ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Mobile Device Penetration Testing

An ever increasing number of people own mobile devices, ranging from iPhone and iPads, through Android and Windows Mobile devices. Through 3G, 4G and Wireless networks, users are able to get online and interact with apps, music and video in just the same way that they would have from a conventional computer or laptop.

Apple have sold more than 110 million iPhones and more than 25 million iPads to date. Similarly Google has activated more than 100 million Android devices since they were released in 2008. One of the reasons the devices have been so popular is due to their ability to download applications from the Apple App Store and Android Market which in 2011 contained more than 900,000 third party applications between them.

The programming language used to develop many iPhone and iPad applications is Objective C, whereas the Android platform is Linux based and uses Java. Both Apple iOS and Android are effectively miniature computers, and consequently the applications that run on them are similar to conventional thick clients or web based applications.

Many of the mobile applications use web based functions which open them up to Cross Site Scripting (XSS), Cross Site Forgery (CSRF) and session hijacking attacks. These attacks are being mutated on mobile applications to capture user displays, keystrokes and to perform tapjacking, (similar to clickjacking) and screen smudging attacks. Similarly, iOS can be susceptible to buffer overflow attacks, and attackers can decompile code to identify security flaws and weaknesses.

The vetting of applications to ensure that they are not malicious has not proven to be effective, with documented instances of applications that could potentially introduce security risks being regularly identified in both the Google Play and Apple App Store. Both vendors have implemented more stringent checks on applications but this cannot completely remove the risk that this presents to end-users and enterprises. In particular Apples content protection and revenue model has resulted in many end-users “jail-breaking” their phones in order to run unapproved applications, this also exposes the IPhone to malicious applications and other security hazards.

ASM has broad experience in security testing mobile devices. Whether it is a phone or tablet based resource, ASM’s security consultants have a solid foundation in identifying security flaws in both device operating systems and applications, as well as helping organizations develop secure applications through the implementation of SDLC (Secure Development LifeCycle) methodologies.