FEDERAL MOBILE COMPUTING SUMMIT

MARCH 28, 2017 | MARRIOTT METRO CENTER | WASHINGTON, DC

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Mobile Collaboration Symposium held on March 28, 2017 in Washington, D.C. in conjunction with the ATARC Federal Mobile Computing Summit.

I would like to take this opportunity to recognize the following session leads for their contributions:

MITRE Chair: Pat Benito

Challenge Area 1: Mobile Application Security
Industry Lead: Tim LeMaster, Lookout
MITRE Lead: Carlton Northern
MITRE Lead: Mike Peck

Challenge Area 2: Mobile Technologies
Government Lead: Rick Jones, GSA
Industry Lead: Steve Taylor, Intel
Industry Lead: Kathleen Urbine, DMI
MITRE Lead: Jeff Stein

Challenge Area 3: Mobile Technology Roadmap
Government Lead: Jon Johnson, GSA
Industry Lead: Gary Bradt, Zimperium
MITRE Lead: Mike Schoenfeld

Challenge Area 4: Tactical Mobility
Industry Lead: Paul Nelson, Thursby Software Systems
MITRE Lead: Greg Kern

Challenge Area 5: Mobile Health
Government Lead: Dr. Joseph Ronzio, VA
Industry Lead: Larry Littleton, IBM
MITRE Lead: CJ Rieser

Below is a list of government, academic and industry members who participated in these dialogue sessions:

Challenge Area 1: Mobile Application Security

Pat Benito, MITRE; Bob Clemons, NIAP; Michael Cull, TSA; Anne Dalton, DHS; Guy Francois, DoD-VA IPO; Anthony Glynn, DHS; Greg Hixson, GSA; Shoaib Ibrahim, Treasury; Tom Karygiannis, Kryptowire; Sean Kenney, Booz Allen Hamilton; Mike McHugh, DOJ; Noelle McMillan, U.S. Marshals Service; Michael Ogata, NIST; LaDavia Powell, FDIC; Stephen Rossero, DoD; Stephen Ryan, Proofpoint; Mark Schmitz, GAO; Derrick Smith, DOJ; Jeff Williams, DLA

Challenge Area 2: Mobile Technologies

Kelly Adams, GSA; Richie Busigo, DLA; Nicholas Diaz, Booz Allen Hamilton; Wendy Fairfield, SurePassID; Coburn Flippen, CFTC; Chris Gorman, Monkton; Andrew Gregory, FBI; Mindelin Logar, FBI; Alan Oakes, USDA; Kathleen Robinson, Intel; Michael Ross, DHS; Dennis Turner, CFTC; David Wellington, DoD; Patrice Yuh, FBI

Challenge Area 3: Mobile Technology Roadmap

Vernelle Archer, USDA; Eric Atala, U.S. Census Bureau; Mark Battaglini, Booz Allen Hamilton; Robert Burdette, NIH; Bobby Duffy, DHS; Bob Ellington, DOT; Angela Emrich, USDA; DJ Kachman, VA; Kevin Kipp, IRS; Vinod Kumar, USDA; Chien-Chi Lin, VA; Ken Luersen, DHS FEMA; Sean McLaren, U.S. Census Bureau; Pattabhi Nunna, Booz Allen Hamilton; Thomas O'Connor, Copper River IT; Jon Rolf, NSA; Rick Townsend, IRS; Carlos Trevino, U.S. Coast Guard; Lauren Withum, U.S. Census Bureau

Challenge Area 4: Tactical Mobility

Stephen Booher, Booz Allen Hamilton; Allen Brindle, Samsung; Denise Harris, FAA; Meenakshi Kak, DoD-VA IPO; Aris Lambropoulos, Booz Allen Hamilton; Michael Stovall, Shadow Soft; Suzette Wright, FAA

Challenge Area 5: Mobile Health

Will Alberts, DoD; Vanessa Batoon, VA; Bill Cerniuk, VA; Yvonne Cole, DoD-VA IPO; Joe Dachuk, SurePassID; Jeff Forbes, U.S. Navy; Shama Hussain, PCMG; Michelle Lynch, University of Virginia; Cathy Lynn Metcalf, DoD-VA IPO; Gegory Pappas, FDA; Gaurav Seth, DoD-VA IPO; Neil Sethi, VA; Ray Zelenak, PCMG

