An Overview of the Mobile Security Ecosystem

Federal Mobility Metrics Working Group (FMMWG)

September 2021

Federal Mobility Group

ATARC

Advanced Technology Academic Research Center
designed by government • led by government • attended by government

Acknowledgments

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of the **Mobile Security Ecosystem Overview** paper, authored by the members of the **Federal Mobility Metrics Working Group (FMMWG).**

I would like to take this opportunity to also recognize the following organizations for their contributions:

ATARC
ATSG Corporation
Blackberry
CISCO
CISMobile
General Services Administration
Global Accounting
IBM
ISEC7.com
Kryptowire
Lookout
The MITRE Corporation
MobileIron
NowSecure
Zimperium
Department of Defense
Department of Energy - National Nuclear Security Administration
Department of the Interior
Department of Veterans Affairs
Department of Homeland Security – Cybersecurity & Infrastructure Security
Agency U.S. Agency for International Development

Thank you to everyone who contributed to the ATARC-FMMWG Mobile Security Ecosystem Overview.

Sincerely,

Tom Suder, Founder, Advanced Technology Academic Research Center (ATARC)

David Harris, Lead Federal Mobility Group, FISMA Mobility Metrics Working Group

Table of Contents

Executive Summary

The Federal Mobility Group (FMG) believes that agencies and departments can use a combination of mobile security elements in the ecosystem to produce better outcomes for managing the risk of using mobile device assets to access agency resources while also protecting user privacy. A desired outcome of this paper is to increase federal agencies' knowledge and awareness of currently available mobile security features and tools to help reduce risk from using mobile devices.

This paper describes the security features of the mobile security management ecosystem (tools, technologies, products, and services) and aims to provide initial guidance that facilitates agencies' development of enterprise-wide mobile security strategy and policy, including a program for mobile Government Furnished Equipment (GFE).

The mobile management ecosystem primarily consists of Enterprise Mobility Management (EMM) systems, which have been deployed for several years. The implementation of these products has attained an advanced maturity level across the federal enterprise. EMM systems typically include Mobile Application Management (MAM) capabilities to manage mobile applications installed on enterprise mobile endpoints. EMM systems are increasingly referred to as Unified Endpoint Management (UEM) as they undergo product lifecycle updates to encompass traditional endpoints, such as laptops and desktops, in addition to mobile endpoints.

An additional element in the mobile security ecosystem is mobile app vetting (MAV) systems. MAV systems help identify vulnerabilities by detecting coding flaws and security risks in mobile software at several stages during the development lifecycle and even after the software has been deployed to a mobile device. They can also detect configuration flaws, which provide administrators opportunities to continually enhance their organizations' security posture by addressing configuration issues. At a minimum, in the event they cannot directly address all security challenges on the device, administrators can use knowledge gleaned from MAV assessments to take steps to address remaining risks and mitigate extant threats.

A more recent entry into the mobile device security ecosystem is Mobile Threat Defense (MTD). MTD systems are designed to help detect the presence of malicious apps, network-based attacks, mobile phishing attacks, improper configurations and known vulnerabilities in mobile apps or the mobile operating system (OS) itself.

Finally, an inherent part of the mobile security ecosystem is the mobile OS. Modern mobile OSes include an increasing array of capabilities that protect the integrity of the system code as well as the application code that executes on the OS. These OSes also make other security services available to higher-level application and system code, including secure protocols, cryptography, auditing, access control, and enterprise policy management.

About the FMG FISMA Mobility Metrics Working Group

The Federal CIO Council established the Federal Mobility Group (FMG) and tasked it with improving cybersecurity, governance, and accountability for federal mobile device usage and programs. Co-chaired by mobile leaders from DHS, GSA, and NIST, the FMG sponsors a Federal Information Security Modernization Act (FISMA) Mobility Metrics Working Group (FMMWG) that is focused on updating the FISMA mobility metrics for fiscal year 2022 and beyond.

The FISMA Mobility Metrics Working Group continues to work with vendors and service providers of UEM, MTD, and MAV systems, as well as mobile OS vendors, to identify opportunities to make the FISMA mobility metrics a more robust data capture that reflects both advances in mobile security capabilities and the evolving mobility threat landscape. In collaboration with industry, the FMMWG developed a new metric for fiscal year 2021 to measure the extent of MTD system deployment. This new metric was submitted and approved by the Cybersecurity and Infrastructure Security Agency (CISA) and OMB and is a component of the FY21 FISMA data call.[1]

