**Hsiang Lo**

**CS 370 Introduction to Security**

**Week 1: Problem Set 1**

Instructor Name: Rakesh Bobba

# **Introduction**

The purpose of this assignment is to help you gain a better understanding and insight into the concepts and definitions we learned in Week 1 and help you see how they are applied.

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* What is Cybersecurity? re
* Key Concepts of Cybersecurity
* Cybersecurity Terminology
* Cybersecurity Strategy
* Cybersecurity Principles

Also make sure you read Chapter 1 form the textbook.

# **Questions**

Please answer all of the questions below.

## What is Security?

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

There are many reasons as to why securing cyberspace or computer systems and data is challenging. The main three reasons are that it’s because of ever changing systems, environments and adversaries and complexity of system.

Technology is constantly changing on a daily basics. Security mechanism improves overtime and requires constant monitor and updates. At the same time so does the adversaries. Adversaries improves on their strategy and are good at finding the weak spots of a system or security mechanism. A single flaw can bring down the entire system. Lastly, the complexity of a system can easily cause flaws in the system as security may not have been thought through on every level. This is often due to the fact that security tends to be afterthought rather than designed in.

## Key Security Notions/Attributes

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

The six key properties/attributes of computer security are the following,

1. Confidentiality – Preventing unauthorized access or disclosure of data/information
2. Privacy – Preventing unauthorized access or disclosure of information/data about people.
3. Integrity – Preventing against unauthorized modifications to data integrity, origin integrity and system integrity
4. Availability – Ensuring timely availability of data, system, service and etc.
5. Authenticity – Property of being genuine; can be verified and trusted
6. Accountability – Requirement for entity actions to be traced uniquely to that entity

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

Non-repudiation is the idea that one cannot repudiate one’s actions. This is a concept covered under accountability which talks about the requirement for entity actions to be traced uniquely to that entity. An example provided talks about how paying a credit card and later claiming never having done the transaction violates the concept of non-repudiation.

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 reported here

- <http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/>

**Notes**

* whether it was an effort to steal from accounts or to demonstrate that the hackers could penetrate even the best-protected American financial institutions
* The JPMorgan hackers burrowed into the digital network of the bank and went down a path that gave them access to information about the names, addresses, phone numbers and email addresses of account holders.
* JPMorgan employee halted the attack of more sensitive information
* The hackers were able to attain high administrative privileges within JPMorgan’s network, rooting more than 90 servers and rummaging through customer databases with detailed information for 76 million households and seven million small-business online accounts.
* As one former employee explained: “It’s as if they stole the schematics to the Capitol — they - can’t just switch out every single door and window pane overnight.”

Based on the gathered notes, it can be determined that in this example, the adversary, the hackers, while has not been determined with a set motive, they were still able to compromise the system and stole essentially the “blueprint” of the security system/database. It is not known whether any customer’s information was downloaded, therefore, this is a case of violation of the confidentiality property of the six key attributes.

* Attack on a federal Website reported here

- <http://abcnews.go.com/blogs/politics/2013/01/anonymous-hijacks-federal-website-threatens-doj-document-dump/>

Notes

* Activists from the hacker collective known as Anonymous assumed control over the homepage of a federal judicial agency this morning.

It would appear that the only damage the hackers did was hacking into the website and threaten to release embarrassing internal documents. Based on the hack of the website, it is clearly a breach of Integrity. Since the website was not accessed but modified. The act of WRITE set it apart from confidentiality and becomes Integrity in this case.

* Wifi-hotspot incident reported on here

- <https://www.cnn.com/2014/10/03/travel/marriott-fcc-wi-fi-fine/index.html>

Notes

* Marriott has agreed to pay a $600,000 fine after the Federal Communications Commission found the company blocked consumer Wi-Fi networks last year during an event at a hotel and conference center in Nashville.
* [Federal law prohibits people from using a device](http://www.fcc.gov/encyclopedia/jammer-enforcement) that interferes with cellular, GPS or wireless networks.
* Instead, Marriott employees were using the hotel's own Wi-Fi system to block other people's hot spots, the FCC official said.
* Marriott employees had used "containment features of a Wi-Fi monitoring system" at the hotel to prevent people from accessing their own personal Wi-Fi networks.