Thank you to everyone who contributed to the MITRE-ATARC Mobile Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)
Host organization of the ATARC Federal Mobile Computing Summit

March 2017 Federal Mobile Computing Summit Report

Patrick Benito, Marie Collins, CJ Rieser, Darshan Kadam, Mike Schoenfeld, Jeff Stein, Greg Kern, Carlton Northern, Mike Peck, Justin F. Brunelle
The MITRE Corporation

Tom Suder & Tim Harvey
The Advanced Technology Academic Research Center

Table of Contents

1 Executive Summary

The Federal Mobile Computing Summit includes a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, and discuss prominent challenge areas in mobility. In some cases, potential solutions for key challenge areas were identified by session participants. The discussions were government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks.

Participants representing government, industry, and academia addressed five challenge areas in federal mobile computing:

1. Mobile Application Security
2. Mobile Technologies - Continuous Integration, Delivery and Deployment
3. Mobile Technology Roadmap: What's Next?
4. Tactical Mobility
5. HealthTrac: How Mobile Technology is Transforming Healthcare

This white paper summarizes the discussions in the Collaboration Sessions. Drawing from these discussions, MITRE and ATARC developed the following actionable recommendations for the government, academia, and industry:

Continue Joint Commercial/Academia/Government Mobile Roadmap Brainstorming
Joint roadmap planning across commercial, academia, and government benefits all parties involved. Commercial agencies benefit by understanding the needs of the government and can help align their product roadmaps to government needs. Academia benefits by gathering information to target new research. Government agencies benefit by gathering important information and ideas to better shape their roadmaps and identify partnership opportunities with other government agencies and academic institutions.

Government agencies should identify forums to bring commercial companies and academic institutions together on a routine basis to develop and refine their mobility roadmaps. Data generated in the Federal Mobile Summit provides a good starting point for agencies to create (or refine) their mobile roadmaps.

Create Governance for Mobile Spectrum Use
Mobile spectrum availability is critical for tactical mobile systems. Spectrum usage and planning requires close coordination with both government and commercial entities, both in the US and outside of the US. This is often very complex and many agencies lack the guidance and experience to do this.

The government should establish governance for spectrum use to help organizations determine what spectrum they can use, and how they can request the use of a spectrum in a given area.

Establish a Technical Vision to Guide Organization's Development Efforts

A clear, easy to understand technical vision can help all stakeholders understand their organization's direction and goals for mobility. This is key to not only socialize investment plans and goals, but also for gathering feedback from the users of the mobile solutions. Agencies should strive to create a technical vision for their mobility program, but also ensure it is shared across the user community.

Along with the technical vision, a reference architecture should be developed by all agencies deploying mobility that depict the as-is state of mobile IT as well as the to-be state of mobile IT. Furthermore, the reference architecture should be published and easily accessible by agency employees. This is useful for both the business and engineering communities to better understand not only the future direction of mobility, but also what the current solution looks like and what needs to change to get to the desired future state.

Pilot a Continuous Integration Program Before Proceeding with Organization Wide Adoption

Adopting continuous integration concepts, processes, and technologies can be a challenging undertaking. Continuous integration has a ripple effect across key areas of an organization, and all impacted parts of the organization need to work towards the same set of goals.

Due to the complexities of continuous integration and big impacts it has on culture, process, and technology, organizations should not conduct a "big bang" adoption of continuous integration. Rather, organizations should create a pilot program to experiment with and learn how to apply continuous integration principles to the larger organization. Results from such a pilot can be used to conduct a larger rollout of continuous integration across the larger organization.

Establish a Security Guide for Mobile Application Developers

Mobile app security is critical for all government agencies. Navigating the existing guidance for first time developers can be daunting. For example, the National Information Assurance Partnership (NIAP) Protection Profile for Application Software provides useful guidance to security analysts performing app vetting, but it can be difficult to understand by app developers without security expertise.

Guidance should be developed for mobile app developers to securely develop apps. This guidance should be easy to use and understand by developers that do not have a security background or by developers that have never developed apps for the government.

