The C-I-A Triad

Courtney D. Spencer

Old Dominion University

Table of Contents

Abstract

This paper highlights the intricacies of the C-I-A triad and goes in depth on to further protect against attacks with malicious intent. In a relationship in the world of cybersecurity the expectations for networks whether they be private or public to be secure is no different than a personal relationship. Gaining a deeper understanding of how the three key principles, Confidentiality, Integrity, and availability are relevant in the cybersecurity world you can then realize just how important the triad is in maintaining a sense of order in information security.

Keywords: Confidentiality, Integrity, Data, Core Principles, Availability

The C-I-A Triad

Relationships are a very complex to navigate, requiring an ample amount of time, understanding and tolerance to make sure that all parties involved are happy. There are four major types of relationships consisting of romantic relationships, friendships, business partnerships, as well as fans followers and clients. It's safe to say that all people are familiar with being involved in many if not all of these four major types of relationships. In a romantic relationship people usually have s particular set of expectations that vary from person to person however there are a few that tend to stay the same. In the event that the romantic relationship is exclusive, the expectation is that both parties are to stay loyal to each other and not "step outside the relationship". In the event that cheating has occurred no matter how painful the reality of the situation is the hope is that the cheater would be honest and confess what happened behind close doors. In friendships no matter what you age you are people often tell secrets to their closets friend(s) as a form of venting or freely expressing various emotions. In this relationship as well as many of the other, the expectation is that the information is confidential and will stay between the party's involved. In any of the relationship a person may currently have, it's safe to assume that when one party needs the other, they will be available to attend to their needs. If you call your mom you want her to answer the phone. If you call a tow truck you assume that someone will be available to cater to your needs due to the fact you are paying for a monthly service. If you need a friend the hope is that your friends will be there to help you through whatever situation you may need her/him for. In the world of cybersecurity the expectations are no different. Three letters make up what is commonly referred to as the C-I-A Triad and together make up the foundations of an organizations security infrastructure. Confidentiality , Integrity, and Availability make up the C-I-A Triad and is critical to data protection. Understanding the

intricacies of all three components, how they are relevant to not only the cybersecurity aspect of things but also the business side of the relationship and how the C-I-A triad affects both sides of the relationship financially are crucial in the world of cybersecurity.

Initially when most people hear the letters CIA together, they often think of the Central Intelligence Agency which is an independent United States government agency. Although they are not exactly the same, the U.S government agency CIA and the C-I-A Triad in reference to cybersecurity principles do both deal with the security aspect of things. As previously mentioned the letters in the C-I-A triad stand for Confidentiality, Integrity, and Availability. The first letter being the C, Confidentiality protects potentially sensitive information that clients may have from being stolen by people with malicious intent. Information security is all about protecting information not just for privately owned businesses but also for government agencies, personal home networks and public networks. An attack can happen anywhere, anytime and at any location and in order for the confidentiality to be maintained the data must be protected not only while in storage, but in process and in transit as well. No matter what type of information is on the network it is a necessity for users to be confident that they can operate and conduct business as normal without worrying about their more sensitive data being accessed and exploited by an attacker. If an attacker wanted to violate the confidentiality aspect of the triad, he/she can capture network traffic, perform port scanning techniques, eavesdropping techniques and even use social engineering techniques like shoulder surfing. In fact it is said that, "Violations of confidentiality are not limited to directed intentional attacks. Many instances of unauthorized disclosure of sensitive or confidential information are the result of human error, oversight, or ineptitude" (Gibson, Chapple, & Stewart, 2018). More often than not people tend to feel comfortable in places like the office or even their favorite coffee shop and too often let their guards down not

thinking about who may be around them or what their intentions might be. In an environment such as the office at work an individual could go to the printer and while attempting to multitask goes to the copy room intending on making a few copies, leaves and also goes to grab a cup of coffee from the break room. In this situation the employee was only trying to cut down on the time being wasted but in the meantime left an important document exposed therefore violating the confidentiality of that classified file. In this situation there is no way of knowing if someone read the document while unattended or if another copy was made and now in the hands of an unauthorized person. This same situation could apply to an individual that has root privileges and walks away from and access terminal while data is left on the monitor. There are many other instances where pure human error can lead to the violation of confidentiality such as failing to fully authenticate a remote system before transferring data, not properly encrypting a transmission, or even accessing malicious code that opens a back door. While breaches are commonly due to human error they can also be due to an oversight in security policies or other security controls and luckily there are countermeasures to help protect against such threats and vulnerabilities. Things like network traffic padding, rigorous authentication procedures, and extensive personnel training are all steps that can be taken to further ensure the confidentiality aspect stays secure.

