Information Assurance Impacts of Mobile Architecture in a Training System

Graham Fleener
U.S. Army PEO STRI
Orlando, FL
graham.fleener@us.army.mil

Andrew Maxon
Cybernet Systems Corporation
Orlando, FL
amaxon@cybernet.com

ABSTRACT

Training systems can benefit enormously with the integration of mobile architecture into the accreditation boundary as Warfighters are immediately familiar with the user interface. This enables the system developer to tap into a wealth of built-in functionality that would otherwise take years to develop. One of the latest Information Assurance (IA) challenges training systems face in today's continually evolving cyber threat environment is the secure integration of mobile architecture to ensure the continued protection of data and adherence with constantly evolving regulations. Our paper will discuss the significant issues Government Project Managers (PM) now face integrating mobile architecture into their initial system designs, as well as Configuration Management and Information Assurance Vulnerability Management (IAVM) processes.

We will address the many IA issues to integrating a mobile architecture in a training system to include technical security challenges, current and expanding IA requirements, industry best practices and using a risk management approach to ensure the system successfully completes the Certification and Accreditation (C&A) process and receives an Authorization to Operate (ATO). We will outline the numerous IA requirements currently governing mobile architecture, and the upcoming requirements DoD is proposing for the future.

To better train the Warfighter, industry and Government are rapidly progressing with the innovation that mobile architecture facilitates, enabling solutions that previously would never be possible. IA requirements and solutions must keep pace with innovation to ensure the way in which we train and fight is protected and secure. Finally, we will discuss a number of use cases within training and simulation systems that are currently undergoing the process of integrating mobile architecture into their accreditation boundary and lessons learned from those use cases.

ABOUT THE AUTHORS

Mr. Graham Fleener is the IA Manager (IAM) for Project Manager of Training Devices (PM TRADE) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Fleener served in the U.S. Marine Corps and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee. Mr. Fleener obtained both his Project Management Professional (PMP®) and Certified Information Systems Security Professional (CISSP®) certifications. Mr. Fleener holds a Bachelor of Science in Information Systems Technology from the University of Central Florida.

Mr. Andrew Maxon is the IA Division Technical Manager for Cybernet Systems. He holds a Bachelor of Science in Information Systems Technology from the University of Central Florida, with a focus in Network Security and has multiple industry certifications including the CompTIA Security +. He has certified and accredited numerous training and simulation systems for the U.S. Army, U.S. Navy, U.S. Marine Corp, and is currently Cybernet's Lead Security Engineer for the U.S Navy Littoral Combat Ship Shore Based Trainer.

Information Assurance Impacts of Mobile Architecture in a Training System

Graham Fleener
U.S. Army PEO STRI
Orlando, FL
graham.fleener@us.army.mil

Andrew Maxon
Cybernet Systems Corporation
Orlando, FL
amaxon@cybernet.com

MOBILE ARCHITECTURE DEFINED

Mobile architecture is defined as the culmination of mobile devices, mobile applications, and supporting infrastructure to create a feature rich and secure user experience. The Department of Defense (DoD) has strived to ensure mobile devices, mobile applications and the supporting infrastructure are a top Information Technology acquisition priority. Consumerization has given momentum to the expectation of having the same convenience and functionality for work as users have in their personal lives. The use of mobile devices including smartphones and tablets by military and civilian employees increases each year. The training and simulation community has responded to users by initiating a number of innovative mobile architecture pilot programs. Examples include incorporating mobile architecture into range target controllers and Combat Trainer (CT) mobile devices. Additionally, many training systems are incorporating mobile devices for real time After Action Reviews (AAR).

One of the primary challenges for implementing mobile architecture is ensuring it is securely configured in accordance with Information Assurance (IA) regulations. This would include ensuring the system has the ability to go through the DoD IA Certification and Accreditation Process (DIACAP) to successfully achieve an Authorization To Operate (ATO). Within the training and simulation community, a subsequent challenge is to securely implement mobile architecture in a special purpose system designed for a unique training requirement. The necessity to balance operational need versus security is never more prevalent than within the mobile architecture framework.

As a migration to mobile architecture presents numerous exciting innovations, with it comes countless numbers of vulnerabilities and threats. This paper will document and explore a number of threats emerging with the implementation of mobile architecture. Gaining a thorough understanding of the risks and threats involved with the push to mobile will aid in making sound choices prior to integration.

This paper will demonstrate traceability to DoD Instruction (DoDI) 8500.2 IA controls in an effort to document and gain visibility to the existing IA controls that will be governing mobile architecture. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), Interim Security Configuration Guides (ISCG), and Security Requirements Guides (SRG) pertaining to mobile architecture will be referenced and discussed to provide an understanding of the mobile security model being established by DISA.

This paper will present and discuss case studies of mobile architecture within the training and simulation community. Live training has a number of potential use cases in the earliest stages of implementation. A number of requirements are emerging that could be best met with the incorporation of mobile architecture.

Current commercial industry best practices and security features inherent to mobile architecture will be discussed and outlined. This paper will provide an in depth description of each layer of security necessary to ensure a holistic approach to mobile architecture security is achieved. When considering the defense in depth approach to securing the mobile architecture ecosystem, there are a number of layers that must be addressed. These layers include ensuring IA is proactively implemented on the device, the data, the applications, the network, and the cloud.

