Security Challenges in Mobile Enabled Enterprises

With the influx of powerful mobile devices, smartphones, Personal Digital Assistant (PDA) and tablets, enterprise mobile applications have already become indispensible in the day-to-day operations of many organizations. In this white paper, we elaborate the reasons why enterprises are striving towards mobile enablement by allowing employees to use smartphones and other mobile devices at work. This creates a host of security challenges that we have addressed in this document, through TCS’s mobile security offering – Secure Mobile Enablement Framework (SMEF). The framework has been proposed as a holistic mobile security management strategy that will help enterprises solve key issues relating to rapidly increasing mobility adoption.

**General Terms**

Enterprise Mobility, Security Challenges, Smartphone, Tablets

**Keywords**

About the Authors

Colonel Rajmohan, CISSP
Colonel heads the Security CoE practice of TCS Niche Tech. Delivery Group (NTDG). He has led varied security initiatives in emerging areas and architecting end to end security solutions for strategic consulting engagements for many industry verticals.

Ruchi Choudhary
Ruchi leads the Mobile Security initiatives of TCS NTDG group. She is involved in creating awareness on secure application development guidelines on mobile platforms and actively working with customers on addressing their mobile security solutioning requirements.

Somen Das
Somen is an Application Security Analyst. Specialized in Static & Dynamic application vulnerability assessment techniques, he is actively involved in spreading awareness on secure application development and related guidelines across industry verticals. He has front ended many solutioning requirements from customers on creating application security frameworks for web and native applications. He is also Local Chapter Leader - OWASP Bhubaneswar.
Table of Contents

1. Introduction 5
2. Business Drivers for Mobility Momentum in Enterprises 6
3. Enterprise Mobile Security Challenges 8
4. Secure Mobile Enablement Framework 14
5. Conclusion 15
### List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation/ Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>E2E</td>
<td>End to End</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Device Assistant</td>
</tr>
<tr>
<td>RIM</td>
<td>Research In Motion</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>SMB</td>
<td>Small and Medium Business</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMEF</td>
<td>Secure Mobile Enablement Framework</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes–Oxley</td>
</tr>
<tr>
<td>TCS</td>
<td>Tata Consultancy Services</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Introduction

Massive growth in the mobile ecosystem has transformed operations in the enterprise world with respect to mobile devices. Increasing globalisation and on-the-spot information requirement is also catalysing the mobile enablement of the global workforce. More and more employees are taking advantage of mobile devices to access emails, spreadsheets, databases, and ERP applications using either personal or company-owned devices.

Due to inadequate access control policies and lack of information on securing mobile devices, IT departments had to completely ban such devices or risk insecure access inside the enterprise firewall. But as new mobile devices continue to appear on the enterprise network, a secure mobile enablement framework is a key IT programme requirement.

This paper highlights various aspects of security that require extra focus when enabling mobile devices in an enterprise. Emerging trends in usage patterns and evolving models of managing mobile devices are also discussed here. As part of the TCS SMEF a number of steps have been proposed to enable an enterprise evolve a mobile usage and management strategy. Customised security processes, methodology and solutions are proposed to cover the entire spectrum of issues that need to be addressed.
Business Drivers for Mobility Momentum in Enterprises

Recent developments in the mobile device market have reached an inflection point. With post-PC devices taking over the workplace, IT managers are looking to draft plans that allow employees access to internal business applications from their mobile devices. In addition to emails, enterprises are actively considering porting Customer Relationship Management (CRM) and other proprietary in-house applications onto the mobile platform.

### Mobile Application And Device Initiatives Are Key Priorities For Enterprises In 2010

**“Which of the following initiatives are likely to be your firm’s top telecom / communications adoption priorities over the next 12 months?” (3 and 4 on a scale of 1 [not on our agenda] to 4 [critical priority])**

