Module Eight: Portfolio Reflection

At the planning phase of development cycle, defense in depth is a very crucial part of our security tools mechanism since we will have multiple layers that act accordingly depends on the threat level of attacks. Besides that, proper use of coding standard implementation that adhere to CERT C++/C is also minimizing the security risk

With zero trust model similar to triple A implementation for authentication to identify user identity, authorization to confirm privilege, and accounting to monitor activities for the purpose of protection against security breaches with intrusions of internal or external attacks.

Implement security policy as we go is the best way to suppress the security threat level throughout the software development cycle. Leave the implementation of security to the end may ease the testing stage at first, but deployment and monitor stage will take a severe hit of loophole and vulnerabilities that can affect program performance and security issue

With network infrastructure, data encryption is also an important part of protecting sensitive data from malicious attacks. Such use cases for data at rest, in flight and in use. For data in flight and in use, using the correct protocols to encrypt the transmit and receive will avoid man in the middle attacks, whereas, key can be verified between sender and receiver in order to decrypt the data.