


May 31st, 10:30 AM

Facilitating Forensics in the Mobile Millennium through Proactive Enterprise Security

Andrew R. Scholnick
SNVC LC

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Scholnick, Andrew R., "Facilitating Forensics in the Mobile Millennium through Proactive Enterprise Security" (2012). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 9.
<https://commons.erau.edu/adfsl/2012/thursday/9>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



FACILITATING FORENSICS IN THE MOBILE MILLENNIUM THROUGH PROACTIVE ENTERPRISE SECURITY

Andrew R. Scholnick
SNVC LC

ABSTRACT

This work explores the impact of the emerging mobile communication device paradigm on the security-conscious enterprise, with regard to providing insights for proactive Information Assurance and facilitation of eventual Forensic analysis. Attention is given to technology evolution in the areas of best practices, attack vectors, software and hardware performance, access and activity monitoring, and architectural models.

Keywords: Forensics, enterprise security, mobile communication, best practices, attack vectors.

1. INTRODUCTION

The exploding popularity of smartphone technology has greatly outpaced related advancements in the area of information security. Exacerbating this problem is the fact that few organizations properly understand the new contexts in which security is (and is not) an applicable concern. As a result, many enterprises that should be concerned about the security posture of their smartphone device users are, in actuality, unknowingly at risk of being compromised. These evolutionary changes regarding communications technology have precipitated a need to rethink both the interrelationships and the distinguishing factors influencing information security in enterprise voice and data infrastructure. With ever-expanding functional capabilities and the ever increasing nuances they impose on information security models, a new way of thinking about enterprise security is needed. At a time when many traditional enterprise infrastructures are only now acclimating to models integrating internet presence and/or VOIP capabilities, and while they are still reeling to accommodate the emergence of social media concerns, the new breed of mobile devices which have emerged since the introduction of the iPhone and the iPad have shattered old paradigms for data protection by introducing entirely new methods for transporting and accessing data and data networks.

Paramount within the discussion of how data security issues have been impacted by these evolving technologies is an understanding of the significant paradigm shifts which are emerging in the digital and communications worlds. The still-embryonic emergence of personally-focused digital mobility, which is itself an outgrowth of changes in wireless communications capabilities, has triggered a fast and furious stream of innovations which are continuing to revolutionize how people think about their personal manner of interaction with all aspects digital technology, especially with regard to professional assets available from their employer's enterprise environments. Overall, the confusion surrounding rapid evolution in any technology arena often results in draconian posturing from the enterprise security community until such time as things become more 'sorted out'¹. This document attempts to identify the current primary areas of confusion surrounding secure adoption of mobile technology, and examines the impact of the current paradigm shifts on the enterprise by evaluating the security of both the underlying communications technologies in play and the resulting changes in access technologies being built to exploit their evolving capabilities. Working within the context of this paradigm shift, information assurance and enterprise security issues are considered and problems regarding the enablement of better and more informative forensic tools are discussed.

¹ Gallagher, Sean (2012), "Why the next 'ObamaBerry' might run Android or iOS", <http://arstechnica.com/business/news/2011/11/will-the-next-obamaberry-be-a-nexus-or-an-ipad.ars>, 28-JAN-2012

2. THE NEW PARADIGM

“What does it do?” This is a question which has probably greeted major advancements in technology since the invention of the wheel. The answers to this question can have profound implications in the realm of security. Nowhere is this truer than with the introduction of mobile phones into the enterprise environment. When first introduced, for example, one might have reasonably surmised that these devices were ‘just wireless phones’. As the technology evolved however, they quickly incorporated the basic functionality of pagers – an advance which has further evolved into the Simple Message Service (SMS) text messaging capability prevalent today. Further evolution of the devices allowed for the incorporation of cameras, geo-location technology, and practical computer-equivalent functionality. This evolutionary metamorphosis has introduced powerful technological changes which represent a considerable shift in the overall security posture of the mobile phone.

What was once a simple voice communication tool is now a powerful ‘Swiss army knife’ offering a wealth of ever increasing capabilities² with an ever broadening spectrum of potential points of compromise. In short, a potential nightmare for any organization concerned with information security. Unfortunately, the technological changes have been so pervasive, and adoption of the resulting computer powered multifunction portable communication technology (better known as ‘smartphone’ or ‘smart device’ technology) has occurred so rapidly, that accurate and appropriate identification of potential security risks has not kept up, resulting in a growing concern for impending crisis³.

2.1 An Evolutionary Shift

Key to understanding the shift in paradigms is a need to appreciate the factors driving modern-day technological change. Today’s workforce has learned that it is possible to have access to high quality business resources regardless of where they are, when they want it, or what type of device (desktop, laptop, tablet, or smartphone) they wish to use. Arguably, there are three primary categories of end-user demands which are contributing to the still-evolving technology solutions coming into prominence:

- Simplicity – easy to use, well integrated, interoperable
- Performance – high speed, full color, real time
- Comfort – safe to use, feels good, easy to access

The breakthroughs in communications technology represented by the new breed of mobile devices have fueled a headlong charge by innovators striving to create newer and better resources for a ravenous market. Resulting from this explosion of creative energy is a multifaceted shift in access paradigms, usage models, and interaction scenarios which are necessitating the rethink of outdated security practices⁴.

