Vincent Yasi

CS 370 -Intro to Security-

Problem Set 1

Q1 [3 pts]: Articulate 3 reasons why securing cyberspace or computer systems and data is challenging?

- In the modern day, cyberspace and computer systems are very complicated. With the complexity comes many, many pieces which need to be monitored and secured, and the amount of pieces only grows each day. Because of this, it is easy for pieces to be overlooked or for new attack avenues to be hidden. This can lead to challenges in keeping these systems secure.

- Also in the modern day, technology is evolving and changing rapidly. There are always new things that need to be secured, and they are always different from that which came before. Therefore, new security measures need to be devised to secure these new things, and new attacks can be devised based on the new technology, which also need new security solutions.

- At its core, computer systems are designed by humans (as we have not yet devised AI quite to that level yet). And, humans are naturally fallible. Even with the best efforts and intentions, there always exists the possibility of security holes or oversights. No person, or even group of people, is perfect. Because of this, very little security can be perfect, or at least perfect and still usable in a valid sense. As well, because people are fallible, they cannot think of and design against every possible type of attack that may be devised by another human.

Q2 [6 pts]: Name and define the six key properties/attributes of computer security?

- **Confidentiality:** preventing the unauthorized access of data
- **Integrity:** ensuring data against unauthorized modification
- **Availability:** making sure data is available when needed, and in a usable manner
- **Privacy:** an individual's right to control of their data against unauthorized means
- **Authenticity:** ensuring data is from a valid/the correct origin
- **Accountability:** being able to trace actions back to their source, and to ensure the actors cannot deny their actions

Q3 [3 pts]: What is non-repudiation and what security property/objective covers non-repudiation?

Non-repudiation is the ability to be unable to deny your actions or involvement in them. It is also the ability to trace an action back to its source without the ability for doubt or dismissal. This is covered by Accountability, where each user, attacker, entity, etc. is able to be held accountable for their actions and easily traced.

Q4 [9 pts]: Classify each of the following as a violation/breach of one or more of the six key security properties

Attack on JP Morgan bank

This attack breached Confidentiality, Privacy, and Accountability. As this was mostly a breach of customer and banking data, it is a breach of both Confidentiality and Privacy. The personal data of customers was found and taken, thus breaching the privacy of those customers. As well, this data was company data, and the overall workings of JP Morgan's system were also leaked, all of which is also a breach of Confidentiality. There is also a breach of Accountability, as the article suggests there are some leads as to the culprits, but no firm way to tell just who did the attack. Therefore, there is no Accountability and ability to trace the actions back to their perpetrator.

Attack on a federal Website

This attack is a breach of Confidentiality, Integrity, and Authenticity. The breach of Confidentiality is because the hackers were able to get hold of, and threatened to leak, internal Justice Department documents, which should have remained secure. It is an Integrity breach because the hackers have taken control of the site, and so there is no guarantee that what is retrieved if one accesses the site is what the site is supposed to be. There is no guarantee of integrity of the site and its contents. It is an Authenticity breach because, due to being under the hackers control, there is no way of verifying where exactly the site data came from when accessing it, and in fact it is most likely that it is not coming from the source one thinks it is at first glance (the Justice Department).

Wifi-hotspot incident

This seems to just be a case of breach of Availability. Consumers expected to be able to access WiFi with little to no issue, but were blocked by the actions of Marriot and its access was greatly limited by them. Beyond the availability issues, the article does not suggest any other breaches. Once the availability hurdle was overcome, the article suggests the WiFi service provided the same security features as is found in any other WiFi. However, forcing consumers to only use their WiFi does open up the possibility for any of the other breaches, as a single point of entry gives Marriot all the power.

Q5 [4 pts]: Compare and contrast Confidentiality and Privacy.

At the surface, the two properties are very similar. They both concern the access of data by unauthorized sources. However, Confidentiality typically concerns the act of preventing the unauthorized access, and is generally viewed and assessed from an objective standpoint. Meanwhile, Privacy is concerned more with the control of data and is concerned with a person's data and their rights. A person has Privacy with their data and the right to control how it is accessed and distributed, while Confidentiality concerns preventing access of that data by unauthorized means.

Q6 [4 pts]: What is the difference between Attack Surface and a Vulnerability?

A Vulnerability is any thing which can be exploited or used in an attack. An Attack Surface, meanwhile, is the vulnerability and similar things which can actually be used in an attack. Something may be a vulnerability, but if it cannot be accessed by the attacker, it is not in the attack surface. Vulnerability is a classification of a thing, mostly separate from other factors. An Attack Surface, however, has a scope, and therefore certain vulnerabilities, even though they exist, may not be in the attack surface available to an attacker.

Q7 [4 pts]: Explain how the terms threat and attack related?

A threat is more theoretical, and represents something which could happen or is possible. An attack is more concrete, and describes an actual plan and ability to carry out a threat. A threat may be it is possible to decrypt a ciphertext by using a padding oracle, while an attack is the actual plan to use the padding oracle and how specifically that will result in a decrypted ciphertext, and may even go as far as to describe the actual attack itself taking place.

Q8 [4 pts]: What is the difference between snooping and spoofing? What security properties do they threaten?

