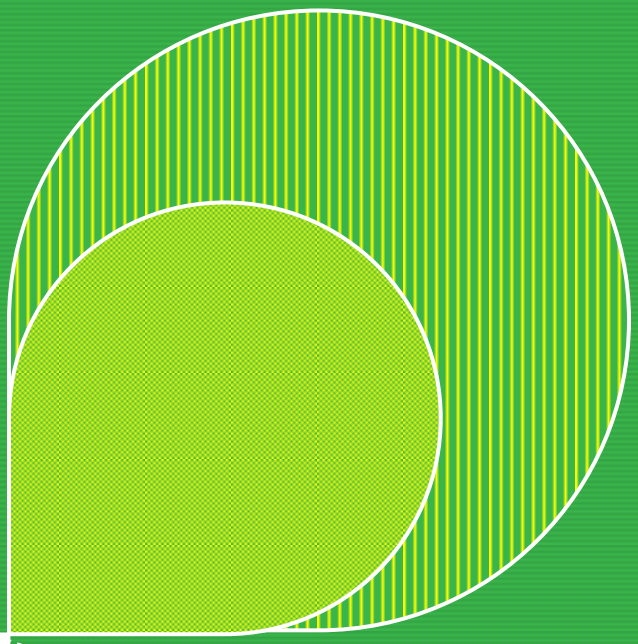
March 2014, HAPPIEST MINDS TECHNOLOGIES

Elevation of Mobile Security Risks in the Enterprise Threat Landscape

Author
Khaleel Syed



Copyright Information

Elevation of Mobile Security Risks in the Enterprise Threat Landscape

Enterprises are rapidly adopting innovative mobile applications to transform their business capabilities as the mobile presence is critical for businesses to attract, retain and communicate with customers; it has become an integral part at both work and in their personal lives.

The newer mobile computing technologies are increasingly embraced by the consumers across the globe, and this exponential growth of mobile devices and business applications has attracted a large number of well-organized cyber criminals and independent hackers, who are seeking monetary benefits with highly competent modus operandi.

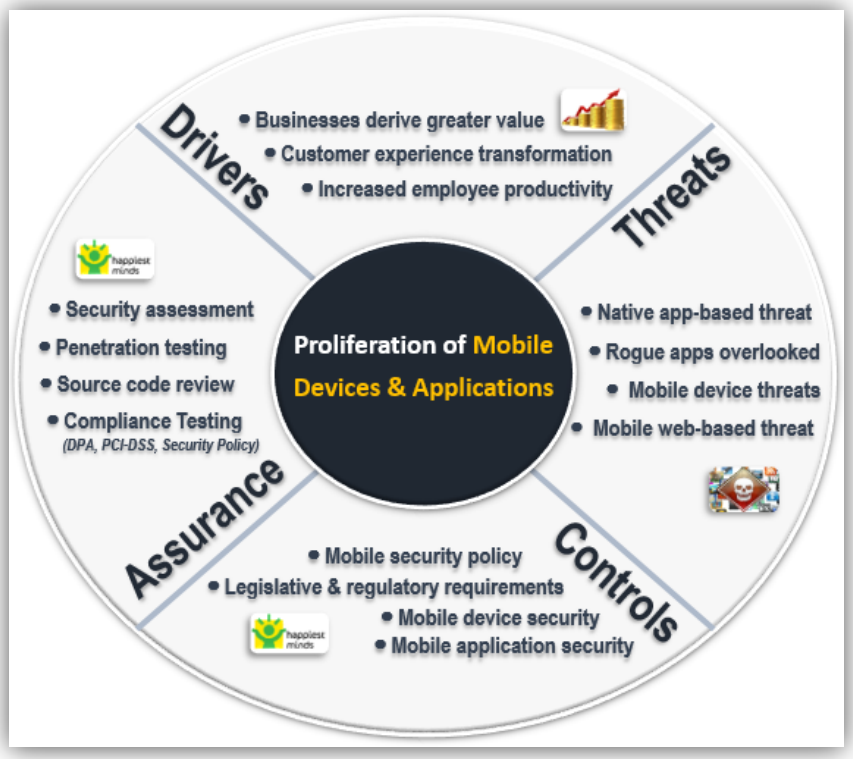
Business Drivers

Prevalence of mobile devices and applications in today's market has been entirely recognized by many corporates and is subsequently being leveraged to boost the sales and marketing initiatives for new businesses through innovative enterprise mobile apps with enhanced functionalities.

Transformational customer experience with access to exclusive content and wide range of personalized services available anytime and anywhere has been powered by customer-facing mobile apps.

Organizations are rapidly adopting enterprise-class internal mobile apps for several business functions to drive greater efficiencies.