2.1.1 User Perception

At the heart of many current enterprise security problems is the rapidly emerging shift in social attitudes towards digital communication capabilities. Succinctly, the user community knows it is now possible to integrate everything needed for doing business into a single device they can carry with them at all times, and they want that greater flexibility and lower cost capability now. When combined with the rapidly changing technological environment, this ‘I want it now’ attitude

² Fei, Liang, (2012), “Mobile app market set for increased growth”, <http://www.globaltimes.cn/NEWS/tabid/99/ID/692610/Mobile-app-market-set-for-increased-growth-Gartner.aspx>, 29-JAN-2012

³ Thierer, Adam (2012), ‘Prophecies of Doom & the Politics of Fear in Cybersecurity Debates’, <http://techliberation.com/2011/08/08/prophecies-of-doom-the-politics-of-fear-in-cybersecurity-debates/>, 28-JAN-2012

⁴ Simple Security (2012), “Mobile security market in for exponential growth”, <http://www.simplysecurity.com/2011/09/30/mobile-security-market-in-for-exponential-growth/>, 31-JAN-2012

encourages potentially disastrous *snap judgment* decision-making which can result in impractical security models based on outmoded demand, usage, management, and maintenance models. Thus, the shifts in underlying communications technologies influencing this attitudinal progression embody many of the primary factors to consider when defining an appropriate way forward.

2.1.2 Tools and Resources

For most people, the dynamic shift in the function, performance, and scope of communication tools which is currently being experienced, can be summed up in two catch-phrases: social media and cloud computing. These two areas of influence dovetail beautifully with the perpetual enterprise-organization search to enhance collaboration and standardize capabilities. Therein lays the problem...

Powerful new technologies have already become ubiquitous for private use, and the modern worker is demanding that they be allowed as business resources too. Powerful new search engines make it easy to find data; but in most workplaces the user is still tied to the old-fashioned relational database. Amazing and versatile collaboration environments are popping up all over the internet facilitating geographically agnostic coordination and transfer of data among friends, classmates, families, job seekers, and gossips; yet the average team leader must continue to 'make do' with email (if lucky, with remote access), voicemail, conference rooms, and, where available, occasional access to a VPN connection or video conference. Yet talk of new file sharing and desktop virtualization services abound in the media, and 4G 'hotspots' are advertised at the local coffee shop. Meanwhile, at present, few or none of these innovative tools and resources is provided to the workforce effectively by their employment enterprise.

2.1.3 Boundary Changes

Who would have believed back in 2000 that security professionals in 2012 would look back at them, nostalgically thinking about how much simpler things were? What once were clearly defined borders for wire-line digital access and data-centric information security have morphed into a world of network-integrated real-time video feeds, geolocation, universal access, and terabyte pocket-drives. The combination of high-volume portability, target tracking, and unsecured endpoints has obsoleteed many formerly effective best practices, virtually overnight. Because of these changes, information believed to be well protected by firewalls and access controls is being found, with increasing frequency, to be exposed in previously unanticipated ways.

3. CONCERNS OF THE ENTERPRISE

Yesterday's designs for tomorrow's solutions must be rewritten today. Sufficient information exists to predict where infrastructure needs and technological capabilities are headed. Technology plans derived based on goals statements established prior to 2010 should be considered suspect and reviewed for necessary course-correction. Any such goals and plans derived prior to 2007 should be reassessed with even greater prejudice. Why? Two words – iPhone (introduced in 2007) and iPad (introduced in 2010). The introduction of these devices has revolutionized the way in which society views everything in both the personal and business communications realms. The explosive emergence of corresponding *open source* (Google Android) and proprietary (RIM Blackberry PlayBook) commercially viable technology in the same arena require a reassessment of the very meaning behind a concept like Enterprise Security. These new tools have redefined the framework upon which future-facing productive work environments must be built. By analyzing the nature of these changes it becomes possible to implement integrated proactive and reactive tools and architectures focused on affordably and effectively protecting the enterprise.

3.1 Problem Definition

Within today's multifaceted communications technology framework it has become necessary for security professionals to identify logical areas for conceptual delineation and use them to define appropriate methods for segmenting the overall security problem into more manageable pieces. This

section will identify three major areas of concern, and provide a high-level perspective for why they are applicable to protecting the enterprise environment.