2 Introduction

During the most recent Federal Mobile Computing Summit, held on March 28th 2017, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in mobile computing. Subject matter experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of mobile computing technologies and research in the government. Participants ranged from the CTO, CEO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs)[1]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology[2]. MITRE works in partnership with ATARC to host these collaborative sessions as part of the Federal Mobile Computing Summit. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in mobile computing, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curricula development, and to help produce graduates ready to join the workforce and advance the state of mobile computing research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 Collaboration Session Overview

Each of the five MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed:

1. Mobile Application Security
2. Mobile Technologies - Continuous Integration, Delivery and Deployment
3. Mobile Technology Roadmap: What's Next?
4. Tactical Mobility
5. HealthTrac: How Mobile Technology is Transforming Healthcare

[1] https://www.mitre.org/about/corporate-overview
[2] http://www.atarc.org/about/

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 Mobile Application Security

Mobile application security is a broad topic that spans many areas to include application development, app stores, vetting, sandboxing, and management. Understanding what government agencies and industry are doing in this space and where problems are occurring is an important part of improving the security posture of our mobile devices. The participants in this session discussed end-to-end strategies for security that span the lifecycle of an application.

3.1.1 Session Goals

The goal of the joint session, with participants from the government, industry, and academia, was to:

- Identify mobile application strategies and best practices in use within the government and private sector that could be documented and shared with others.
- Discuss the current government mobile app vetting standards and criteria (such as NIST's Special Publication 800-163[3] and NIAP's Protection Profile for Application Software) as well as any applicable private sector standards to identify pain-points, gaps, and potential improvements.
- Discuss current capability gaps of app vetting tools, mobile threat protection tools, as well as integration with Enterprise Mobile Managers (EMMs) and their place within a greater mobile security strategy.

3.1.2 Session Summary

The session was well attended with participants from a variety of government agencies as well as commercial industry. Discussion began with an update on the NIAP Protection Profile (PP) for Application Software. Feedback on the PP has been very positive. It is hard to gauge its impact because the only metric that is tracked is the amount of formal evaluations which is very few. Informally, there are many organizations that are using it as their app vetting criteria but this is not tracked.

Conversation then shifted towards gaps with current policies. The group noted that the definition of mobile device in NIST Special Publication 800-163 is out-of-date given the advanced capabilities of today's smartphones and tablets. The Risk Management Framework was noted as not being clear. The NIAP Protection Profile for Application Software was discussed as providing clear criteria for evaluators of apps, but not for app developers. A companion document that helps developers appropriately implement security into their applications would be valuable. Both Google and Apple provide useful guidance to developers, but this guidance could be complemented by something that specifically addresses the PP requirements.

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf

This led into discussion about a lack of a good way to assess tools for effectiveness. A set of measurements or metrics does not exist for this. MITRE offered a recently open sourced and publicly accessible report and set of test applications called MITRE Vulnerable Mobile Apps[4]. The assessment criteria is based off of the Application Protection Profile and a set of test apps have been open sourced so that organizations can run them through tools that they are evaluating.

The OWASP top 10 for Mobile 2016[5] provides a good listing of prioritized things to watch for in application security. The National Cyber Center of Excellence Mobile Threat Catalogue[6] and MITRE's ATT&CK Model Mobile Profile[7] were also discussed as good sources for mobile threats and information for how to combat them.

Conversation then shifted to Mobile Backend-as-a-Service (MBaaS). There seems to be interest in government organizations but adoption is slow. There are many evaluations currently in progress and the Government is trying to understand how this industry paradigm could work in a Government setting. MBaaS has the potential to reduce the attack surface by reducing exposure to enterprise data access points and providing reuse of critical components.

Continuous assessment is being used at some agencies but not all. There are some evaluations currently going on. It's a great way to improve an agency's security posture but it can be expensive, but requires the agency to provide a good business case for using it.

There was good discussion on the subject of app vetting reciprocity. The group discussed the potential for a US Government wide repository of app vetting results that could be used for reciprocity purposes. When one organization evaluates a specific version of an app, it posts their results including underlying evidence data to the repository. Other organizations could then use those results, applying their own risk algorithms to determine whether or not the risk level is acceptable or if further evaluation needs to be performed. The group noted that there are many small government agencies that may not be able to individually afford app vetting tools and may only have a small number of apps that require vetting.

