Mobile Application Security Framework

Pawan Kumar Yadav
Practice Leader - Enterprise Mobile Solutions

and

Rajneesh Mishra
Mobile Application Architect - Enterprise Mobility

SDG

[technology + passion] – risk

Overview

Enterprise Mobility is rapidly expanding opportunities for companies to enhance clients' engagement levels and simplify and improve their interactions. Unfortunately, those opportunities also create significant security threats for businesses and consumers.

The result is that dynamic threat detection and protection are now fundamental to mobile application security. These measures must assess threats dynamically at the point of access, rather than relying on a more traditional implementation in the infrastructure, on the device, or in the network. In other words, in the new mobile era, trust must be established dynamically rather than based on statically determined factors.

"At least 80% of mobile apps have security and privacy issues that put enterprises at risk."

IT Best Practices Alert,
Network World, February 2013

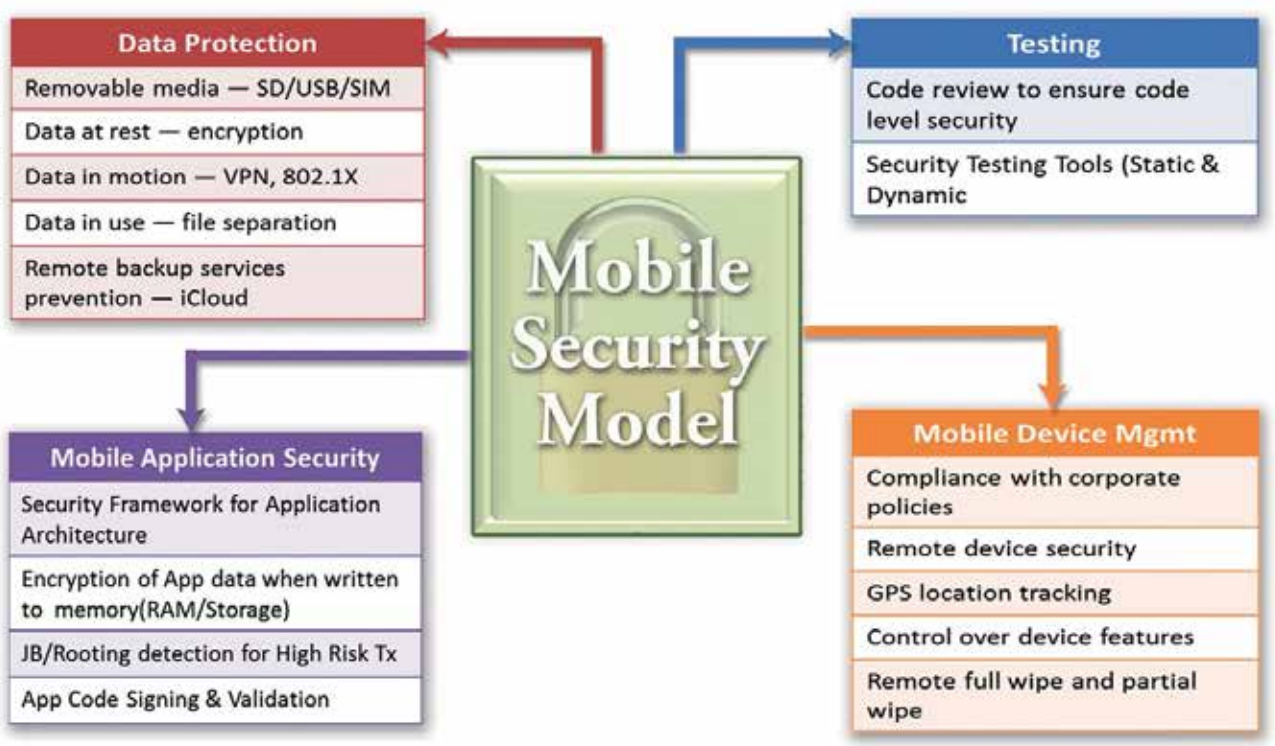
A successful mobile security framework considers new threat models around mobile devices, and then leverages emerging technologies such as device fingerprinting, OS reputation, jailbreak detection, and location with augmented reality (AR) to help determine threat levels and allow or restrict transactions based on risk profiling.