[1] FY21 FISMA Data Call

Introduction

The increased use of mobile devices over the past decade to conduct government business has been extensively documented and is well known across the federal chief information officer (CIO) community. As a result, threat actors are increasingly turning their attention to mobile devices and the mobile infrastructure environment to seek opportunities for malicious exploitation that can cause harm or reputation damage to federal agencies. The recent COVID-19 pandemic event has increased the attack surface associated with mobility as the government has transitioned to a highly mobile and dispersed workforce.[2] This paper identifies mobile security components, tools, and capabilities to help counter threats to the mobile ecosystem, reduce the risk to government mobility programs, and protect user privacy. The target audience for this paper is the community of IT and cybersecurity decision makers who plan and implement management, security, and privacy protection programs for mobile assets (devices, identities, applications, etc.). These programs are built to secure government mobile devices along with the information and government information systems to which the devices have access. The foundational premise of this effort is that cyber risk can be reduced in the federal mobile ecosystem through increased awareness of cyber threats, and by enabling mobile cybersecurity practitioners to implement the strategies, solutions, and guidance identified in this paper.

Deployment Model and Government Use Cases

An important consideration for implementing effective mobile security management is the specifics of the mobile device deployment model used and the government use case for how the mobile device supports the mission. Considerations for both areas will drive the strategic planning needed to identify and implement the best approach for securing the mobile ecosystem.

Deployment Model:

The deployment model is a key aspect and growing area of importance for mobile device lifecycle management. It describes how a mobile device is provisioned and deployed for use by government and government-associated personnel (e.g., federal contractors). There can be a wide range of acquisition processes and device handling that takes place before agencies provide the mobile device to the end-user. The effectiveness of a mobile device security program can be increased by the government exerting more control during the onboarding process for these devices. Lifecyle processes can be implemented that tightly couple device acquisition with best practices for secure device configuration.

Strong configuration control measures present the opportunity for mobile devices to be pre-authorized for government use and pre-programmed to only allow desired security configurations and security products before the devices are delivered to end-users. Weaker configuration control measures, e.g., applying security features or settings after the device has been delivered to the user, could result in increased risk due to delayed implementation of security tools and features, and/or misconfiguration of security settings. An example of stronger configuration control is the use of Apple's Device Enrollment Program (DEP) (currently referred to as Automated Device

[2] https://enterprise.verizon.com/resources/articles/analyzing-covid-19-data-breach-landscape/

Enrollment)[3] or Samsung's Knox Mobile Enrollment[4] (or other Android) workflows. These device enrollment methods allow customers to set up devices to enforce enterprise supervision out of the box. Using these workflows, agencies can enforce the ability to pre-configure each device per their enterprise UEM policy.

An early government intervention and control capability for mobile devices may require a more mature and comprehensive enterprise mobile device program encompassing device life-cycle functions. Such an enterprise approach may not be attainable for some departments/agencies that have more autonomous and highly de-centralized operating models. To the extent that agencies can push and advocate for earlier intervention and control of government-owned mobile devices, the mobile program managers and cybersecurity practitioners will be able to implement more secure deployment while also protecting user privacy.

For future FISMA mobile device metrics, the FMMWG may examine agency deployment models as referenced above and the degree of administrative control of the mobile device prior to end-user provisioning.

Government Mission Support Use Case:

The government-specific use cases are an important consideration for planning the most appropriate mobile security program. Use cases can range from using mobile devices on the front line to fight wildfires or perform law enforcement functions, to the use of mobile devices for routine government business when working from home or during travel. Travel to international locations presents additional risk to mobile device users; guidance to mitigate risks to mobile devices during international travel is available from several sources.[5] [6]

There may be use cases for shared mobile device use for pooled mobile resources, e.g., by U.S. Border Patrol personnel. GFE mobile device end-users may be seasonal personnel or even volunteers. Additionally, there may be a range of identity-proofing processes for mobile end-users depending on the sensitivity of the government mission or government business the end user will conduct with the mobile device. For inventories of mobile devices that are planned for highly sensitive missions with access to sensitive data, a high level of security and threat protection will be needed to adequately protect these assets. For example, where extensive use of mobile devices in public Wi-Fi areas is anticipated, mobile program managers should factor in the increased threat landscape for that scenario and the strength of security controls needed for those devices to access sensitive government data. This particular use case may require the use of a more in-depth approach for mobile device protection that leverages the conditional access capabilities that can be obtained by using the combined security capabilities of the mobile security ecosystem. Conditional access (or risk-based access) based on near real-time risk posture

[3] Apple - Automated Data Enrollment, September 2020
[4] Samsung - Knox Mobile Enrollment, May 2021
[5] NSA - Mobile Device Best Practices When Traveling OCONUS (nsa.gov), June 2018
[6] OSAC - Traveling with Mobile Devices: Trends & Best Practices (osac.gov), February 2019

assessment is a core tenet of an evolving set of cybersecurity paradigms collectively known as "Zero Trust Architecture".[7][8]

The Mobile Management Ecosystem

Threats to mobile devices are more prevalent and increasing in scope and complexity.[9] Users of mobile devices desire to take full advantage of the features available on those devices, but many of these features provide convenience at the expense of security. Mobile device security products implement secure configurations and security functions to help reduce exposure to mobile threats.

