7-1 Journal: Consider the Motive for the Attack

Joel Meza

Professor Trevor Hodde

February 17, 2022

CS 405 – Secure Coding

Southern New Hampshire University

**Consider the Motive for the Attack**

Most hackers’ intentions to begin hacking is for several reasons where it may fluctuate as they gain more experience. Some of the desires that a hacker got for hacking is extortion which defines as obtaining important data that can be led to wealth income or personal desire by force. Threats that a hacker makes are built under social engineering aspects which the plan is to literally make an individual or user believe in what is shown to them, where they fall into it and by themselves are led to act where they expose or reveal important data. Considering the motive that any hacker must attack is very simple to be defined by one word, “Ambitious” because of power they’ve gained over the years as they continue to manipulate a software system. That’s where their dark desire takes over for the fact of them getting wealthier in monetary income and defiant to what they believe is good for themselves which makes them even more selfish individuals. The motive of an attack becomes pleasurable for theses black hat hackers to consider themselves powerful and dominant to take any chances to reveal confidential data where it leads them into the security safe or vault of an institution or from a simple individual account.

Not all hackers have this arise to ambition, but some hackers that are considered white hat are privileged to be known to stop any attack which their desire is to find certain vulnerabilities within a software program and help an institution to protect themselves. This has led us to a new perception which helps us understand the stand viewpoint of a hack cyberwar in general for what hackers are targeting when they try to compromise an account from an individual or an institution. Security must be enforced since the beginning of a software project to make it secure, safe, and reliable before the software program is exposed to public where it gives us security leverage to monitor any future exploits or hack attacks within a security layer in depth. For example, Virtual Private Network (VPN) is logically built for unauthorized intruders to keep a network safe and not able to grant access to a security level of a device or web page which keeps these attacks of ever happening due to the dedication and security that is enforced.

My approach to security practice is considering by what is being built from the software project and what scale size data is being used from a company which will required within the software program. What I learned of security best practices was Triple A and Defense in Depth to always be considered first while a software project is developed. Triple A is considered to be necessary to help authenticate an authorized individual from the institution, authorization to be enforced to determine if they are who they are which needs to be verified and validated within the organization, and accountability is used in the company’s security to investigate when, where, how much, how often, and why an individual is granted permission to the company’s defense in depth layers. Defense in Depth (DiD) must be enforced to protect high confidential information in different sectors of the company which involves personnel of company, the rights to work in a sector, but if they are authorized to work in a sector by the company then our security layer must always protect admission to a certain layer of security even if that individual has access to that security layer to prevent any misbehavior in a software program.

Now for a new software team developer, I will have them understand how to problem solve any vulnerabilities that a software program may have when being developed. Vulnerabilities that they are facing to problem solve can be found where there are exploits in such a program; for example, a buffer overflow or underflow which causes unexpected behavior or unauthorized input to our program. They will learn what is an exploit and how to prepare the security best practices to see for themselves what hackers are looking into when compromising a software program. This example insight can lead a new developer to start keeping first security in mind even before trying to build a plan to develop a new software program. To always keep security layers on point in every stage of the software development and deployment operation lifecycle where it determines more safety, reliability, and assurance for a software system to perform as expected and doing so they’ll value security while meeting application requirements along the way.

One example of this concept that I can reflect on could be SQL injection vulnerability, which has helped me understand to create a data structure and algorithm that can only help to strengthen more the security of constant data that’s passed through. Because it keeps certain characters or integers at a limit range where pointers could be used like in a linked list known data structure; for example, to only allow certain bits of data into an algorithm. In conclusion, this will prevent for an exploit from happening or ever allowing new bugs to appear within the source code being built. Overall, I’ve learned different exploits and vulnerabilities that I can recall and keep my mind to forever think security first, because security protection is our obligation as software engineers to protect personal data of an institution, organization, and personal accounts that could jeopardize their personal identity, wealth income, and even their own dignity.