A Layered Approach to Mobile Security

Time-tested best practices for managing security of information systems are being rewritten in the mobile enabled world; distribution of data, applications and devices has brought the focus back to security. The traditional mode of risk containment within the enterprise using perimeter controls is no longer valid, as the perimeter has been broken. Consumerization of IT has changed the IT landscape and IT administrators are now required to support myriad systems with flexibility of choice provided to the end user. Ensuring data and application security within a Secure Enterprise Infrastructure is critical to the success of mobility initiatives. The paper will discuss the threats and risks in a mobile environment and list steps an organization can take to handle mobile security. Various process and technological remediation controls available to the administrator are analyzed before closing with information on certain promising high assurance security measures.
About the Author

Rajmohan, CISSP

Education
MS in Computer Security
MS in IT Management
Naval Postgraduate School, Monterey, CA

Summary of Experience

Colonel Rajmohan has over 20 years of experience in information technology and specializes in Information security. He is a veteran from the Indian Army. He has had an illustrious career within the communications and IT wings of the Army and held senior command appointments. He was the first army officer to be invited to Naval Postgraduate School, CA and graduated with honors. He was awarded the best international student plaque for his outstanding contribution in academics and community work. Subsequently, he pioneered the army secure wide area intranet and was instrumental in setting up the secure data center. He also oversaw the setting up of the cyber security establishment and the security operations center. He has made significant contributions in the area of digital Image watermarking having introduced the concept of content based watermarking and has published in leading journals on the subject.

Rajmohan has been with TCS for two and half years and currently heads the mobile Security group at Tata Consultancy Services. He oversees secure development methodology for mobile applications and reviews security architecture of TCS mobility solutions.
## Table of Contents

1. Abstract 1  
2. Table of Contents 3  
3. Executive Summary 4  
4. Introduction 5  
5. Mobile Security Threats and Challenges 5  
6. Building Security for Mobility 6  
7. Mobile Security Strategy 6  
8. Mobile Security Policy 7  
9. Building a Security and Management Infrastructure to Support Mobility 8  
10. Mobile Application Security 9  
11. Mobile Data Protection 10  
12. Other High Assurance Mobile Security Measures 12  
13. TCS Approach to Mobile Security 13  
14. Conclusion 14  
15. References 14
Executive Summary

Mobility has opened new opportunities for businesses but has also introduced new risks. Employees or customers embracing mobility must not lower the security posture of an organization, mobile apps must protect confidential customer information and organization IP, and loss of devices should not expose organizations, employees or customers to vulnerability in any way. The challenge is to enable productivity without increasing risk.

Mobile device portability and typical usage scenarios have made mobile devices powerful assets that introduce a host of new risks previously unknown to the enterprise IT space. The probability of losing these devices is non-negligible and puts the data and apps on or accessible by them at risk. Use of a common device for personal and official usage introduces privacy concerns. Increased usage of wireless networks and cloud services outside organization control can expose data through network vulnerabilities.

Businesses must consider a layered mobile security strategy wherein risk based security controls are embedded in security policy, infrastructure, applications and data objects. Organizations must extend their security policy and articulate an acceptable mobile usage policy that addresses privacy and confidentiality concerns. Security policy must be supported by a mobile monitoring and management infrastructure to ensure compliance. Based on the maturity of its mobility program and its risk profile, organizations must deploy mobile management solutions. With a central security-monitoring dashboard, a company can enforce security policy and remotely deploy and manage apps securely.

Though some MAM solutions provide secure containers for apps, they cannot be used as an alternative to a robust mobile application security program. Mobile operating systems typically provide a number of built-in security features that applications must use. Organizations must employ a Secure Software Lifecycle Management style and build security into the design of an application and track it through its life cycle. Every mobile app must undergo vulnerability assessment and penetration testing before it goes live.

Organizations run the risk of facing steep penalties in case of a reported loss of personally identifiable information. Data protection is therefore essential and is the last defense against any attack. Data confidentiality is typically achieved by having a clear organization wide data classification policy, a need-to-know based disclosure policy and implementing encryption of data at rest and in motion, as an encrypt-all strategy may neither be feasible nor productive. Organizations must evolve a data protection strategy based on risk assessment and deploy adaptive strong authentication and access control measures to control data access in the first place. This must be complemented with encryption and data loss prevention controls.

