Nitin Nagavel

CPRE 431

M04 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!

1. What is the main difference between machine-executable and macro viruses?
   Machine Executable viruses are attached to .exe files while macro viruses infect the materials with the .exe files.

2. What are three broad mechanisms that malware can use to propagate?
- Parasitic Code that attach that are attached to exes and spread when the application is initiated
- Media devices
- Network

3. Consider the following fragment:

```
legitimate code
if date is Friday the 13th;
        crash computer();
legitimate code
```

   What type of malware is this?
   This is a virus because its written as code and waits for a logic bomb that is executed to mess up the target's computer.

4. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?
   First report the USB to the InfoSec office of the work area, then destroy the contents, or if possible report to the authorities. To determine the contents, view the content in either a VM or a software forensics system that is safely monitored with less loss if anything were to happen.

5. Suppose while trying to access a collection of short videos on some website, you see a pop-up window stating that you need to install this custom codec to view the videos. What threat might this pose to your computer system if you approve this installation request?
   You could infect the system with a wide variety of malware.

6. Suppose you have a new smartphone and are excited about the range of apps available for it. You read about an exciting new game that is available for your phone. You do a quick Web search for it, and 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 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?

   This is a worm, that is spread by sending texts to everyone in the address book. This in turn can be sent to a wide variety of contacts that may lead to them believing is an actual text from you.

7. Why do many DoS attacks use packets with spoofed source addresses?

   They use spoofed source addresses because this prevents the victim from blocking or tracing the source address where the malware is being launched.

8. What is the primary defense against many DoS attacks, and where is it implemented?

   Primary Defense against DoS attacks include the use of firewalls, router rules, antivirus, or switches protocol.

9. In order to implement the classic DoS flood attack, the attacker must generate s a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 9.5-Mbps link? How many per second if the attacker uses a 2-Mbps link? Or a 10-Mbps link?

So 1 packet = 500 bytes which equals 4000 bits. Therefore:

- 1 mbps = 1 million bits
- 1 Packet = 4000 bits
- 9.5 mbps = 2375 packets per second
- 2 Mbps Link = 500 packets per second.
- 10 Mbps Link = 2500 packets per second.