exploiting a vulnerability, entering the lab and stealing material. In other words, it can be seen as **the result of an attack**.  
Note, that even if we think about this scenario as a possible risk, this is not a vulnerability because we do not say anything about what is the weak point of the lab which allows the thieves to steal the equipment.
  - (b) Credit card numbers were stolen  
**Answer:** **Impact** – this sentence expresses the result of an attack (e.g., exfiltration of data, for instance using malware)  
Additionally, you can also think about this as a **Threat**, if this sentence describes a feared event, that the credit cards numbers are stolen and the thieves can use them to commit fraud.
  - (c) Users choose weak passwords  
**Answer:** **Vulnerability** – this opens the door for an attack (guessing the password is easier).  
This could also be seen as **Threat** as users' accounts could be more easily compromised.  
This is not an **Impact** as the fact that users have weak passwords does not indicate any impact yet. If an adversary guesses a given user's password, then there will be an impact to be considered.
  - (d) A backup system stopped working  
**Answer:** **Impact** – the sentence describes damage done to the system (potentially as a result of an attack, e.g., denial of service on the backup server).  
Additionally, you can also think about this as a **Vulnerability** if the backup system that is down can be exploited by an adversary to delete or modify files in the system without the possibility of recovering them later.
  - (e) A hacker can install malware  
**Answer:** **Threat** – the sentence describes a feared event - who might attack the system and how would this attack be performed.  
You can also interpret it as an **Impact** if it is the result of the hackers detecting another vulnerability and getting into the system in order to install malware.
  - (f) Students can see the exam questions before the test  
**Answer:** **Impact** – the sentence describes a harm done to the system as a result of an attack (e.g., students steal the professors office keys)  
**Threat** – the sentence describes a feared event, that the students may have access to the exam questions.

- (g) A machine learning algorithm that is used to make important decisions is biased, or has a significant error rate


**Answer: Impact** – bias and errors in automated decision making can lead to unfair consequences. Bias often occurs due to the use of biased data, for example in predictive policing. High error rates in deployed systems are also a reality, for example in the use of facial recognition by UK police forces.

You can also think about this as a **Vulnerability** if the biased in the algorithm can be used by a malicious adversary to perform an attack.

- (h) I am staying at a hotel that gave me access to my room without verifying my identity

**Answer: Vulnerability** – this means that someone else can enter your room very easily and steal your personal belongings (generally, an attack known as social engineering).

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, ...)

**Answer:** No. The environment is not considered as adversarial. It does not act purposefully to break the system.

- (b) I need to keep my valuable laptop in my car to go shopping

**Answer:** Yes. In this scenario, there is an adversary that wants to actively and purposely steal my laptop.

- (c) I need to build a boat that floats under adverse conditions (storm)

**Answer:** No. The sea and the storm are not considered as adversarial. They do not happen at the worse moment and their goal is not to sink the ship.

- (d) I need to store the secret final exam on a server open to the internet

**Answer:** Yes. In this scenario, there can be an adversary that purposely will try to use the fact that the server is connected to the internet to try to steal the exam.

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

**Answer:** Yes. In this scenario, there can be an adversary that tries to impersonate the lawyer with an aim to extract confidential information from the conversation.

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

**Answer:** No. This is a bug, the attack is not intended. It is not considered as an adversarial act.

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

**Answer:** Yes. The issue is that the OS vendor claims to offer a security feature but in fact relies on another party. For example, Microsoft's BitLocker defaults to using the machine's hard drive built-in encryption, which is an issue when it is broken in many SSDs.

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

**Answer:** Yes. This means that your internet traffic (including passwords, card numbers, ...) could be visible to others.

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

**Answer:** It depends on which border you are trying to cross. Although most people are not considered as "people of interest," border control in some countries can ask for your passwords, for example, when travelling to the US from the UK. Likewise, when coming back to the UK you might find yourself asked for passwords.

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

**Answer:** Yes. You could unintentionally be using compromised software which is why vendors tend to cryptographically sign software.

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

**Answer:** Yes. It could be that you are using software or hardware that is intentionally compromised. For example, some western countries (particularly those part of Five Eyes) have expressed concerns about Huawei's role in developing 5G infrastructure.

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

**Answer:** Yes. If it seems likely that someone else has had physical access to your phone, they could have tampered with it in many ways.

