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?
- 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?

- Systems, environments, and adversaries are constantly changing and evolving
- Security isn't always built into a design
- Defenders need to plug every hole, attackers just need to find one hole

Key Security Notions/Attributes

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

- Confidentiality: Preventing unauthorized access or disclosure of data/information.
- Privacy: An individual's right to decide who gets access to information/data about them.
- Integrity: Preventing against unauthorized modifications.
- Availability: Ensuring timely availability of data, system, service, etc.
- Authenticity: Property of being genuine (can be verified and trusted).
- Accountability: Requirement for entity actions to be traced to that entity.

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

- Non-repudiation is the property that prevents someone from falsely claiming to never have performed an action. This is covered by the Accountability objective.

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/
    - Violation of privacy and confidentiality (since no changes were made to any account data)
- Attack on a federal Website reported here
  - http://abcnews.go.com/blogs/politics/2013/01/anonymous-hijacks-federal-website-threatens-doj-document-dump/
    - Violation of integrity, availability, and authenticity (because a legitimate website was defaced, which prevented users from accessing the service provided by that website.)
- Wifi-hotspot incident reported on here
  - https://www.cnn.com/2014/10/03/travel/marriott-fcc-wi-fi-fine/index.html
    - Violates availability (because free access to personal internet connections was blocked by Marriott).

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

- Confidentiality: keeping data private. Data is confidential to authorized parties.
- Privacy: keeping people's data private. The individual gets to decide who has access.

Both are similar due to being concerned with the security of data. They are different in the way the security is approached. Confidentiality is concerned with he data itself, while privacy is concerned with the owner of that data deciding who has access to it.

Security Terminology

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

- Attack Surface: A reachable and exploitable vulnerability.
- Vulnerability: Weakness in the system that is able to be exploited.

An attack surface can contain a vulnerability, but a given vulnerability may not be within an attack surface.

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

- A threat and an attack are related because they both refer to a way in which a system can be compromised. A threat is a set of conditions that can lead to a breach in security, and an attack is the breaching of that security.

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

- Snooping is essentially "recon." It refers to information being deliberately received by the wrong person (e.g. "listening in" on a conversation). Snooping threatens confidentiality, privacy, and accountability.
- Spoofing is impersonation. It refers to an adversary pretending to be a legitimate entity in order to gain access to information. Spoofing threatens authenticity and integrity.

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?

- Four types of security mechanisms are needed because all attributes of security need to be protected and enforced. Prevention mechanisms are great to have, but in the event that they fail (because it only takes one vulnerability to be able to breach security) the other mechanisms are in place to help lessen the potential damage. If prevention is successful, the other mechanisms are in place to help back up the prevention mechanism. All of the mechanisms work together to keep systems secure.

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

- Recovery mechanisms are backups. These allow a system to be recovered in the event of loss of data/assets. If a system is compromised with ransomware, it can be recovered from a backup to an earlier state, before the system was attacked. This helps prevent total loss of a system or its data.

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

- Incentives are very important in order to maintain good security. If the incentive for a good security policy is not good enough, then the policy will suffer because of it. The same goes for mechanism and assurance.
    - Incentive for policy needs to be good enough for the designer to make a good security policy.
    - Incentive for mechanism needs to be good enough for the designer of the security mechanism to want the mechanism to perform well.
    - Incentive for assurance needs to be good enough for someone to want to use the system. Incentive can include good security practice and policy.

Security Principles

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

- "Least privilege" refers to every entity within an organization not being given more privileges than is necessary to do their job.
- "Separation of privilege" refers to critical operations being secured with at least two different protections (e.g. two passwords, two keys, 2-factor authentication).

  Least privilege is different from separation of privilege because separation of privilege requires more than one input to allow access to a system (can't launch a nuke with one key). Least privilege still allows an entity to complete their task.

  Least privilege is similar to separation of privilege because both principles limit the privileges of one single entity.

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

- Using “sudo” exemplifies the principle of least privilege. This is due to the fact that always running as a superuser gives the user more privileges than is necessary to complete their task, while sudo allows the user to access superuser privileges to complete a task when needed.

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

- Psychological acceptability refers to the need for systems to be easily usable, in order to help maintain the security of the system. If the system is not easily usable, then it could be configured incorrectly, leading to a vulnerability.

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.