Vulnerabilities

A weakness in a system that can be exploited by a threat actor to gain unauthorized access

Memory injection
Inserting Malicious code into a program's memory. The attacker leverages vulnerabilities that allow them to execute arbitrary code.
- Code Injection
- Buffer Overflow
- DLL Injection

Fixed by secure coding practices such as input validation, to find miss configurated inputs use vulnerability scans

Virtualization Vulnerabilities
Virtual machine Escape -> An attacker runs code on a VM which allows them to break out and interact with the host or other VMs
Resource Reuse -> Sensitive data can remain in system resources and be accessed by other processes

API Vulnerability
Insecure Interfaces and APIs -> Cloud Services are accessed through interfaces and APIs, which, if not properly secured, can be exploited

Mobile Vulnerabilities
- Jailbreaking -> Process of removing software restrictions imposed by the OS (get the root of the phone)