3.1.1 Technology Trends

Perhaps the most significant advancements in technology impacting the integration of mobile device use with enterprise security models are the advent of both deployed 4G cellular networks, which offer access to greater bandwidth, and cool-running quad-core CPU technology⁵ for use at the heart of mobile devices. These advances present a ‘good news / bad news’ dichotomy to enterprise security professionals. The bad news is that we can now expect to see more sophisticated and powerful attacks against and through mobile devices (thanks to the CPU enhancements), and more damaging exfiltrations capitalizing on the higher bandwidth. The good news is that more complex and effective defenses are now possible, thanks also to the CPU and bandwidth enhancements.

3.1.2 Device Vulnerability

From an enterprise security standpoint, the most noteworthy threats represented by mobile devices stem from three primary attack vectors: eavesdropping, infection, and theft. All three of these risks are magnified by the lack of sufficient protection on mobile devices both through their operating systems and the applications they run. Insufficient security-focused device management and control options distress any enterprise operations team attempting to implement acceptable mobile device management (MDM) solutions while ineffective application marketplace quality controls facilitate unsuspecting installation of apps containing malware. Added to the already challenging problems presented by browser exploitations and popular document viewer and other third-party tool vulnerabilities⁶, the intricate problem of mitigating mobile device vulnerabilities can seem daunting.

3.1.3 Infrastructure Vulnerability

Depending upon specifics of the enterprise architecture, additional aspects of two attack vectors, eavesdropping and infection, may exist. Again, the problem stems from insufficient security-focused device management and control options available in device operating systems and resulting failures presented by the diversity of MDM solutions currently available.

3.2 Understanding Protection Issues

The primary issues regarding protection of enterprise environments without impeding use of mobile technology result from the intersection of two questions: what type of access does the user need (the access model) and what will happen to the data being accessed (the usage model). By understanding the answers to these questions, many of the necessary steps for providing effectual mitigations and for facilitating development and implementation of responsive and dynamic forensics tools become self-evident. With this information in hand it is subsequently possible to define effective and comprehensive security architectures for the modern enterprise.

3.2.1 Access Models

As identified earlier in this work, recent advances in technology are fueling the already explosive evolution and adoption of mobile technologies in ways that are significantly impacting worker perspectives and expectations. Consider, for example, that less than a decade ago the VPN was generally considered to be an enterprise-level tool. Utilizing them to provide personal access into an enterprise environment was deemed inappropriate for the vast majority of individual workers. In fact, few workers actually requested such capabilities from their employers because the tools and network

⁵ Purewal, Sarah Jacobsson (2012), “Nvidia Quad Core Mobile Processors Coming in August”, http://www.pcworld.com/article/219768/nvidia_quad_core_mobile_processors_coming_in_august.html, 30-JAN-2012

⁶ Quirolgico, Steve, Voas, Jeffrey and Kuhn, Rick (2011), “Vetting Mobile Apps”, Published by the IEEE Computer Society, JUL/AUG 2011

connectivity required to properly utilize such access were prohibitively expensive. Even when costs were not a major factor and where the enterprise environment supported such access, the personal equipment and home connectivity used to exploit such access was often ponderously slow, rendering it undesirable to many. In light of existing technology improvements, as well as looming exponential performance leaps, this entire paradigm has become invalid.

Within the same span of time, technologies have emerged which allow an attacker to target resources that were previously seen as well-protected. Email servers, customer service portals, limited access kiosks, and other common tools and utilities have been, and continue to be, successfully compromised by direct and indirect attack. Similarly, techniques believed sufficient to protect the data flowing to an endpoint believed to be secure have proven to be just as lacking in veracity. Successful attacks against cryptographic keys, security and authentication certificates, and even the protocols that utilize them have been repeatedly in the news and recounted at numerous technical conferences. Introduction of mobile device capabilities require that formerly improbable attack vectors be reevaluated and mitigations and protections identified for use.

It should also be noted that the primary access models discussed below are generally used in combination, to provide a form of *defense-in-depth*, by layering the overall security model. Thus, while requiring a password for user authentication provides a degree of protection, collecting the password from the user through an encrypted envelope (like an SSL tunnel) is even better. In fact, encrypting the password before passing it through the tunnel can enhance protection of the authentication credential even further.

3.2.1.1 Authentication

Arguably the oldest and most prominent access model used for computer security is password authentication, where a secret is held by the user and shared with a system or application to gain access. While more complex authenticators have evolved over the years (such as time-sensitive and out-of-band tokens, biometric sensors, physical authentication credentials, and digital certificates), the basic principle of this access model is that users must authenticate themselves to the system using theoretically unimpeachable credentials such as one or more shared secret and/or dynamic authenticators. The degree of *geographic independence* obtainable through introduction of mobile technology to enterprise environments can severely upset the dependability of many, previously trusted authenticators. Biometrics, for example, is virtually useless as a remote authenticator since the assurance they provide as an authenticator is tied to physical presence. A security model that considers accepting them remotely risks introduction of attack possibilities based on credential counterfeiting and hijacking which would otherwise have been improbable or impossible within an enterprise infrastructure. Similar issues exist for physical keying devices, such as DoD CAC and PIV cards because their authentication data is static, and could thus be intercepted in transit, bypassing the need to authenticate to their embedded credentialing.

