**2-1 Journal: Defense in Depth (DiD)**

Chris Bridges

Southern New Hampshire University

CS 405: Secure Coding

Professor Mill

13 September 2025

Defense in depth is the concept of creating multiple layers of security where overlaps in coverage can mitigate the risks of attacks or vulnerabilities. Effective use of defense in depth can create a secure environment without unnecessary confusion or complexities, which can be counterproductive. An example would be a login process that requires a username, password, and 2 factor text message authentication. This is effective enough to prevent unauthorized access, but adding another layer, like a USB physical key or a card reader, adds unnecessary complexity and potential complications to logging in. Effective defense in depth techniques create effective security without adding the potential for additional vulnerabilities. Layers of depth should be adjusted based on the sensitivity of the information as well.

Time, money, reputation, and operational considerations are important when discussing defense in depth. Every additional layer of security requires resources like time or personnel for setup, training, monitoring, and implementation. Additional layers could have a financial cost as well. Some tools may require additional hardware, licenses, or employees to implement the heightened security. The reputation of companies can change depending on their defense-in-depth protocols as well. More secure products can gain customer trust and approval, but overengineering security could result in a product that is difficult to use, problematic, or time-consuming. Operational considerations are required for defense in depth. Controls that restrict productivity or delay competitiveness can be just as harmful as an actual attack.

Various aspects of defense in depth can be implemented to suit the customer’s requirements. Hospitals may use physical security badges to access patient data in an environment where quick and efficient access is preferred over other methods, like text message 2-factor authentication and login. Banking institutions use defense in depth on purchases by looking at previous geographic data and spending habits to block unauthorized transactions. Layers of security can vary depending on the customer, their requirements, and how much security is needed in their situation.