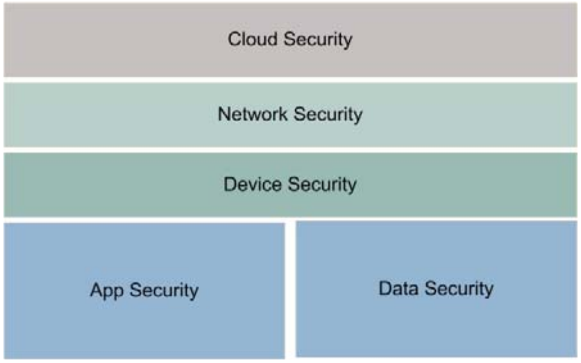


Figure 1. Defense in Depth Approach to Mobile Architecture

Figure 1 above identifies each layer of the defense in depth approach to mobile architecture. This paper will conclude with solutions and processes that can be used to ensure mobile architecture is integrated into DoD training and simulation systems in a prudent and secure manner. A focus on user education and proper mobile architecture management will be presented with key takeaways to be used on current and future programs.

MOBILE ARCHITECTURE CYBER SECURITY THREATS

The threats associated with mobile architecture are continually expanding, and research has shown mobile users are actually more susceptible to attacks than their desktop counterparts. For example, mobile users are three times more susceptible to fall for phishing attacks than their desktop user counterparts. A number of reasons serve as possibilities to explain the additional risks associated with mobile architecture. Most notably is the visual difference in the graphical user interface (GUI) as compared to the desktop interface. The lack of visual feedback, such as a mouse over showing the uniform resource locator (URL), limits the user's ability to identify a phishing attack. See Figure 2 depicting the dramatic increase in known mobile operating system (OS) exploits in the past six years.

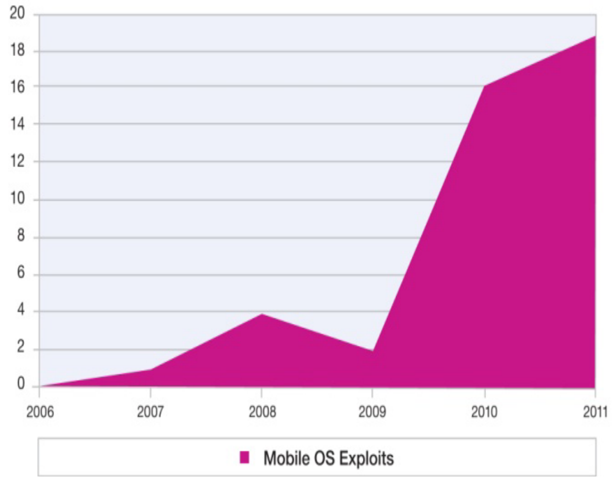


Figure 2. Mobile OS Exploits 2006-2011

A number of recent studies have emerged documenting the lack of user experience with protecting mobile data. For example, a recent study conducted by the National Cyber Security Alliance reported, "75% of nearly 1,200 American mobile users polled said they are aware of threats to their devices, as well as data they access and store. Seventy percent of respondents said they have some type of data security measures or solutions embedded in their devices, but only 50% could name the specific type of security they have. Another 58% said they don't know enough about threats to decide whether or not they should implement a security solution." A January 2012 survey of IT professionals conducted by Dimensional Research documented, "many organizations blame mobile device use directly for increased security issues. Seventy-one percent of respondents to the Dimensional poll said the growth in security events they have suffered during the past two years correlates with increased smartphone and tablet use. Another 78% of respondents said the number of devices in use at their companies has at least doubled during this time period." As these studies have shown, there is a significant amount of work ahead to educate and change the corporate culture to protect mobile data.

Malware on mobile OS's are continuing to increase with many experts reporting the Android® platform leading in the number of exploits. Apple® maintains rigorous vertical control of their platform to include a strict code review process. Additionally, developers publishing apps for Apple must reveal their actual identity which is thoroughly validated by Apple.

Lost and stolen devices are an additional risk associated with mobile architecture. With the increased operational tempo of today's Warfighter, the risk of losing a mobile device must be accounted for in a mobile security management plan. A number of technical controls and features of a Mobile Device Management (MDM) software suite can address the loss of a mobile device, including a remote wipe of the data. According to a recent study by Symantec called the Honey Stick Project, "96% of people who picked up lost smartphones tried to access personal or business data on the device and only 50% of the smartphone finders contacted the owner to return the device." If a mobile device is lost or stolen, technical controls must be in place to prevent data from being compromised.

Mobile application vulnerabilities are a risk that must be addressed when procuring software for mobile architecture. The DoD and Army are addressing this with a new process being worked to establish a DoD and Army App Marketplace. The marketplace would be similar in concept to the Apple iTunes® model. Strict code reviews and developer accountability would be integrated into each app that goes live. The ability to set up the infrastructure of a secure online mobile app marketplace will be crucial for ensuring mobile architecture is securely implemented for the Warfighter.