The group discussed a "catch twenty two" where the participants agreed that organizations shouldn't blindly trust other organizations Authority to Operate (ATO) as there are differing use cases between organizations and differing security postures. Sharing results however is potentially impractical because of licensing issues that are stipulated by many of the app vetting tools. In other words, to share results from tools

[4] https://mitre.github.io/vulnerable-mobile-apps
[5] https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
[6] https://pages.nist.gov/mobile-threat-catalogue/
[7] https://usmile.at/symposium/2017/program/franklin-peck

both organizations need licenses to the tools that created the results. There was talk as to whether utilizing a standard report mechanism where data is pulled from the tool report and into this new format would satisfy the licensing requirement but the answer to this question is unknown and most likely dependent on each vendor.

Agencies need specific guidance for applications that they develop, vet and use, such as something that takes into account current policy as well as specific policy/guidance from the agency. There are some potential "gotchas" that are encountered in the wild like iMessage, which uses encryption. While this is normally a good thing, it can be bad because the organization needs to monitor and record official communications.

3.1.3 Recommendations

The Mobile Application Security collaboration session participants identified the following recommendations:

- Develop guidance for app developers for how to securely develop apps. The NIAP Protection Profile for Application Software provides useful guidance to security analysts performing app vetting, but it can be difficult to understand by app developers without security expertise.
- Each organization has its own acceptable level of risk, driven by its own unique environment and use cases. In order to enable organizations to make their own risk determinations, app vetting tools must provide detailed results with evidence, not just simple yes or no results. Additionally, any centralized repository of app vetting results must provide this evidence information as well.
- Work is still needed to streamline app reciprocity. Licensing agreements with vendor tools won't allow for the sharing of the results that come their tools but blindly accepting an ATO from another organization may not adequately provide the same level of security where there are differing security postures.
- Mobile continuous assessment and threat monitoring capabilities should be explored further. There is great capability with these product offerings but price can also deter some organizations from pursuing an implementation. Business cases should be constructed to determine if the value outweighs the costs.

3.2 Mobile Technologies - Continuous Integration, Delivery, & Deployment

Commercial mobile technology evolves at a very rapid pace, often faster than government acquisition cycles. This leads to organizations sustaining obsolete mobile technology. Government mobility programs need to be able to evolve with the commercial sectors to ensure the best technology is provided to employees to improve their productivity, happiness, and security against emerging cyber threats. Continuous integration is a software practice through which each incremental change to an asset is automatically tested, providing feedback about any issues that result. This session identified programmatic and technical approaches to continuously integrate and deploy

new mobile technology -- including hardware and software -- into the enterprise, and capture best practices and lessons learned on continuous mobile integration.

3.2.1 Session Goals

The goals for this session included:

- Develop an understanding of the infrastructure components and the interactions of a prototypical continuous integration pipeline for software development, as well as understand the concepts of continuous delivery and deployment.
- Investigate if and how continuous integration principles can be applied to mobile hardware assets.
- Discuss cultural and organizational issues that may arise in the adoption of a continuous integration strategy.
- Identify, at a high level, the testing requirements for mobile technologies, both for hardware and software.

3.2.2 Session Summary

This session opened with a definition of what continuous integration is and how it is used in software design. Continuous integration was defined as a software design practice in which every incremental change is tested to determine whether it can be integrated with the existing software code base. Starting from this point the definition was expanded to a practice in which continually changing inputs are continually tested in order to identify issues as soon as they arise.

Next the group decided to focus on what was termed the mobile ecosystem in which mobility solutions exist. This ecosystem consists of a variety of components both under and outside the control of the federal government such as the operating system of a mobile device, the physical device hardware, the networking environment, and MDM profiles loaded on a mobile device, specific versions of apps and software running on the device as well as other factors. In evaluating this problem space, the group agreed that mobile solutions cause unique issues for the federal government. In the past, for example, the federal government was able to affect and plan for change, in this new ecosystem model, however, the government is often forced to react to change.