<table>
<thead>
<tr>
<th>Initiative</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement or expand network security solutions</td>
<td>65%</td>
</tr>
<tr>
<td>Implement or expand collaboration solution(s)</td>
<td>47%</td>
</tr>
<tr>
<td>Support more mobile applications for out-of-office users</td>
<td>46%</td>
</tr>
<tr>
<td>Migrate more voice traffic to VoIP</td>
<td>45%</td>
</tr>
<tr>
<td>Support more mobile devices or smartphones (not laptops)</td>
<td>44%</td>
</tr>
<tr>
<td>Implement or expand WAN optimization-acceleration</td>
<td>40%</td>
</tr>
<tr>
<td>Implement or expand unified communications (UC) solutions</td>
<td>37%</td>
</tr>
<tr>
<td>Implement or expand IP videoconferencing</td>
<td>37%</td>
</tr>
<tr>
<td>Support more mobile applications for workers in the office</td>
<td>33%</td>
</tr>
<tr>
<td>Implement or expand carrier Ethernet services and transport</td>
<td>26%</td>
</tr>
<tr>
<td>Implement or expand use of third-party-as-a-service solutions</td>
<td>25%</td>
</tr>
<tr>
<td>Implement or expand use of third-party-manage services</td>
<td>21%</td>
</tr>
</tbody>
</table>

Base: 1,992 North American and European enterprise executives
Responses for “Don’t know/does not apply” have not been included

Source: Enterprise and SMB Network and Telecommunications Survey, North America and Europe, Q1 2010

Source: Forrester Research, Inc.

Figure 1: Mobile Evolution in Enterprises
Apart from smartphones, tablets and a whole new array of computing devices built around the newer mobile platforms are demanding access to enterprise resources. There are a number of drivers for this phenomenon:

**Quicker decision making**

Mobility provides instant access to business intelligence databases and accelerates the decision making process by employees when away from the office.

**Employee convenience**

The ongoing trend to ‘bring your own device’ in enterprises will drive overall enterprise smartphone adoption. As per Forrester Research, Inc. 56% of firms now officially support personally owned smartphones.

---

**Nearly 20% of Employees Use Smartphones, And Many Leverage Basic Applications**

**4-1** Nearly 20% of employees use smartphones for work

“Do you use smartphones for work purposes?”

- I have a smartphone that I use for work 18%
- I only use my smartphone for personal use 20%
- I do not have a smartphone 62%

*Base: 5,519 North American and European business technology end users*

**4-2** Most employees currently use basic mobile applications, IM and navigation for work

“Which mobile applications do you use on your smartphone for work?”

- Email 92%
- Voice 86%
- Calendar 80%
- Maps/navigation (e.g., GPS) 57%
- Instant messaging (IM) 50%
- May company’s intranet/portal 43%
- Company-specific application 35%
- Social media for work (e.g., Linkedin, Twitter) 26%
- Team collaboration (e.g., Sharepoint) 20%
- Video viewing (not videoconferencing) (e.g., Youtube) 19%
- Webconferencing (e.g., WebEx or Citrix GoToMeeting) 18%
- Sales force application 16%
- None of above 1%

*Base: 971 North American and European business technology end users who use a smartphone for work (multiple responses accepted)*

*Source: Forrsights Workforce Employee Survey, Q3 2010*

*Source: Forrester Research, Inc.*

---

*Figure 2: Survey on use of personal mobile devices for business*
Increased productivity

Use of mobile devices is shown to increase enterprise productivity significantly according to a survey conducted by an independent research group. The survey brings out a host of reasons for employees being away from the workplace, which account for a considerable amount of lost productivity time, in the absence of mobile empowerment of employees. Moreover, it’s not just simply mobile enabling the workforce but providing the right mobile technology that provides a further boost to productivity.

Availability of data anywhere, any time

Among the best applications of mobile technology that enterprises are providing for their businesses is effective data sharing. Managers can respond to important Request for Proposals (RFP) or perform reviews as and when required, sales managers can check inventory levels of products and the help desk executives can serve customers round the clock from practically any location. Allowing vendors and customer access to information in the enterprise applications is viewed today as a crucial benefit, particularly to the business.

Enterprise Mobile Security Challenges

Figure 3: Mobile Security Threats
Mobile devices will be an important part of the future workforce and look to be poised to stay. They are almost everywhere, convenient to carry, equipped to be used as a computer and at the same time can be used to make calls. More organisations are attempting to mobile enable their workforce by the end of 2011-12. According to Forrester Research, Inc. the worldwide mobile worker population is set to increase to more than 600 million by 2015 (see Figure 4).

