Nova Southeastern University

College of Computing and Engineering

**Assignment 1**

**ISEC 660 Advanced Network Security**

Winter 2021

Due date: 1/24/2021

Total Points: 100

**Section II. Questions** (80 points, all questions are equally weighted)

**Q1. Explain the following basic security principles:**

**fail-safe default:** This means that all access decisions should be based off permissions.

**complete mediation:** This means that all type ofaccess should be checked against some type of access control system.

**open design:** This means the design is not a secret but is public information.

**separation of privilege:** This means that multiple parties are needed to complete a task and that task can’t be dependent on one single entity.

**least privilege:** This means that the user only has the privileges needed to complete a task and nothing more.

**isolation:** This means separating data from a public to a private network, this separates the private network from the open world.

**defense in depth (layering):** This means layering security with many practices such as hardware, software, policies, and physical controls. Not just relying on one.

**Q2. In section 1.5, the textbook shows three areas of network attack surface: enterprise network, wide-area network, and the Internet. Show an example of each of these attack surfaces. (Chapter 1)**

**Q3. Describe the general concept of a challenge-response protocol. (Chapter 3)**

In the challenge-response protocol, a user tries to authenticate with a server. The server then issues some type of challenge that the user must solve to be authenticated. In a real-world scenario, a server sends a hashing process to a client who enters their password into that function/method. If the result of the logic matches both what the client and server have then they are authenticated. The challenge is inputting something into an equation to match their answer.

**Q4. Assume passwords are selected from four-character combinations of 26 alphabetic characters. Assume an adversary is able to attempt passwords at a rate of one per second.**

1. **Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password? (Chapter 3)**

(best case/worst case)/2 = (1/26^4)/2 = (1/ 456,976 seconds)/2 **= an Average of 63.46888 hours.**

**b. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?**

(26 x 4)/2 = 104/2 = 52 attempts, 1 second = 1 attempt, **so 52 seconds.**

**Q5. Briefly define the difference between DAC and MAC. (Chapter 4)**

Discretionary Access Control and Mandatory Access Control are essentially opposite in nature when it comes to who decides the privilege rights. When it comes to DAC, the creator of the content gets to decide who has what rights to that content. An example of this is using “chmod 777” in Linux to give open privileges. When it comes to MAC, the system decides who was those rights and no longer the content creator. An example of this is an Access Control List in Windows.

**Q6. For the DAC model discussed in Section 4.3, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for each entity that is both subject and object) A directed line from a subject to an object indicates an access right, and the label on the link defines the access right.**

**a) draw a directed graph that corresponds to the access matrix of Figure 4.2a**

**b) Is there a one-to-one correspondence between the directed graph representation and the access matrix representation? Explain. (Chapter 4)**

**Q7. Explain the nature of the inference threat to an RDBMS. (Chapter 5)**

The Interference threat to RDBMS happens when a user can make multiple calls to multiple tables to be able to figure out more sensitive information. An example of this would be if a nefarious user needed information from Table A and Table B, to be able to access Table C. Another example is if this first 6 digits of your SSN were stored in Table A and the last 4 digits of your SSN were stored in Table B, an attacker could combine that information to guess your SSN. When designing a database, it is important to remember that combined data from multiple tables should not expose confidential information.

**Q8. What are the disadvantages of database encryption? (Chapter 5)**

Database encryption poses some issues regarding Key Management and Inflexibility.

When it comes to Key management, every user that requests to decrypt the database for retrieving or persisting information will need the key for decryption. This does add a layer of security but does makes managing the database more difficult because now all users and their keys will need to be accounted, adding a layer of resources to be used up.

When it comes to inflexibility, since the content of the database is stored in a hashed value. It makes searching the true contents of that database a little more pragmatic. Now added resources will need to be implemented to compare search contents in the hashed form making the database less flexible.

**Q9. What mechanisms can a virus use to conceal itself? (Chapter 6)**

**Viruses and conceal themselves in many ways:**

**Stealth:** This is when a virus conceals itself by hiding in a manor that is hard to detect on the system.

**Polymorphism:** This is when a virus will change its signature to evade systems with signature detection. If the same signature is used over and over eventually the system would catch on.

An analogy of this a is a leopard that changes its spots.

**Metamorphism:** This is when the virus completely rebuilds itself not only to produce a new signature but also becomes a whole new code base. An analogy of this is a tiger who becomes a lion.

**Encryption:** This is when a virus encrypts its contents and traffic to be less noticeable, on the downfall the decryption key of that virus adds another point of reference for the antivirus to detect.