3.2.1.2 Protective Tunneling of Data in Transit

Without straying into a lengthy discussion of the ultimate ineffectiveness of existing computer encryption techniques, it should be taken as historically axiomatic that as computing power increases, even the best encryption algorithms eventually get cracked. Since all data tunneling protocols rely on some form of computer based encryption (such as SSL, TLS, and various VPN technologies) it must be accepted that, until encryption technology becomes significantly advanced beyond current designs, this particular weakness will be an ongoing threat. Fortunately, the evolution of more sophisticated algorithms has effectively mitigated this risk until now. However, the protocols and underlying software engines which are utilized to incorporate encryption into their various protection schemes have, themselves, proven to be unnervingly susceptible to attack. (This particular threat vector is a lingering and well-discussed security issue with impact beyond the direct scope of this work.)

Many infrastructure analysts believe that this lingering issue for securely moving data between mobile device users and the enterprise at the back end is effectively solved by use of VPN technology. With the advent of convenient, acceptable-performance mobile VPN technology rapidly cresting the horizon, it therefore might appear that satisfactory protection for corporate connectivity is at hand. This is a false perception.

The manner in which all current mobile device operating systems implement network support for VPN connectivity has a gaping security hole in it. This hole is a *feature* often referred to as ‘split tunneling’. This feature of mobile devices neglects to perform a function deemed essential to the default functioning of their larger computer cousins – routing all network traffic to the created VPN tunnel unless explicitly instructed otherwise, through overrides to configuration defaults. In order to address this specific problem, enterprise implementers must be able to alter the configured functionality of the mobile device OS, until such time as device OS vendors begin incorporating better enterprise-level security tools into their systems. While problematic but conceivable for open source systems such as Google’s Android OS, only a cooperative vendor can mitigate this risk with their proprietary operating systems, such as Apple, Microsoft, and Research In Motion (RIM).

3.2.1.3 Misdirection and Brute Force

Perhaps the conceptually simplest group of protective access models involves both active and passive techniques for hiding in plain sight and for manual inspection and validation. Often clustered together under the banners of *firewalling* and *intrusion detection* these techniques involve brute-force processing of flowing data, occasionally requiring collaboration from endpoint systems and software. For instance, while firewalling is largely about restricting the flow of data based on one or more elements of network addressing, many network services (such as email, web servers, and VPNs) allow the system administrator to modify a key component of addressing – the logical access port. While requiring configurations changes at the enterprise back-end as well as on the users’ endpoint devices, this misdirection can be exploited to provide a degree of camouflage to services provided for remote access. In recent years this capability has become ubiquitous and can be found in many home wireless technologies. On the ‘down side’, support for port reassignment on mobile devices is limited to individual application-specific implementation. On the ‘up side’, app-level support for port reassignment is prominent enough that it remains a useful tool for evolving enterprise environments.

Strictly the providence of back-end infrastructure, manual inspection and validation of moving data presents an interesting conundrum for enterprise security. While malware and intrusion detection systems based on this principle can prove to be extremely effective, they are not only costly, but also may be defeated by some of the very-same tools used with the intent of protecting the enterprise. After all, you cannot detect and protect against threats you cannot see, and SSL, TLS, VPNs, and other encryption-based technologies can prevent brute-force data traffic inspection tools from ever seeing the threat. The thoughtful enterprise administrator may mitigate this failing by employing malware and threat detection tools on their deployed desktop, laptop, and server systems, but comparable technologies for mobile devices are still in their infancy and provide little, if any, real protection.

3.2.2 Usage Models

While there are many variations of usage models for systems and data, when discussing the paradigm shift in enterprise security being caused by advances in mobile device technology, only two broad-brush usage models are pertinent: securely accessing data and securely storing data. Although valid arguments can be made for the use of application-level security models for mildly sensitive data, the corresponding overhead involved in providing secondary protections and tracking user-specific access contexts quickly becomes unmanageable. For this reason, these two usage models are discussed as systemic models applicable to enterprise security, rather than application level models. Stemming in large part from the lack of sufficient security-focused functionality available from mobile device operating systems, addressing these two areas of concern is often perceived to be either prohibitively

costly or completely out of reach.

Continuing to avoid straying into a lengthy discussion of the inherent risks in using existing computer encryption techniques, it should be duly noted that issues regarding the ultimate failings of modern computer encryption implicitly complicates any discussion of how to protect data while in use and at rest. However, modern encryption tools can invariably slow attackers down and should therefore be utilized wherever and whenever available.