Organizations with low-risk appetite could consider some high-assurance mobile security measures that are resilient against man-in-the-middle attacks that target software based systems. Mobile virtual desktop infrastructure (VDI), or always-on VPN, is a solution that provides higher security at the cost of user experience and productivity. Another option is the Trusted Execution Environment (TEE), which is a separate hardware protected execution environment that runs alongside the rich OS and provides...
security services to that rich environment. Higher security assurance typically comes with higher integration costs and reduced usability. TCS recommends a risk-based, cost-effective, holistic mobile security solution with focus on user experience and enhancing customer engagement.

**Introduction**

Enterprises are rapidly adopting mobility due to its immense business benefits and great user experience. Traditional IT and security restrictions imposed on the systems and software that could enter the enterprise networks have been replaced by flexible approaches in the Bring Your Own Devices (BYOD) era. The advent of mobility has brought a paradigm shift in how IT is sourced, managed and monitored. Though there is a universal acceptance of the value of mobility, there is also a universal concern as to how enterprise security will be addressed with the consumerization of IT. The traditional perimeter defense strategy is no longer valid as employees use wireless and provider networks to access enterprise systems. Devices for personal use are also being adopted as the devices of choice for enterprise access. These flexible approaches have introduced privacy and confidentiality concerns for both employees and corporations.

Secure mobility is critical to a successful enterprise-wide rollout. Balanced and compliant security controls need to be in place prior to rollout in order for employees to accept businesses monitoring and controlling security management of their personal devices. The triad of people, process and technology has to complement each other to provide a robust security framework that stays resilient despite mobility.

**Mobile Security Threats and Challenges**

Mobility introduces new risks and threat vectors that hitherto were uncommon. Four major risks are as follows:

- **Loss of devices.** Mobile devices tend to get misplaced and lost. They can be left unattended for brief moments, allowing a person with malicious intent to potentially gain improper access to their applications and data. Enterprises have to plan for such contingencies, as the number of lost devices is typically very high.

- **Traversing insecure Networks.** Employees roaming in and out of the enterprise network typically traverse on insecure WiFi/3G/4G networks outside enterprise control. Traditional network security needs special focus on network and information access controls based on location and type of device used for access.

- **Overlap of personal and official usage of devices.** In a BYOD scenario, a single device is used for both personal and official use. Personal information and business information reside on the same device and intermingling is possible. Maintaining confidentiality of corporate data is critical, but care also needs to be taken not to trespass into users’ privacy. A balance between users’ rights and an enterprise’s right to monitor and manage its data has to be achieved.

- **Cloud based data storage and back up services.** Cloud based storage and backup services outside the enterprise network are increasingly being used to store and back up data from mobile devices; this
is a potential source of data leakage. Strong controls on how data is stored and backed up are therefore required.

**Building Security for Mobility**

Secure rollout of mobility requires risk assessment, formulation of mobile security policy and deploying security controls. Mobility introduces new threat vectors, and an enterprise can broadly classify its mobile security program into five distinct categories as depicted below:

![Figure 1: Enterprise Secure Mobility Rollout Program](image)

**Mobile Security Strategy**

- Security controls make the task of a determined attacker difficult, though not impossible. A good security strategy must therefore employ a defense in depth strategy with a multilayered security envelope. This makes the task of the determined attacker extremely difficult and time consuming. In a worst-case scenario, should the controls be breached, an alert should generate and damage should be contained. A layered security strategy thus provides an acceptable risk posture allowing business to embrace technology.