**Q10. What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware? (Chapter 6)**

A backdoor is usually some means for someone to access a device, other than the owner. And this means of access is usually hidden and the owner sometimes just doesn’t know how to or can’t use it or more likely doesn’t even know about it’s existence.

A rootkit is basically the software that creates a backdoor. Meaning, once a hacker gains access to a system, they plant some software that later allows them hidden access to the system without hacking it again. That’s a rootkit. On classic systems that follow Unix rules and similar, the root user is the admin that has full system access. So, that is what the term rootkit means. It’s a software kit that provides root level access to a system. And preferred hidden.

A (ro)bot is basically some application that automates stuff. If for example you visit a website that offers a chat right away, you might notice, that the conversation seems a little bit tedious. That is because you are not dealing with a human. Something on the other side filters your text for specific keywords and when it recognizes a keyword, it offers some default answer. The piece of software that does that for example, is a bot. Quora for example uses this stuff for content reviews.

Just separate the terms in keylogger and think of keys as in the keys on your keyboard. And now you should understand, what a key logger does! It logs everything you do on your keyboard. So, in case a hacker plants one on your device, it’s usually just a matter of time, until you enter a password on some website and voilà…

Spyware is just the bigger category, which stuff like key loggers fall into. Basically stuff that reports data about you to someone else. And usually unwanted.

So, can all of them be in one and the same piece of malware? More or less. Less because spyware is a category, not a specific tool. But otherwise it would be possible. I’m not sure if it is likely though. I wouldn’t be surprised to find a key logger in a rootkit. But a bot… not so much. But yes… it’s possible.

Backdoor: A back door is a piece of software that allows access to the computer system by passing the normal authentication procedures. There are two groups of backdoors. The first group works much like a Trojan which is manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload.

Bot: A bot is a remotely controlled malware program that is installed onto a computer without the knowledge or consent of the computer's owner secretly taking it over. This type of program may have complete control over the operation of that computer and its Internet functions, but usually does not reveal its presence to the computer's owner or users, or try to interfere with the normal operation of that computer.

Keylogger: Captures keystrokes on the infected machine to allow an attacker to monitor this sensitive information. Since this would result in the attacker receiving a copy of all text entered on the compromised machine, keyloggers typically implement some form of filtering mechanism that only returns information close to desired keywords (e.g., "login" or "password" or "paypal.com").

Rootkit: A rootkit is a set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding. This provides access to all the functions and services of the operating system. With root access, an attacker has complete control of the system and can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand.

Spyware: Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.

**Q11. Define a distributed denial-of-service (DDoS) attack. (Chapter 7)**

Recognizing the limitations of flooding attacks generated by a single system, hackers invented tools for the use of multiple systems to generate attacks. That is called a distributed denial-of service attack.

**Q12. What defenses are possible against TCP SYN spoofing attacks? (Chapter 7)**

[**https://www.interserver.net/tips/kb/syn-flood-attack-prevent/**](https://www.interserver.net/tips/kb/syn-flood-attack-prevent/)

**Section III. Article summary** (20 points)

Please read the article “Security Controls for Computer Systems” at the following URL.

http://www.rand.org/pubs/reports/R609-1/index2.html

especially section " IV. AREAS OF SECURITY PROTECTION". Answer the following questions.

1. What are the categories of “leaking points” and why are they different?

2. Please give 1-2 case studies – either hypothetical or real-world cases that belong to “communication leaking point”. What are the possible ways to mitigate the leading point you choose? Elaborate your answer.

Note that your answer should not simply be a high-level review based solely on the RAND report – try to go deep into the technical details and refer to external materials. Answer to these two questions should at least be a 1-page single-spaced document. I would appreciate your critical thoughts on these questions. For external resources, please include a list of references, and use the APA format for citations and references where appropriate.

For APA formatting requirements, please refer to <https://nsufl.libguides.com/writing/apa>.



Certification of Authorship of Assignment

Submitted to (Professor’s Name): Dr. Wei Li

Class/Semester: ISEC660 Advanced Network Security, Winter 2021.

Students’ Names: Eric Webb

Date of Assignment: 1-24-2020

Title of Assignment: Assignment #1

Certification of Authorship: By submitting this document we certify that we are the authors of this paper and that any assistance we received in its preparation is fully acknowledged and disclosed in the paper. We have also cited any sources from which we used data, ideas or words, either quoted directly or paraphrased. We also certify that this paper was prepared by us specifically for this course.

Students’ Signatures: Eric Webb