Introduction

Table of Contents:

Background Noise: Youtube

Key Security Concepts (The Big Three)

> Confidentiality -- Integrity -- Availability

Threat Model Design

Users: you will need to identify every possible person that might end up interacting with the system and add them as a user type. Then for each user type describe what they are allowed to do and what they cant do.

Assets: this is basically any device, data, hypothetical, physical thing the system owns. From Bob's coffee to his office security camera.

Attackers: remember the assets? now you are tasked to write every worst case scenario imaginable to every one of the assets. And dont forget to name the attack and the attacker.

Security policies: what security policies should be enforced to prevent threats from achieving their goals

Yapping hell AKA: Principles for building secure systems

Principle	Definition
economy of mechanism	Simple Design = Less Vulnerabilities
fail-safe defaults	default system configuration should be as conservative as possible (deny all access, ask questions)
complete mediation	resource access control, who is allowed to touch what, log all actions.
open design	open source is awesome
separation of privileges	no single person or process should have enough privileges to complete a critical operation alone
least privilege	limit privileges as much as possible
least common mechanism	minimizing the amount of shared resources, functions, or mechanisms
psychological accountability	security measures (passwords) should be user-friendly
isolation	make each component of the system independent and isolate users from critical resources
encapsulation	try to hide the implementation and processes of your system, users dont need to know HOW it works
modularity	instead of having a huge system, divide it into small manageable parts
layering	use multiple defense layers, dont rely on just a single one
least astonishment	a program or interface should always respond in a way that is least likely to astonish a user

Kerckhoffs' Principle

1. The system should be secure even when the attacker knows all the internal details.
2. The system should rely only on the security of the KEYS.