FEDERAL SUMMITS

OCTOBER 2017 FEDERAL MOBILE TECHNOLOGY SUMMIT REPORT[*]

March 6, 2018

Collin McRae, Patrick Benito, Chris Brown, Dave Keppler, Jeff Stein,
Kevin Boston, CJ Rieser, Justin F. Brunelle
The MITRE Corporation

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

[*] APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. CASE NUMBER 17-3231-XX. **©2018 THE MITRE CORPORATION. ALL RIGHTS RESERVED.**

Contents

1 Abstract **3**

2 Introduction **4**

3 Collaboration Session Overview **4**

3.1 Modern Mobile Security in the Federal Government 5

3.1.1 Session Goals 5

3.1.2 Session Summary 5

3.1.3 Recommendations 6

3.2 Network of Things / Internet of Things 6

3.2.1 Session Goals 6

3.2.2 Session Summary 7

3.2.3 Recommendations 9

3.3 Next Generation Mobile Solutions 9

3.3.1 Session Goals 9

3.3.2 Session Summary 9

3.3.3 Recommendations 11

3.4 Tactical and Field Deployments 11

3.4.1 Session Goals 11

3.4.2 Session Summary 11

3.4.3 Recommendations 13

4 Conclusions and Summit Recommendations **13**

Acknowledgments **14**

1 Abstract

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 four challenge areas in federal mobile computing:

1. Mobile Security in the Federal Government,
2. Network of Things / Internet of Things,
3. Next Generation Mobile Solutions, and
4. Tactical and Field Deployments.

This white paper summarizes the discussions in the collaboration sessions. Drawing from these discussions, MITRE and ATARC developed this paper presents actionable recommendations for the government, academia, and industry.

Establish faster device validation policies

Government agency mobile device policies should be updated to take two years, as current validation policies with longer timescales inhibit the adoption of new technologies. This policy should be enacted alongside the creation of agency specific mobile security strategy to enable faster and safe adoption of new technologies.

In addition, new policies will allow for the government to leverage existing private sector technologies to enable further granularity over mobile device permission control. This will directly aid existing efforts and will facilitate better integration of new technologies.

Establish a requirements-first approach to Internet of Things Devices

Internet of Things (IoT) devices quickly iterate, and vendors are often more focused improving specific technologies rather than security implementations. Approaching IoT devices with an understanding of the security concerns at the time of acquisition will allow for security holes to be filled using existing technologies, as well as guide vendors towards more secure devices. This requirements-first approach will also inform connectivity problems faced by IoT devices and allow for a better utilization of existing and emerging IoT technologies.

2 INTRODUCTION

During the most recent Federal Mobile Computing Summit, held on October 24th, 2017, four 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) [5]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology[1]. 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 four 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:

- Mobile Security in the Federal Government,
- Network of Things / Internet of Things,

[1] https://www.atarc.org/about

- Next Generation Mobile Solutions, and
- Tactical and Field Deployments.

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

3.1 Modern Mobile Security in the Federal Government

This session examined the ever-expanding mobile ecosystem relating to security, identity and trusted access.

3.1.1 Session Goals

- Discuss the evolution of mobile security in the government over the last five years and identify reasons why agencies are still struggling to adopt secure mobile solutions.
- Identify current technology solutions that implement organizational security policy.
- Identify gaps that exist between existing policy/guidance and today's modern mobility landscape.

3.1.2 Session Summary

The initial discussion targeted the challenges that agencies were facing executing their mobility programs. There was a common theme among the participants that there was a lack of government executive understanding of mobile security infrastructure and why it is important. There are also problems related to cost, policy, and skill requirements. Particularly, there is a gap between the policy requirements and the real-world implementations. There is lots of confusion regarding the correct set of policies to deploy to support application vetting, derived credentials and mobile application development. Attracting talent that has the appropriate knowledge, skill, and abilities (KSAs) is common theme generally with security engineering but particularly acute with mobility.

The discussion then shifted to the technical challenges faced in today's mobile environment. Participants asserted current industry mobility solutions were highly fragmented, with no single provider for an end-to-end solution. Current Enterprise Mobility Management (EMM) solutions require integrations with external services to provide application vetting and threat management. Further, a lack of a common set of industry Application Programming Interfaces (APIs) does not exist that can easily enable integration of mobile security products. EMM APIs are currently proprietary and require custom integration coding.

The session ended with a discussion of the rapidly moving mobility environment. Apple and particularly the large variety of Android devices get upgraded at a pace that exceeds policy and certifications. This includes both hardware update cycle and the operating system updates that are pushed down regularly. Agencies do not want to take the risk of using out of date hardware or software due to the slowness of certifications. The rapidness of updates also caused problems for application developers that need to keep code updated to take advantage of the latest features provided by the operating system. The participants noted that a better patch management tool would help alleviate this issue.

