Scribe Notes

Viruses are structurally classified in many forms, one example is prepended:

Prepended Virus:

Virus selects an uninfected file and attaches itself to the top of the file. It doesn't change anything in the file. Easier to clean and detect since one only needs to notice that the file size has changed and remove the infection from the top.

Appended (Post-pended virus):

Changes the pointer values in the file so that the infected segment is executed first, even though it's at the bottom of the file. Difficult to clean because of the need to readjust the pointers, but still easy to detect, as the file size is increased in the same way.

Embedded Virus:

Inserts code in the middle. Lots of changes in pointers of the file and so causes damage. More complex than the previous two viruses. Change of file size can still be detected.

Compression Virus:

Virus detects an uninfected file, compresses it, and attaches itself to one of either ends of the file. Compressed file size plus the virus equals the original file size. To detect: compute hash values of unaffected files and store them. Standard practice for file integrity. Hash values can change for a number of reasons – doesn't indicate if the file is affected by a virus. Repairing the file is difficult.

Virus classification (By Target):

Boot sector:
Virus infects the first piece of code executed when system boots up. All subsequent files can be affected, if the system boots at all.

File Infector:
Infests files that the OS considers to be executable.

Macro Virus:
Embedded in macro code. Infects documents (such as Office-style ones) and exploits “macro” capability.

Virus classification (By Method Of Concealment)

Encrypted Virus:
Generates and keeps a random key and uses it to encrypt the host file and itself. Used in conjunction with compression.

**Stealth virus:**
Designed to protect itself from antivirus software. Can make the host file appear to have the same size as it did before it was infected, hide the host file, and conceal outgoing messages (as in the case of a virus that launches denial of service attacks). May also prevent the antivirus from scanning the file that is hosting the virus.

**Polymorphic virus:**
Changes with every infection, changing the signature when it goes from one host file to another. It can change by rewriting the order of its instructions, by introducing trivial “dummy” instructions that don’t change the functionality, and encrypting itself. Most viruses today are polymorphic.

**Metamorphic virus:**
Rewrites itself completely at every infection, which means that the behavior of the virus changes along with the structure. Very difficult to detect.

**Email Virus:**
Viruses ordinarily attach themselves to host programs to propagate to other programs, but email viruses are similar to worms in that they can infect attachments and send themselves to everyone else on one's contact list.

**Virus Countermeasures:**

**Prevention:**
Ideal, but difficult. Don’t share drives or floppy disks. Don’t let anyone insert any jump drives in your system (unless they’re read-only, perhaps).

**Detection:**
followed by identification and removal. Containment is needed when virus is detected and later virus is removed. If the infection is detected but can’t be identified, isolated, or removed, the entire file may need to be replaced.
Antivirus technology is evolving

**Antivirus Generation:**

**First-generation scanner:**
Requires a signature to identify known viruses

**Second-generation scanner:**
Uses heuristic functions to search for fragments of probable virus infection. Hash functions are also used.

**Third-generation scanner:**
Memory resident programs, continuously looking for viruses in system. Searches based on behavior rather than signatures or heuristics. Can create a baseline from observing ordinary behavior but can also look for behavior specific to certain viruses. Potential for many false positives, however.

**Questions**

1. Q: Why is it so important to have the virus’ code run before the host program’s?
   A: if the host is allowed to run, the virus will find it difficult to spread before things change. The virus is run first to have the most flexibility in the system. For example, if the virus was hosted by an anti virus program, it would need to run first otherwise it could be detected.

2. Q: do viruses ever infect non .exe files like word documents and photos/videos?
   A: Viruses can infect non-executable files if anything in them can be executed, including photos, videos, and word files, because other programs do execute them.

3. Q: is there any famous examples of stealth viruses. How are they detected by antivirus software?
   A: It will be discussed later.

4. Q: is modern virus protection software capable of catching almost any type of virus? or are there certain types of viruses that there are not currently methods of detecting?
   A: Modern antivirus technology is very good, but new kinds of viruses do pass through sometimes.

5. Q: Where can we find more information about what is expected from us in the presentations?
   A: There is no presentation of the posters, but be present on the day and ready to answer questions about them.

6. Q: The MS Word exploit with .doc files: Does that still exist in .docx and does it exist in .rtf as well?
   A: Viruses can propagate from different documents formats if the macros are still there.

7. Q: Have you heard of the new “KRACK” wireless vulnerability that was recently announced which affects Wi-Fi users?
   A: Yes, KRACK is a vulnerability within the WPA2 standard. A virus or human would need to attack it for any damage to occur.
8. Q: do viruses ever use anti virus software to their advantage?  
   A: Haven’t heard of viruses using anti-virus software. This question will be looked into.

9. Q: What's the difference between anti-malware and antivirus technology?  
   A: They are used interchangeably.

10. Q: I've heard viruses can be embedded in images. How does this work, since images aren't "executed"?  
    A: When a program renders an infected image, it can execute a virus because the virus enters as input.

11. Q: Why is it said that Macs do not get infected by viruses?  
    A: It is an incorrect statement. Viruses exist in Macs and all other known operating systems.  
    Virus developers often want to attack the largest possible field, and Windows has good market share.

12. Q: How do router manufacturers push out changes to patch vulnerabilities like KRACK when there are thousands of routers? Do many personal routers go unpatched?  
    A: Managing security is a big concern in security. These are personal routers. There is a debate as to who has control of personal routers. Cable companies consider these end point of their infrastructure and so have control over their router. If an ISP takes no action, it can be a problem for the user. If a commercial router hosts a web server, it's hard to say how the patch would affect it. The administrator would have to decide what's best. Furthermore, patching is very difficult and slow to occur when the issue is in the specifications because changes must be made to every implementation. Wi-Fi should still be safe to use because the attack is proximity based.

13. Q: what happened recently with the WPA2 wifi hack?  
    A: Nothing seems to have happened yet. Vulnerabilities in specifications are difficult to remove. It will take some time to patch the flaw. The average wi-fi user should be mindful about their chances and take care. One very important thing for an attacker is proximity, so keeping the range of the network safe can help.

14. Q: what's the best antivirus program out there?  
    A: Can’t pick a “best” antivirus as they have different strengths. It’s important to have one, though.
15. Q: As more cars become connected and have issues, Jeep UConnect bug, are we going to expect cars to run custom versions of antivirus?

A: It's going to be tricky. There are a lot of different cars with very specific computers. Keeping the car’s network from being accessible is one concern.
Even light bulbs can be hacked these days. They have minimal firmware, so it’s hard to give them any anti-virus software.
A malware tool gives protection but comes at a cost, anti virus software is a stop gap solution.
Virus detection
Embedded systems like those in vehicles are not large enough to run a fully fledged anti-virus. It is better to design them defensively from the ground up.