Based on the notes provided, it has become apparent that due to Marriot’s action of using their own Wi-FI system to block other people’s hot spots, Marriot has violated Availability of the Key Security Notions/Attributes. By using the containment feature of a Wi-Fi monitoring system, Marriot limited the timely availability of data and service of the general public.

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

Confidentiality is about the prevention of unauthorized access or disclosure of data/information. Privacy on the other hand, is about the prevention of unauthorized access or disclosure of information/data about people, an individual’s right to decide who gets access to information/data about them.

While both confidentiality and privacy both deals with access or disclosure of information, the main different here is that privacy has to be about people. For example, if the receipe of coco-cola was stolen, it would be a breach of confidentiality but not privacy because the receipe itself isn’t about people or a single person.

## Security Terminology

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

A vulnerability is a weakness in the system that could be exploited to violate security property of interest. An attack surface is a reachable exploitable vulnerability. The difference here is that an attack surface must be both reachable and also exploitable.

Not all vulnerabilities are exploitable, and thus, an attack surface is also one that is accessible by the adversary/attacker.

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

A threat is a set of circumstances that has the potential to breach security and cause harm. An attack is when an entity exploits a vulnerability in a system to violate a security property/attribute. In this case, an attack is the realization or action of the threat by an adversary. It’s like a sequence of event!

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

Snooping or interception is the unauthorized interception of information. This violates the idea of confidentiality which focuses on the breach of data in terms of READ. In comparison, spoofing or masquerading deals with the impersonation of entity by another. This most directly violates the key security notion/attribute of Authenticity as the term deals with property of being genuine, can be verified and trusted. Since the act of spoofing means pretending to be another individual. If this succeed, the system failed to verify and mistrusted the spoof.

## Security Strategy

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?

The four types of security mechanisms are prevention, detection, response and recovery. The reason why we need all four mechanisms is because we can’t be certain that prevention will certainly work. If that fails, the system should then detect the attack. In order from preventing more damage, they can then switch to response. And then finally return to a secure stage.

The reason why we can’t simply just use prevention mechanism is because it is so unlikely to ensure that you can be a hundred percent successful at preventing. The assumption that prevention will certainly work is most like going to be a wrong assumption. If that fails, we must be prepared for additional unwanted damage from the adversary. Main way hackers break into system is the violation of assumptions. And that is why we must not also make the assumption that prevention will work.

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

Recovery mechanism is the restoration of the function back to normal. Such as a backup storage, if an attack take place, you can restore the data from a remote secure storage. This is essentially the last steps of the security mechanisms. You simply want to restore and recover lost data or lost system.

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

Right incentives drives the policy, mechanism and assurance. We need to be certain those individuals are held responsible for the building of the security system. If the incentives aren’t there, how can we be certain that they will be responsible for the system design.

## Security Principles

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

Least-privilege talks about how every program and every user of the system should operate using the least set of privileges necessary to complete the job. On the other hand, Separation-for-privilege talks about how critical operations should be protected using two or more keys that can then be separated. In a sense they are both trying to maximize the security overall. Separation-for-privilege requires two authorized users to make it work while least-privilege assign everyone with the least amount of privilege necessary to complete something.

Q13 [3 pts]: Describe the principle exemplified by the practice of using “sudo” instead of

always running as a “superuser”?

The concept here is essentially still least-privilege with some least common mechanism as well. By using sudo, you are requiring an extra layer of check-up to ensure that the action being taken out is intended by the right and privileged user.

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

The principle of psychological acceptability is also known as usability. It is essentially saying that human interfaces are designed for ease of use in terms of user interface and helps users routinely and automatically apply the protection mechanisms correctly.

# **Submission Details**

Submit a PDF file with the questions and your corresponding answers.

The assignment is worth 60 points. It is due Wednesday of Week 2 at Midnight.