A risk that must be acknowledged is a rush to implementation without sound mobile security policies and user education in place. Many organizations are aggressively fielding mobile devices to get them in the hands of Warfighters and Civilian employees, without having the luxury of proper planning time. MDMs and other mobile security software packages are in their first generation and are still being tested by security compliance organizations like DISA, Common Criteria, and the National IA Partnership (NIAP). Proper IA, logistics, and sustainment cost impact planning must be considered prior to implementation and fielding.

Mobile devices are typically sold with GPS transmitters installed by default. As a result, a recent vulnerability has emerged known as geolocation abuse. This involves exploiting one's physical location and privacy for potential gain. Among other potential uses, if not protected, is an aggregation of numerous geolocations of Warfighters, allowing troop movements and battle plans to be inadvertently revealed.

DOD MOBILE ARCHITECTURE IA REQUIREMENTS

A number of DoD IA controls currently govern the compliance of mobile architecture to ensure an ATO is achieved. DISA STIG requirements have traceability back to the following DoDI 8500.2 IA Controls to ensure IA is appropriately implemented. Identifying the requirements for mobile architecture at the earliest possible point in the acquisition is necessary for program success.

Categories of Mobile Security

The controls can further be broken down into the five categories for mobile security to include the device, the data, the applications, the network, and the cloud. The IA Controls below are for a Mission Assurance Category (MAC) III Sensitive system, which is the security level for a majority of the training and simulation systems. The minimum IA Controls for mobile architecture should include, but not be limited to, the following examples:

Device Security

- DCAS-1: Acquisition Standards: Ensure mobile OS's are selected from the NIAP Approved Products List (APL), or the Common Criteria (CC) list. Currently, only Windows Mobile and Blackberry are certified on the CC or NIAP, but DISA publishing guidance for Android and Apple iOS. For the Army, Common Operating Environment (COE) guidance should be referenced as well.
- IAIA-1: Individual Identification and Authentication: The deployment of a secure device passcode policy is a first line of defense against unauthorized access to mobile devices.
- DCCS-1: Configuration Specifications: Mobile architecture DISA STIGs are in early and draft stages, but are continually being updated and maturing for mobile devices. As final and mature versions are released, compliance will be essential to achieving an ATO. See the references section of this document for a full list of DISA mobile architecture STIGs, ISCGs, and SRGs.
- DCSR-2: Specified Robustness – Medium: Mobile products should be selected that meet a robustness level of medium, as defined by NIAP to "provide for layering of additional safeguards above good commercial practices."
- IAAC-1: Account Control: The system should incorporate an approved account management policy to include the ability to configure the mobile device remotely through an MDM.
- ECLO-1: Logon: Mobile device configuration policies should align with current DISA STIG settings to include denying access after multiple unsuccessful attempts, limiting the number of unsuccessful attempts in a given time period, and employing a time-delay control system at a minimum.
- ECWM-1: Warning Message: The mobile device, prior to granting access to users, should warn that they are entering a Government owned information system.
- PESL-1: Screen Lock: The MDM should be able to activate and remotely push the settings for a screen lock given a specified period of inactivity.

Data Security

- ECCR-1: Encryption for Confidentiality (Data at Rest): Federal Information Processing Standard (FIPS) 140-2 approved encryption should be incorporated for protecting data at rest in the event the device is lost or stolen.
- ECNK-1: Encryption for Need to Know: FIPS 140-2 approved encryption should separate the data for need to know.

Application Security

- ECRC-1: Resource Control: The system should employ the ability to ensure no

residual data is left on the device in the event it is reissued to different personnel.
- ECTP-1: Audit Trail Protection: The MDM should have auditing capabilities of the mobile device events, with the ability to safeguard audit logs.

Network Security

- ECWN-1: Wireless Computing and Networking: Mobile devices should be configured with unused wireless functionality disabled and should prohibit the ability for the end user to reconfigure wireless capabilities.
- ECCT-1: Encryption for Confidentiality (Data in Transit): FIPS 140-2 approved encryption should be incorporated for protecting data in transit through commercial and wireless networks.
- EBVC-1: Virtual Private Network (VPN) Controls: Mobile devices should have the ability to connect to VPN servers.

Cloud Security

- PRTN-1: IA Training: A program should be established for personnel supporting a cloud data center to ensure compliance with IA roles and responsibilities. Additionally, mobile device users should have training and education on the risks associated with mobile devices.
- CODB-1: Data Backup Procedures: Data is backed up weekly for MDM servers and mobile devices.
- VIVM-1: Vulnerability Management (VM): An IAVM plan should incorporate mobile devices in existing processes to ensure mobile OS updates and IA Vulnerability Alerts (IAVAs) are installed in a timely manner.

TARGETRY RANGE AUTOMATED CONTROL AND RECORDING (TRACR) MOBILE ARCHITECTURE USE CASE

The TRACR system supports the planning, execution, and review of targetry training at non-instrumented Army training ranges. TRACR allows users to develop automated target control scenarios with an easy-to-use scenario development interface that supports time and event based automated and manual target control. Currently, TRACR is a standalone system with no connections outside of its accreditation boundary. Providing target control capabilities through the use of a mobile device is a feature the project team is currently developing. See Figure 3 for more information on the envisioned accreditation boundary for TRACR with cloud and mobile architecture integrated.

