ISEC 400 Homework 6 Name: Megan Leonard

Answer the following questions based on your reading of the textbooks, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. **[5 points]** What are the main purposes of authorization? How is authorization related to authentication (if at all)?

The main purposes of authorization are to determine if the person’s permissions are high enough for the task they are trying to do, it helps with security by giving people different levels of access with the systems. Authentication is a means of making sure that the person is who they say they are to help protect the system. It relates to authorization as they are both looking at the person and determining if they should be allowed access.

1. **[5 points]** Are read, write, and execute permissions sufficient for controlling access to web applications? Why or why not? How do these compare to CRUD-style permissions?

These are not sufficient for controlling access to web applications as the users are able to interact with functions on the system itself which can cause problems. The CRUD-style permissions only allows access to various pieces of data as it limits the person’s affect on the system and keeps them from altering any settings or running any functions.

1. **[5 points]** How do the horizontal and vertical authorization layers promote a defense-in-depth strategy? Describe the steps through the vertical and horizontal layers for a single web request.

The vertical authorization layers use the defense-in-depth by making access layers so if a person wanted to reach a web request, they would have to have the permission to the hardware, operating system, and then the web server as the higher permissions require the person to have the lower ones as well. The horizontal layers mean the person must have the permission to the left of the permission they need. This means that if you want to be able to reach the web request, you would need to have permission to the web browser to access the web server.

1. **[5 points]** Describe how the 3x3 custom authorization mechanism works. How does custom authorization compare against using a third-party plug-in library for authorization?

The 3x3 model looks at the what and when as the dimensions each having three parts. The what dimension looks at the subjects, objects, and operations. The when dimension looks at the before loading interface, before requests are submitted, and before granting final access. The custom authorization mechanism is specifically based around the organization that is using it while the third party will have a reusable software that is sold to others so it can be more complex but may also come with known problems.

1. **[5 points]** Of the session management best practices, which are the top three in importance? Describe each best practice with some detail.

The first of the best practices, would be to never keep session state on the client as this would let people sessions to one another by sending another the http address as it is all right there. The second practice is to use a cookie for the session ID instead of a form or in the URL as if it is in the URL, then others could access that session if they have the URL. The cookies keep the session localized and to that person. The third best practice is session timeouts. Timeouts are best used to limit the time of the session so that it will not be able to be used after a specific amount of time using absolute to limit the time the session is there and idle to force a re-authentication after a limited amount of time.

1. **[5 points]** In approximately 300 to 400 of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered this week in class. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Ask at least one question that your instructor can answer in the returned assignment or class discussion.

This week we looked into more authorization methods and session management. Authorization is always an interesting topic to cover even if I enjoy authentication more. Being able to limit the access of the person based off of a set of permissions is always fun to discuss as we can also look at the permission systems that are used for authorization. CRUD is a topic that I have not really heard before this year as my second practicum class is using this for my team project for access. I have not heard of the horizontal and vertical layers before, but I can see the appeal as they help with determining the level of importance and defense in depth. The 3x3 model is one that I will have to work on remembering as it is two parts with three points so I can help think of it like the 2(3)model as it is two sets of three. Session management is a topic that I have gone over in a lot in my classes as there are a lot of attacks that can happen through the sessions. My questions for this week are, in the AAA services of security do you have a favorite and do you prefer the horizontal or vertical layer for authorization?

Citation:

Whittaker, T., &amp; Whitney, T. (2022). Week06 Power Point. Retrieved March 5, 2023, from <https://franklin.instructure.com/courses/11070/files/1516720?module_item_id=623553>