- Traditional security was built around a strong perimeter. Movement of data across this perimeter crossed specified gateway points that were fortified and monitored round-the-clock. With mobility, the perimeter is less relevant. BYOD has further complicated matters introducing disparate systems and software into the enterprise. Security professionals now have to work around this; new layers of security controls need to be added and more vulnerable layers need to be strengthened.
A security policy fortified with controls for mobility is the first tier in a multi-tiered security architecture for secure mobility. The security policy is complemented by technological controls in the infrastructure, namely Mobile Device Management (MDM) and Mobile application Management (MAM) solutions. These solutions monitor and manage mobile devices and add to the existing security infrastructure. The security policies implemented by MDM and MAM solutions provide an important line of defense but do not reduce the importance of building secure applications; application security and data security provide the final lines of defense against malicious attacks. This is significant in an environment where devices are lost easily and the risk of applications falling into the wrong hands is relatively high.

Mobile Security Policy

Enterprise Mobility Strategy will have an impact on how security controls will need to be prioritized and deployed. The right strategy will ensure an improved user experience without compromising security. Enterprises typically have one of two models of embracing mobility: either “Bring Your Own Device” (BYOD) or “Corporate Owned Personally Enabled” (COPE). A BYOD environment creates a heterogeneous environment and calls for a number of controls to be enabled to ensure that the security posture of the organization is not diluted. In a company provided equipment scenario, the company can manage security in a cost effective manner by smart selection of devices and applications.

The security policy of an organization is the foundation for a secure enterprise. In a mobility scenario, the security policy must be appropriately drafted to incorporate the changes brought about due to mobility. Employees must be unambiguously told of the expected behaviours, monitoring and security management controls that will be put in place as well as how they may be potentially liable in case of security policy violations. Limits to company liability must also be stated and employees must sign up to accept the terms of the policy before being permitted to use their own devices to access business information. The policy will be different between BYOD and COPE environments; some areas of the security policy that will require changes are:

- Policy against Rooting and Jail Breaking
- Data privacy and confidentiality policy
- Remote wipe policy
- Mobile access control measures
- Camera usage policy
- Policy on apps that use GPS within company premises
- Removable media usage policy
- Data access policy (Wi-Fi / 3G / other)
- Loss and replacement of mobile Device
- Termination policy.
The security policy must be comprehensive and comply with any country or state specific regulations. In certain geographies it may not be enough to have the employee sign up on the acceptable use policy but the policy itself must be legally tenable. Rules regarding access to corporate data, geo fencing controls and limitations of use of third party applications in either individual liable devices or corporate liable devices be clearly articulated in the revised security policy of the organization.

Building a Security and Management Infrastructure to Support Mobility

IT infrastructure and operations professionals will require making the infrastructure stronger with MDM or MAM solutions to securely manage mobile devices. These solutions typically support multiple platforms and more importantly extend security policies to both corporate-liable and employee owned mobile devices. According to Forrester’s recent Network and Telecommunications Survey, 31% of firms have implemented a MDM solution and another 42% of firms are interested in doing so4.

Mobile application Management (MAM) solutions typically wrap mobile management capabilities into mobile application store solutions. Some of the MAM solutions provide a ‘Secure’ container for applications to work within and aim to provide security for insecure applications. The encrypted containers sand boxes all the data within it. Some solutions offer policy APIs that can be called from mobile applications to enforce per app policies such as restricting copy-paste or even delete data and applications if permissions are revoked. MAM solutions target application level control on security. In a BYOD environment, controlling only the enterprise applications in relation to the entire device could also provide comfort to employees on their privacy and save the employers from accusation of privacy intrusion and subsequent liabilities. However, from a security perspective, it may be desirable to have a balanced combination of both device level and application level controls.

Some of the key security functionalities that mobile management solutions provide are:

- Jailbreak detection - Rooting on Android or jailbreaking on iOS device provides applications and users unrestricted access to system resources. This also provides means to bypass remote management and IT control. A number of security features available on the mobile OS that protect the applications and data from malicious abuse become dysfunctional in a rooted device. Ability to detect this on a device and deny access to them is a critical functionality of an MDM solution.
- Remote Data wipe - Selectively wipe corporate data from devices that have been reported lost or have fallen into wrong hands.
- Password Policy Enforcement - Enforce strong password or PIN policy for device access.
- VPN / Encryption support for devices which don’t have native OS support.
- Active Sync Device Restriction: Ensure only registered devices gain access to the network and not devices that have gained access through Active Sync.
- Data Loss Prevention Support
- Security policy enforcement (authentication and encryption requirements, device lock, selectively disable device functionalities such as camera and GPS)
- Device backup and recovery.
Central dashboard for IT and security administrators with inventory reports, admin alerts, real time monitoring, logging, and help desk support.

