Security Principles

- **Principle of Least Privilege** - It expresses the idea that each part within a system should only be granted the lowest possible privileges needed to achieve its task. Whether referring to users on a machine or lines of code in a program, correctly adhering to this discipline can greatly narrow the attack surface.

- **Zero Trust** - It is a security model takes the Principle of Least Privilege and carries it to its ultimate conclusion. This model advocates for removing all implicit trust in networks and has a goal of protecting access to resources, often with granular authorization processes for every resource request.

- **Open Security** - It is somewhat counter-intuitive principle, states that the security of a system should not depend on its *secrecy*. In other words, even if an attacker knows exactly how the system's security is implemented, the attacker should still be thwarted. This isn't to say that *nothing* should be secret. Credentials are a clear case where the security of a password depends on its secrecy. However, we'd want our system to be secure *even if* the attacker knows there is a password, and even if they know the cryptographic algorithm behind it.

- **Defensive In Depth** - It advocates for adding defenses to as many layers of a system as possible, so that if one is bypassed, another may still prevent full infiltration. An example of defense in depth outside the context of cybersecurity would be a garage that requires entering an electronic code, using a key on a bolted door lock, and then finally disabling a voice-activated internal alarm system to open the garage.