3.1.3 Recommendations

- Agencies need to craft policy for two-year adoption of most mobile devices. Do not rely on validation programs that have longer timescales that might inhibit the adoption of new technologies. Agencies should also adopt a separate "mobile security strategy".
- Agencies should carefully review the new guidance presented in NIST Special Publication 800-63-3 [3] which may allow for modern authentication options in addition to derived credentials.
- Mobile security architectures should incorporate the Trusted Internet Connections (TIC) 2.0 reference architectures [2] to increase security posture and incident response capabilities.
- Segregate mobile apps types (e.g., Government off the shelf (GOTS), Commercial off the shelf (COTS), Enterprise mobile apps) and create appropriate application risk profiles.

3.2 Network of Things / Internet of Things

As Internet of Things (IoT) growth continues, and IoT devices and concepts are used in mission and business critical use cases, the security of these devices will become more and more important. Industry and Government face significant challenges in this emerging market.

3.2.1 Session Goals

- Identify key security challenges with using IoT devices.
- Outline a framework for assessing the security of IoT devices.

3.2.2 Session Summary

The session began with a level setting discussion using the ATARC July 2017 IoT working group's definition [1]:

> IoT is an infrastructure of networked objects (cyber-physical devices, information resources, and people) that interact with the physical world through sensors and actuators. This infrastructure enables the collection, transport, storage, assessment and action on data done with or without human intervention.

Given the wide scope of the IoT market and the term's many definitions therein, the group agreed upon this version and used it as a common basis for discussion. As part of this, the group considered the roles people play in IoT applications as well as the delineation between IoT devices and mobile devices. The group discussed how mobile devices can play different roles within the IoT, acting as sensors, gateways, or user interfaces. Also discussed was how mobile and wearable devices have stronger connections to human users, whereas other classes of IoT device are more associated with places and things. The group concluded it is important to consider how people may play a part in IoT architectures as users and decision makers, and additionally as the subjects of sensing and actuation (e.g., with wearable or medical devices).

The discussion then turned towards enumerating the variety of security challenges. Legacy infrastructure is a common source of risks. Many devices designed and deployed under different security assumptions are being networked, undermining security models. For example, networks of devices intended to be air-gapped (e.g., industrial or vehicle control networks) may later be made Internet-accessible. Device lifecycles are also not often given enough consideration, and IoT devices may range from short lived consumer items to long-duration industrial components. Given the rapid pace of development in the IoT space, what is new today will rapidly become tomorrow's legacy equipment. The discussion next turned to problems due to scale. In quantity, small-scale devices can have large scale effects as evidenced by the Mirai botnet[2] and similar events. Further discussion also drew attention to how IoT must avoid introducing new points of failure and fragility into critical infrastructure, such as the food supply, manufacturing supply chains, and electric grids.

A point of debate within the group centered on the roles, responsibilities, and incentives of the different stakeholders in an IoT deployment. First, there are open questions regarding who bears the responsibility for security at different stages of IoT-driven supply chains, particularly with regards to the monetary costs of security. This led to the observation that certain

[2] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

stakeholders at different stages often lack the necessary incentives to invest in security. The group noted that technological solutions exist for many common IoT security problems, yet those solutions may not always be implemented by the suppliers of IoT technology. Similarly, the group remarked that consumers of IoT also bear some responsibility to become better educated about security, and thus create a greater market demand for those features. Discussion then turned to the distinction between information technology (IT) and operational technology (OT) professionals, regarding which the group observed that much of the demand for IoT systems comes from the OT side where a security culture is less ingrained and factors, such as availability, are prioritized.

The heterogeneous and dynamic characteristics of IoT ecosystems generated much conversation. IoT architectures consist of many-to-many relationships between devices, and those relationships can shift drastically over time and in space. More adaptable security approaches emphasizing resilience and risk-management will be needed. The group observed that classic enterprise security approaches that assume more static architectures will not scale well to IoT. Operators of IoT devices face significant device management problems. At one extreme, many devices never receive software updates to fix security vulnerabilities, and device owners and security personnel must find alternate means to mitigate problems. At the other, device vendors may actively push updates that significantly alter device behavior without the operator's knowledge or control. Those deploying IoT systems are often not availed of adequate capabilities to measure and manage risk like they enjoy in the IT space.

Privacy was raised as a significant issue, particularly in consumer-focused IoT market segments. The group discussed information permanence, and how once data is collected it will continue to exist in vendor databases, be traded, and aggregated. Some participants commented that consumers readily give up their data for convenience and other features, yet others questioned whether they do so conscious of the ability for many small pieces of data, innocuous in isolation, to be aggregated and processed into comprehensive behavioral profiles, especially with the advent of ever more powerful data mining and machine learning techniques. The group noted that medical devices are an obvious exception where the public is acutely sensitive to privacy. The discussion then pivoted to how much responsibility average consumers should bear for protecting their own privacy, noting that by and large they are not security experts, and questioning how reasonable it is to demand they should have to be experts.

