CSCI3403 Cyber Security HW7
Name: Chen Hao Cheng

**Review Question Chapter 6**

1) What are three broad mechanism that malware can use to propagate?
   i) Social engineering attack that assures users to ignore security mechanism to install malware or react the phishing attacks
   ii) The accomplishment of software is either done over network by worms or locally or drive by downloads to permit the malware to copy
   iii) Existing executable or interpreted content with the infection of virus that is consequently transmitted to other system

11) What is the difference between a "phishing" attack and a "spear-phishing" attack, particularly in terms of who the target may be?

| Phishing attack | Spear-phishing |
|---|---|
| An attack electronic communication, then the attacker can get information from the user | An attack through email from the known parties like individual or business |
| The user login credentials, passwords, or banking information are gained by attackers | These attackers are different from the phishing attacker |
| The website such as gaming page, banking login page or similar site that will suggest the user to enter login information in order to authenticate his account and to prevent from locking | When the user enters his data in the fake website, those details will be recorded by attackers, such as spam |
| After the user enter his information in the fake website, the information has been recorded, and then the attacker will use this information to access other resources. | These attacks particularly used in well sourced organizations and industries |

## Problems Chapter 6

3) The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produces by the metamorphic code

| Original Code | Metamorphic Code |
|---|---|
| move ax, 5<br>add eax, ebx<br>call [eax] | move eax, 5<br>push ecx<br>pop ecx<br>add eax, ebx<br>swap eax, ebx<br>swap ebx, eax<br>call [eax]<br>nop |

Metamorphic virus:

The metamorphic virus can change each infection. This can be loaded without user knowledge and execute against the user's wishes.

Effect after the metamorphic code:

- It changes the original code to interrupt the signature, but it does not affect the semantics of the original code
- The semantics of the original code is not affected, but it interrupts the signature of the original code by changing the behavior
- The second, third, fourth, sixth, eighth are useless in metamorphic code

5) Consider the following fragment:

```
legitimate code
if data is Friday the 13th;
        crash_computer();
logitimate code
```

What type of malware is this?

This malware used in the given fragment is **logic bomb**.

**Logic bomb:**

1. A code inserted in malware that explodes when some certain actions trigger.
   (i) In the fragment, it checks if the date is right date (Friday 13th).
   (ii) If the condition is true, call the function crash_computer
   (iii)Once triggered, a bomb may alter or delete data or entire files, or some other damage

6) Consider the following fragment in an authentication program:

```
username = read_username();
password = read_password();
if username is "133t h4ck0r"
        return ALLOW_LOGIN;
if username and password are valid
        return ALLOW_LOGIN
else return DENY_LOGIN
```

What type of malicious software is this?

This kind of malware is **Back door**

**Back door:**

i) Also known as **trapdoor**
ii) A secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.

In the fragment:

i) It checks whether the username is "133t h4ck0r". If it's right, then return allow_login
ii) It checks whether the username and password are valid. If it's valid, then return allow_login.
iii) If both are not right or none of them is right, return deny_login

Therefore, the authentication program allows the secret admission to the username "133t h4ck0r" into a system, and allows the common security access procedures to the users with valid username and password.

10) Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it and see that a version is available form one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book". Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? What types of malware might it be?

The malware is **Trojan horse** while the user wants to install a game app.

1) User should be doubting whether this permission is needed for a game.
2) Relatively, it's a malware that collects details of the user contacts and also return them to the attacker through messages, or permit the code to send messages to the user contacts.
3) Trojan horse is a malicious piece of code that is delivered through the mail or web page that causes damage to the data or system

4) This would cause the threats to the confidentiality, integrity, and availability to the system.

Problem 11)

If the user opens the PDF attachment, then the malicious scripting code in the PDF attachment would run and the user should select the Open button. This selection of "Open" button might be worm or Trojan house code.

Worm: is a program that run separately and can spread the working version of itself into more hosts on a network, generally by exploiting software susceptibilities in the target system.

Trojan horse: is the malicious piece of code that is delivered through the mail or web page that causes damage to the data or system

**Checking the suspicious:**

- The user should check the suspicions without threatening the system. It can be done by scrolling the scroll bar and checking all the code about to execute.
- While examining the code, the user should select the Open button and check whether the code is suspicious

**Type of attack associated with message:**

- This is a spear phishing attack, which requests the user to click on a link and then install spyware that can steal the data

**Number of people received the email:**

- The specified email can be sent to one or a small number of people for whom the information would look reasonable.