The discussion next shifted to an exploration of some of the main problems federal agencies face when a change in the mobile ecosystem does not integrate correctly. The first issue identified was business continuity. Simply put, whatever features existed and worked before an update need to continue functioning after that update. A secondary issue was potential security flaws or fixes that could be introduced by an app update. Both of these issues are compounded by a third problem -- version control of mobile assets. Mobility solutions do not make it easy to downgrade to previous versions of software. Although users can often delay an upgrade, it is difficult -- if not impossible -- to downgrade in many cases. This, in turn, lead into a discussion of when and how to

apply updates. On one hand, users could wait until a new update was tested before applying it, however, in some cases updates are security-related and there is a level of risk in waiting until the update has been fully tested. The group did not come to a decision on this specific thread of discussion.

The group identified two additional areas to discuss: training and triage techniques. In the current mobile ecosystem, when a breaking change happens and is not picked up by testing, the support desk employees will often be the first individuals to detect an issue. A potential problem for helpdesk staff occurs when they do not have the same capabilities as a user. For example, if the helpdesk staff does not have access to Wi-Fi they will be unable to assist in diagnosing a new issue that arose with Wi-Fi connectivity after a recent update. Additionally, when an issue arises it needs to go through an entire triage process before it can be addressed and/or fixed. The flow of information could go from service desk to service desk manager to engineering back to service desk as well as to the app vendor who will eventually fix the bug. This information flow needs to be well documented and communicated so that new issues can be easily triaged in the future.

Finally, as the discussion wrapped up, the group came to the consensus that there is much more to explore in this discussion area. The group identified the key areas in which further research is warranted including suggestions to investigate some of these areas with pilot programs.

3.2.3 Recommendations

The collaboration session participants identified the following recommendations:

- Create a pilot program to experiment with, and learn how to apply continuous integration principles to the larger organization.
- Provide helpdesk staff with the equipment and capabilities they need in order to correctly diagnose user problems, as well as appropriate techniques and procedures to triage problems that arise.
- Identify an organization or group within an agency to own and lead continuous integration efforts.

3.3 Mobile Technology Roadmap: What's Next?

Identifying a Mobile Roadmap is essential for effective mobility deployment/adoption in an organization due to the increasing complexity of mobile solutions and the fast evolution of mobile technology.

3.3.1 Session Goals

The goals for this session included:

- Defining a mobile digital workplace.
- Identification of an agency's challenges in moving toward a mobile workplace.

- Identification of the important enablers/drivers in moving toward a mobile workplace.

3.3.2 Session Summary

The Mobile Roadmap Collaboration Session focused on the drivers to move an agency to a digital mobile workplace where work is what you do and not where you go to do it. Attendance for this collaborative session was well over 35 people and there were several contributors that conveyed insight and perspective on their organization's mobility challenges and initiatives.

The participants qualified that a digital mobile workplace must get the business data in the hands of its agency's employees, partners, collaborators, and public (stakeholders). Access to business data must be high-speed, real-time, secure, and on a need to know basis. Users desire to realize the benefits of mobility in their jobs like they are already experiencing in their personal lives with their personal mobile phones and apps like Google Maps, Uber, WeatherBug, and Facebook.

The challenges in moving forward with mobility were discussed first and categorized by devices, apps, infrastructure, organizational/environmental, and security. Participants noted that security had a role in each of the categories identified. *Devices* challenges included IT not having the resources to keep up with the pace of new mobile technology (e.g., mobile phones, OS versions). Also, the difficulty of choosing the appropriate device management program (e.g. Bring Your Own Device (BYOD) device, Choose Your Own Device (CYOD), and Corporate Owned Personally Enabled (COPE). *Apps* challenges included the struggle in developing valued custom business apps based on sound business cases and requirements gathering processes. Also, they faced the hard problem and expense of vetting available commercial apps, especially business apps that manage business/personal data in a third-party cloud. *Infrastructure* challenges included providing high speed, secure access to data. Also, the business must eliminate the duplication of data stores throughout its enterprise and provide central and accessible interfaces for tapping into the agency's business data. *Organizational/Environmental* challenges included leadership not completely understanding the benefits of a mobile workplace and not willing to allocate the resources to make it happen. *Security* challenges included the managing of credentials for authentication/authorization at all levels of the enterprise mobility architecture.

