5-1 Case Study: Triple A and Defense in Depth

Joel Meza

Professor Trevor Hodde

February 1, 2022

CS 405 – Secure Coding

Southern New Hampshire University

As more research is done, I start to understand better in depth why is defense security so important and the major role it’s used in software development and operation as an essence. In this assignment, I will speak about a good example to clarify better how Triple A and Defense in Depth is used. For the example, I’ll use an article that historically made in impact to cybersecurity which is called, “Equifax Data Breach” by USA Today. This data breach failure occurred on March 7, 2017, where to be known that Apache Struts had recommended to upgrade their software for security purposes. The known scandal of this security failure made a great impact not just on the company’s name, but to all the afflicted one hundred and forty-seven Equifax’s customers nationwide.

This security breach chaos was caught in the catalyst first news, where data was intercepted by hackers which got to a deep layer of security, plus gone over the security protocols which supposably were delayed, prior to the article; where Equifax did not respond on time for a new upgrade which made them an exposed target for hackers to trigger into their database. Although this data breach impact was exposed within deep defensive layers, it had also caused red flags of suspicious activity from the Equifax’s higher executives which did not take the correct security measures before the confidential data was exposed. Where it’s known that the amount of security intervals where the hackers got into, were easily accessed to acquire inside the system and gain confidential data from million known American customers. This caused a sour taste to the higher executives of Equifax which lawsuits were made against them because of their corrupted behavior.

The compromised data breach was exposed to hackers by a client’s complain from their own portal website. As it was tracked down, the hackers had used a SQL Injection vulnerability that should’ve been restored or easily maintained by security upgrade from a software engineer, but the adjustments were not made on time. Potential threat occurred when the hackers had pulled confidential data from the database server of Equifax made by an encrypted format which was left hidden by these hackers for several months. Failure on upgrading the certificate encryption was the cause of this data breach despite of their urgency to update their certificate encryption on one of their software system tools. Along with the late announced data breach from several months by corporate, this was a major key factor to the threat attack in being so successful. However, Equifax regulations to reinforcing security measure was not clearly a priority which considering these regulations, this could’ve been avoided for any type of data to be compromised. Therefore, I believe that feedback in communication is key for future security protocols to be more reliable, secure, and with several layers of security to make any type of software program or system safe.

For access vulnerabilities, we need to reinforce “Triple A” which is known to be the authentication, authorization, and accountability, first before working on a new or existing user prior to giving them clearance into a software program or system. Triple A is a very reliable source and security layer policy which protects a program or system from any unauthorize user to be wrongfully granted access. To better use authentication, authorization, and accountability, we must get some data from a safe user within the registration process first, which can help us to validate or authenticate them as a safe user. Once we acquire their unique input credentials that are provided from this safe user, then we can use that same data to verify or authorize their identity before getting complete access. Monitoring the process is to be accountable in each portion of the security layer from attempting to log in into a webpage portal and distinguishing if the user is safe and really who they say they are, on despite of how much time duration they tried to attempt to gain access in a particular security layer measure. The ideal purpose of Defense in Depth (DiD) in consideration, is the reference of information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the [confidentiality, integrity, and availability](https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/) from a network and its data within them (“Center for Internet Security”, 2021).

**Citations**

1. Bomey, N. (2020, February 10). USA TODAY: *How Chinese military hackers allegedly pulled off the Equifax data breach, stealing data from 145 million Americans.* **Retrieved From:** [**https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/**](https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/)
2. Anonymous. (2021). Center of Internet Security: *Election Security Spotlight – Defense in Depth (DiD).* **Retrieved From: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-defense-in-depth-did/**