1. **Review Question 6.1** What are the three broad mechanisms that malware can use to propagate?

   1) Infection of existing virus that can then spread to other systems. 2) Exploit of vulnerabilities in software either locally or over network via worms or drive by downloads to replicate malware. 3) Social engineering attacks that convince users to bypass security measures to install trojans or respond to phishing attacks.

2. **Review Question 6.11** What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?

   Backdoor: 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: remotely controlled malware program that is installed onto a computer without knowledge or consent of the computers owner, and secretly take 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 an infected computer 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 compormised computer, keyloggers typically implement some form of filtering mechanism that only returns information close to desired keywords such as "password", "wellsfargo.com", other sensative keywords.

   Rootkit: is a set of programs installed on a system to maintain covert access to that system with root privileges while hiding. This gives unrestricted

access to functions and services of the os. The attacker can have full control of the system to add/remove files, monitor processes, and send/receive network traffic. And gets backdoor access whenever.

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.

All of the above can absolutely be present in the same malware since some could definitely go hand in hand.

3. **Problem 6.3** The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produced by the metamorphic code.

```
1 Original Code      Metamorphic Code
2   move eax, 5        move eax, 5
3   add eax, ebx       push ecx
4   call [eax]         pop exc
5                      add eax, ebx
6                      swap eax, ebx
7                      swap ebx, eax
8                      call [eax]
9                      nop
```

The original code is altered without affecting the actual semantics of the original code. Lines 2, 3, 6, 7, and 8 are all ineffective instructions that do nothing. The point of this is to throw off software that searches for viruses in machines. By mixing up the lines, it makes it dramatically harder to track down malicious code.

4. **Problem 6.5** Consider the following fragment:

```
1 legitimate code
2 if data is Friday the 13th;
3   crash_computer();
4 legitimate code
```

What type of malware is this?

This malware is a Logic Bomb. The predefined condition is the data check where if met, will execute the code that crashes the computer.

5. **Problem 6.6** Consider the following fragment in an authentication program:

```
1 username = read_username();
2 password = read_password();
3 if username is "133t h4ck0r"
4   return ALLOW_LOGIN;
5 if username and password are valid
6   return ALLOW_LOGIN
7 else return DENY_LOGIN;
```

What type of malicious software is this?

This is a Backdoor software. This is due to the condition that checks for a specific username that can bypass the normal security check and allow this unauthorized person to access the system.

6. **Problem 6.10** 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 ad see that a version is available from 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 "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?

Yes, you should definitely be suspicious about this app. If granted permission, the app could send spread a malicious software to all your contacts through a text message that people think is coming from you. This malware could be considered a virus since it obviously needs a system (host) to infect in order to thrive.

7. **Problem 6.11** Assume you receive an e-mail, which appears to come from a senior manager in your company, with a subject indiciation that it concerns a project that

you are currently working on. When you view the e-mail, you see that it asks you to review the attached revised press release, supplied as a PDF document, to check that all details are correct before management releases it. When you attempt to open the PDF, the viewer pops up a dialog labeled "Launch File" indicating that "the file and its viewer application are set to be launched by this PDF file." In the section of this dialog labeled "File," there are a number of blank lines, and finally the text "Click the 'Open' button to view this document." You might also note that there is a vertical scroll-bar visible for this region. What type of threat might this pose to your computer system should you indeed select the "Open" button? How could you check your suspicions without threatening your system? What type of attack is this type of message associated with? How many people are likely to have received this particular e-mail?

As the user opens the PDF attachment, malicious code embedded could be ran and if the user selects the Open button, then there is a possibility of a worm or Trojan horse code being obtained. In order to check your suspicions without compromising your sytem, you could do many easier things like using someone else's computer. Or getting a hardcopy directly from your manager. A technical approach could invole a sandbox where you isolate your system and open the email attachment through a virtual machine. This attack could be considered worm propagation, macro virus, or a Trojan Horse. Every person in the manager's email contact list could have received this email.