3.2.2.1 Data at Rest

Obviously there is a need to protect valuable enterprise data intended for local storage on a mobile device. Even when available, because not all mobile device operating systems provide native support for file encryption, provision for encryption of stored data is generally difficult to access and may interfere with application functionality, device performance, and data portability. Also, when implemented, effective enterprise employment of this capability can be impeded by those manufacturers desiring to ‘protect the user experience’ by allowing dangerous manual overrides. Further compounding the risk, should the security posture of the mobile device operating system become compromised, enterprise-sensitive security keys could be revealed to malicious parties.

Make no mistake, if a device is lost or stolen then the information on it could eventually be seen by undesirable viewers. Only through use of the most current and strongest encryption systems can this eventuality be delayed.

3.2.2.2 Data in Use

Probably the most serious inherent threat to the enterprise security posture of a mobile device operating system that has unfiltered, unprotected access to the internet is that the operating system may become unknowingly compromised through ‘drive by’ attacks from websites, side-channel exploitations, or malicious attachments to non-enterprise email messages. Although most mobile device operating systems provide a system-enforced isolation between running applications, once the OS is compromised this protection is easily circumvented by malware. Malicious tools such as key-loggers, screen-grabbers, and memory scrapers are then employed to acquire seemingly protected enterprise data. Thus providing some form of enterprise-level protection to the mobile device operating system from internet-based attack becomes a critical element of ensuring protection of data in use, a logical association necessitated specifically by the advent of mobile device technology.

4. ENHANCING PROACTIVE DEFENSE AND EVIDENTIARY DISCOVERY

In the evolving universe of cyberspace, counterattack is not an option – it is illegal. This leaves mitigation (proactive defense) and forensics (evidentiary discovery) as the primary weapons for protecting enterprise security. Without adequate enabling enterprise-centric tools, effective enterprise security is nearly impossible. Comprehensively unaddressed until recently, strategies and tools for effectively protecting the enterprise while enabling seeming unrestricted use of mobile technology is finally beginning to emerge. This section will discuss several of the most promising of these advancements and provide practical examples for deployment and use in the enterprise environment. Incorporating device-level technologies, back-end control tools and techniques, and supplemental enhancing services, these innovations present realistic solutions that are available to the enterprise security administrator right now.

4.1 Device Ownership

The core principle behind many, sometimes draconian, enterprise security policies is a simple one: “If we don’t *own* it, we can’t trust it”. Therein lays the riddle... how to take ownership of a user’s mobile device without argument, anxiety, and legal malediction? Although the obvious simple solution is to provide a separate enterprise-use device, another viable answer is to manage perceptions so that enterprise ‘assimilation’ of a personal device is perceived to be of benefit to the user. New technologies are emerging which allow this assimilation at little or no additional cost to the enterprise,

which can provide their users with a variety of services including:

- Automated secure backup of all device data
 - Including assurance of secure and private handling of personal assets.
- An unfettered ‘sandbox’ for personal use
 - With less restrictive protections still available from corporate firewalls and filters
- One device supporting personal and business phone numbers
 - Shared number or unique⁷
- Access to all the tools and resources they have been begging for
 - Online files, intranet, collaboration tools, search engines, video and teleconferencing, etc.
- Company-paid phone service⁸
 - Much less expensive than many people think, competitive with existing phone systems
- Eliminate phone-carrier bloat-ware on the phones
 - Only enterprise-vetted apps are allowed in the device’s protected enterprise section

It should be stressed that there already exist practical, cost-effective, secure options for providing these benefits to mobile device users who need access to enterprise attachments and resources. Central to all of them is the need to address security limitations imposed by the device operating system. This is why the enterprise must *own* the device. The cornerstone of any effective mobile device enabled enterprise security architecture is the ability to rely on the security posture of the endpoint device. A key component for one such solution is available today for free, courtesy of the NSA. As of January 2012, the NSA has made available a Security Enhanced (SE) version of the Android operating system⁹ for open use, and is planning widespread adoption within the agency itself¹⁰. This phone operating system even boasts support from a comprehensive security compliance monitoring and management tool. The resulting OS-level improvement in encryption, security policy enforcement, compromise detection, and overall device control represents a solution for the problem upon which all other significant resolutions depend.

That was the good news. The bad news is that, at present, each of the remaining primary *non-Android* device OS providers cannot, or explicitly will not, currently support many or all of these requirements. For this reason, the majority of solutions possible today are Android-centric. Within the remainder of this Device Ownership discussion, unless otherwise explicitly noted, the solutions referenced should be considered specific to the Android universe for this reason.

⁷ There are several options including VoIP clients such as Skype and OoVoo, or number consolidation platforms like Ribbit, Phonebooth, and GoogleVoice.

