Aaron Shipley

CS 405

DiD Journal

Southern New Hampshire University

Wasim Alim

9/11/2022

Defense in Depth, DiD, is the Cyber Security practice of arranging multiple lines of defense to protect an asset (YouTube, 2017). Multiple layers of defense can range from software patches and updates, firewalls, anti-virus software, IPS, AES Encryption / Decryption and secure coding standards and practices implemented by software engineers and developers. DiD helps provide multiple layers that provide a type of defense against attacks or vulnerabilities in their own respective manner. These vulnerabilities do not line up with other layers, making an attack much harder when all layers are implemented properly.

But how much is too much? With new forms of attacks and vulnerability exposures happening at a rapid pace, one must ensure they have implemented the proper number of layers in order to protect their system or network adequately. The addition of layers can cross a line of too much. How does one decide when it is too much? There is no set pattern or blueprint as to how many layers are enough before crossing the line to too many. This will be based on the user’s needs of the system or network, and the potential for attack. When layers add up to create an unreasonable time loss for the user, too many layers have been implemented. For example, a banking app must be secure in all aspects of protecting their user’s sensitive data due to the financial ramifications of an attack on a banking app. Multiple layers will need to be put in place to protect users, such as secure encryption / decryption methods, firewalls, secure coding practices, etc. The bank could look to protect this data even more by requiring the user to sign in for every page on the app, but this would be time consuming, frustrating for the user, and overkill if the proper layers are be utilized correctly from the initial implementation. This is just one example of finding the proper tradeoffs between ultimate security and practical use of a system or network.

In terms of developing secure systems, money is always at the forefront of decisions being made. As businesses are tasked with developing new systems, budgetary concerns can alter the way developers utilize DiD in a system. By having a limit of money for a system, some areas will ultimately need altering to make it fit within the financial constraints set forth. Looking at the example above, implementing additional layers of encryption and decryption will protect the system even more, but it is not feasible financially for a system to do so. This would be an area that would be cut to meet financial goals. Training and implementation of secure coding standards is always a factor in DiD. Even with an endless budget, developers who are not properly trained in secure coding standards and practices that are up-to-date and recognized as effective will still compromise a system. By having personnel properly trained, a system may be more secure due to the implementation of layers, and not so much the number of layers. Quantity can be overruled by quality in this matter.

Like a snowflake, each system is unique in its own way. DiD will be unique to each system as well. Depending on multiple factors, DiD will be implemented to secure the system while providing a practical, and usable system for the user. Some factors that may be considered when deciding the layers to implement to a system will be the data types that will need to be protected, physical location of where the data will be stored, training of the development team, requirements the stakeholders have brought forth for the developers to implement into the system, likelihood of attack on the particular system. When determining the likelihood of attack, one should weight on the side of caution and assume the system is highly likely to be attacked and think of as many potential scenarios where an attack might occur. This process goes hand in hand with the proper training aspect of DiD. By having well-trained developers, more scenarios may be brought forth to help ensure the system is as secure as possible against these scenarios.

References

CISA. (2021). *Defense in depth*. CISA. Retrieved September 11, 2022, from https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/defense-in-depth

G. Yendamury and N. Mohankumar, "Defense in Depth approach on AES Cryptographic Decryption core to Enhance Reliability," *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2021, pp. 1-7, doi: 10.1109/IEMTRONICS52119.2021.9422567.

YouTube. (2017). *Cyber Security Minute: How does defense in depth work?* *YouTube*. Retrieved September 11, 2022, from https://www.youtube.com/watch?v=lnIRqw0jutA.