Mobile Application Security Review - Checklist

Platform	Check	Description	Status
Data Protection			
All	Local storage	Look for files and directories under the application directory to check for any sensitive information	
iOS	plist files	Look at the plist file to check for any sensitive information	
All	Check Keyboard cache	Monitor keyboard cache file	
iOS	Check snapshots	Browse application, press home button before checking this	
All	Check ClipBoard	Verify clipboard file for any changes	
All	Check SQLite Database file	Look for SQL files (Usual extensions are either .sqlite or .db or .sqlitedb)	
All	Log Files	Check crash reports, application log files and device log files to check for sensitive information stored in log files	
All	SQL Injection against local DB file	Check database log files to see types of queries used in the application.	
Android	Check "debuggable" flag in manifest file	Check debuggable flag is true/false	
Session Management			
iOS	Cookie.binarycookies file	Extract cookies from cookies.binarycookies file to verify what application is storing in cookie	
iOS	Extract data from keychain file	Use keychain dumper to extract keys from the keychain to verify what application is stored in keychain file	
Privacy			
iOS	Does application run in the background	Check info.plist for "application does not run in background flag"	
iOS	Information in PUSH calls	Check what information is sent in Push calls	
iOS	Does application gather personal information	Check whether the application gathers UDID or location tracking	
Android	Does application gather personal information	Look for usage of "Build" class in the application	
iOS	Check for third party call	Look for a pattern in the binary to see if an application is making any third party calls	
All	Remembering information in	Check sensitive fields to check whether	

	sensitive fields	autocompletion and remember values options are enabled/disabled	
Reverse engineering			
iOS	Is binary encrypted	Use otool to check whether files are encrypted	
iOS	Run binary in gdb to check for sensitive calls	Run binary in debugger to check any unsafe API calls	
Android	Decompile binary	Decompile binary and look for any unsafe API calls	
Network Connection			
All	Check network connection from the application	Check what type of connections is made from the application	
All	Check SSL handling	Check how the application is handling SSL certificate	
Client Side web exploitation			
All	WebView control	Check whether the application uses webView control	
Logging			
All	Check what information applications logs		