A number of IA requirements, as outlined in the previous section, will need to be addressed with mobile architecture being incorporated into the system. The system will be adding a Common Criteria/NIAP approved Wireless Access Point (WAP) to allow the device to communicate throughout the range. A number of WAPs from numerous manufacturers are currently on the approved lists including Cisco, Fortress, and Motorola. Android is the mobile OS currently be evaluated for installation on a tablet mobile device. An MDM solution will be evaluated from a risk mitigation and cost benefit viewpoint, with the understanding for this effort that two to four tablets will be deployed per range. The use of single hardened configuration files could potentially be used to replace many of the functions of an MDM for this use case. For example, Dell currently has a DoD approved application package file (APK) for Android to control and restrict a number of device functions.

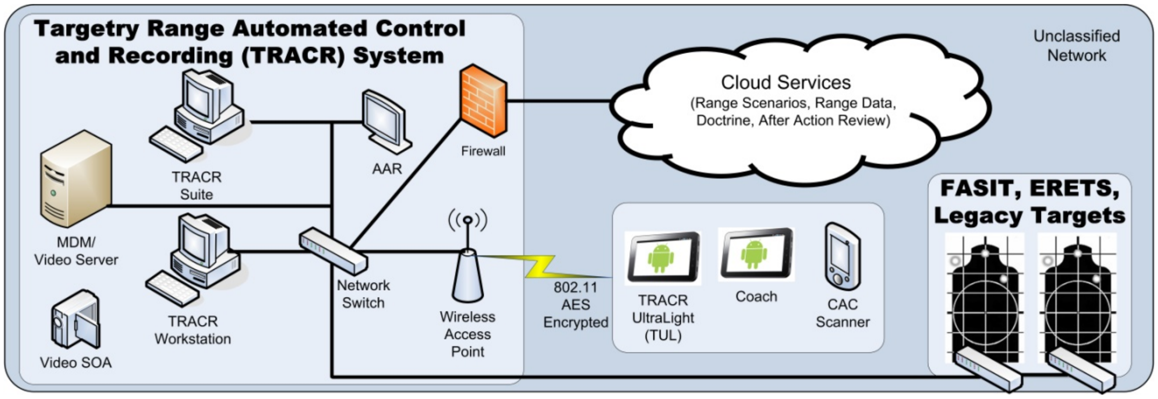


Figure 3. TRACR Mobile Architecture Potential Use Case

COMBAT TRAINER (CT) MOBILE ARCHITECTURE USE CASE

The CT Mobile Architecture potential use case is for Combat Training Centers (CTC) and Homestations to provide training units real time feedback during force on force exercises. The incorporation of a mobile device into the system would allow CTs to gather more training data on the battlefield to provide a realistic and accurate AAR. This use case could potentially incorporate cloud services from a cloud service provider such as DISA Rapid Access Computing Environment (RACE). Figure 4 documents a prospective high level view of the CT device data flow.

A number of IA requirements as outlined in the previous section will need to be addressed with mobile architecture being incorporated into the system. The process for adding mobile architecture into the system will start at hardening the device and then work through protecting the data, the applications, the network, and finally, the cloud or data center. Protecting the device will start at the OS selection as well as full compliance with applicable STIGs. Data at rest and data in transit encryption will be addressed to ensure data protection on the device and over the air (OTA). With a system of this size and potential number of devices, an MDM solution will be necessary to protect the data and the network.

