CSC 6585

Midterm Exam 2024

Secure Software Development, Computer Science, Tennessee Tech University

Instructions

This is an open-book, open-notes exam. Answer questions to the best of your ability, working **on your own**. Each question is worth 10 percent of the exam grade. Some questions have multiple parts; all parts have the same weight. You may answer as many questions as you wish, but **only the 10 best answers** will be counted.

Handwritten and scanned or photographed documents are fine, but you are expected to write legibly and to use reasonably correct grammar and spelling; answers that cannot be read or evaluated will not receive any points. Please do not create ASCII art diagrams.

Be sure to state your assumptions explicitly.

Questions

1. Your company uses an online data-sharing system for communicating in real time with partners. The online system is pre-configured, provisioned, and maintained by a third party.

   Is the data-sharing system inside or outside your company's system boundary? Justify your answer.

2. You work for a logistics company and maintain your corporate database on a cloud provider's platform. Consider the following.

   - Serrice Technology provides telematics (telematics is hardware and software for monitoring a fleet of vehicles) and pushes information to your cloud database. This information includes vehicle location, weight, and health.
   - Ascension Financial Services has a data feed from your cloud database. This information includes contract fulfillment, payment processing, and accounts due.
   - You communicate with your drivers using a third-party communication provider, Sonax Industries.

   Draw the components of this system, identify trust boundaries, and label all flows. Be sure to state your assumptions.

3. A software system has a large set of configuration options, stored as JSON files with one JSON file per component. These files are stored in a git repository, allowing users to switch configurations (using branches) and to roll back to prior configurations if problems are detected.

a. The git repository can be stored locally in the software's configuration folder (an application-specific folder under `AppData` on Windows, `Library/Preferences` on macOS, and `~/.config` on Linux). What, if any, concerns would you have with this arrangement?

b. The git repository can track a remote cloud-hosted repository, enabling settings sync across multiple machines. What, if any, concerns would you have with this arrangement, distinct from those identified in part a?

4. Consider this proposed definition. "A software system is secure iff there is no series of inputs to the system that results in output of the content of a file unless the final input in the series originates from the file owner."

   Now consider the CIA triad. For each of the elements of the triad, does the above definition address that element? Explain.

5. Consider a simple web store. A back end server provides the business logic, while the front end runs in a web browser.

   a. Draw a block diagram of this scenario, labeling all information flows. You should include the end user, web browser, front end software, back end server software, server hosting environment, inventory database, authentication server, customer information database, payment processing contractor, the administrator interface (for simplicity we will assume it runs natively on the server), and the system administrator.

   b. Specify the system boundary for the server software by identifying its interfaces.

   c. For every control or information flow in your diagram for part a, determine if the flow crosses a trust boundary. Consider bidirectional flows to be a single flow for the purpose of this part.

6. A piece of financial software has the following logic. Here `RESULT` is a result code, `Acct` is an account structure, and the `LOCK` and `UNLOCK` macros prevent a race condition. Note that `static` functions in C are private to the containing module.

```
static RESULT _deduct(Acct * account, int value)
{
    if (account->balance < value) {
        return INSUFFICIENT_FUNDS;
    }
    account->balance -= value;
    return OK;
}

RESULT deduct(Acct * account, int value)
{
    LOCK(account);
    RESULT result = _deduct(account, value);
    UNLOCK(account);
    return result;
```

```
}
```

a. What happens when the value is a negative number and the account balance is positive?

b. How would you recommend addressing this problem in the given code? Be specific about how you would change the code.

7. Canada and the US decide to connect information processing systems based on the Bell-LaPadula model. Fortunately, the two countries have exactly the same sensitivity levels. To preserve state secrets, both countries introduce an additional security modifier: CAN-ONLY for Canada and US-ONLY for the US, and corresponding clearance tags: CAN for Canada and US for US. These sensitivity levels are independent of the usual TOP SECRED, SECRET, CONFIDENTIAL, UNCLASSIFIED forms.

   Is the resulting system still Bell-LaPadula secure? Consider each of the required properties and whether it holds for the composite system.

8. Recall the five functions for physical security and classify each of the following security measures to those functions. Identify which function or functions are addressed by each.

   a. A login screen states that the system is for official use only by US government employees, and that misuse of the system could result in fines or jail time.

   b. After three successive login failures the system logs you out and blocks your IP address.

   c. After a two login failures the system forces you to wait a full minute before trying again.

   d. The system detects when a specific file is read and, if that is detected, the stored disk encryption keys are randomized and the system is shut down.

9. Recall the NIST five functions and classify each of the following security measures as one of those functions. Identify which function or functions are addressed by each.

   a. You hire a lawyer to advise you about the relevant laws governing the specific data you intend to collect and store.

   b. Your system periodically autosaves its current state to a git repository.

   c. The system implements a "watchdog timer." If the timer ever counts down to zero, an alarm is reported through the endpoint monitoring software.

   d. Your IT team runs a "tabletop" exercise with the scenario that you detect an intrusion in the network.

10. A software system checks the host key of a connecting machine and requires that the user identify themselves with both a password and a 2FA token. For as long as the user is logged in, the software periodically sends a challenge to the remote host and then checks the reply to re-authenticate the connecting machine. While the user is interacting with the system, biometrics are collected and compared to the user's baseline.

Is this an example of defense in depth? Why or why not?

11. Consider the CIA model of Confidentiality, Integrity, and Availability. Different contexts require different security measures.

    a. Give an example of a system where confidentiality is more important that the other two properties. Explain.

    b. Give an example of a system where integrity is more important that the other two properties. Explain.

    c. Give an example of a system where availability is more important that the other two properties. Explain.

12. Consider the HRU command definitions and the safety rule, and let A be the access control matrix.

    a. Create a command foo that accepts two subjects, a and b, and an object name X. The command checks that A(a,b) contains FOO that that A(b,a) does not contain FOO and, if both are true, it adds object X with owner a.

    b. Consider the command you wrote for part a. Does the command ever leak the right FOO from the system? That is, is it safe with respect to the right FOO?

13. The HRU paper shows that, given a Turing machine, we can convert the question "Does this Turing machine halt on all inputs?" to a protection system and the question of whether it is safe. Thus if we could answer the latter, we would also be able to answer the former, and thus solve the Halting Problem. Since we are confident the Halting Problem cannot be solved in general, it follows that it is undecidable whether a given protection system is safe.

    A friend shows you a design for a protection system and tells you that they can prove it is safe. Is that possible? Why or why not?

14. Your goal is to gain access to my iLearn account for this class. Build an attack tree starting with this goal. The leaves of the tree should be specific actions, but you do not need to be more detailed that the example given in class.

15. An attack has an 10% chance of succeeding and, when unsuccessful, there is a 25% chance of being detected. Assume detection results in a change to the system preventing the attack in the future. Create an attack graph that represents this situation and label the edges with actions (success, failure, detection, no detection) and probabilities. Assume the attack will be repeated until it either succeeds or is detected, and capture that in your graph.

16. [Extra 10 points] What is the overall probability that the attack in question 15 eventually succeeds?