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

**Answer:** Yes, this can be a problem. Facial recognition cameras have been used in a variety of contexts from Taylor Swift concerts to football matches. In principle, their use is intended to increase security, but in practice, it has mostly lead to important privacy concerns as the legal framework for this (and storage of recorded data) is a very grey area that is open to abuse.

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?

**Answer:**

**Threats** (who is the adversary?):

- Students who bypass the software blocks
- Teachers who might control the usage of the iPads or locate the students when it is not required
- IT software admin (for example watching students via the camera)
- Malicious third parties who want to steal information from the iPads or track the students

**Vulnerabilities** (where can the system break?):

- Software blocks that limit what websites the students can use
- Integrity of the information what the students are doing with them at all times
- Wrong access policies

**Likelihood** (might this happen?): Very likely so far, since the students already found the way to bypass the blocs and tamper with the software.

**Impact** (what if bad things happen?):

- The iPads can be used by students for malicious or non-education related purposes
- Loss of money for the school
- Malicious third-parties can locate and control the students

**Protection:** Depending on how the whole idea can be implemented, there might be many protections. In a more general way you can think about them as:

- Introduce new, better access policy
- Improve the software managing the blocks
- Require students to leave the iPads at school

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?

**Answer:**

**Threats** (who is the adversary?):

- An insider of the system, e.g., an engineer who can access the customers ball draw or manipulate the algorithm

- Organised criminal group who has large resources in terms of skills and computation, e.g., create multiple accounts using a bot, bridge the security of the server running the lottery
- The clients, who want to cheat on the lottery, e.g., if they can submit votes after the final draw or more than one ballot
- The lottery owners, if they want to cheat and never allow the winning draw to happen
- Third-party adversary who might not have a financial incentive, instead, wants to steal information about the clients

**Vulnerabilities** (where can the system break?):

- The server where the lottery is running, e.g., no backup, possibility to steal clients' information from the server etc.
- The website, user GUI operating the lottery, e.g., no strong multi-factor authentication, phishing attacks etc
- The network channel between the potential winner and the lottery/bank system, e.g., no SSL or link encryption etc.

**Likelihood** (might this happen?): Yes, if there are no steps taken to design and develop a secure system, it is highly likely as financial incentive is very large.

**Impact** (what if bad things happen?):

- The system might deceive the winning draw by the company
- The server on which website/system is running might be attacked by a malicious third-party who can compromise the result
- The customers' personal details might be leaked
- The client might maliciously win 1M

**Protection:**

- Shared responsibilities among system designers/developers
- End-to-end encryption
- Multi-factor authentication
- Strong verification

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

**Answer:** Peer review provides assurance that the paper has been evaluated by (in theory) qualified people, which generally leads to trustworthy results. Nonetheless, it should also be balanced with the reputation of the venue in which the paper is reviewed and published as the quality can noticeably vary. Mistakes are also possible, even in published papers (follow up attack papers frequently follow), and their assumptions do not always hold in the real world.

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

**Answer:** Well known individuals and companies that have a history of designing secure systems do warrant higher trust levels, but it is always possible for mistakes to happen so blind trust should be avoided. Many authors of good work also produce work that is not so good.

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

**Answer:** Similar to the above, an implementation of a system that is well known or provided by a well-known individual or company can usually be regarded as secure. Again, however, bugs or side-channel attacks are always a potential reality, especially in projects that involve thousands to millions of lines of code.

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

**Answer:** Open source allows for many independent people to look at the code and check for potential flaws. This is extremely useful, and a good way of increasing trust in a system, especially with regards to backdoors or other hidden “features.” Unfortunately, this does not offer strict guarantees as flaws still exist. For example, Heartbleed (<http://heartbleed.com/>) was introduced in 2012 but was not publicly discovered until 2014, while it was potentially known to a few parties during that time (<https://en.wikipedia.org/wiki/Heartbleed#Exploitation>).

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

**Answer:** Published, independent audits of a system’s security are not error-free, but they are one of the best guarantees of a system’s security. On other occasions, audits happen behind closed doors which can introduce doubts that the audit was correctly performed with the right levels of independence.

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

**Answer:** This is always a good thing, systems can run with different levels of performance and stability depending on the environment they’re in. However, it is still possible for other things on your machine (e.g., some software running concurrently) to interfere with the system in a way that was not tested.