3.2.3 Recommendations

- Device vendors should clearly communicate the capabilities of IoT components. End users, particularly in the consumer space, need the tools and information about device security to make informed decisions. At the same time, end users must do more to specify their requirements and demand more secure devices.
- Relatively simple techniques can address a significant fraction of security problems. Isolating, quarantining, and other compartmentalization techniques can mitigate many of the aforementioned problems. Similarly, asset management and device discovery tools are becoming more available, offering the ability to find and remove unnecessary devices and risks.
- Interoperability challenges can create opportunities for security. The need for gateways and translators between incompatible devices create choke points where security can be implemented.
- IoT operators should take advantage of resilience techniques more than static defenses. Utilize dynamic models to establish trust in a device over time, adjusting its privileges up and down accordingly. Also, leverage opportunities created by diversity and scale to cross-check the actions of untrusted devices using fault tolerance techniques.

3.3 Next Generation Mobile Solutions

Mobility and complementary technologies, such as augmented/virtual reality (AR/VR) and wearables, are already popular in the consumer market. Government agencies are seeing an increase in demand from their users' to include these, and other emerging tech, as part of their mobile offerings.

3.3.1 Session Goals

- Explore the impact of current and future developments in mobile technology
- Identify ways these developments can be brought to bear upon both current and future issues faced by the federal government.

3.3.2 Session Summary

Although the goal of this session was to look forward towards developments in mobile technology and evaluating how they can solve present- and future-day issues it became quickly apparent that main concerns of participants were more present-day focused. To start the session, moderators posed the following questions:

- What technologies are your users asking for now and what do you expect them to ask for in the future?
- What future technologies do you see making an impact on how you conduct business today?

Using these two questions as a starting block the group started to discuss what issues their agencies were currently facing. The group discovered that most, if not all, of the issues brought up during the discussion could be solved by applying current mobile solutions existing in the private sector. However, for a variety of reasons federal agencies did not currently have access to this technology. The group conducted an in-depth discussion about various types of issues to which individual agencies were seeking solutions.

The first issue facing participants was the need for a mobile helpdesk capability for fleet vehicle management. They were seeking the ability to add a mobile helpdesk chat capability for users who borrow a fleet vehicle. In the case a user ran into an issue with the vehicle they could use an app-based chat capability to help diagnose it. The next issue discussed was a need for enhanced geo-fencing-based Mobile Device Management (MDM) solutions. Current MDM solutions allow for point-radius-based geo-fencing and a set of participants was seeking better granularity. Participants wanted the ability to geo-fence specifically against country borders with the ability to disable specific capabilities of the phone (with a good level of granularity) based on the phone's location.

A participant was seeking a mobile solution for technician management. When a support call went in they wanted the ability to see what technician was closest, dispatch that technician, and then be able to deliver to that tech context specific information such as the specifications for the machinery, a parts list, a service history, what parts are available etc. This could be either be presented via a mobile tablet, or in the future via a wearable technology paired with AR/VR.

In a similar vein, another participant was looking for a mobile dashboard capability for facility management. Upon arriving to a facility, a manager would be able to pull up a list of the current status of the supply chain, what items were arriving that day, what item still needed to be processed from the night before, what equipment (if any) was broken, who called in sick that day, and what their expected need for personnel would be.

As the group discussed solutions to these problems, it became apparent that although the solutions to these issues could be solved with current day technology there were significant roadblocks in the federal space preventing these solutions from being implemented (e.g., policy and security requirements).

As the discussion moved towards impediments there was a general consensus that the government has not yet found the perfect balance between too much and too little security.

3.3.3 Recommendations

- Federal policies should be evaluated to determine where changes could be made that would allow for the easier adoption of new technologies that currently existing the market place.
- Pave an easier barrier to entry for future technologies.

3.4 Tactical and Field Deployments

This session focused on outlining the current and emerging tactical and field mobile solutions and recommending best practices to improve their interoperability.

3.4.1 Session Goals

- Create a portrait of existing and emerging field mobile systems.
- Provide recommendations to improve connectivity to take advantage of mobile technologies.
- Provide recommendations to improve interoperability at the unit, agency, and national levels.

3.4.2 Session Summary

This session began with defining the environment the participants were going to be talking about: what are the capabilities of mobile devices used in the government today? One of the primary uses of mobile field applications was up-to-date situational awareness. This is not limited to tactical applications that could display friendly and enemy locations and points of interest, but anything that could give the user information about the local environment, including weather, terrain, and input from fielded sensors. Field mobile systems also tend to have an unreliable connection to home base, so ad-hoc mobile networks are common to keep connectivity between members of a group or unit in the field. Thus, it is important for application developers to consider the importance of seamless transition between full capability with connections with backend services and degraded capability when these connections are not available. Maintaining a connection with the homebase has benefits for keeping awareness of the mobile users' status as well, such as with the tracking of biometrics. Finally, emerging technologies that are starting to make an impact in the field are AR/VR, either through a phone camera or head mounted display, as well as a variety of wearable devices and sensors.