Unique Challenges with Mobile

- ***Portability.*** *Mobile device portability devices make it difficult to secure network boundaries and create the need to secure multiple cloud data access channels.*
- ***Geo-fencing maturity.*** *A technology that secures mobile devices by creating a "virtual fence" or secure radius based on location. This can be used in several ways to generate notification or restricting TX based on fencing parameters. Additionally, there is some question as to this technology's maturity.*
- ***Loss or theft.*** *Mobile devices are at higher risk of theft and are easy to misplace or lose.*
- ***Resistance to password requirements.*** *Mobile users prize convenience and are more likely to be irritated by the need to create strong passwords to secure their devices.*
- ***Encryption challenges.*** *It can be difficult to encrypt or remember to encrypt removable media such as SD cards.*

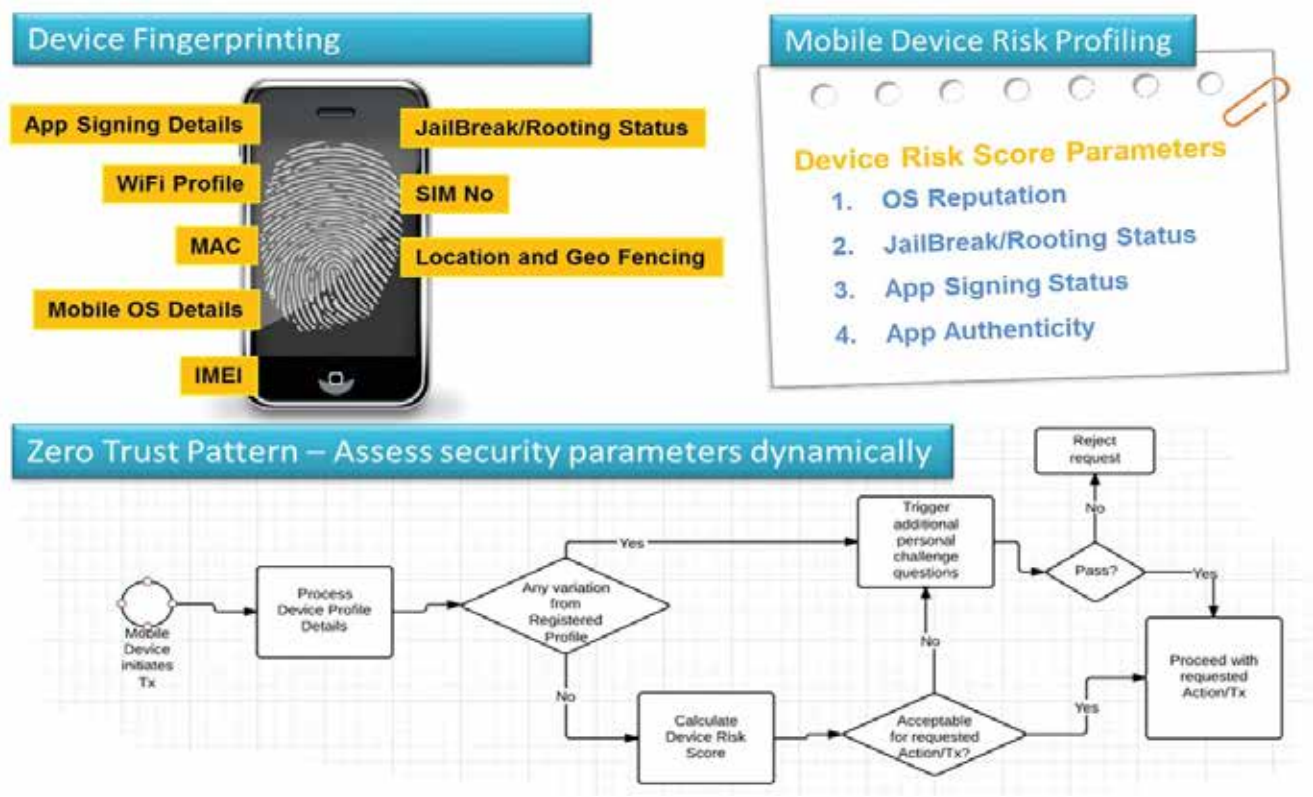
Mobile Application Security

The trend toward mobile device open platform functionality is expected to continue and increase. With this openness comes the potential for unrestricted access to mobile resources and APIs by unknown or untrusted applications, which could harm the user, the device, the network—or all of the above—if access is not managed by suitable security architectures and network precautions. The mobile security model below covers various application security risk aspects and provides guidelines to eliminate them.