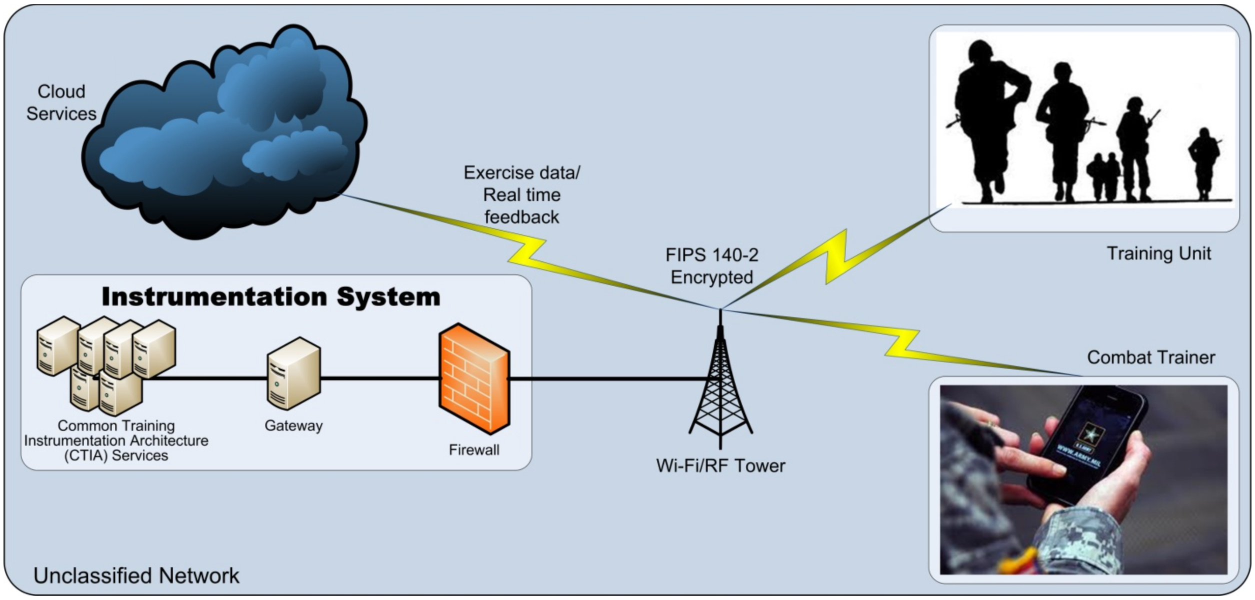


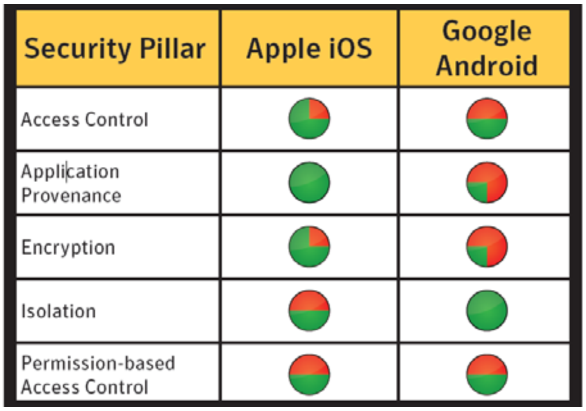
Figure 4. Combat Trainer Mobile Architecture Potential Use Case

BEST PRACTICES FOR MOBILE SECURITY

As mobile device adoption continues to skyrocket, so does the sophistication of these devices and the way in which people access, view, and manipulate data on them. These innovative new approaches to user interfaces and content exposure make the mobile warrior more efficient and more powerful than ever before. However, these advances add a number of new key challenges to enforcing security. Vendors have responded to these challenges with new tools, features, and settings that allow for better management of security on mobile devices. It is important to understand that not all mobile devices implement security in the same way. When developing a security plan for mobile devices being used in training systems, close attention should be given to each vendor's specific architecture. Careful thought should be given to how data flows through multiple layers and the best practices for implementing security on the device, data, applications, network, and cloud.

Device Security

There are many different manufacturers of mobile devices and OS's. However, two main competitors have emerged in this space, Apple iOS and Google Android. According to Jumptap.com, combined, these competitors made up 91% of the mobile OS market in 2012. Each takes its own custom approach to device security. Recently Symantec performed a study on security in mobile architectures in order to understand each manufacturers approach. We can see by Figure 5 below that neither Apple nor Google have been 100% correct in their approach to security. Each manufacturer has taken a different methodology to implementing mobile security features on their platforms. Figure 5 documents strong OS security features in green and weak features in red.



Security Pillar	Apple iOS	Google Android
Access Control	◕	◑
Application Provenance	🟢	◔
Encryption	◕	◔
Isolation	◑	🟢
Permission-based Access Control	◑	◑

Figure 5. Mobile Security Feature Implementation

The first line of defense for securing any device from unwanted access is to enforce a passcode policy. Every mobile user who has either corporate or Government data stored on his or her device should have a passcode enabled. IT administrators will find many of the same password policies that they would normally see in standard desktop computing environments are also found in mobile architectures. Both Apple iOS and Android can enforce complex alphanumeric passcodes with minimum passcode lengths, minimum complex characters, maximum passcode age, passcode history, auto-lock, grace periods, and maximum number of failed attempts. These granular controls keep unauthorized access to a minimum.

These controls can be easily implemented and managed by MDM servers, enabling administrators to change a device's security configuration while the user is on the move. Configuration profiles can be created and distributed for different levels of users. Within iOS devices these profiles can restrict access to key features of the device, such as Siri, FaceTime, the camera, screen captures, application installations, purchases, gaming, and much more. Administrators can also control access to applications, iCloud, and security and privacy settings. These profiles can be signed and encrypted in a way that prohibits users from changing settings without first completely wiping the device.

Devices can be further secured by the use of progressive passcode timeouts. If a device is lost or stolen, the device will progressively become more unusable as incorrect passcodes are entered. Each time the wrong passcode is entered, the device will lock for an extended amount of time, incrementing the lock time with each consecutive failed login. After too many failed logins, the device will initiate an automatic wipe to keep the data on the device secure. The ability to start a local wipe protects the device against brute force attacks.

Data Security

Data must be secured at all times in the event a device is lost or stolen. A survey released by Credant Technologies in September 2008 found that in just a six month time period 31,000 New Yorkers left behind mobile devices in taxi cabs. Additionally, a survey by Credant Technologies in November of 2011 found that nearly 2,200 hand-held devices were lost in just 15 malls, of which half of the devices were never claimed. As people are continually on the move, it is expected that a certain percentage will lose their mobile device during their travels. In addition, the popularity of some products has led to an increase in stolen mobile devices. For these reasons it is extremely important to encrypt data while it is at rest on the device.