After the landscape of mobile field technologies was established, the discussion moved to the question of improving interoperability between various technologies and organizations. Inevitably, the domain is filled with a multitude of interface standards and message formats which makes interoperability between many technologies difficult and costly. Caution should be used by any organization attempting to create a "standard of standards" as this can potentially exacerbate the problem. Any new standards should be well-publicized and, most importantly, have buy-in from the community it is targeting. One solution that was discussed to improve interoperability between local units with different capability sets was "ad-hoc sharing," where software is designed so that for the duration of a mission or incident, it can be shared on a temporary basis from one unit to another to enhance coordination. This can help prove out the value of a system without the risk of up-front vendor costs and allow the most successful systems to rise to the top as they are tried and adopted by more organizations. For coordination between small units, the focus of thinking should switch from person to person communications to machine to machine communications.

The third main topic the group discussed was improving connectivity among mobile systems. Several points were brought up as essential to maintaining good connectivity. A standard of robustness should be established and maintained by defining critical features that rely on connectivity between devices or with a backed server, and when services are degraded there should be a graceful step down in capability that is able to maintain usefulness with the information the device can obtain from the local environment. Whenever possible, known resources such as maps should be downloaded to a mobile device before going out to the field to reduce the need to stream them in remotely. This ties into being aware of power consumption which means striking a balance between offloading computation heavy tasks to a remote server and being judicious with limiting overly frequent remote communications which can also unnecessarily drain power. More generally, this is an important consideration when devising requirements-avoiding overtaxing computational and power resources is essential in the mobile environment where these are limited and ignoring this could result in field users losing their mobile capability at inopportune times or being forced to carry large numbers of batteries with them.

3.4.3 Recommendations

- Interoperability
  - Coordination and buy-in is key when developing interoperability standards for a community of interest.
  - "Ad-hoc sharing" can improve interoperability and allow new organizations to test a new system.
  - As mobile and wearable devices proliferate, think of the user as a system.
- Connectivity
  - Maintaining good connectivity starts at the requirements level-critical capabilities and their communication resources must be defined to ensure that the mobile capability maintains usefulness in both ideal and degraded environments.
  - Power and bandwidth consumptions are critical considerations in a mobile environment so these must be optimized and balanced-avoid performing unnecessary computation or remote server requests. Favor preloading resources on the mobile device and using remote servers for computationally heavy tasks.
  - For network flexibility, consider creating services that can be run on diverse platforms, including the mobile devices themselves, backend servers, or in the cloud.

4 Conclusions and Summit Recommendations

As with past Federal Mobile Summits [4], 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:

Establish faster device validation policies

Government agency mobile device policies should be updated to take two years, as current validation policies with longer timescales inhibit the adoption of new technologies. This policy should be enacted alongside the creation of agency specific mobile security strategy to enable faster and safe adoption of new technologies.

In addition, new policies will allow for the government to leverage existing private sector technologies to enable further granularity over mobile device permission control. This will directly aid existing efforts and will facilitate better integration of new technologies.

Establish a requirements-first approach to Internet of Things Devices
IoT devices quickly iterate, and vendors are often more focused improving specific technologies rather than security implementations. Approaching IoT devices with an understanding of the security concerns at the time of acquisition will allow for security holes to be filled using existing technologies, as well as guide vendors towards more secure devices. This requirements-first approach will also inform connectivity problems faced by IoT devices and allow for a better utilization of existing and emerging IoT technologies.

ACKNOWLEDGMENTS

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[3].

REFERENCES

[1] ATARC. Atarc iot innovation lab. `https://www.atarc.org/working-groups/iot/november-2015/`, 2015.

[2] Federal Network Resilience. Trusted Internet Connections (TIC) Reference Architecture Document Version 2.0. Technical report, Department of Homeland Security, 2013.

[3] `http://www.fedsummits.com/mobile/`

[3] P. A. Grassi, M. E. Garcia, and J. L. Fenton. NIST Special Publication 800-63, Digital Identity Guidelines. Technical Report Special Publication 800-63-3, National Institute of Standards and Technology, 2017.

[4] T. Harvey, T. Suder, M. Peck, G. Seth, M. Russell, P. Benito, and M. Collins. August 2015 federal mobile computing summit collaboration session summary. Technical report, The MITRE Corporation; The Advanced Technology Academic Research Center, 2016.

[5] The MITRE Corporation. FFRDCs – A Primer. `http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf`, 2015.