



TECHNOLOGY WHITE PAPER

SecureIT Mobile Enterprise

The Three Pillars of Enterprise Mobility:
Security, Privacy, and Freedom

Rob McCammon
VP, Product Management
Open Kernel Labs, Inc.

FEBRUARY 2011

Contents

Introduction	3
The Three Pillars of Enterprise Mobility	3
Who Should Read This White Paper	3
Enterprise Mobility	4
Mobility Trends – 2011	4
Challenges	5
Gaps in Current Solutions	7
Introducing SecureIT Mobile Enterprise	8
Background	8
Solution Architecture	8
Secure Enterprise Mobility	9
Conclusion	12
Coming Soon to Handsets and Tablets	12

Introduction

This white paper examines an important emerging paradigm in mobile computing - enterprise mobility. In particular, it looks at converging trends in mobile/wireless and enterprise IT that define enterprise mobility, and how to serve requirements for secure implementation of this paradigm.

The Three Pillars of Enterprise Mobility

Effective enterprise mobility rests on three pillars: security, privacy, and freedom. This white paper explores the challenges in supporting these pillars and how a new product from OK Labs, SecureIT Mobile Enterprise, meets the following real world needs:

- Secure deployment of enterprise apps and access to corporate data and services
- Protection of user privacy and separation of worker and employer assets
- Freedom to use all available device functionality, including the ability to install applications and freely surf the web

This white paper proposes a reinvention of current implementations of enterprise mobility that strengthens and enhances the three pillars, building on mobile virtualization.

Who Should Read This White Paper

This white paper is intended help the following organizations and individuals understand the challenges involved in enterprise mobility definition and rollout:

- Enterprise: CIOs, Chief Security Officers, and IT Directors
- Mobile Operators: Solutions Architects and Enterprise Market Segment Specialists
- Device OEMs: Product Managers and Systems Software Architects
- Chipset Solution Providers: Product Managers and Systems Software Architects

Enterprise Mobility

The term “enterprise mobility” looms large in business and technology headlines, as the mobile/wireless ecosystem struggles to accommodate two intersecting phenomena:

- An increasingly mobile workforce
- Ubiquitous mobile devices and the applications that run on them

What does enterprise mobility actually involve? Let’s look at the Forrester Research definition:

The ability of an enterprise to connect to people and control assets from any location. Technologies that support enterprise mobility include wireless networks, mobile applications, middleware, devices, and security and management software.

That definition, while accurate, leaves much to the imagination – *connect to which people and why*, and *control which assets for what purpose*? It also raises a deeper question – how is enterprise mobility different from traditional enterprise connectivity? Some answers to these questions can be found in the following trends:

Mobility Trends – 2011

Mobile Workforce: Many of today’s workers find themselves outside of corporate headquarters – that’s more than one billion mobile workers, or one third of the global workforce (Forrester). These workers need to view company data, create documents, communicate using corporate email, and access company applications from smartphones and tablets remotely, just as they would at their desks.

Consumerization of Enterprise IT: For a decade or more, corporate employees have had the benefit of using company-supplied equipment for productivity in the office and on the road, including mobile phones, laptop computers, and other devices. Today, employers and employees would rather leverage worker-owned device – 40% are already doing so (Juniper Networks). BYOD (bring your own device to work) saves acquisition and maintenance costs and lets workers choose and use the smartphones and tablets that fit their lifestyles and work habits.

Open Mobile OSes: Today’s smartphones and tablets increasingly deploy open and open-source OSes – Android, Linux, etc. Speeding development and encouraging innovation, today’s community-built platforms increasingly dominate the mobile landscape.

Applications Markets: 2010 was the year of the mobile application. Developers created hundreds of thousands of apps for iPhone, Android, and other platforms. Smartphone and tablet owners responded with billions of downloads. Unfortunately, the apps offered in these marketplaces vary greatly in quality and security. CIOs rightly worry that workers’ favorite games, apps, and social media clients provide direct vectors for viruses, spyware, and other threats.

Cloud Computing Adoption: Across enterprise and SMB, IT departments increasingly virtualize the data centers that once occupied basement floors or entire buildings. Migrating enterprise applications and data to the Cloud goes hand in hand with enterprise mobility – access to decentralized assets can be decentralized as well.

