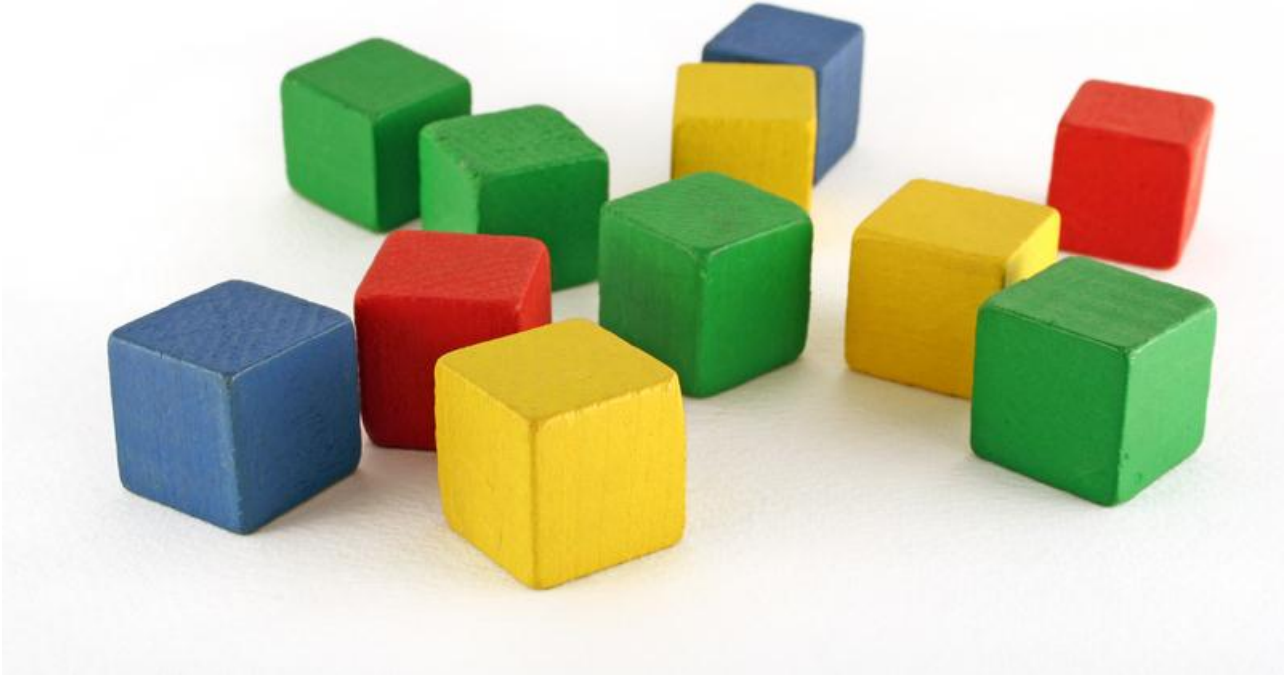
Security Compass

Mobile App Pen Testing

How to proxy the device?



Proxy the Device

iOS

- Emulator
  - Works on HTTP Proxy settings of OSX
  - For SSL add proxy cert to OSX's trusted cert store
- Device
  - Settings on device has a native HTTP Proxy setting for WiFi networks! ☺
  - For SSL add cert to iOS trusted store by opening cert in Safari

Android

- Emulator
  - "http-proxy" flag when running AVD works only with browser. Hit or miss! ☹
  - Tsocks is a better option on Linux boxes
  - For SSL MiTM add proxy cert to /system/etc/security/cacerts.bks
- Device
  - Rooted with Cyanogen ROM (iptables support)
  - Autoproxy tool adds GUI to iptables
  - Same solution as emulator for SSL MiTM

Blackberry

- Device
  - No native proxy support. ☹
  - WiFi MiTM with proxy support on Linux
  - Will not connect to Ad-hoc AP.
  - Easiest solution: use Pineapple WiFi router ()
  - Apps provide a dialog box to accept bad SSL certs. So SSL MiTM for pentesting is easier.