Zero Trust Pattern

A zero trust pattern assesses security parameters dynamically and determines risk based on any variance from a registered profile. It triggers a second level of authentication to fulfill transactions if it detects any mismatch in the profile. If the profile does not match, it then calculates a risk score and blocks access or triggers a second level of authentication if the score is less than a predefined safe limit.



Device Fingerprinting

Device fingerprinting is the process of checking unique characteristics to authenticate a device. Some of these identifiers are:

- ***MAC address.*** *A media access control (MAC) address is a unique identifier assigned to network interfaces for communications on the physical network segment. It returns a value that can be used to add the device to a user's safe device list.*
- ***Operating System details.*** *The name and version of a device's OS can also be used to help create a unique fingerprint.*
- ***Wi-Fi Profile.*** *Wi-Fi profile is the collection of properties collected from a device's active Wi-Fi connection. The application is coded to trigger a second level of authentication if the system detects any change.*
- ***Location.*** *GPS capabilities can determine the current user location.*

In addition to this basic information, other variables are analyzed: cookies, language, and remote control of device, wireless application protocols, and associations to other devices with histories of fraudulent activity. By examining all these different layers within a device, digital fingerprinting establishes and maintains a distinct device ID—even when fraudsters try to modify system settings to disguise their true identities.

Mobile Device Risk Profiling

Risk-based authentication is a method of applying varying levels of stringency to authentication processes. It takes into account the profile of the agent requesting system access to determine the risk profile associated with a transaction. The risk profile includes various device attributes and triggers a second level of authentication to fulfill the high-risk transactions.

- ***OS Reputation.*** *OS reputation is based on OS name, version, and vulnerabilities. A mapping is created based on vulnerabilities such as built-in security, application security, data protection, security certificates, etc. in the mobile OS. Mapping assigns a score which is used to block the transaction if the score is less than the predefined safe limit.*

- ***Jail broken/Rooted Status.*** *Jailbreaking is a process of removing the limitations on devices running the proprietary mobile OS through the use of software and hardware exploits. Jailbreaking permits root access to the device, allowing the download of additional applications, extensions, and themes that are unavailable through the official App Store. The system can leverage the device's rooting or jailbreaking status to allow or block high-risk transactions.*

- ***App Signing Status.*** *Application signing creates a digital wrapper that confirms that the code has not been modified since the signature was applied. It also allows app stores to control the testing and approval process before the application is published publicly. Verification of code signing status helps determine whether or not a transaction should be entertained.*

- ***App Authenticity.*** *The unique internal name provided to an application can help determine the authenticity of a transaction. The application compares the bundle ID to a predetermined definition, and entertains the transaction only if there is a match.*

Transaction Risk Profile		
Transaction ID	**Description**	**Risk**
1	View A/C Details	LOW
2	Funds Transfer	HIGH
3	Order Statement	LOW
4	Order Check Book	MEDIUM
5	Update Contact	HIGH

Device Risk Profile				
Mobile OS	**App Sign Status**	**App Authenticity**	**Jail-Broken**	**Risk**
Android	Y	Y	N	LOW
Android	N	N	Y	HIGH
Android	Y	N	Y	HIGH
iOS	Y	N	Y	HIGH
iOS	Y	Y	N	LOW

Treat Model - Actions			
Transaction ID	**Transaction Risk Score**	**Device Risk Score**	**Action**
1	LOW	LOW	Allowed
2	HIGH	HIGH	Reject
3	LOW	HIGH	Conditional Allow
4	MEDIUM	LOW	Conditional Allow
5	HIGH	MEDIUM	Reject

About SDG

SDG is a leading provider of technology, consulting and risk management solutions to strengthen enterprise businesses while managing IT risk.

A combination of technology, thought leadership and a relentless passion for customer success defines SDG's approach to partnering with enterprise brands, but with the added ingredient of specifically focusing on mitigating IT risk with every client engagement.

"SDG helps enterprises realize their dreams by helping them develop, manage and deploy solutions with acceptable risk."

Whether it is strategic advisory, design, implementation or managed support, SDG is focused around six practices: Risk and Security; Identity and Access Governance; Collaboration; Quality Assurance and Validation; Mobility; Cloud and CRM.

SDG helps enterprises realize their dreams by helping them develop, manage and deploy solutions with acceptable risk. We help enterprises realize the opportunity of technology, increase innovation, improve speed-to-market and maximize returns on investment to shareholders.

With more than 20 years of experience partnering with global brands on complex business and IT challenges, SDG is the perfect choice for enterprises in need of strategic support and technology solutions. SDG is passionate about finding the right solution to help your organization compete effectively.