Daoud Sogoba

CS-405: Secure Coding

Professor Trevor Hodde

October 26, 2021

Defense in depth is a methodology by which institutions can protect physical objects, software, personnel, and other such things using layered redundant security systems. It allows institutions to limit the risks associated with the use of security systems that cohabitate but do not actively work together. The common threads of focus for institutions wishing to employ the defense in depth methodology on their systems are projections of cost for the implementation of systems, the time and training requirements for the implementation of those systems, as well as the effects on the user experience while using the institutions product. Take for example a company whose primary value is providing users with access to cloud-based storage solutions. An institution whose encryption technology is applied in many layers to the user data may find that that accessibility speed may not be suitable for end user support and retention. In other words, these systems may prevent the users from readily accessing their data which is the primary reason for their subscription to the service. Elise circumstances the institution may deem that their defense in depth is too deep.

One of the primary ways that defense in-depth can implement various solutions for security often revolves around the thing being protected. If end users would like to store, a family heirloom aim a safety deposit box. A bank can be expected to provide defense in depth using largely physical but also software-based measures. These may include but are not limited to luxate blocks, cages within the vault, reinforced volts, cameras, and security guards.