A perspective of Happiest Minds on the proliferation of mobile devices & applications



All customer-facing or enterprise internal apps are developed as either native apps, mobile web apps or hybrid apps:

Mobile Native Apps are platform specific installable apps that can be downloaded from internal app bank for corporate use and available at online mobile app stores for personal use. The native apps take full advantage of the mobile device features such as contacts and location details; and are designed to work in both online and offline modes.

Mobile Web Apps are platform independent, non-installable apps that are same as web applications, which are accessed by a browser and are typically written in HTML5, and designed to work in both online and offline modes.

Hybrid Apps are a combination of native and mobile web apps, with the browser embedded within the native app.

An indicative list of categories of professional-grade apps

The continuous advancements in mobile technologies have disrupted every industry across all regions in the past five years and continue to break its own records year after year.

The categories of professional-grade mobile applications have greatly expanded with real-time updates to the consumers, which is led by Messaging & Social followed by Securities & Utilities, Work & Organizing, Productivity, Education, Finance, Entertainment & Media, Lifestyle & Shopping, Games & Sports, Health & Fitness and News& Magazines.

Mobile Threats

Mobile security threat landscape is a growing concern, as we witness the emerging trend of financial transactions using M-Commerce and M-Banking applications on mobile devices. Broadly, these mobile security threats can be categorized under the native app-based threats, mobile web-based threats and mobile device-based threats.

Mobile device-based threats

Rogue applications downloaded from untrusted sources and installation of unapproved applications that expose the mobile devices to all kinds of cyber-attacks and dangers. The inability to detect and prevent the use of jail-broken or rooted devices in corporate environments increases the threat landscape particularly when enterprises deploy the security infrastructures within the corporate intranet to control the mobile device connection but not in de-militarized zone or secured perimeter network. Alongside, improper policy enforcement by the mobile security products can lead to unexpected security vulnerabilities in the production environment.

Mobile security threat categories

Native application-based threats

Installable native applications can be downloaded from several trusted or untrusted sources, where the threats can be broadly categorized under **(1) vulnerable mobile applications** that may have code flaws or tampered applications for fraudulent purposes; **(2)malicious software or malware** that performs undesirable actions or provides a backdoor to the attacker; **(3) data privacy threats** where a legitimate application or spywares gathers user's sensitive information to perform identity theft or financial fraud.

Mobile web-based threats

Not all the corporates create native applications considering the associated security risks, but would prefer to deliver the online services via web-based applications where the web-based threats such as browser exploits, drive-by downloads, cookie stealing, phishing scams and many more are applicable to the mobile devices.

Security Controls

As mobile devices and enterprise-grade applications continue to pervade the workplace, the corporate information security and privacy office is exploring and continuously researching on new mobile security solutions to safely deliver and manage the applications and services that employees need to conduct business.

Enterprise mobile security risks have elevated from the device level issues to mobile apps and business data that is processed, exchanged and stored on the mobile device. Hence, protecting the mobile devices, applications and corporate data in a robust threat landscape must adopt a multi-layered security approach.

Corporates dealing with mobile-based financial transactions must define a customized security policy for the mobile users, which should address all the applicable regulations and legislative requirements for payment security and data privacy.

Device vendors and security software vendors offer a wide range of IT controls for securing mobile devices and applications. Basic security settings provide by the iOS, Android and Windows phone operating systems control the device access, avoid untrusted source for apps download, verify harmful apps prior installation and phone encryption.

Security measures for mobile devices & applications

The advanced security solutions delivered by product vendors offers more sophisticated security capabilities such as detection of malicious apps recently discovered, the native apps lock to control access to other installed apps, the safe browsing to warn or protect from the malicious websites against phishing and the anti-theft feature to remotely locate, lock down and wipe the stolen device.

In addition, the antivirus on-demand scans of all installed apps and memory card content, as well as on-access scans of apps upon first execution, helps corporates protect against viruses, malware, adware, and spywares. The privacy scans that assess the access rights and intents of installed apps enable the organization to identify and manage potential privacy risks. Furthermore, some premium solutions have the ability to track and perform specified actions when the mobile device leaves a set perimeter.

Small and medium-sized enterprises are aggressively adopting the independent mobile security software, but the large corporates prefer to deploy a centralized policy enforcement and management model that includes Mobile Device Management (MDM) and Mobile Application Management (MAM).

Mobile security experts at Happiest Minds Technologies have enabled several corporates across various industry segments to identify and deploy the best suitable centralized solution for Mobile Security Management that helps corporates to standardize the mobile user and device authentication mechanism, integration of Active Directory (AD) infrastructure, manage secured remote access into corporate network for mobile users, control or restrict connectivity to the removable media devices and untrusted wireless networks, mobile device containerization to segregate the user's workspace from personal space to protect the business applications and data from a wide spread of threats.