Challenges

The above trends reflect an exciting and increasingly well-provisioned reality. However, these trends – and enterprise mobility in general – bring new challenges and concerns to enterprise IT.

Mobile Device Provisioning and Management

From an enterprise IT perspective, smartphones, tablets, and other mobile/wireless devices present challenges to provisioning and management not encountered on more familiar notebooks and desktop computers:

- **Deployment Path** – Many mobile devices must be provisioned through operator/carrier channels – not through direct programming by IT staff
- **Deployment Mechanisms** – Putting software and enabling services on mobile devices usually involves “over the air” transaction rather than installation to disk and local configuration – many mobile devices don’t even have user-visible file systems
- **Device Management** – Mobile device management (MDM) is often an all-or-nothing affair: IT either takes over the entire device or takes a step back to let operators or users do it for them. MDM software is evolving to give IT staff finer-grained control, but because they have little or no control over factory installed (pre-loaded) software, large gaps remain between mobile and desktop management capabilities

Security

Mobile handsets, tablets, and other wireless devices are perceived to be the weakest links in the enterprise security chain. Even with the vagaries of securing desktop systems, enterprise IT has made its peace with that environment, and has well-established tools and procedures for protecting PCs, workstations, and notebooks running Windows and other desktop OSes.

Securing mobile devices, however, reminds IT professionals of the situation with desktop systems from a decade ago. The menace is real – in the last 12 months, threats to mobile software have jumped 250% (Juniper Networks).

Malware and Other Exploits – As mobile devices become more powerful and complex, they present larger and more inviting “attack surfaces” to the black hats of the world. Add to this complexity of untrusted content and programs downloaded from app stores, web-based exploits and wireless hacks. Threats to mobile device software then include:

Over the last decade, enterprise IT made its peace with desktop security. Today, mobile devices are perceived as the weakest link in the enterprise security chain.

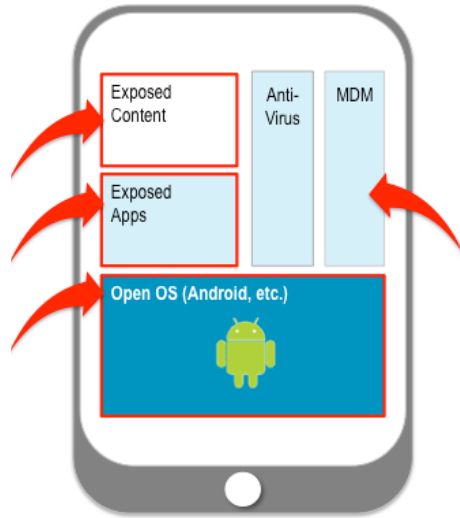


Figure 1: Threats to Mobile Software.

- Viruses and spyware from downloaded apps
- Zero-day exploits in system and user software
- OS-level exploits of open platforms such as Android
- Threats to anti-virus and MDM software itself

Secure Access – The raison d’être of enterprise mobility is to enhance productivity by providing access to business assets and processes. Opening up business-critical data-bases and applications with unsecured access from mobile devices is one of the main inhibitors to adoption of enterprise mobility. Threats to this access incur on the device itself, and to local data, applications, and browsers, and can be carried upstream to corporate assets hosted in data centers and in the Cloud.

Separating Assets – A key internal threat to security is the commingling of personal and enterprise assets. These assets include diverse types of applications and data, such as personal and corporate finances, personal and business email, and operation and automation of home appliances and the factory floor.

Privacy and Functionality

Most discussions of enterprise mobility start and end with the benefits to company management, such as enhanced employee productivity and reduced capital equipment and operational costs. If companies really want to maximize ROI from mobility, they must consider the needs and habits of mobile workers. Employers ignore worker predilections at their own risk. If forced to carry devices with limited functionality that impinge on their personal lives, users will continue to carry two devices: one for work, and another for their personal lives.

Locked-Down Devices – The shortest path to secure enterprise mobility is a fully locked-down device that exclusively serves for access to corporate assets. In the past, this meant a company-supplied phone; today, with BYOD, it usually means crippling an employee-owned device to limit the security risks described above.