Application management- remote delivery of applications patches and updates ensuring integrity of applications and only authorized access to selected applications.

**Mobile Application Security**

- Mobile devices sport a number of channels such as voice, SMS, and data. The devices also typically contain hardware such as microphone, camera, touch-screen interface, gyroscope and accelerometer. Mobile applications can access all of these features and therefore can do more harm if compromised. Popular operating systems such as iOS, Android and Windows Phone have evolved, providing a number of security features that can enhance the security of the application and user data. Knowledge of these features and their correct use is critical.

- Mobile applications are typically one of three types and have different security profiles:
  - **Native** - Applications that operate off the native mobile device operating system leveraging its APIs. Applications can store data locally and hence data security of these applications becomes paramount.
  - **Web applications** - Applications that are accessed through a web browser. These may be regular web sites or a separate mobile web application optimized for mobile attributes. Well known web application vulnerabilities need to be addressed here. A secure browsing context should be used for web access.
  - **Hybrid applications** - applications that are hybrid of native and web and operate by leveraging web pages inside a dedicated native application wrapper. Sensitive data can be handled at the backend while client application can provide enhanced user experience and business functionality. A fine balance between usability and security can therefore be achieved.

- Mobile applications are typically targeted in a number of ways, exploiting weaknesses of the application design and development. Some of these include:
  - Improper sensitive data storage
  - Buffer overflow
  - Dynamic runtime injection
  - Permissions misuse
  - Privilege escalation
  - Improper SSL validation
  - Improper configurations

- Organizations must have a secure software development lifecycle process in place. Secure application design must take an approach that encompasses a number of defensive measures designed to protect data and systems from a variety of attack methods. A mobile application typically must employ an
authorization framework, enable compromise detection and provide robust security framework integration with platform and third party APIs as necessary to maintain data confidentiality at rest and in motion.

- Each platform has its own peculiarities; developing a secure application requires adhering to best practices as relevant to the platform. Security must be built into the design of the application. Some recommended key principles for building applications securely are:
  - Avoid storing sensitive information on the client end. If it is essential to do so for some reason (such as offline access), then the data must be stored securely, incorporating best practices for encryption. Many applications utilize encryption to protect sensitive data; however, many flaws in the technique allow an attacker to retrieve or deduce the key, or extract the key from the operating system.
  - Avoid caching of data. Take proper care while storing data in log or debug files, cookies, web history, web cache, property lists, files and SQLite databases. Inescapable caching must be done securely.
  - Fully validate SSL/TLS certificates and sessions.
  - Implement file permissions appropriately.
  - Handle authentication and sessions properly. Implement two factors or adaptive multifactor authentication.
  - Implement encryption controls correctly.
  - Avoid unintended information leakage
  - Resist runtime manipulation.
  - Leverage code obfuscation and anti-tampering to complicate reverse engineering.

- Every mobile application must undergo vulnerability assessment and penetration testing, as both a standalone application as well as within the context in which it will eventually operate. All network level activity and any web interfaces that it uses must be tested to ensure that they are secure as well. Tool based Black and White box testing complemented with manual review by security consultants ensures that a secure mobile application rolls out.

**Mobile Data Protection**

- Data protection is the last bastion in security that can protect users and organizations from attacks that have breached all the other layers of security. Protecting data is also critical for organizations in order to comply with government or industry regulations, maintain privacy and protect intellectual property. Organizations run the risk of facing high penalties in case of a reported loss of personally identifiable information.

- Data confidentiality is typically achieved by having a clear organization wide data classification policy; a need-to-know based disclosure policy and encrypted data at rest and in motion. An organization-
wide, encryption-based, data protection strategy will require a comprehensive system for managing security keys and privileges. Data security in the mobile world has gained even more importance, as data tends to travel on unsecured wireless networks, often outside of enterprise control. Mobile devices also tend to get misplaced or lost easily, thereby exposing the data in a running or stored state to a malicious user.