![Enterprise mobile worker forecast diagram](https://via.placeholder.com/150)

Source: Forrester Research, Inc.

Forecast: Global Enterprise Mobile Users, 2010 to 2015

**Figure 4: Enterprise Mobile Workforce Forecast**

SMBs are increasingly turning to tablets and cloud applications to boost their business as these show almost limitless potential as a valuable resource, essential to the on-the-go businessman. However, the benefits of this increased mobility come with growing risks. Full-time connections via email, VPN and enterprise applications combined with local storage of data on mobile devices, increase the potential for exposure of sensitive, confidential and legally protected data. An unauthorised user on a mobile device can be as dangerous as an intruder sneaking into enterprise headquarters.
Device level protection

The portability of mobile devices allows for continuous access to business and personal information, regardless of location which makes such devices easy targets for theft or misuse. As mobile devices are portable, they are more likely to be lost or stolen. To prevent unauthorised usage of the device, enterprises need to consider solutions that allow device locking, memory card security, call barring etc.

Content protection

The security implications of an executive’s e-mail inbox or calendar, records meetings and briefings retrieved by a competitor could be catastrophic. Recent incidents have confirmed that even contact information can also cause problems if it falls into the wrong hands. Organisations therefore need to protect all forms of data on their employee’s mobile devices and not just application specific data by encrypting device and card memory, data backup and application signing.

Apple iOS and Google’s android platforms employ several key security mechanisms like - Mandatory Code Signing, Sandboxing, Trusted Boot, Device Encryption, Data Protection, and Address Space Layout...
Randomisation. A judicious use of these features during application development along with complementary and strong external application agnostic controls provides the required content protection assurance.

Diversity of mobile platforms

The diversity of mobile platforms that enter the enterprise network is fast becoming a major security challenge for enterprises. There are already six major software platforms for smartphones which include the Apple iPhone, RIM BlackBerry, Microsoft Windows Mobile, Google Android, Palm and Symbian.

The tablets are also not far behind with its popularity taking a huge increase in 2010. As per an independent research group, the percentage of employees bringing tablets to work grew more than 100 percent in 2010. This necessitates planned device management and security policies across platforms. Device diversity requires enterprises to evolve an assured and implementable security policy as part of a holistic mobile device management strategy.

Unauthorised Bluetooth or Wi-Fi access

Recent studies reveal that most mobile device users enter the enterprise network without permission with the majority disregarding company security policies and procedures. Mobile phone users also use hands-free bluetooth headsets, allowing hackers a hole for ‘BlueSnarfing’ data on the device or ‘BlueBugging’ to gain control of the device. Uncontrolled wireless network connections can lead to unauthorised device access.

Researchers at University of Ulm, Germany claimed that 99 percent of Android devices are vulnerable to attack when they’re used to log into a site on an unsecured network. According to the research, devices running on Android 2.3.3 or older are vulnerable because of a faulty client login authentication protocol. 
Use of disallowed devices

Organisations need to be wary of employees using smartphones for both work and personal use as this would result in accessing sites and applications that may not have come from trusted sources and could potentially create a back door entry for Trojans and malwares into the corporate network. Maintaining separate personal and corporate profiles, installing only approved applications and clear segregation of corporate and personal data is critical in building a secure enterprise network.

Malicious software

Viruses, trojan horses, and worms are well-known threats to conventional workstations and laptops. As mobile usage has increased exponentially with both wireless and broadband connectivity, mobile devices have become the latest target of sophisticated malware. Some of the examples comprise background calling applications that rack up exorbitant long distance bills for victims and trojans that
send short message service (SMS) messages to premium rate numbers. An Android mobile wallpaper malware application that collected personal data like browsing history, SMSs, and voicemail password were among the broadly discussed topics at the Black Hat security conference 2010. Malicious applications such as these actually target the Android platform fairly easily, due to its open submissions policy. A malware management strategy for the mobile environment is a critical component in an enterprise mobile enabled network.