Snooping is observing or otherwise gaining information you are not meant to. It generally breaches Confidentiality and Privacy. Spoofing is creating a forgery, or otherwise changing or displaying a false thing as the genuine article. It breaches Authenticity and Integrity.

Q9 [5 pts]: Why do we need 4 types of security mechanisms? Why couldn't we simply use prevention mechanisms? If we are successful in preventing we don't need the other mechanisms do we?

Ultimately, it is almost never possible to prevent all security attacks. The field of computers, etc. is always changing, and it is nearly impossible to think of and see all possible security vulnerabilities. As such, if we only use prevention, then those vulnerabilities we do not see or account for can get through, and there will be nothing to protect against them when they do. Therefore, we have the other three mechanisms, too, to help address that which cannot be addressed by Prevention alone. Prevention is also a pre-emptive mechanism. Without the other mechanisms, there would be none once an attack does occur (and because of the above, eventually it will).

As well, each mechanism provides a function Prevention cannot. Detection allows one to know if an attack has occurred (Prevention allow just assumes none ever happens). Response provides actions to take when an attack does happen. Recovery provides the actions to take to recover and restore from the attack. Prevention alone will not provide this additional, and needed, actions and abilities.

In a perfect world, Prevention alone may be able to provide all our security needs. If every attack is stopped before it even happens, then there would be no need to detect, respond, and recover from an attack. However, the world is not perfect, and so Prevention alone will only leave wide gaps in our security system and its abilities if Prevention fails.

Q10 [2 pts]: What are recovery mechanisms? Can you give an example?

Recovery mechanisms are those used in response to an attack, and aim to restore a system to the state it was in before the attack occurred. An example of such a mechanism would be backup files. If all files and other parts of a system are constantly backed up and kept up to date, if an attack destroys or otherwise damages the data in the system, the back ups can be used to restore the system back to the state it was in before the attack.

Q11 [6 pts]: Explain why the right incentives are important. Specifically explain how the right incentives are necessary for policy, mechanism and assurance.

The right incentives are needed because otherwise a system is not likely to be utilized how it was designed. A system can be designed in the best and most perfect way, and address every security concern and every need, but if someone is not incentivized to use the system in the correct way, or the way it was intended to be used, then the design and the system become heavily hampered from its ideal state, or even completely useless.

In respect to policy, the system is designed to achieve a certain goal. If the correct incentives are not used, then a person may not use it to achieve this goal. A computer system may be set up to be used to run an assembly line, but unless the appropriate incentives are used, such as recording how often the assembly line program is used, then a person may instead use the computer only for games, and not achieve the systems intended policy.

In respect to mechanisms, the system may be designed with certain mechanisms, intended to be used in certain ways, to achieve the goals of the policy. Without proper incentives, the mechanisms may be disregarded, and therefore not achieve their intended purpose. For example, in order to enhance security, a system may use two-factor authentication. However, unless the proper incentives are used, such as reprimand if two-factor is not active, a person may disable two-factor authentication and bypass that security feature specifically designed into the system.

In respect to assurance, the system is designed with the assumption that the measures chosen can be relied upon to perform their intended functions. However, without proper incentives, a person may use the mechanisms in the unintended way, which can lead to issues. For example, a system may be implemented with a password mechanism, intended to be used with a secret password known only to the user. Without proper incentives, like checking the person's work area, that person may simply write down the password in a place easily discovered by others, therefore compromising the integrity of that mechanism.

Q12 [4 pts]: Compare and contrast "least-privilege" and "separation-of-privilege"?

Separation of Privilege aims to divide the privileges or other things needed to execute certain tasks (typically ones vital to the system) into separate pieces, and to ensure these pieces are kept separate from each other. This protects against any one compromise of the privileges from taking down the

whole system, or at least the section the privileges pertained to. By separating them, it makes it harder and less likely that all pieces needed to take down a section can be compromised.

Least Privilege focusing on reducing the amount of privileges any particular user/node in the system has, so as to also protect the overall integrity of the system. In this case, if a user has only the privileges needed to complete their task, if they are compromised, the attacker only gets these privileges, and nothing more. If a user had more privileges than they required, that would only lead to more possible damage if they are compromised, while not affecting or improving their normal work ability.

Both of these aim to protect and minimize damage concerning privileges if a compromise occurs. It restricts the size of the leaked privileges (by either dividing privileges up into multiple parts, or creating the smaller "pool" of privileges that could possibly leak if a compromise were to occur). By restricting the privilege leak size, it also reduces the possible damage.

Q13 [3 pts]: Describe the principle exemplified by the practice of using "sudo" instead of always running as a "superuser"?

This uses the principle of Least Privilege. If a user can complete their tasks with only a subset of the overall privileges (using sudo instead of the full superuser), then if they are compromised, the damage is only limited to those privileges they have, and not the entire privilege set. This offers enhanced protection for the reasons explained above.

Q14 [3 pts]: Explain the principle of psychological acceptability.

If something is more psychologically acceptable (often said to be more user friendly), then a person is more apt to use it, and to use it in the intended way(s). As a system/mechanism is often designed with a particular way of use or purpose in mind, then being able to get a person to use it in that way will better help it perform its purpose, and will protect against unforeseen issues and vulnerabilities.

People will instinctively use things and do things in the easiest and least effort ways. If you want something used in a particular way, then you need to make that particular way the easiest one.