Brian Engel

Module 2 Journal: Defense in Depth

**How deep is too deep, and what’s the tradeoff?**

How deep is too deep really depends on a few aspects. One is the tradeoff between security and performance. As security increases, performance will decrease because security measures use resources for things like encryption. Another aspect to consider with Defense in Depth is as the complexity of the defense increases, it becomes harder to manage and maintain. The last aspect that really sticks out is diminishing returns on the investment. As more layers are added, the probability that a problem will reach that level decreases, but the cost is always going to be present. For something that needs to be as secure as possible, like medical, financial, and defense applications, the cost is worth it. However, for simpler applications, there is probably a point where it isn’t worth the added security. Figuring out how many layers you need really depends on all these factors.

**What are some time, money, reputation, and operational considerations?**

The more layers of defense you have the longer it takes to update and patch security. Monitoring requires more time as well. Money is always a consideration for Defense in Depth. Every layer you add costs more money and probably won’t catch as much as higher layers. The level of security is directly influenced by the amount of money you can spend on it, with diminishing returns. Reputation is another huge consideration for security. By not having sufficient security and getting attacked and having a data breech of sensitive data or worse having sensitive equipment fail can severely damage a business's reputation. It can also cause accidents, lawsuits, fines and other monetary punishments that are much more costly than having the proper security in the first place. For operational considerations, security should keep bad actors out while letting authorized individuals proceed with what they need to do. It should also not hinder the functionality of the application it is protecting by using more than what is absolutely needed in resources.

**What are some additional aspects of DiD that make it unique for each situation?**

The thing I like about the concept of Defense in Depth is it is not a one size fits all solution. You add layers of defense until the application is as secure as you need it, you run out of funding, or it starts affecting performance. It also makes sense for applications that require special layers for complying with certain requirements such as regulatory requirements. Defense in Depth also allows for additional layers to be added at a latter time, as new vulnerabilities are discovered or additional funding is made available.