After mobility deployment challenges were discussed, the participants took on a discussion of the important enablers/drivers that can overcome these challenges and move an agency to a mobile workplace. Just as listed above, these discussions were also categorized by devices, apps, infrastructure, organizational/environment, and security.

The *Devices* discussion focused on implementing a successful BYOD device management program. CYOD and COPE programs can be interim solutions and more expeditiously defended and approved, however the long-term solution for government

agencies is BYOD because of logistics and employee satisfaction factors. Stakeholders desire to use one secure mobile device for their business and personal apps. This device must sandbox personal apps and data from business apps and data. Agencies must also reconcile the legality issues of BYOD.

The *Apps* discussion focused on an agency's ability to standardize on a development platform including the need to employ good prototyping tools, to provide agility and short delivery times for all mobile development projects. Also, standardize on mobile testing strategies and utilization of mobile test clouds to test the endless permutations of devices, OS versions, and form factors. This will help to reduce mobile project costs and deliver quality business apps to the agency's stakeholders. During the discussion, both a CDC and FDA representative indicated that their representative agencies employ a policy of Cross Platform (CP) development first unless a project entertains extreme performance, user interface, or device level functional requirements. CP development is a code-once and deploy many approach, and it also will leverage the skillset of HTML5/JavaScript developers, which are in large supply.

The *Infrastructure* discussion focused on an agency having a strategic and tactical plan and an enterprise mobile reference architecture. The duplication of enterprise business data must be eliminated. The master business data must be centralized to be encapsulated by an enterprise application program interface (API) Bus that can be tapped easily by all the agency's developed business apps.

The *Organizational/Environmental* discussion focused on leadership and a champion for the agency's mobility initiative. This mobility champion must be well versed in risk management to balance the high business potential of mobility with the security issues. Although mobility security risks are real, leadership cannot allow their mobility program to come to a grinding halt because of them.

The *Security* discussion focused on multi-form authentication including biometric forms. Also discussed was incorporating standard security design and test processes within the mobile development app lifecycle. These processes should be based on the NIAP PP for Application Software.

3.3.3 Recommendations

The collaboration session participants identified the following recommendations:

- Government agencies should include API management as part of their roadmaps, and ensure that these expose enterprise data, as well as allow developers to create larger capabilities from these APIs. These APIs should be accessible by both traditional IT, mobile IT, and IoT devices.

- Government agencies should put emphasis on refreshing mobile IT on a routine basis, to try and keep up with the commercial sector, as well as increasing user satisfaction.
- A technical vision and associated reference architecture should be developed by all agencies deploying mobility. This should depict the as-is state of mobile IT, as well as the to-be state of mobile IT. Furthermore, the reference architecture should be published and easily accessible by agency employees. This is useful for both the business and engineering communities to better understand the current situation, and future direction of the mobility program.

3.4 Tactical Mobility

The average American has more functionality in their mobile device then Warfighter has during daily operations and combat. For years, the Department of Defense (DoD) was at the leading edge on innovation but that now has shifted to the commercial market leading the defense sector. Using commercial products, instead of custom made component the DoD can save money. Securing a commercial product for the Warfighter still remains a challenge. The same issues that face the DoD also apply to First Responder during daily operations and disaster relief. This session will explore the challenges organizations face of taking commercial mobile devices and deploying them in secure tactical environment and discuss the mobile use cases from the field, lessons learned and best practices in tactical mobility.

3.4.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Identify the challenges of an organization may face in taking commercial mobile devices and deploying them in secure tactical environment.
- Identify lessons learned and best practices in tactical mobility that can be applied to warfighters and First Responder, alike.
- Identify areas where the government and the commercial sectors can work together bring greater functionality to the tactical level.

3.4.2 Session Summary

The session was well attended by participants from a variety of government agencies, both military and civilian, as well as commercial industry. The session began with a discussion of security. Security of the device, security of the data and security of the communication infrastructure were all discussed. Several key topics emerged:

- *Root of trust.* This includes the full end to end traceability of the hardware being purchased to the software running in the hardware. Many leading mobile hardware vendors use production facilities outside of the US, leaving the hardware vulnerable. The third party applications, unless properly vetted could expose mobile devices to threats.