Employee Privacy – An often-missed factor in adoption of enterprise mobility is the converse of enterprise security – employee privacy. If protecting corporate assets on a device means baring private user information and apps to employer scrutiny, users will choose not to use that device.

Choice of Applications – A key motivation for users to invest in smartphone and data plans is to gain access to compelling applications and services, such as games, lifestyle apps, and video. Enterprise mobility regimes will not succeed if they destroy that investment by blacklisting and banishing apps and services that users crave.

If forced to carry devices with limited functionality that impinge on their personal lives, users will carry two devices: one for work, and another for their personal lives.

Gaps in Current Solutions

Today's enterprise mobility involves a mix of end-point security, anti-virus (AV) software, and suites of mobile device management (MDM) software that host on devices and gateway servers in data centers and in the Cloud. These technologies are necessary and powerful, but leave critical requirements unmet. In particular, MDM and security rely on the integrity of the underlying smartphone OS and software stack, which are vulnerable to exploits.

AV Software

Web-connected desktop computing has become a minefield of malware. During the last decade, malware attacks cost businesses worldwide over \$15 billion USD per year (Computer Economics). With the rise of smartphones and tablets, mobile malware is poised to follow suit. Smartphones may already be infected at twice the rate of Windows PCs (SANS Institute).

On the desktop, as new malware and exploits surface, AV software vendors, as well as platform and applications suppliers, provide updates and patches. Best practice among IT teams is to evaluate and apply those remedies in a timely fashion. Mobile device software, on the other hand, has a much harder time keeping up with rapidly evolving malware. There are more mobile platforms (multiple deployed versions of Android, iPhone, Linux, RIM OS, Symbian, Windows Mobile/Phone, etc.) and rapidly multiplying applications (200,000 for Android alone, as of January 2011).

Equally important are the logistical hurdles to remediation – mobile software updates, while frequent enough to overwhelm device OEMs and operators, occur much less often than their desktop equivalents. This gap in frequency comes from dependence on initial pre-load deployment, challenges in pushing out and installing FOTA (firmware over the air) updates, and end-user inattention to software maintenance. Moreover, AV (and MDM) solutions are themselves subject to attacks and exploits, and can become vectors for infection.

MDM

Integrated mobile device management software suites bridge many gaps in enterprise mobility, including application provisioning, security policy enforcement, device location, backup, wipe, and other management functions. MDM trends toward horizontally comprehensive solutions, preferably from a single vendor. While this approach eases procurement and support, it can also result in broad, shallow solutions that do not integrate the best in class capabilities for all functions.

MDM software typically involves a mix of low-level firmware, system software, and application middleware components. As such, MDM is at least partially dependent upon the integrity of mobile OSes and mobile networks. If either of these is itself compromised, then MDM software is effectively compromised as well.

Secure IT Mobile Enterprise reinvents enterprise mobility by building on mobile virtualization.

Introducing SecureIT Mobile Enterprise

To meet the challenges of enterprise mobility and bridge gaps left by existing solutions, OK Labs introduces SecureIT Mobile Enterprise. SecureIT Mobile Enterprise reinvents enterprise mobility by building on the OK Labs core mobile virtualization platform, the OKL4 Microvisor. It complements and fortifies MDM, AV, and other mobile technologies, resulting in an ideal mix of security, privacy, and functionality.

A software and services solution, SecureIT Mobile Enterprise helps companies deploy and manage enterprise applications and services alongside personal ones. Using OKL4 Secure HyperCells (virtual machines), SecureIT Mobile Enterprise isolates personal applications, services, and data from business-critical ones.

By supporting both open personal and trusted enterprise domains on a single physical device, SecureIT Mobile Enterprise reconciles the needs of the individual and the enterprise.

Background

SecureIT Mobile Enterprise has its roots in secure and certified systems. In 2010, OK Labs introduced [SecureIT Mobile Government](#), targeting mobile devices for national defense, first responders, and public safety. With SecureIT Mobile Government, OK Labs helps OEMs, integrators, government contractors, and public sector agencies use COTS mobile hardware to build Obamaberry-type¹ devices for a fraction of the cost of legacy bespoke systems.

With SecureIT Mobile Enterprise, OK Labs brings military-grade security to enterprise mobility.