- Encryption on mobile devices can be enabled using built in operating system capabilities or third party software with centralized management tools. Popular operating systems such as Android and iOS provide native support for device level encryption. Organizations must require employees to enable this in order to connect to enterprise systems. Data on encrypted devices can only be recovered if the correct PIN is supplied. Modern mobile operating systems also provide access to standard networking protocols for authenticated, authorized and encrypted communications.

- Though encryption is a great way to protect data, as a word of caution, organizations must be aware that correctly implemented modern encryption algorithms make it impossible to recover data in the absence of a key. A lost key is as good as data loss. Putting a key management and retrieval system in place is therefore essential.

- An organization’s data protection strategy could also revolve around protection based on the risk exposure to the data. Strong authentication, strict access control and accountability mechanisms for less sensitive data access are some examples of this type of implementation. The associated overhead costs of key management and lost-key help desk support may further support this view. Complementing this with remote data wipe capabilities will further reduce risk exposure. An organization’s data protection strategy must maintain good balance based on risk assessment.

- Mobile devices can easily fall into the wrong hands as they can be left unattended. It is therefore important to ensure, from an application perspective, that the right user is at the other end. A strong and adaptive multifactor authentication policy is therefore an essential requirement. Strong authentication must not adversely impact usability, hence the need to build an adaptive authentication that demands strong authentication for high risk and less frequent transactions.

- Strong multifactor authentication can be built using One Time Passwords (OTP), digital certificate based challenge response authentication, or Grid. These can be integrated into an enterprise Public Key Infrastructure (PKI) solution and an enterprise authentication server with built in Hardware Security Module (HSM) to improve its overall security strength. An enterprise PKI provides flexibility of using digital certificates for encryption and authentication adaptively. However, enabling applications to obtain, store, and process certificates securely is not trivial, and a holistic PKI solution coupled with a key management solution must be considered for the same. The challenge in implementing these directly on mobile is the safe storage of the private keys or seed required for OTP generation. Storing it securely in key chains and credential storage locations provided by the OS provides good usability but suffers from limitations faced by all software based security controls and may not withstand a sophisticated attack. The next section will deal with two ways that hold promise in obviating this problem at varying costs.

**Other High Assurance Mobile Security Measures**
- Mobile Virtual Desktop Infrastructure (VDI) - VDI vendors have begun offering VDI clients for mobile platforms. These solutions provide remote access to desktop or server environments at the cost of user experience and performance. The data does not leave the server or desktop and hence offers a higher level of security. Organizations working in a low risk, highly regulated industry that want to provide remote access to highly sensitive applications may opt for mobile VDI solutions.

- Mobile App Risk Management - Mobile applications downloaded from app stores carry a risk of malicious behaviour. Enterprises can use cloud based platforms, which provide reputational feeds of mobile applications to enterprises that integrate with enterprise EMM / MDM / MAM solutions, quantifying the risks of the applications on the devices accessing the enterprise. This enables enterprises to rollout a role and risk based application usage policy.

- Always-on-VPN - This approach involves routing all data traffic back to the company through an encrypted tunnel. This impacts performance, increases traffic load on corporate security and networking infrastructure, and complicates personal usage. However, this also ensures that all organizations’ centrally implemented countermeasures apply to mobile as well.

- Trusted Execution Environment (TEE) - GlobalPlatform (http://www.globalplatform.org) is standardizing TEE technology. The TEE is proposed to be a separate hardware protected execution environment that runs alongside the Rich OS and provides security services to that rich environment. The TEE offers an execution space that provides a higher level of security than a Rich OS. The TEE protects the user input entered through the touch screen or keyboard. It also protects the data displayed on the screen and protects the transaction details from modification by a hidden malevolent application. It is resilient against key loggers and man in the middle type of threats. The TEE provides secure storage area for sensitive data such as encryption keys, PINs and OTP seeds. Secure credential storage provides ways to securely perform VPN authentication or implement an OTP solution for Strong Authentication. The TEE as envisaged by Global Platform is as depicted-below.