Regulatory compliance mandates

mCommerce applications have gained widespread popularity and payment options such as Near-Field Communications (NFC) are widely adopted today. The mobile device is therefore becoming a very lucrative target and enterprises need to anticipate an increasing number of malware targeted at intercepting valuable financial information. Regulatory requirements such as PCI DSS compliance and SOX impose further burden on the enterprise to not only protect data but also credibly demonstrate that compliance requirements are met.
Secure Mobile Enablement Framework

The mobile industry is sprouting rapidly with new devices that use increasingly sophisticated capabilities released almost every day. To increase business efficiency and be connected to evolving technologies, enterprises need to offer their workforce the necessary ecosystem to work when on-the-move.

While enterprises are planning to offer business solutions on mobile devices, hacking technologies and/or methodologies are also evolving and a single security solution cannot address all potential security threats and vulnerabilities. To provide a strong security mechanism, combinations of solutions are implemented at different levels based on enterprise mobile application security requirements.

TCS’s strategic approach can help enterprises develop customised security processes, methodology, and tailor-made solutions. Building on our rich experience in the entire spectrum of secure software development and IT services, TCS has evolved the Secure Mobile Enablement Framework. The framework using in-house methodologies and products will not only help enterprises address the key challenges of rapidly increasing mobility adoption, but also help them directly manage enterprise mobility services, by ensuring an E2E secure mobile ecosystem.

TCS approaches enterprise mobile security from five distinct directions:

- **Mobile Security Assurance Program:** During initial stages of the development cycle the designers/architects/developers are trained on secure design & development practices for mobile applications. The framework provides a mechanism to create a secure software development life cycle for mobile applications beginning from creating threat models to eventually building and testing the code. The uses of key security enablers provided on all leading platforms are demonstrated. Necessary OS specific checks are instituted to prevent critical applications from exposing vulnerabilities.

- **Mobile Security Testing:** Mobile applications are tested rigorously both as a black box and white box followed by exhaustive manual review by platform experts.

- **End-to-End Mobile Security Consulting:** This includes developing enterprise mobile security policies, security assessment of mobile ecosystem, developing secure mobility strategy as per enterprise requirement and risk assessment.

- **Data Protection:** Customised solutions and frameworks for protecting sensitive data at rest and during transit.

- **Mobile Device Management:** This includes deployment, configuration and integration of leading industry products to centrally manage varied mobile devices connecting to the corporate network. The system caters to application provisioning and de-provisioning, policy enforcement, round the clock monitoring and incident management. This ensures the survivability and security of enterprise data under any eventuality.
Conclusion

Smartphones and tablets are important productivity tools that should be leveraged for enterprise businesses. Many large and SMB enterprises are providing their employees with smartphones and tablets believing it would increase productivity and the overall enterprise revenue. Such a move may boost employee productivity, but would also create security challenges for enterprises.

It is time that enterprises view mobile security holistically keeping in mind the people, processes and technology to mitigate associated risks. A comprehensive solution includes training people to use mobile devices securely, extending desktop and laptop security policies to mobile devices, and implementing mobile security technology solutions ranging from developing secure mobile applications to protecting data while on rest or in transit.
No single solution can address all the myriad security issues pertaining to the mobile ecosystem; to have and make four or five security applications work well together at an optimum cost model could be challenging. TCS’s Secure Mobile Enablement Framework along with its in-house products will not only help enterprises address the key challenges of rapidly increasing mobility adoption, but also help them with the direct management of enterprise mobility services through the promise of an End-to-End (E2E) secure mobile ecosystem.

References
2 Market Overview: Smartphone Management, Forrester Research, Inc., August 26, 2010
5 Catching AuthTokens in the Wild, University of Ulm, May 13, 2011
7 Android App Swipes User Data, Fast Company, Jul 29, 2010

All the references used in this paper are for information and educational purposes only & has no commercially value in it. Although the information contained have been compiled or arrived at from sources believed to be reliable, no representation or warranty, expressed or implied, is made as to their accuracy or completeness and neither the information nor the forecast shall be taken as a representation for which TCS incur any responsibility. This document has no strategic and business value associated with it. Opinions expressed are exclusively of authors and not of the group.
Contact
For more information, contact dinesh.sawrirajan@tcs.com

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

About Tata Consultancy Services (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