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?

- You must secure all points of “entry” to secure a target, whereas an attacker must only find one vulnerability to compromise it.
- Difficulty of use in security tools and methods can hinder a user’s ability or willingness to properly secure their system.
- Security is an afterthought in nearly all software composition.

Key Security Notions/Attributes

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

- Confidentiality: prevent unauthorized access to data.
- Privacy: Confidentiality as it concerns personal data / data concerning people.
- Integrity: prevent unauthorized writing / changing data.
- Availability: a service being up / accessible in a timely manner.
- Authenticity: property of being genuine.
- Accountability: the actions of an entity should be traceable to that entity, and non-repudiable.

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

- Nonrepudiation is where someone who has done some thing is unable to repudiate (i.e. dismiss involvement) in such action. This falls under

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/
- Attack on a federal Website reported here
  - http://abcnews.go.com/blogs/politics/2013/01/anonymous-hijacks-federal-website-threatens-doj-document-dump/
- Wifi-hotspot incident reported on here
  - https://www.cnn.com/2014/10/03/travel/marriott-fcc-wi-fi-fine/index.html

  - JP Morgan: Breach of privacy, as user account info was accessed – as the article states: "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."
  - Federal Website: Both Availability (Anonymous placed a banner on the site as seen at the top of the article, removing timely access to the site's original content), and Confidentiality – they claimed to have accessed many DOJ records they would release if their demands were not met – if this claim is true, there is an aspect of confidentiality to this attack.
  - Marriott Wi-Fi: Availability Breach – users were not able to access the internet in a timely manner.

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

- Confidentiality deals with access to data; privacy deals with access to personal data or data about people.

Security Terminology

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

- Vulnerabilities are places in which a system is weakened, or maybe accessible. The attack surface is the sum of accessible, exploitable vulnerabilities.

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

- A threat is something (be it an adversary, or an 'environmental condition') that endangers a system. An attack is the act of exploiting a vulnerability to attempt to compromise a system.

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

- Snooping is a violation of confidentiality where someone tries to get access to data about someone else (sometimes engaged in by companies, sometimes people – if the data is about people, then the property of cybersecurity is privacy). Spoofing is to fake a “From” address – i.e. to spoof a MAC address to masquerade as another system on a network – this is a violation of the principle of accountability and authenticity.

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?

- Relying solely on preventative measures implies that we are 100% sure those protections will work – which is not an assertion we can make. Therefore, there is a chance – cynically, I would say a likely chance – that the defensive measures are not sufficient to defend a system. Therefore, access to that system will eventually fall into the hands of the opponent, at which time the remaining security mechanisms become crucial to understanding what is going on in our system, as well as being able to safeguard data, respond to the incident and recover.

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

- A recovery message for a system varies greatly by the system and the attack. One example would be a terminal server that you need access to so that you can control power distribution to a city. If an attacker were to endanger the availability of this service to the operator (i.e. getting into the system and changing password), this could have disastrous effects for the city. Therefore, the electricity company could implement a backup system with a different password / setup (so that it is not also vulnerable to the same attack) and have some method of switching control to this recovery system, thus nullifying 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 necessary for each of these steps to ensure that the step is executed by people who desire to get it right.
    - Policy: When people are setting policy, their incentives must be set so that they are encouraged to generate policy that is effective at securing the system, rather than just completing policy for the sake of fulfilling a requirement.
    - Mechanisms: given the crucial nature of each of the mechanisms, they need to be implemented correctly so that they are as effective as they can be.
    - Assurance: the incentives need to be correct for those whose job it is to assure that the implementation of the policy is done right so that we can be sure that the policy is acted upon correctly. Otherwise, the policy could not be implemented, which would not be good.

Security Principles

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

- Separation of privilege refers to there being 2 or more keys that are required to access certain accounts or permission levels. Least privilege refers to using the minimum privileges required to complete the task at hand.

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

- This is least-privilege – the amount of code that will run with root privileges is much larger when you run everything (even things that dont need it) as root than when you just run sudo when needed.

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

- Psychological Acceptability refers to the usability of certain security mechianisms. For example if some mechanism is not user friendly, then it is unlikely it will get adopted, resulting in less security.

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.