⁸ Gray, Benjamin; Kane, Christian (2011), “10 Lessons Learned From Early Adopters Of Mobile Device management Solutions”, Forrester Research, Inc., Cambridge, MA

⁹ Naraine, Ryan (2012), “NSA releases security-enhanced Android OS”, <http://www.zdnet.com/blog/security/nsa-releases-security-enhanced-android-os/10108>, 29-JAN-2012

¹⁰ Hoover, Nicholas (2012), “National Security Agency Plans Smartphone Adoption”, <http://www.informationweek.com/news/government/mobile/232600238>, 05-FEB-2012

4.1.1.1 Mobile Device Management (MDM) and Mobile Risk Management (MRM)

The core of any device's enhanced forensic potential, regardless of OS, will center on the availability of more comprehensive monitoring and tracking capabilities both inside the device and at the back end. For this reason available management tools should be closely scrutinized before an enterprise decides on which vendor's product will be selected to provide this capability.

Although still somewhat lacking in effective security control features, because of various OS limitations, several MDM vendors are rumored to already be implementing support for the NSA's SE Android OS¹¹. Until these products begin to appear, one MRM solution provider, Fixmo¹², already offers support for an OS-integrated monitoring and management solution comprehensive enough to have been deemed acceptable for Sensitive But Unclassified (SBU) use with DoD resources. Among this solution's features are the ability to monitor, track, and control various device characteristics, provide enhanced app security controls, sandboxing, FIPS-certified cryptography, control device resources (camera, radios, etc.), and handle overall device security policy management, compliance monitoring, and control. This product also provides comparable capabilities, where possible, for Apple iOS, and RIM Blackberry as well as integrated features supporting Good Technology secure enterprise email apps. It should be noted that several other vendors, such as 3LM, BoxTone, and AirWatch, have voiced plans to improve their support for enterprise security in ways which would provide comparable functionality, but in most cases delivery dates have not yet been specified.

4.1.1.2 Mandatory Boot-Time Captive Tunnel (A Truly Secure VPN)

Just as MDM/MRM capabilities are at the core of a device's forensic potential, a 'mandatory VPN' is at the center of any manageable device protection solution. The reason for this is straightforward; if the device must connect to the enterprise VPN before it can touch the internet, then all of the enterprise's existing investment in network-level infrastructure protections can be brought to bear to protect browsing, email, and other network communications without unduly jeopardizing the existing enterprise security posture. In this way the enterprise can also monitor and control access to apps, weather through redirection to an enterprise-run 'app store', monitoring of installable apps as content, or outright blocking of access to non-enterprise app resources. While this capability is not currently supported or allowed by any major cellular carrier, there is a way around them. This leads us to the discussion of the Mobile Virtual Network Operator...

4.1.1.3 Mobile Virtual Network Operator (MVNO) Hosting

Although possessing a secure device operating system and the management tools to control it are critical, they are of no value if the enterprise administrator cannot use them on a device. Since existing cellular carriers currently do not support enterprise customization of the device OS in the manner needed to support these needs, a way must be identified for obtaining affordable service for enterprise devices which does permit use of an enterprise-customized OS. This is where the concept of an MVNO becomes important, and the distinction for the enterprise between 'owning' the MVNO and having it 'hosted'.

The simplest way to understand what an MVNO is and why it is important would be to think of them as a mobile communications carrier who does not actually own any cellular towers. Instead, an MVNO purchases bandwidth from other carriers at a discount and resells it under their own brand. Cricket Wireless is an example of an MVNO. Realizing the potential value of supporting enterprise infrastructure with this technology, companies such as CDS Telecommunications of Ashburn Virginia¹³ have begun packaging hosted services tailored toward providing this secure architectural solution to the market. By enabling the enterprise itself to act as a cellular service provider with

¹¹ Project website: <http://selinuxproject.org/page/SEAndroid>

¹² Company website: <http://www.fixmo.com/>

¹³ Corporate website: <http://www.CDSTelecom.com>

competitive rates, the MVNO solution gives the enterprise the ability to lock their mobile operating system and device management infrastructure into the ‘subscribing’ device – controlling all aspects of data flow, call monitoring, security, and even application availability and installation. By using a hosted source of their MVNO activity, the enterprise gains the advantages of high bandwidth utilization from the primary carrier, resulting in lower overall rates for connectivity. Also, rather than needing to customize the Android OS themselves, or purchase MDM/MRM licenses in limited volumes, the MVNO host would bear the burden of providing and maintaining the modified OS and passing through high volume licensing and sublicensing discounts for the preferred management tools.

4.2 Application Management

Having established the preferred infrastructure necessary to support Device Ownership, it is now appropriate do discuss a variety of enhanced Application Management capabilities which can allow the enterprise to further protect itself from malicious or risky device software (a.k.a. apps) without the need for burdensome resource allocations. By exploiting the various app and resource monitoring capabilities made possible through a comprehensive MRM solution, not only does on-device enforcement of user and app compliance with enterprise security policies becomes possible, but the ability to collect and monitor more comprehensive data for forensic use at the back-end is also enhanced.