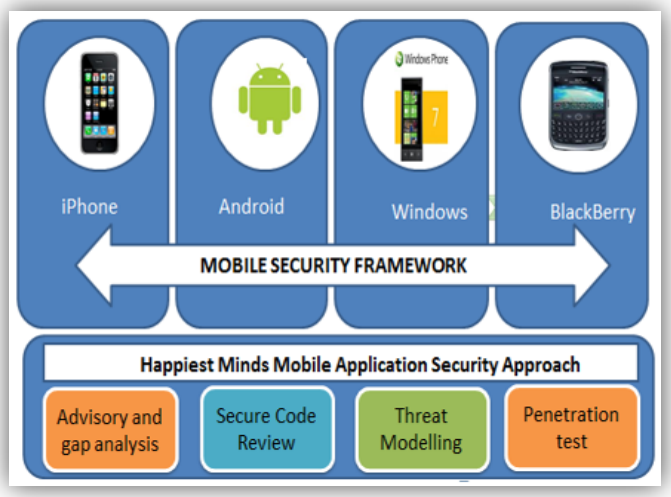
Security Assurance

Permitting the usage of mobile smartphone devices and multi-purpose or mission critical applications in corporate environments by conducting a detailed technical assessment of security controls would enable the stake holders to identify, assess and diligently manage mobile security risks.

Mobile security assessment for device security and application security testing are broadly categorized as;

- *Native mobile application penetration testing*
- *Mobile website penetration testing*
- *Hybrid application & website penetration testing*
- *Native application secure code review*
- *Mobile device security & configuration review*
- *Secure SDLC consulting on threat modeling & coding*.

Mobile Application Security Framework developed by Happiest Minds provides a range of specialized services across all the security assessment types, including security advisory and gap analysis.



Mobile Application Security Framework

Advisory and gap analysis covers review the mobile application artifacts such as security requirements based on asset value and data protection requirements in accordance with the applicable legislative and regulatory requirements. Recommend suitable countermeasures to mitigate the security design flaws and emerging threats for securing Enterprise Mobile Devices with reference to OWASP, CERT, SANS, NIST security standards and guidelines.

Threat modelling for mobile applications involves understanding of the application functionality with entry points in mobile platforms, followed with defining attack vectors to cover all possible scenarios and attack surfaces such as exposed API or RPC, malicious users, third party components and services, mobile storage, web browsing ad content

handlers. Assurance services on threat modeling enables the developers in identifying the most credible threats that have the greatest potential impact to the mobile applications as indicated by industry standards & frameworks.

Secure code review or static code analysis involves code crawling to understand the business logic with possible security vulnerabilities in the mobile native application code and mobile platforms by using automated tools and manual techniques to identify the business logic flaws and code level flaws or vulnerable codes such as insecure use of hybrid technologies, client-side data caching and storage issues, client-side reflection based attacks and incorrectly implemented application encoding and encryption including OWASP Source Code Flaw Categories, CERT, SANS and MSDN Secure Coding Standards.

Penetration testing adopts the hybrid approach of specialized automated tools and manual assessment techniques in mobile application security testing to cover various usage scenarios and all the inherent threats in accordance with industry best practices and mobile security guidelines from applicable legal and regulations for payment security and data privacy. The security assessment team at Happiest Minds conducts both blackbox and graybox testing to ensure a comprehensive coverage of all the attack vectors and scenarios.

Native applications penetration testing covers dynamic analysis with debugging of running applications on simulators, emulators and compatible mobile platforms to perform permission analysis, control flow analysis, dataflow analysis, security configuration, input validation, server side controls, session management, client side injection, authentication and authorization, side channel data leakage, broken cryptography, sensitive information disclosure, data protection, insufficient transport layer protection and exception handling.

Mobile web application penetration testing covers all the security vulnerabilities applicable to the web applications that includes web server with unsafe configuration and software bugs, client-side vulnerabilities, insecure cookie handling, improper session handling, authentication bypass, circumventing application logic, input validation, function level access control, use of vulnerable components, insecure direct object referencing, shared hosting vulnerabilities, improper cryptography implementation and form manipulation.

Mobile device configuration review covers the adequacy of device security and application security policy enforcement that includes use of unapproved applications, access control configuration, crytography implementation, restriction on removable media or wireless connections, mobile device containerization and relevant security settings for device hardedning.

Security compliance testing primarily focuses on payment acceptance mobile applications that meets the security guidelines mandated by PCI Data Security Standard (PCI DSS), Data Privacy Act (DPA) and other applicable regulatory and legislative requirements.These security requirements would prevent the card holder account data from being intercepted when entered into a mobile device, from compromise while processed or stored within the mobile device and from interception upon transmission out of the mobile device.

Conclusion

Mobile security experts at Happiest Minds will help assuage the enterprise mobility concerns by arming you with knowledge of mobile device security threats and how to implement protection measures and leverage mobile devices and applications that will protect the account data in the devices to boost sales. Mobile computing technology will be ruggedized to be unaffected by regimented threats from different sources.