All iOS and Blackberry devices offer full device hardware encryption, while only a few models of Android devices have this feature. iOS uses 256-bit AES encryption by default and offers an API that opens up hardware encryption to developers, allowing them to take advantage of this important security feature. Device backups can be encrypted to safeguard backed up data on the user's computer. Encryption can also be enabled for email. The encrypted data can be further protected by leveraging the user's unique passcode with hardware encryption to generate a strong encryption key, ensuring the device is secure even if it is compromised.

While encrypting data at rest is a good defense, it is important to have an offensive move to play when dealing with lost or stolen devices. An MDM feature called Remote Wipe is a key offensive tool to help protect and secure important data. This feature allows an administrator to initiate the wipe of a device remotely in the event it is lost or stolen. This builds upon the devices passive layers of security, enabling administrators to proactively protect data resting on a lost device. According to a survey by Ferris Research in 2008, 65% of organizations across all sectors ran a version of Microsoft's Exchange email collaboration suite. Since Exchange 2003, Microsoft has continued to develop MDM features for managing devices connected through the ActiveSync protocol. Additionally, third party MDM servers can manage many security features, including remote wipe.

To expand on what Apple has done for data security at rest, it is important to look at the implementation of security in the cloud. iCloud seamlessly backs up important data to Apple servers, and seamlessly shares the content across the user's devices. Having iCloud enabled protects the integrity of the data by creating a new backup when connected to Wi-Fi. iCloud secures content first by encrypting the data that is sent across the internet, and second by storing the data in an encrypted form. This protects the data at rest, both on the device and in the data center. Additionally, secure tokens are used for authentication to access the data from any Apple device, including non-iOS devices.

Application Security

Both Apple and Android take application security very seriously. However, each company takes its own approach to application development. Both platforms designed security at the core of their OS and application control by implementing "sandboxes" to protect the data during runtime. Sandboxing restricts applications from reading and writing other applications data. This approach also shields system files, resources, and the kernel from the user's application space.

Application signing is a key tool to authenticate software that runs on the device. Apple offers a very strict development program and code-signing method. In order to receive the certificates needed to digitally sign the code, Apple has to confirm the developer's identity. Google also offers code signing, but they offer a route to develop open source applications for Android devices, which largely differs from Apples tightly run App store operations. Apple's tightly controlled application distribution networks help to further protect against viruses and malware, while Android devices continue to be plagued by these nuisance programs.

Both iOS and Android platforms use a secure authentication framework for applications. Usernames and passwords are encrypted in a secure token that protects the user's identity. An authentication token is then provided to authenticate a user. Apple stores tokens in a keychain that is partitioned; ensuring credentials stored by third party programs cannot access other programs identities. The keychain is then used to sync credentials across a wide range of devices.

One area in which Apple's iOS excels is in its common cryptography architecture. Apple has created API's to allow developers to take advantage of multiple common cryptography schemes, such as Advanced Encryption Standard (AES). As well, they offer an AES 256-bit hardware crypto engine, with Secure Hash Algorithm 1 (SHA1) being done in hardware. Hardware encryption maximizes the performance of applications that take advantage of these advanced encryption schemes. Hardware encryption can be used to protect the application data within specific files, making the data inaccessible to both the application and potential intruders while the device is locked.

In addition to local application security, MDM servers can be leveraged to remotely manage third party applications from the App Store or Google Play, as well as enterprise applications created in house. The MDM server can stop unauthorized applications from being installed and authorized applications from being uninstalled. In some cases, these servers can even manage the data that is in the application, keeping sensitive data from being backed up to the cloud.

Network Security

It is important for both workers and Warfighters on the move to have access to important information from anywhere in the world. It is equally important to have secure authentication and encryption mechanisms in place to protect data while it is in transit. Most current smart mobile devices offer the ability to connect to a wide array of VPN technologies, with varying levels of encryption to protect the transmission of data. Careful thought must be taken as to what data should be accessed by mobile phones traversing firewalls and VPN's. Not all data makes sense to display on a mobile device. For instance, displaying a financial database doesn't offer benefits to a worker on the move. For these reasons, firewall and VPN policies should block the ability for mobile devices to reach these important information systems. With the growing number of malware programs for mobile platforms, unrestricted VPN access could open a direct door for malicious access.

Documented in figure 6, and according to a new report from marketing agency Knotice, more than 27% of emails were opened on mobile devices during the second half of 2011, of which iOS accounted for over 22%.

Percentage of Emails Opened	**% on Mobile**	**% on Desktop**
2nd Half 2011 Opens	27.39%	72.61%
1st Half 2011 Opens	20.24%	79.76%

Mobile OS	**Phone**	**Tablet**	**Total**
iOS	15.69%	6.54%	22.23%
Android	4.69%	0.17%	4.86%

Figure 6. Percentage of Emails Opened on Mobile Devices by OS in 2011

This unprecedented explosion of mobile email use creates a great need to secure all data communications. Encrypting all email traffic with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption can protect valuable data while it is in transit. In typical corporate environments, devices connect directly to Wi-Fi to receive emails. Instituting Wi-Fi Protected Access II (WPA2) encryption can protect data whether it is an email or an AAR.

