Confidentiality, Integrity, Availability Models

Bernard Ayuyao

Old Dominion University

CYSE 600 36666 Cybersecurity Principles

May 29, 2021

Confidentiality, Integrity, and Availability Models

There are many vulnerabilities that are possible threats for our information systems and the CIA triad or confidentiality, integrity, and availability are the basic security properties that attackers want to attack or exploit vulnerabilities from. Vulnerabilities within the CIA triad can cause potential harm to our systems and we do not want that to happen because we care about our assets that we hold value to. We try to analyze what we are looking at within the CIA triad using models. There are three models that we can look at and each property of the CIA triad has its own model. We look closer to what confidentiality, integrity, and availability are all about through their own process. Each process prevents the attacker from exploiting our assets by preventing them from unauthorized viewing, modification or fabrication, and preserving our data. Once you combine all of the processes together, we get a security framework which makes our system stronger or hardened.

First, we start with confidentiality. From this journal, confidentiality is defined as "the protection of data from compromise, of special interest to the U.S. Department of Defense (DOD)." (Hammonds, 1993, p. 48). Although, we may understand that in today's definition, confidentiality is to ensure that something can be viewed by an authorized user or party. As we get to walk through the steps in the confidentiality model, or Reference Monitor model, you will understand our definition of confidentiality is the same as well as the process the model takes to ensure access. Hammonds writes, "ln Step 1. a subject (e.g., task or process) attempts to access an object (e.g., file, memory), causing the RM to be invoked. In Step 2, the RM attempts to validate the access using a set of rules (generally embodied in its instructions and algorithms) and data containing security attributes of the subject and object. If the check is successful, then in Step 3, the access is permitted otherwise it is disallowed." (Hammonds, 1993, pp. 48-49). This

shows that the process in the model starts with a subject or user who wants to access an asset which we understand it as being viewed. The rest of the steps in the model also shows that this can protect confidentiality by allowing or denying access to our asset.

Next is the integrity model and its process. Integrity is also defined as “the prevention of improper modification, a major concern of the private sector.” (Hammonds, 1993, p. 48). We can agree with this definition and a great example is having a picture taken of you on a nice sunny day with a beautiful background of the ocean and looking professionally groomed. This picture can be stored on your share drive and someone can modify that picture using photoshop and change the appearance of the picture by making your picture appear like it is was taken on a gloomy day with an unattractive background and you having a bad hair day. Hammonds continues writing the steps in the Integrity Model, “In Step 1, the Change Agent (e.g., user, application, operating system, hardware) affects a system Resource, such as a append to a file, or update a database record. In step 2, the modification has the result Resource.” (Hammonds, 1993, p. 49). This process is straight forward and shows what happens when someone like a user wants to affect a resource and having the end result of modification.

The final model is assured service which is also referred to as availability. Hammonds defines assured service as “the prevention of denial of service.” (Hammonds, 1993, p. 48) We understand that availability as an asset that can be used by any authorized users or parties. Hammonds describes the assured service model having two components, an initiator and a processing component. Hammond writes, “The initiator actively seeks die services of the processing component. If successful, the service is performed expected. For example. A user can interact with an application, or system software may invoke one of the system utilities.” (Hammonds, 1993, p. 50). We can see that because of the processing agent, the application was

not usable for the initiator or the user, which then is important for us because that processing agent is what determines that the application should not be usable for this specific user who can be a possible threat to our system.

Finally, what makes the CIA triad a great is that putting or tying all the models together which gives us a good security framework. Combining all models and their components which is the initiator, processing agent, reference data, and resources makes us stronger to the vulnerabilities that an attacker can exploit and cause harm to our system. Hammonds walks through the security framework as, “In step 1, an Initiator invokes a service through a Processing Agent that, depending on the service, may include a Reference Monitor check of the rights of the Initiator. In any event, data is available to the Processing Agent (sept 2) to support its processing. If the processing is authorized, the service takes place (step 3), which may include the invocation of other processing agents in sequence. Step 4 is the transition to the new state of the Resource.” (Hammonds, 1993, p. 51)**.** We can see that when combining the CIA triad models, we get a stronger process because of the monitoring and allowing or denying access throughout the process.

All in all, we have learned what the CIA triad of confidentiality, integrity, and availability means to us and vulnerabilities in the CIA triad can have a potential for an attack. We may understand their definitions but each of them has a process. Each of their process makes our information systems stronger to vulnerabilities from unauthorized viewing for confidentiality, modification or fabrication for integrity, and preserving access for availability. Once we tie all these processes together, we have a stronger security framework which can then have our system hardened from any vulnerabilities that attackers may want to exploit in the future, keeping our valued assets safe.

References

Hammonds, G. L. (1993, August 3). Confidentiality, Integrity, Assured Service: Tying Security All Together. 48-52. Retrieved from https://dl-acm-org.proxy.lib.odu.edu/doi/pdf/10.1145/283751.283775