ISEC 400 Homework 1 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]** Compare and contrast access control lists versus capability lists. In a software implementation of an authorization mechanism in a web-based application, which would you prefer to implement and why?

Access control lists and capability lists are both views of a matrix. They can be seen as two differing views of the matrix as the access control lists will look at the columns to see subjects and the rights they keep on the object. The capability lists look at the rows and the lists of objects and the permissions they keep with the subject.

As we are looking at an authorization mechanism, we can look at how it is set up as it has the permissions users will get to a specific object which is the web-based application. This in mind, I would prefer to implement the access control lists as we are authorizing different users and their rights kept on the object. So, we have a single web-based application with multiple users.

1. **[5 points]** Compare and contrast the Bell-LaPadula and Biba security models. What are the goals of each? How could each be implemented in a software system?

The Bell-LaPadula and Biba security models each have a different primary concern. The Bell-LaPadula model is concerned about confidentiality and will assign labels that correspond with its concern. The Biba model is primarily concerned with integrity so its assigned labels will correlate with it. They both have simple and star properties even if they go in the opposite direction. The Bell-LaPadula model at simple property stops a user from being able to read anything at higher levels. They also can not write or alter objects that are found in the lower levels. The Biba model makes it so that the user cannot read anything lower than their integrity level and stops them from altering any objects higher than their level. The Bell-LaPadula model is best implemented by giving specific users different permissions within the software system. This means that not one person has permission to alter the entire system. The Biba security model can be implemented based off of level of knowledge so that a senior employee could work at a higher level than a novice as they would have different views of the system and different areas they would work best at.

1. **[5 points]** Compare and contrast MAC, DAC, and RBAC authorization models. Are these related to Bell-LaPadula and Biba? If so, how? If not, then why not? Describe at least one situation where MAC, DAC, and RBAC are most appropriately implemented.

Each of the authorization models have the system enforce their access policies. The MAC uses system policy to determine access while DAC uses individual users. RBAC will use the roles in the organization so it can determine access. Bell-LaPadula and Biba models each have their own way or authorization through assigned labels which corresponds to how the system enforces the access policies as it makes sure that the labels determine the level of authorization similar to RBAC with its roles. One situation would be a company database that is split between departments and levels of authority. The MAC will help make sure the person can access the database. DAC is useful for group work within the departments as it allows the chosen people access. RBAC helps with splitting the database access into the different departments using role-based access.

1. **[10 points]** Research *why* industry, academia, and government think that software is insecure. In four or five paragraphs, provide at least three cited reasons and justifications for their opinions. Do you agree? Why or why not?

When it comes to software, everyone has their own concerns about its security. Industry will look at it from a business standpoint. Academia looks at it from a learning perspective such as cheating or classes that exploit these insecurities. The government looks at a bigger scale as software insecurity can cause problems for entire countries.

Looking at software insecurity from an outside perspective has a person asking why they haven’t made it secure. Based off of the articles I was able to find, the overall idea is that while we can work to make some more secure there will always be a level of insecurity. This comes from a lack of trained cybersecurity specialists and people weighing the pros and cons of waiting until the software is completely secure to release it.

In school in the computer degrees, we have classes that will teach us different security methods by showing us how to exploit it. The starting point of understanding the software security within the academia is by understanding where it is insecure.

Industry must look at software release based on how fast it is put out and secure. They are able to see how insecure software can be as they do not always have the time to keep testing and fixing it or the people who are able to do this.

The government has to decide on software based on if it will help or hinder their governing area. They can see where there are insecurities but either can not fix it because of the level of importance or they do not know how. They are able to affect a lot of people with their choices, so they have to decide at which point the pros are greater than the cons.

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 investigated different models of authorization and security. The different aspects of application security are ones that I have heard or gone over before except for the non-repudiation. The reading shows that non-repudiation means that parties of a transaction can does not deny being a part of it. I can see how this is important to security especially when it comes to retracing steps of transactions. It makes me think of how kids will do something bad, get another to join them, then go tell an adult that the new kid is doing something bad and deny being a part of it. Even from a business standpoint like Ebay with having a person pay for an item then Ebay saying that there was no transaction, keeping the money that was sent. Each of the key aspects have their own appeal when it comes to studying and learning about them. My question is out of the key aspects, which do you like the most?

Citation:

Application security - for everyone who doesn't "WannaCry" because of insecure coding habits. SCADEMY. (n.d.). Retrieved January 29, 2023, from <https://www.scademy.com/application-security-for-everyone-who-doesnt-wannacry-because-of-insecure-coding-habits/>

Chong, J. (2023, January 30). Why is our cybersecurity so insecure? The New Republic. Retrieved January 29, 2023, from <https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure>

Daniel Miessler. (2021, August 5). Why software remains insecure. Daniel Miessler. Retrieved January 29, 2023, from <https://danielmiessler.com/blog/the-reason-software-remains-insecure/>

Kavanagh, C. (2019, August 28). New Tech, new threats, and new governance challenges: An opportunity to craft smarter responses? Carnegie Endowment for International Peace. Retrieved January 29, 2023, from <https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736>

Simpson, E., &amp; Conner, A. (2021, November 19). How to regulate tech: A technology policy framework for online services. Center for American Progress. Retrieved January 29, 2023, from <https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/>

Sullivan, B., Liu, V., & Howard, M. (2012). Web Application Security: A Beginner's Guide. McGraw-Hill. ISBN: 9780071776165

Whittaker, T., &amp; Whitney, T. (2022). Week01 Power Point. Retrieved January 29, 2023, from <https://franklin.instructure.com/courses/11070/files/1508860?module_item_id=623382>