- (g) The system is centralised or decentralised

**Answer:** Centralised and decentralised systems correspond to different security models. Centralised systems can be easier to build and more efficient, but they rely on a central party that has to be trusted to not fail or compromise the system itself. A decentralised system removes the threat of a central party failing but can be harder to build and less efficient. Others in the system can still negatively affect the system, if too many of them fail or if they obtain control of the system (e.g., by owning a majority themselves or colluding with others), so some form of trust is still required to an extent. Many systems advertised as decentralised are also simply not decentralised in any meaningful way.

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

**Answer:** This can be a good thing if the given country is trusted to not behave in any harmful way. For example, some may prefer to host their website in a country that is unlikely to take it down or censor it. On the other hand, if the given country is not trusted this can be an important issue if the system or its developers are compromised.

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?

**Answer:** No single party is wholly responsible. The NHS could have made an effort to be more secure, despite millions of pounds in funding allocated to this, and not rely on an unsupported OS. Microsoft could have made more of an effort to make sure users patched their machines and offered free support to XP users for the occasion. The NSA and GCHQ could have done a better job at not hoarding vulnerabilities that affect systems their country and allies rely on due to the risks of losing control of them, and a better job of preventing the use of said exploits once lost to avoid the situation that happened. (This is, of course, idealistic thinking.)

On the other hand, a good amount of blame shifting has occurred. Microsoft blamed the NSA for hoarding exploits despite previously providing the NSA with backdoors into its software, the UK and the US blamed North Korea (<https://www.bbc.co.uk/news/world-us-canada-42407488>) while trying to avoid mentioning that the code used originated from them. The UK government also chose not to purchase continued support from Microsoft for Windows XP after 2015.

- (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?

**Answer:** The broad policies of each organisation are as follows. The NHS is a healthcare service provider that aims to optimise this while managing security and other concerns at a lesser priority level. The NSA (and GCHQ) are tasked with offensive and defensive operations relating to signals intelligence and more generally cybersecurity. Microsoft is a company that sells software, optimising for profit. None of these explicitly clash a priori, but they come into conflict in cases like the WannaCry attack, which highlights the complexity of security issues at this scale.

- (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 of the 200 trusts evaluated had passed NHS Digital’s cyber security assessment, how can this be?

**Answer:** While there are economic reasons for the NHS to not always use the newest software or hardware, this is not the only reason it still operated machines running Windows XP. The issue is that medical machines and software can last a long time, and rely on old drivers and other software which requires Windows XP. Constraints like these exist in other areas, making it hard to effectively implement security without affecting the core purpose of an organisation.

Many Windows 7 machines were also affected. This is because, despite the fact that a patch was issued by Microsoft, the machines were not patched on the NHS’s end. The parliamentary report also mentioned that there were still unpatched machines at the time the report was done. This highlights another important issue, which is that many organisations are not security conscious. Changing this not only requires funding, but also effective training, support and time.

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

**Answer:** It is unreasonable to expect all software to be supported forever. Broadly speaking, very few people still use Windows XP and paid support remains available. On the other hand, it may be the case that security should, at least in some cases, take precedence over being a paid customer or not. This assumes that Microsoft could have predicted the impact, which is unlikely. This also was not the only issue, as many machines running Windows 7 or later were affected because they had not been patched, despite the patch being available. Microsoft could consider forced updates, but people tend to be unhappy when this happens. In the case of the NHS, having a machine stop what it is doing to install an update may also cause issues.

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

**Answer:** The potential conflict between offensive and defensive tasks has been a big point of discussion (<https://www.reuters.com/article/us-usa-cyber-nsa-idUSKCN0VH21H>) due to the risks of one undermining the other. Offensive tasks require developing and storing vulnerabilities (“zero days”) that can be used to penetrate a system when required. Defensive tasks require ensuring that such vulnerabilities are not used against the infrastructure of their country. As many of the systems used worldwide are developed in part in the US, and to a lesser extent the UK, this is problematic as vulnerabilities against those systems are vulnerabilities against companies and systems that fall under the defensive responsibilities. In the case of WannaCry, the NSA attempted to resolve this by notifying Microsoft, which mitigated the impact of the vulnerability but did not entirely fix the problem (or satisfy Microsoft). It is also the case that this was only possible because the NSA knew that the exploit had been lost. If this had not been publicised, or if the exploit had just been independently found by another party then they would not have notified Microsoft.