As training systems evolve, so does the need for data on the move so that instructors can provide accurate, precise, and on-time decisions. In order to facilitate this, Wi-Fi could be used. Implementing WPA2 encryption with 128-bit and 256-bit encryption is needed in these situations, as well as support for Radius authentication. All mobile device networks should start incorporating these advanced security features. There will be an explosion in mobile device adoption within training systems as more network infrastructure and mobile devices become FIPS 140-2 and NSA Suite B compliant, keeping important data secure.

Cloud Security

The rapid adoption of feature rich mobile devices and cloud computing has grown at rates that technology administrators cannot keep up with. As smart mobile devices mature, the want and need for immediate access to important data will grow. Security features and the ability to manage them were an afterthought for many devices. MDM servers have started to fulfill the needs of remotely administering many mobile devices for an organization. MDM servers allow detailed administration of security configurations and profile settings that can be enforced at any time. However, a recent research report by InformationWeek found that only 53% of businesses enforced a mobile device security policy.

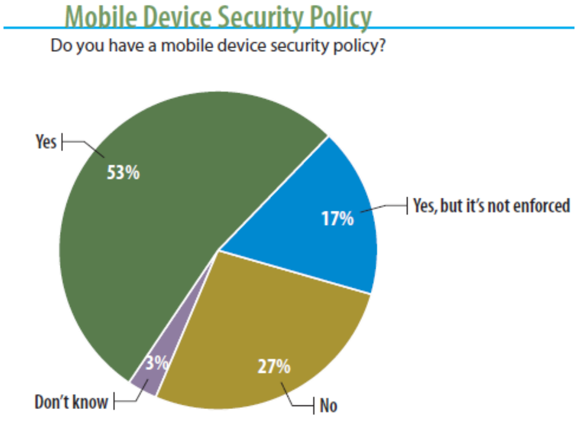


Figure 7. Mobile Device Security Policy

One reason for slow adoption of mobile device security policies is that an important need has been overlooked; the ability to manage updates on devices deployed in an organization. The most important mitigation to vulnerabilities is the ability to stay up-to-date with regular vendor patches. As mobile architecture advances, so will the exploits and need for real time patch management. Apple and Google have already taken a proactive stance by allowing updates to the OS to be pushed over the air, yet neither have a solution for managing mobile patches from an enterprise perspective. As device popularity increases, it is expected that these feature sets will evolve with future versions of MDM servers.

When reviewing MDM solutions one will find an overwhelming selection of competing companies. Gartner and Forrester recommend nearly a dozen different providers for MDM solutions alone. This stems from the open architecture of mobile device management. MDM solutions base their technology on the Open Mobile Alliance (OMA) device management standard. This platform independent protocol offers the ability for administrators to manage a standard set of mobile security policies across a wide array of devices within the network. However, MDM providers are at the mercy of device manufacturers' ability to continually develop new MDM features in future devices.

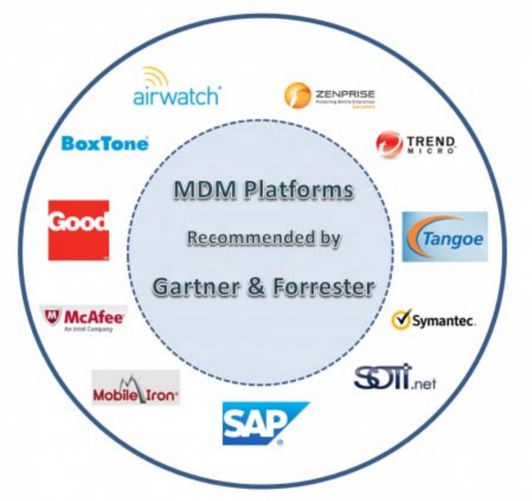


Figure 8. MDM Servers Recommended by Gartner & Forrester

The MDM vendor currently being referenced in DISA STIGs is Good Technology. Good offers a mobility suite custom designed for the Government, with the highest levels of encryption available. Good is currently in use by DoD agencies and has been included in the DISA STIG as part of the solution for securing mobile architecture. While Good's main focus is on email security, they provide a wide range of security features and MDM features that can be implemented over the air. Device communications are closely controlled by Good, routing all traffic through their servers so they can ensure the integrity of data from end to end.

These servers could one day be leveraged to facilitate management of mobile devices in any network, including stand-alone training systems. An MDM solution would allow mobile devices to reach important data across wireless networks, while at the same time allowing administrators to push updated settings and patches. The visibility of mobile devices on the network will allow administrators to appropriately manage the overall risk of mobile devices on the network in real time.

CONCLUSION

Mobile architecture is continuing to grow rapidly, with new devices being adopted in the enterprise and Government at exponential rates. The road ahead for incorporating mobile architecture is primarily about reducing the overall risk to an acceptable level to operate, while allowing innovation to take place in the DoD. There are many current guidelines and emerging STIGs being published for securing mobile architecture as outlined in this paper. We also outlined a number of key takeaways for securing mobile architecture. First, the need for an IA plan up front is never more necessary than with the incorporation of a mobile architecture in a training system. The focus should be on the overall integration of mobile architecture, and not about specific products or devices. Second, the team needs to perform a risk assessment of the known mobile threats to understand what they are protecting against and define the MAC and confidentiality level of the system to determine security requirements. Next, the project team needs to ensure the five categories of mobile architecture security (data, device, application, network, and cloud) are addressed to provide a defense in depth approach. Careful examination of these areas should be made when finalizing the design of a training system with a particular device. Finally, it is vitally important to have the ability to easily manage and sustain the entire fleet of mobile devices contained in the system. As described earlier, an MDM server with the latest DISA approved products is a key tool to securely maintaining a mobile architecture.

