## It is a commonly known fact that hackers have been using Man in the Middle Attacks (MiTM) over computer networks since years to intercept communication between a sender and a receiver. However, what is mostly unknown is that MiTM attacks can and do exist on mobile devices as well. In fact, mobile applications are vulnerable to Man in the Middle attacks in particular. MiTM is also often referred to as a malicious proxy.

## 

## **What does a Proxy Do?**

A proxy is designed to intercept a sender’s request to a receiver. It works in three steps:

* Proxy makes a request on sender’s behalf to the receiver.
* Receiver responds to the proxy
* The proxy sends the information to sender.

Malicious proxies or MiTM attacks work in a similar way. They can intercept, send, modify, and receive data without any of the communicating parties knowing about it. These attacks also work on mobile devices in a similar fashion.

**Mobile Applications and MiTM Attacks**

MiTM attacks on mobile devices also exploit the same vulnerabilities as on traditional devices. If an MiTM attack attempt turns successful, it is mostly because of improper validation of certificates and insecure protocols such as SSL and early TLS versions.

***Certificate Pinning - Preventing the Attacks***

For mobile apps to prevent such attacks from occurring, we need to first see how authentication is carried out by these apps. An effective way, other than mobile app security testing, for preventing MiTM attacks from occurring is Certificate Pinning. This ensures that the particular mobile is communicating with its intended sender. In simple words, certificate pinning allows the mobile device to link certificate to the receivers host name. This can be done when the mobile app is functioning at times where pinning relationships are part of the application development.

Most important of all, you need to pin the certificate to the server’s hostname and validate that the certificate came from a legal root authority. Every control needs to be built into your mobile app. Also, all these controls should be built into the mobile app.