![Figure 2: Trusted Execution Environment](http://Globalplatform.org)
As Figure 2 illustrates, the TEE offers safe execution of authorized security software, known as trusted applications; it also enforces protection, confidentiality, integrity and access rights of the resources and data belonging to those trusted applications. In order to guarantee the root of trust of the TEE, the TEE is authenticated and then isolated from the rest of the Rich OS during the secure boot process.

TCS Approach to Mobile Security

TCS’ approach to mobility rollout revolves around the fundamental principle of risk and role based mobility. The framework works as an enabler for enterprise Mobility. The framework is backed by TCS’ enriched experience in the entire spectrum of secure software development and IT services. The framework is built over its in-house developed methodologies and products complemented with integration with the best of breed security solutions.

Four pillars of TCS mobile Security Offerings are:

- **End-to-End Mobile Security Consulting:**
  - Security assessment of the mobile ecosystem,
  - Developing a secure mobility strategy as per the enterprise’s need,
  - Risk assessment and evolving enterprise mobile security policies.

- **Mobile Device Security and Application Management Infrastructure:**
  - MDM/MAM product selection
  - Application and device provisioning/de-provisioning policy
  - Procedures for requesting and obtaining mobile devices
  - Applications
  - Service selection, use, and product integration in consonance with the security policy.

- **Secure Mobile Application Rollout Toolkit. (SMART) provides methodologies and toolkits for the entire SSDLC of mobile Software Development. These include:**
  - Secure development guidelines for mobile platforms
  - Reusable tool kits for key security functions
  - Secure development training
  - Threat modelling and secure design
  - Mobile applications security testing including source code review and black box testing.

- **Mobile Data Protection. Mobile Data Protection provides customized solutions to guarantee data protection for data at rest & during transit. They are as follows:**
  - Mobile device and data encryption solutions
  - PKI based encryption tools
  - Enterprise key store management solution
  - Digital signing and verification tools
  - Multifactor authentication solutions
Conclusion

Enterprises are faced with the challenge to support and secure a growing population of mobile devices. The challenge is how to maintain a balance between user and corporate expectations without compromising enterprise security and users' privacy. Because of these complexities, there is no straightforward, one-size-fits-all recipe for success when it comes to solving the mobile security puzzle. Nonetheless, organizations must:

- Evolve a risk based mobile security strategy
- Incorporate key ingredients of mobile security into the enterprise security policy
- Pursue a layered approach where MDM/MAM oriented security capabilities are supplemented by the advanced controls described herein for secure access, application security, threat protection, and data protection
- Favour solutions that deliver a high degree of administrative efficiency and low overall TCO and incorporate enterprise-class features, such as centralized management, enterprise PKI/directory integration, and robust reporting
- Engrain security in all phases of application SDLC and complement it with a robust mobile apps security testing program
- Focus on ensuring adequate protection of mobile data, while balancing this with the need for a positive user experience and reasonable cost of ownership

References

2. Enterprise Mobility Guidebook- enterprise Mobility Foundation: http://www.theemf.org/
3. Corporate App Store Environments Open New Market Opportunities: by Michele Pelino, Forrester research, Feb 2012
4. Market Overview: On-Premises Mobile Device Management Solutions, Q3 201, Forrester research. By Benjamin Gray and Christian Kane
7. 42+ Best Practices: Secure mobile development for iOS and Android: viForensics
About TCS Mobility
TCS Mobility delivers best in class mobility services and solutions with complete mobility lifecycle consultation and development service along with customization on top of pre-built solutions to provide the best in class benefits to our customers.

Our passion for providing the very best and comprehensive mobility services and solutions to our customers is realized through our deep expertise in mobility gained through the experience of a strong team that has a career long experience in mobile technologies and a dedicated mobility user experience design team that is committed to leveraging the unique native capabilities of each device platform.

Contact
For more information about TCS’ Mobility contact mobility.solutions@tcs.com

Subscribe to TCS White Papers
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)
Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

IT Services
Business Solutions
Outsourcing