4.2.1 Vetting

The most monumental conundrum accompanying the introduction of mobile device support into any enterprise ecosystem is how to establish weather apps abide with the enterprise security posture before they are installed and without unduly impeding the user’s access. With over 400,000 apps available directly through Google’s Android Market and over half a million currently available in the Apple App Store¹⁴, and annual growth expected to be counted for both in the hundreds of thousands this year, keeping pace with the need to establish the acceptability of desirable apps has already far exceeded the reasonable limit for manual inspection. Further, since an overwhelming number of these apps unnecessarily or inappropriately demand access to resources, both on-device and off, that the enterprise would rather restrict, the already difficult management task can seem intimidating in its vastness. As luck would have it, there already exist a few time and cost effective solutions for mitigating theses difficulties, and many vendors are promising that more are in the works.

4.2.1.1. Eyes-On

Although still an imperfect solution, nothing beats eyes-on inspection of source code performed by a well-trained vulnerability analyst when evaluating an application for safety and security. However, being somewhat time-consuming and labor intensive, this method of vetting software for enterprise use quickly becomes cost-prohibitive for any small enterprise environment. Even for a large and well-funded security team, utilizing eyes-on inspection would be viable only for the most highly suspect mobile applications whose functionality was deemed essential. Third party organizations exist, such as VeriSign’s iDefense team, which can be contracted to provide some of the industry’s best talent for this purpose, but this type of service comes at a high dollar cost and, as such, is likely only to be employed by very large enterprises and MVNO Hosting services.

4.2.1.2 Automation

The field of apps available for mobile devices is already tremendous and is expanding with increasing rapidity. Only an automated evaluation system can be expected to effectively handle the constant onslaught, not to mention the backlog, of available mobile device apps. An obvious solution, almost no effort has been expended in this area to-date. The key word here is ‘almost’. In a February 2012

¹⁴ Fitchard, Kevin, (2012), “Android development speeds up: Market tops 400,000 apps”, <http://www.abiresearch.com/press/3799-Android+Overtakes+Apple+with+44%25+Worldwide+Share+of+Mobile+App+Downloads>, 20-JAN-2012

article¹⁵, CNN reported that Professor Angelos Stavrou of George Mason University has designed such an automated vetting system for the US Government, and it has already churned through over 200,000 of the apps in the Android backlog over the past few months. Kryptowire, a company formed early in 2011 by Professor Stavrou, is preparing to launch a version of this tool for public use sometime in the first half of 2012, as well as some eyes-on vetting services.

4.2.2 Access Control

In the world of mobile devices, the term ‘access control’ (AC) has three connotations. The obvious and most common understanding of the term refers to the ability to moderate access to the functionality of the device itself, for example - by setting a device password for all activity other than answering an incoming call. Additionally, this term refers to the ability to control the permissions which each app installed on the device receives for accessing device resources, such as a camera, local storage, radios, and audio I/O resources. Lastly, AC refers to the ability to regulate the manner in which the device and its apps connect with Internet resources. It is this last area which is most problematic when attempting to define a secure enterprise usage model, in part due to previously discussed Secure VPN concerns. In all of these areas, appropriate on-device (in the OS and the apps) and back-end logging of historical data is imperative to support enterprise forensic needs.

4.2.2.1 Logging On

Perhaps the only area of mobile device security which has been addressed to an adequate degree by existing technology regards device-level access controls. Although there is certainly room for improvement, multiple technologies providing user authentication are available which offer features including:

- Remote-controlled access revocation
- Password retry limits
- Password complexity
- Password aging
- External credentials (CAC/PIV)
- Check-in timers requiring periodic back-end connection

to name a few. In most cases, these solutions provide both on-device and back-end monitoring and management capabilities which are even adequate for use in highly sensitive environments.

4.2.2.2 Device Resources

Of all the mobile device manufacturers participating in today’s marketplace, Apple stands out as the singularly worst prepared for enterprise use when considering the ability to mandate access controls from the back-end. Although a limited degree of control is possible through the use of their access policy mechanism, the device user has the ability to ignore policies without detection. More thorough controls are available for the three other major players, RIM (Blackberry), Google (Android), and Microsoft (WinMobile). However, additional controls are still necessary. For example, the ability for an enterprise to require high-level encryption for stored data, restrict or allow specific Bluetooth devices, and to control access to the device microphone, camera, and GPS on an app-specific basis is only available to a limited degree. The previously mentioned MDR solution from Fixmo is, arguably, the best example of an existing product which addresses this need, pushing available controls to their limit regarding each of the four primary device OS manufacturers. It is also worth noting that in late

¹⁵ Milian, Mark (2012), “U.S. government, military to get secure Android phones”, <http://www.cnn.com/2012/02/03/tech/mobile/government-android-phones/index.html>, 03-FEB-2012

2011 Dell announced a secure version of its Streak device which was secure enough to be deemed acceptable for some uses within the DoD.

