CSS337: Secure Systems
Assignment 1: Secure Design Principles
NOTE: Be detailed in your answers

1. From the list of security design principles discussed in class, choose one that you have familiarity with either through your own experience or from an example you have read about. Give a positive example where the security principle was adhered to in order to improve or maintain security and a negative example where the failure to implement a security design principle resulted in a security incident. (you can choose different principles for positive and negative examples)

I want to talk about the Least Privilege Principle in the list of security design principles. For Cloud APIs and services, they generate the least privilege principles in functions. Granting the service account only the most minimal set of IAM permissions required to execute the function. Set IAM policies on each function to enforce that only certain users, functions, or services can invoke the function. For failure in the least privilege principle, when people of marginalized identities fail, we represent our entire communities. If multiple users have the root access right, when one account get successfully attacked, attackers can use this account to steal and change important data. As an example, in restaurant accounts, when employees are generate the manager accounts, they can cancel any orders they have and get cash from customers or stealing money from restaurants by changing the sales data. When restaurants find out the money lost, it is hard to aim the suspects as every employee may have the ability in doing so. If only manager has the right for deleting orders and employees all have creating orders, then when find out money lost, restaurants only need to focus on managers accounts operation records.

2. In your own words describe what is meant by “defense-in-depth” in security design. Give an example of a combination of security controls that you have seen implemented (or read) that show how the combination of security factors improve the overall security.

Defense in depth is the best practice in protecting the valuable data and information security with layered mechanisms. If one mechanism fails, other steps immediately protecting from the attack. For banks accounts, banks have different layers of protection for money transfers. For perimeter detection, monitors whether an attempt to access an account on a particular device is consistent with previous behavior. For transaction Initiation, uses behavioral profiling to determine whether the type of transaction is consistent with precious transactions, or consistent with the behavior of a peer customer or business. For transaction authentication, uses multifactor authentication and identification like fingerprint authentication or facial authentication. Non-transactional data is used to authorize a transaction at this stage and financial crime platforms use predictive modelling based on outcomes of previous investigations to flag whether a transaction is potentially fraudulent. Bank app also detect and update regularly.