- *End to End encryption of data.* Verifying data is properly protected both on the device and while in transit. Commercial Solutions for Classified (CSfC) required dual encrypted Data at Rest (DAR) and Data in Transit (DIT).
- *Authentication and Authorization for the mobile devices*. Controlling who is authorized to use a given device and access a network, as well as authentication that the user is who they claim to be. Multi-factor authentication can help but could be problematic when Warfighters and first responders are required to wear safety gear that could hinder the use of biometrics.
- *Protection of the communication infrastructure.* The communication infrastructure can be disturbed by jamming, denial of service, physical destruction, and even congestion, in the cases of large gathering of people, like major sporting events. How can the communication infrastructure be protected and add a layer of redundancy?

The discussion of security lead to the topic of user acceptance. If a requirement for security is too high users will likely not want to use the devices. Tedious multi-factor authentication and large, complex passwords going can prohibit the user from being able to perform their duties. Making logging into the device too complicated makes user reluctance to use the devices. If the device doesn't have the correct form factor or if the required safety gears hinder the use devices, those devices will not be used. In many cases, there is also a lack of training given to the users. Several stories were told of users being given a mobile device to should speed up the business/operational processes, and since the user was not given adequate training, the device ended up not being used.

One group of participants spoke of the reluctance their user to accept the devices in fear that the users will be tracked. This lead to a discussion of governance. The group identified a need for user and/or union agreements allow users to use the power of mobile computing without the fear that their organization is monitoring every activity. The current policies in place appears to be lagging behind the technology curve or simply not working in practice. Also, the group discussed the need for governance to address spectrum. Many companies have paid large sums for money to purchase given spectrum from the governments and are reluctant to share the spectrum in fear that it affects the quality of service to their customers.

The last topic that arose during the session was on interoperability. Interoperability between mobile systems from different organizations within the government continues to be an issue. Specifically, there are differences in spectrum, encryption standards, identity and access management, and data standards that prevent mobile systems from interoperating.

3.4.3 Recommendations

The Tactical Mobility collaboration session participants identified the following recommendations:

- Develop guidance for end-to-end hardware and software traceability to assure that the hardware being purchased hasn't been tampered with.
- Establish a shared software vetting program to assist in the third-party software security assessments.
- Develop a standard set of user agreements templates. A "one size fits all" user agreement will not be possible but there should a stand set of user agreements templates that can be created to give organizations a known good starting point as they start to roll out mobile devices to their users.
- Establish governance for spectrum use to help organizations determine what spectrum they can use, and how they can request the use of a spectrum in a given area.

3.5 HealthTrac: How Mobile Technology is Transforming Healthcare

The HealthTrac session is an enduring session at the Federal Mobile Summit, hosted by the DoD/VA Interagency Program Office (IPO). University of Virginia Health System (UVAHS) was pleased to join MITRE and ATARC at the 2017 ATARC Federal Mobile Computing Summit to learn more about the current state of mobile health (mHealth) and collaborate with innovators in how to improve military and civilian care.

3.5.1 Session Goals

The goal for this session was to identify recommendations to agencies to find the right balance of security and usability for mHealth, to ensure good, secure healthcare delivery.

3.5.2 Session Summary

The session started off with a discussion regarding the state of mobile technology in the military today. A participant mentioned the Army has at least one third of all of the US military mobile devices and the vast majority the apps are for military use. It was noted that the working military population will be shifting dramatically as the current workforce retires, being replaced by a significantly younger population. It was stressed that future technology needs to advance to support the needs of the early career (millennial) working generation.

The discussions shifted towards the progress in advancing the health technology of VA physicians. Participants discussed how the VA was providing physicians at certain VA hospitals with iPads. The response has been incredibly positive and patient care has improved due to the accessibility of survey, psychometric, and experimental data. There is definitely a great need for greater access and ease of technology to help with patient care and job workflow. Furthermore, many older veterans have multiple comorbidities that increase risk for suboptimal management due to an insufficient health record and over-crowding of clinics. The benefits of improved mobile computing are likely not restricted to the inpatient environment, however –improving access to patient labs and out-side records readily available may improve promptness and appropriateness of care.