Solution Architecture

Mobile Virtualization

SecureIT Mobile Enterprise builds on the mature and widely deployed² OKL4 mobile virtualization platform. It leverages on-chip memory management and privileged execution capabilities of modern microprocessors like ARM. Its core is a bare metal hypervisor, just like data center virtualization.

Strong Isolation

A virtualization-based enterprise mobility solution features strong separation of trusted (enterprise) and untrusted (personal) operation domains. Company assets and personal data and apps occupy separate, OKL4 Secure HyperCells isolated from one another, running on unique instances of one or more mobile OSes.

¹ <http://techcrunch.com/2009/01/23/up-close-with-the-obamaberry/>

² Over 1.1 billion deployments to date

Security Foundation

During development of mobile devices and mobile software, developers need maximum flexibility to prototype, develop, and test platforms and applications. When it comes time to “cut the cord” and deploy devices and apps to the field, device OEMs, integrators, and operators must go back and re-secure the entire software stack, which includes OS, device drivers, networking, middleware, and applications – tens of millions of lines of code. With so large a security challenge, it’s easy to see why mobile devices are subject to increasing number of exploits.

By contrast, SecureIT Mobile Enterprise builds on the underlying security and small, trusted computing base native to the OKL4 Microvisor.

Microkernel-Based Architecture

The OKL4 Microvisor is based on mature, high-performance microkernel technology. Using a microkernel assures that a bare minimum of code runs in privileged mode for a small trusted computing base. The simple, elegant architecture incorporates fine-grain access-control mechanisms which make OKL4 secure by design (not after the fact), and offers developers and integrators straightforward and secure mechanisms for sharing resources across domains, including device drivers and CODECs.

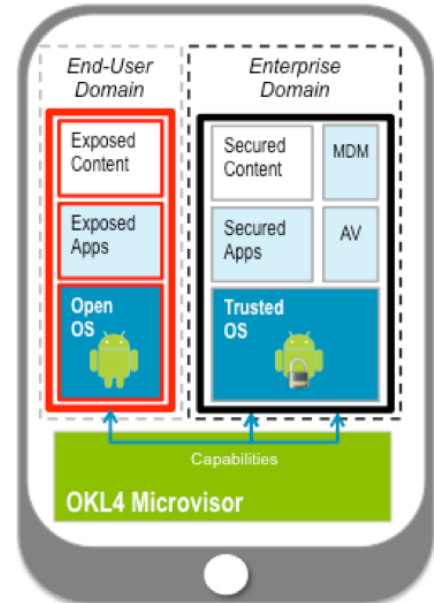


Figure 2: SecureIT Mobile Enterprise Software Architecture

Secure Enterprise Mobility

SecureIT Mobile Enterprise provides “hard” support for enterprise security policy by isolating and protecting:

- Sensitive files and databases
- Local and remote applications and servers
- Voice and text communications (SMS, etc.)
- AV and anti-malware software
- MDM and other agents for remote control and administration

Let’s examine what it actually means to provide this kind of protection:

Protecting Local and Upstream Assets

By isolating user and enterprise domains, SecureIT Mobile Enterprise keeps local and remote corporate assets safe from exploit. On the device, this provides a safe haven for business critical assets.

SecureIT Mobile Enterprise also protects upstream assets and infrastructure. “Golden Master” software, which includes all components and services that interact with company assets, is deployed within the enterprise domain, safe from malware and exploits emanating from the user domain (Figure 2.). Even if mobile users download and install apps containing viruses, spyware, or other compromised software, malware will be unable to access the enterprise domain and reach upstream to servers and gateways hosting enterprise data, services, and MDM solutions.

Protecting the Protectors

Earlier in this white paper, we noted that while helping to secure mobile devices, AV, MDM, and other security, administration and remote control software is itself subject to exploit (Figure 1.). By deploying “protectors” in a trusted enterprise domain, we can isolate it from threats emanating in user-downloaded software. From this secure position, AV software can scan both enterprise and user domains. Similarly, MDM can selectively manage applications and content in either or both spaces.

For even greater security, SecureIT Mobile Enterprise supports deploying AV, MDM, and other critical software in dedicated virtual machines. Microkernel-based OKL4 presents APIs to let developers leverage OKL4 lightweight execution environments, easing porting of today’s standalone software and facilitating future redeployment with other personal and enterprise software loads, including different OSes and apps.