4.2.2.3 Network Virtualization Facts and Fallacies

With regard to access control, the question how to safely provide enterprise users with the ability to access the back-end network infrastructure may be the most misunderstood. Earlier in this work the need to ‘own’ the device OS was discussed. Nowhere is the justification for this requirement clearer than with regard to implementing mobile device access strategies for virtual private network connectivity. The defining logic is simple, if an attacker has a path to the OS that does not force data to travel through ‘industrial strength’ protection systems then the device’s integrity cannot be guaranteed. If the device’s integrity is in question, then the security provided by the VPN must also be suspect. As described previously, utilizing a MVNO architecture mitigates the problem of device trustworthiness. Without such an architecture, no aspect of VPN authentication from a mobile device can be considered safe from compromise.

5. CONCLUSION

The introduction of mobile device technology into enterprises creates a multitude of new problems for security professionals. What were once simple voice communication tools are now powerful multifaceted devices offering a multitude of ever increasing capabilities with an ever broadening spectrum of potential points of compromise. These new tools have redefined the very framework upon which modern work environments are being built. This metamorphosis has resulted in the introduction of powerful technological changes which represent a considerable shift in the overall security posture of the mobile phone, a potential nightmare for any organization concerned with information security. In short, the exploding popularity of smartphone technology has greatly outpaced the ability of many enterprises to update their security infrastructure.

Emerging technology is rapidly making its way to market which greatly enhances the enterprise security posture and provides data monitoring and collection capability to enhance management activity and proactively support potential forensic needs. Affordable commercial solutions, which provide Government and Military grade protections, are emerging in today’s marketplace which greatly enhance the ability of businesses, small and large, to achieve an acceptable security posture supporting integrated use of mobile device resources.

6. ACKNOWLEDGEMENTS

Technology inputs from Professor Angelos Stavrou (George Mason University), Mr. Rick Segal (Fixmo), and Dr. Mark Gaborik (DoD) are gratefully acknowledged as contributing factors to this work.

7. AUTHOR BIOGRAPHY

A subject matter expert at SNVC LC, Andrew Scholnick is a cyber security professional with over 30 years experience in the field. In his most recent position as a technical team leader for the US Army, he guided the efforts of vendor, DoD, and government contributors through the integration of technologies which resulted in DoD approval for the first off-the-shelf Android smartphone solution allowed for Army use. He has previously headed the VeriSign iDefense Vulnerability Analysis Lab and was one of the principle technology innovators who securely connected AOL to the internet.

8. REFERENCES

Fei, Liang, (2012), “Mobile app market set for increased growth”, <http://www.globaltimes.cn/NEWS/tabid/99/ID/692610/Mobile-app-market-set-for-increased-growth-Gartner.aspx>, 29-JAN-2012

- Fitchard, Kevin, (2012), “Android development speeds up: Market tops 400,000 apps”, <http://www.abiresearch.com/press/3799-Android+Overtakes+Apple+with+44%25+Worldwide+Share+of+Mobile+App+Downloads>, 20-JAN-2012
- Gallagher, Sean (2012), “Why the next ‘ObamaBerry’ might run Android or iOS”, <http://arstechnica.com/business/news/2011/11/will-the-next-obamaberry-be-a-nexus-or-an-ipad.ars>, 28-JAN-2012
- Gray, Benjamin; Kane, Christian (2011), “10 Lessons Learned From Early Adopters Of Mobile Device management Solutions”, Forrester Research, Inc., Cambridge, MA
- Hoover, Nicholas (2012), “National Security Agency Plans Smartphone Adoption”, <http://www.informationweek.com/news/government/mobile/232600238>, 05-FEB-2012
- Milian, Mark (2012), “U.S. government, military to get secure Android phones”, <http://www.cnn.com/2012/02/03/tech/mobile/government-android-phones/index.html> , 03-FEB-2012
- Naraine, Ryan (2012), “NSA releases security-enhanced Android OS”, <http://www.zdnet.com/blog/security/nsa-releases-security-enhanced-android-os/10108>
- Purewal, Sarah Jacobsson (2012), “Nvidia Quad Core Mobile Processors Coming in August”, http://www.pcworld.com/article/219768/nvidia_quad_core_mobile_processors_coming_in_august.html, 30-JAN-2012
- Quirolgico, Steve, Voas, Jeffrey and Kuhn, Rick (2011), “Vetting Mobile Apps”, Published by the IEEE Computer Society, JUL/AUG 2011
- Simple Security (2012), “Mobile security market in for exponential growth”, <http://www.simplysecurity.com/2011/09/30/mobile-security-market-in-for-exponential-growth/>, 31-JAN-2012
- Thierer, Adam (2012), ‘Prophecies of Doom & the Politics of Fear in Cybersecurity Debates’, <http://techliberation.com/2011/08/08/prophecies-of-doom-the-politics-of-fear-in-cybersecurity-debates/>, 28-JAN-2012