The session participants discussed the need to bring healthcare into the home to help manage chronic illness and predict and treat acute illness before it becomes burdensome. This concept would have major impact on the care of America's servicemen and women, who deserve high quality medical and psychological care during their years of service and as veterans.

Overall participants agreed that mHealth is still in an early evolutionary phase and that its current fragile requires incredible effort to balance the security required to maintain federal standards and the accessibility essential for prompt, accurate care that acknowledges the strenuous user requirements of providers and patients.

4 Conclusion & Summit Recommendations

As with past Federal Mobile Summits, the collaboration sessions discussions had a common set of themes. While the cultural barriers to adoption, rapid advancement of mobile technology and accompanying user demand for bleeding edge technology, and security remain, success stories are emerging from government adoption efforts. With continued collaboration and sharing, establishing success stories and best practices is becoming more common-place and mobile adoption is becoming easier for government agencies.

Drawing from the discussion and content generated during the Collaboration Sessions, MITRE and ATARC developed several key overarching recommendations:

Continue Joint Commercial/Academia/Government Mobile Roadmap Brainstorming
Joint roadmap planning across commercial, academia, and government benefits all parties involved. Commercial agencies benefit by understanding the needs of the government, and can help align their product roadmaps to government needs. Academia benefits by gathering information to target new research. Government agencies benefit by gathering important information and ideas to better shape their roadmaps, and identify partnership opportunities with other government agencies and academic institutions.

Government agencies should identify forums to bring commercial companies and academic institutions together on a routine basis to develop and refine their mobility roadmaps. Data generated in the Federal Mobile Summit provides a good starting point for agencies to create (or refine) their mobile roadmaps.

Create Governance for Mobile Spectrum Use
Mobile spectrum availability is critical for tactical mobile systems. Spectrum usage and planning requires close coordination with both government and commercial entities, both in the US and outside of the US. This is often very complex, and many agencies lack the guidance and experience to do this.

The government should establish governance for spectrum use to help organizations determine what spectrum they can use, and how they can request the use of a spectrum in a given area.

Establish a Technical Vision to Guide Organization's Development Efforts

A clear, easy to understand technical vision can help all stakeholders understand their organization's direction and goals for mobility. This is key to not only socialize investment plans and goals, but for gathering feedback from the users of the mobile solutions. Agencies should strive to create a technical vision for their mobility program, but also ensure it is shared across the user community.

Along with the technical vision, a reference architecture should be developed by all agencies deploying mobility, that depict the as-is state of mobile IT, as well as the to-be state of mobile IT. Furthermore, the reference architecture should be published and easily accessible by agency employees. This is useful for both the business and engineering communities to better understand not only the future direction of mobility, but also what the current solution looks like, and what needs to change to get to the desired future state.

Pilot a Continuous Integration Program Before Proceeding with Organization Wide Adoption

Adopting continuous integration concepts, processes, and technologies can be a challenging undertaking. Continuous integration has a ripple effect across key areas of an organization, and all impacted parts of the organization need to work towards the same set of goals.

Due to the complexities of continuous integration, and big impacts it has on culture, process, and technology, organizations should not conduct a "big bang" adoption of continuous integration. Rather, organizations should create a pilot program to experiment with, and learn how to apply continuous integration principles to the larger organization. Results from this pilot can be used to conduct a larger rollout of continuous integration across the larger organization.

Establish a Security Guide for Mobile Application Developers

Mobile app security is critical for all government agencies. Navigating the existing guidance for first time developers can be daunting. For example, the NIAP Protection Profile for Application Software provides useful guidance to security analysts performing app vetting, but it can be difficult to understand by app developers without security expertise.

Guidance should be developed for mobile app developers to securely develop apps. This guidance should be easy to use, and understand, by developers that do not have a security background or by developers that have never developed apps for the government.

5 Acknowledgements

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit. The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the FedSummits web site[8].

[8] http://www.fedsummits.com/mobile/