Complementing Mobile Device Management

SecureIT Mobile Enterprise provides an enhanced foundation for MDM software, complementing – and sometimes exceeding – MDM functionality. Let’s review key MDM capabilities and how SecureIT Mobile can make them more secure and comprehensive:

Asset Tracking: SecureIT Mobile provides a secure execution environment for asset tracking software and device identification data. Location software runs far from the prying eyes of downloaded spyware and other exploits. Location information needed by mobile users (GPS data, location-based services, etc.) can be selectively and safely shared among enterprise and user domains.

Backup: From within the enterprise domain, business-critical data, applications and configuration data can be backed up securely to data center or Cloud-based storage with complete independence from operations in the user domain.

Device Wipe/Restore: In cases of device loss, theft, or changes in user employment status, MDM software can completely erase (and restore) data and apps contained within the enterprise domain. A user’s personal software and data are left intact. Devices essentially return to their pre-BYOD state and behavior.

FOTA: Firmware over the air is a capability present in many mobile devices, but is often under-utilized. Usually, provisioning and management software runs “beneath” mobile OSes, limiting FOTA visibility and granularity of access to software hosted on the OSes it helps to update and to the OSes themselves. With SecureIT Mobile Enterprise, FOTA agent software can host in a dedicated VM and more easily manage and update the contents of other VMs without the need for resource-sapping patching and padding.

Indeed, mobile virtualization also enables a new vision of VOTA (virtualization over-the-air), bootstrapping virtualization onto mobile devices and leveraging this key technology to update firmware, system software, and applications.

Troubleshooting and Diagnostics: With its ability to instance multiple virtual machines, OKL4-based SecureIT Mobile Enterprise makes the perfect host for diagnostic software. Software probes can be hosted alongside enterprise applications or occupy dedicated virtual machines.

Updates to OS and applications: SecureIT Mobile Enterprise helps to implement and mediate software update mechanisms. Updates to system software and business-critical applications can proceed apace in the enterprise domain without impacting operation of user domain apps, and vice-versa. Since each domain is implemented by unique virtual machines, each can also be rebooted without affecting the other.

Conclusion

This white paper illustrates how OK Labs SecureIT Mobile Enterprise upholds the three pillars of enterprise mobility – security, privacy and freedom – through use of mobile virtualization. It has examined the enterprise mobility challenge from multiple perspectives of enterprise management, enterprise IT, and mobile workers, and pointed to a new implementation path for this valuable paradigm.

Without SecureIT Mobile Enterprise:

- Enterprise security and management software restricts device capabilities that enhance user productivity
- Employees eschew company devices in favor of more private and flexible personal ones
- Bring Your Own Device (BYOD) is a non-starter, and enterprise mobility ROI falls short of expectations

With SecureIT Mobile Enterprise:

- Employees bring personal devices to work and happily let employers install enterprise mobility solutions without losing privacy or device functionality
- Enterprise security and management requirements are met
- Employers enjoy productivity gains by letting workers use software and services they want

If your organization is considering implementation of enterprise mobility, SecureIT Mobile Enterprise offers compelling benefits that ease rollout and improve ROI by:

- Preserving user privacy and freedom to fully use the capabilities of the device, enhancing enterprise mobility uptake and ROI
- Keeping malware and other exploits from reaching enterprise applications and data, on the phone and upstream in the Cloud and data center
- “Protecting the protectors,” keeping malware from degrading AV and MDM software
- Retaining valuable device and software capabilities to boost worker productivity
- Providing a security policy framework with OKL4 capabilities, offering fine-grained control over resource sharing and APIs (application programming interfaces) that cross between domains

Coming Soon to Handsets and Tablets

OK Labs is working closely with mobile device OEMs, integrators, mobile/wireless operators, and other ecosystem players to accelerate availability of the unique value and capabilities offered by SecureIT Mobile Enterprise. Let OK Labs sit down with you and your supply chain partners to find the shortest path to enterprise mobility for your organization.

To learn more, visit <http://www.ok-labs.com/>. You can also call us at +1-312-924-1445 or email us at info@ok-labs.com.