Hanah Deering

2-1 Journal: Defense in Depth(DiD)

CS 405 Secure Coding

Southern New Hampshire University

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

Defense in Depth, or more commonly known as DiD is a type of cyber security where several layers of security controls that are independent of each other are used to protect valuable data and information. Several layers are used just in case one layer fails; another one will be operative as a backup so that there is a constant layer of security. With the revolutionized digital world, we work and play in, security must be a top priority. These layers can be described as but aren’t limited to firewalls, malware scanners, intrusion detection systems, and data encryption. A great analogy to describe DiD is a castle. There isn’t just a big front metal door protecting intruders, there is a bridge, a moat, castle walls, soldiers, and potentially anti-siege equipment. One single layer of security will never be able to protect fully against any hackers/intruders. But when using the many different layers of DiD combine, you can close and exposed gaps rather than relying on a singular security solution. But there is tradeoff here. There have been many examples I can think of where I enabled a security feature on both my work and personal computer, that later prevented me from opening simple applications such as Microsoft Word due to potential security concerns. The main trade off is security exposures/user’s defense for computer freedom or operations.

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

As we all know, developing programs takes time and money. But what we never really think about is the amount of time, money, and reputation that can be lost when a security breach happens. All the above (time, money, and reputation) can be compromised due to a successful attack. The time alone spent repairing any breaches and fixing any security vulnerabilities, can be detrimental to the success and reputation of a company. It is easy to lose consumers or users when there are poor computer security systems in place. We can also take into consideration operational functions of a company when it comes to the potential impact of a security breach. Daily operations can come to an abrupt halt until the company fixes the damages or exposures. This means a potential loss of profit.

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

Additional aspects that make it unique for each situation are the number of options we have for the types of security layers. These layers can come in many different forms but aren’t limited to the following:

1. Firewalls
2. Malware Scanners
3. Password/Password Encryption
4. 2-Factor Authentication
5. Intrusion Detection
6. Network Security
7. Data Encryption