CS 433/533 HW2 Key

1. Virus question

- Finds files without a certain signature
- Adds them to list
- Waits for a condition
- Unalives those files when the condition is met

2. A program is written to compute the sum of the integers from 1 to 10. The programmer, well-trained in reusability and maintainability, writes the program so that it computes the sum of the numbers from k to n. However, a team of security specialists scrutinizes the code. The team certifies that this program properly sets k to 1 and n to 10; therefore, the program is certified as being properly restricted in that it always operates on precisely the range 1 to 10. List different ways that this program can be sabotaged so that during execution it computes a different sum, such as 3 to 20.

- A malicious entity can:
    - Change the program's memory to change the k and n variables.
    - Change the code of the program

3. One way to limit the effect of an untrusted program is confinement; controlling what processes have access to the untrusted program and what access the program has to other processes and data. Explain how confinement would apply to the earlier example of the program that computes the sum of integers 1 to 10.

- If the memory of the process running the program is protected, other malicious entities can't directly modify it, making it a little bit safer.

4. Provide answers for these two situations; justify your answers.
    a. You receive an email message that purports to come from your bank. It asks you to click a link for some reasonable-sounding administrative purpose. How can you verify that the message actually did come from your bank?
    b. Now play the role of an attacker. How could you intercept the message described in part and convert it to your purposes while still making both the bank and the customer think the message is authentic and trustworthy?

- Check very thoroughly if the email domain matches, but this also is tricky because they can use very similar-looking letters yet still be different.
    - Just use their brains to see if this looks like a legit email from a bank
    - Forward the email to the bank's support and ask them if this is legitimate
    - Call the bank yourself and ask about this email
    - Look at the link without clicking to see if it looks fishy

- Insert malware
    - Swap the link with a fake website that looks just like the original, use that to steal credentials

5. Give an example of an object whose sensitivity may change during execution. Describe the difficulties of an operating system handling such a change in sensitivity. For example, how does it deal with a subject who, having originally qualified for access to an object, now should lose that access right?

- All of the changes and actions performed on the object by that subject must be revised, this needs audit logging.
- Access control must dynamically start enforcing the new permissions, which means that the trust policy should be default no-trust-always-check, so that all accesses are monitored and caught by the access control.

6. What are some other modes of access that users might want to apply to code or data, in addition to the common read, write, and execute permission?

- Change access control
- Change ownership
- Append
- Delete
- Some others

7. Describe a mechanism by which an operating system can enforce limited transfer of capabilities. That is, process A might transfer a capability to process B, but A wants to prevent B from transferring the capability to any other processes. Your design should include a description of the activities to be performed by A and B as well as the activities performed by and the information maintained by the operating system.

- A asks for a capability from OS, specifying it wants a limited transfer capability
- OS prepares the capability, marks its owner as A, and marks it as transferable
- A tells the OS that it wants to change the owner of the capability to B, but without transfer rights
- OS acknowledges and changes the ownership to B, but marks it as non-transferable.

8. List two disadvantages of using physical separation in a computing system. List two disadvantages of using temporal separation in a computing system.

- physical
    - Cant share resources
    - Lots of hardware
- Temporal
    - Cant parallelize, scheduling is a mess

    - Hardware goes underused

9. A flaw in the protection system of many operating systems is argument passing. Often a common shared stack is used by all nested routines for arguments as well as for the remainder of the context of each calling process.
    a. Explain what vulnerabilities this flaw represents
    b. Explain how the flaw can be controlled. The shared stack is still to be used for passing arguments and storing context

- Stack overflow
    - Stack corruption
- Protect the stack
    - Address space layout randomization