When referring to the second letter in the C-I-A triad , the I represents integrity and is responsible for the prevention of unauthorized alteration of data. In this section of the triad the focus is on making sure that attacker has not taken a document modified and then continued to send it through as if nothing ever happened. When you send an email to a co-worker containing important information, the assumption is that what you wrote is going to be exactly what your co-worker receives. If the email you sent matches up with what your co-worker receives, the

integrity of the email is intact and he/she can no respond accordingly. When the email is not what the sender wrote , the data integrity has been compromised and this can happen in a number of different ways. Not only is the data is susceptible to be corrupted in transit but it can also be unintentionally modified in memory or on a disk. Like human error can compromise the confidentiality of data, integrity can also be corrupted by basic human error. For instance you are working on a resume and you have two copies of the same resume. On the first resume you are working on you have notes to the side of the document, highlighted words, underlined phrases, and bold letters. However on the second resume you are planning for it to the final draft, no highlighted words, no more notes, and everything is exactly how you prefer it to be. If you overwrite a section of the second resume in hopes that you are working in the first resume which is the draft, this can in fact be seen as a loss of data integrity. In this situation the document you have been working on, you now notice pieces of the resume have been altered and are now missing key points. If the second resume without corrections have not been backed up to the computer then there is a high chance you may not notice the mistake before sending it off to future employers. Now the wrong information has been sent and you may not ever realize what happened unless you are confronted on the receiver end. In transit an attacker can perform a man-in-the-middle attack to intercept the data. As Messier stated, “Integrity isn’t only about the contents of the data. It may also be the integrity of the source of the information”. This means that writing a letter is not as simple as it may have once been. Now when looking at the integrity of the messages, it is important to loos for things like a digital signature to ensure that person you communicating with is in fact the person who wrote the letter. The possibilities are endless when it comes to ensuring the integrity of data. A few examples could be to incorporate strict access control , intrusion detection systems, hash total verifications and even interface restrictions.

There are many other countermeasures that can be taken to further ensure the integrity of data those previously mentioned are just a few examples.

The last principle in the C-I-A Triad is availability giving subjects timely and uninterrupted access to objects. Lack of availability may not always be because of malicious activity. Imagine you are having a stressful day and while talking to your mom she says "call me whenever you need me, I have open availability today so I can help you with your problem". In her saying that you now expect to when you call your mom with a question, she will be available to talk to you throughout the day. Imagine that whenever you call her, she does not answer the phone. In doing this she is not being very available to you but that does not necessarily mean that she is maliciously ignoring you. Something might have come up to where she was just unavailable at the specific moment. Similar situations of services or information being unavailable but without malicious intent may occur. Putting information on an external drive is not an uncommon practice and often are actually a preferred method when having to carry around data files or other resources. But what happens when you forget the external drive at home? The files on that specific drive are now unavailable but nothing malicious happened to them, you simply don't have access to the files when you need it. The data has not been lost or altered, but is still not where you currently need them to be which is in fact a breach of availability. Although it is possible to have a breach in availability without malicious intent, it is also possible for an attacker to perform a malicious attack. For example a Denial of Service or DoS attack denies access to a service and contributes to that particular service being unavailable for traffic to take place. Like integrity and confidentiality one cannot be maintained without the other. Availability needs both integrity and confidentiality to function effectively Without all three principles of the C-I-A Triad, attacks are more susceptible to take place. In violation to the

confidentiality principle, port scanning, shoulder surfing, escalation of privileges, etc. can take place. In violation of the integrity principle attacks such as logic bombs, errors in coding and applications, malicious modifications and numerous viruses can happen. With availability not being maintained correctly threats like device failure, DoS attacks, communication interruptions and even environmental issues are able to take place. In 2018 the Executive office of the president of the United States wrote a document called The Cost of Malicious Cyber Activity to the U.S. Economy that found the following:

> Using survey data from 254 companies, Ponemon (2017a) computes an estimate of how much each cost component contributes to the immediately observable loss and comes up with the following ranks and percent contributions to the total (in parentheses): (1) information loss (43 percent); (2) business disruption (33 percent); (3) revenue losses (21 percent); and (4) equipment damages (3 percent), (advisers, 2018).

The survey goes into go into further detail on the disbursement of finances when it comes to dealing with malicious attacks. With the triad principles compromised malicious cyber activity is now able to take place at a higher rate and in 2016 it was estimated to cost the United States economy between $57 billion and $109 billion dollars.

In ensuring that the C-I-A triad stays in tact we can further protect against attacks with malicious intent. In a relationship in the world of cybersecurity the expectations for networks whether they be private or public to be secure is no different than a personal relationship. In gaining a deeper understanding of how the three key principles, Confidentiality, Integrity, and availability are relevant in the cybersecurity world you are now able to protect yourself and/or your network from outside threats.

References

Advisers, T. c. (2018, February). *The Cost of Malicious Cyber Activity to the U.S. Economy.* Retrieved from www.whitehouse.gov: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Gibson, D., Chapple, M., & Stewart, J. (2018). Security Governance Through Principles and Policies. In *CISSP® Certified Information Systems Security Professional: Official Study Guide, Eighth Edition* (pp. 1-48).

Messier, Ric. (2019). Security Foundations. In CEH v10 Certified Ethical Hacker Study Guide (pp. 49-82). Hoboken, NJ: John Wiley & Sons.