It should be noted a number of Commercial Off The Shelf (COTS) products are mentioned in this paper. However, in no way does our discussion of current manufacturers of mobile products act as an endorsement. Products and solutions should be selected by organizations based on their requirements and the needs of their users.

REFERENCES

Department of Defense, (2004). *Directive 8570.1 IA Training, Certification and Workforce Management.*

Department of Defense, (2007). *Directive 8500.01E IA.*

Department of Defense, (2003). *Instruction 8500.2 IA Implementation*.

Department of Defense, (2007). *Instruction 8510.01 Department of Defense IA Certification and Accreditation Process (DIACAP).*

Defense Information Systems Agency (DISA), (2011). *Android 2.2 (Dell) Security Technical Implementation Guide* Retrieved April 30, 2012 from http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

Defense Information Systems Agency (DISA), (2011). *Mobile Operating System Security Requirements Guide* Retrieved April 30, 2011 from http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

Defense Information Systems Agency (DISA), (2011). *Apple iOS 4 (Good Mobility Suite) Interim Security Configuration Guide (ISCG)* Retrieved April 30, 2011 from http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

Defense Information Systems Agency (DISA), (2011). *General Mobile Device (Non-Enterprise Activated) Security Technical Implementation Guide (STIG), Version I* Retrieved April 30, 2012 from http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

Program Executive Office for Simulation, Training and Instrumentation (PEO STRI), (2011). *Basic Accreditation Manual (BAM).*

Simply Security.com, (2012). *Users Aware of Mobile Security Threats, but Fail to Protect Devices*. Retrieved June 14, 2012 from http://www.simplysecurity.com/2012/03/05/users-aware-of-mobile-security-threats-but-fail-to-protect-devices/

Checkpoint, (2012). *The Impact of Mobile Devices on Information Security: A Survey of IT Professionals.* Retrieved June 14, 2012 from http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Symantec, (2012). *The Symantec Smartphone Honey Stick Project.* Retrieved June 14, 2012 from http://www.symantec.com/content/en/us/about/press kits/b-symantec-smartphone-honey-stick-project.en-us.pdf

Credant, (2011). *Consumers Lost Thousands of Smartphones at the Busiest Shopping Malls in the United States According to Credant Survey*. Retrieved June 14, 2012 from http://www.credant.com/news-a-events/press-releases/265-consumers-lost-thousands-of-smartphones-at-the-busiest-shopping-malls.html

Credant, (2008). *Mountains of Mobiles Left in the Back of New York Cabs.* Retrieved June 14, 2012 from http://www.credant.com/news-a-events/press-releases/187-mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html

Knotice, (2011). *Mobile Email Opens Report 2nd Half 2011*. Retrieved June 14, 2012 from http://www.knotice.com/reports/Knotice_Mobile_Email_Opens_Report_SecondHalf2011.pdf

Symantec, (2011). *A Window Into Mobile Device Security*. Retrieved June 14, 2012 from http://www.symantec.com/content/en/us/about/media/pdfs/symc_mobile_device_security_june2011.pdf

SYS-CON Media, Inc. (2012). *To MDM or not to MDM?* Retrieved June 14, 2012 from http://wireless.sys-con.com/node/2291227

Baseline Mobile (2009). *10 Best Practices for Mobile Device Security*. Retrieved June 14, 2012 from http://mobile.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/

Apple, (2012). *iOS Security*. Retrieved June 14, 2012 from http://images.apple.com/iphone/business/docs/iOS_Security_May12.pdf

Slashgear, (2012). *Android OS Apocalypse in 2012 predicted by IDC*. Retrieved June 14, 2012 from http://www.slashgear.com/android-os-apocalypse-in-2012-predicted-by-idc-06232629/

Jumptap, (2012). *Jumptap February MobileSTAT Report Shows Uphill Battle for Android and iOS Competitors.* Retrieved June 14, 2012 from http://www.jumptap.com/android-and-iphone-now-hog-91-of-mobile-os-market-share/

Information Week, (2011). *BYOD Requires Mobile Device Management.* Retrieved June 14, 2012 from http://www.informationweek.com/news/mobility/business/229402912

IBM Global Technology Services, (2011). *Securing Mobile Devices in the Business Environment.* Retrieved June 14, 2012 from http://www-935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_business_environment.pdf

Office of the DoD Chief Information Officer v2.0, (2012). *DoD Mobile Device Strategy v2.0.* Retrieved June 19, 2012 from http://www.defense.gov/news/dodmobilitystrategy.pdf

The Museum of Email and Digital Communications, (2008). *Ferris Research Completes Most Comprehensive Survey of Business Email Systems to Date*. Retrieved June 14, 2012 from http://email-museum.com/reports/ferris-research-completes-most-comprehensive-survey-of-business-email-systems-to-date/