This paper examines the following components of the mobile management ecosystem and their security capabilities that contribute to secure mobile device use:

- Unified Endpoint Management
- Mobile Threat Defense
- Native Mobile OS Security Features
- Mobile App Vetting

These four areas can be viewed as foundational mobile device security pillars (Figure 1) for achieving secure mobile device usage and greater privacy protection. When planning mobile security programs, the contributions of each area should be considered in the context of the use case/mission so that an effective strategy can be employed to weave together these four pillars to achieve maximum impact on reducing exposure to cybersecurity and privacy risk.

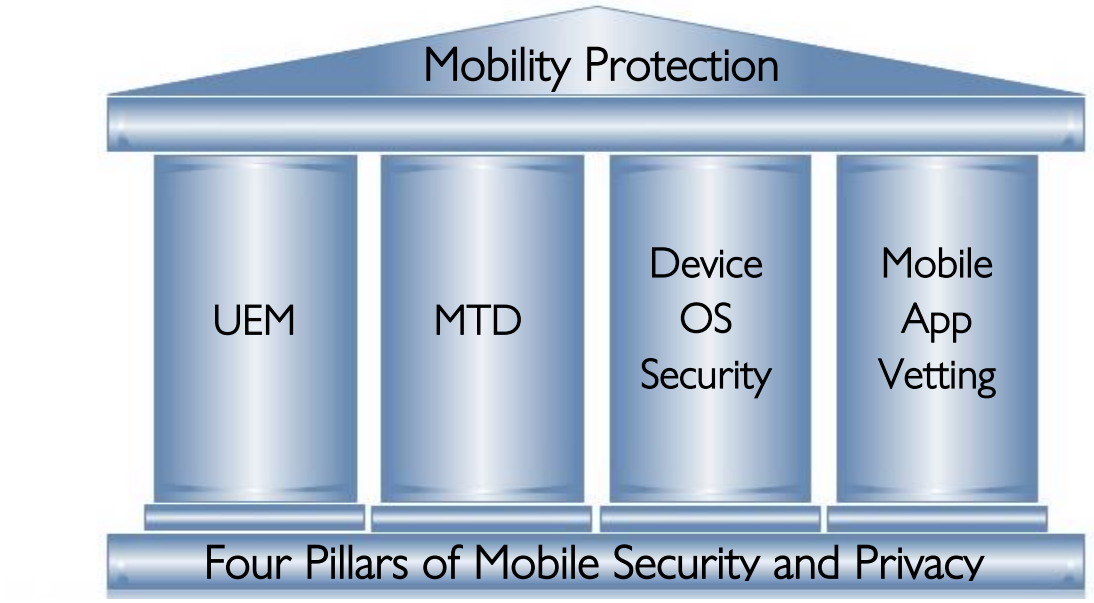


Figure 1. The Four Pillars of Mobile Device Security

[7] NIST - SP 800-207, "Zero Trust Architecture", August 2020.
[8] NSA – "Embracing a Zero Trust Security Model", February 2021.
[9] US allies' national security officials targeted with NSO malware

Unified Endpoint Management (UEM)

EMM systems were early government tools in the quest to implement security management capability for government owned mobile devices. These EMM capabilities are increasingly being referred to as UEM as they undergo product lifecycle updates that provide a single management interface for mobile, laptop/workstation, and other devices. UEMs provide capabilities to enforce standard security configurations and policies on mobile devices, distribute managed mobile apps, and allow for reporting on devices that are out of compliance. UEMs can deny mobile devices access to enterprise resources if the devices fall out of compliance with agency policy. UEM products allow device enrollment/registration and automated lock-down to comply with agency security policies specified for a particular mobile OS. UEM products can also automate the installation and binding of end-user/device identity credentials to support identity governance objectives for the mobile environment. Additionally, UEMs can configure approved enterprise services such as VPN and Wi-Fi settings on mobile devices and remotely configure mobile apps. In the event of a lost or stolen device, UEMs can remote wipe the device to remove government applications and data.

Mobile Threat Defense (MTD)

MTD systems can augment traditional mobile device security solutions to help manage risk for mobile assets. Although MTD is becoming the preferred term, the terms *mobile threat protection (MTP)*, *mobile endpoint security*, and *endpoint protection* also are interchangeably used. MTD products provide near real-time monitoring of the risk state of the device and share that information with enterprise UEM and security information and event management (SIEM) solutions for remediation and awareness of threat posture. NIST SP 800-124[10], NIST SP 1800-21[11] and NIST SP-1800-22[12] provide comprehensive analysis and standards for MTD deployments.

MTD systems are designed to detect the presence of mobile phishing attacks,[13] malicious apps, network-based attacks, improper configurations and known vulnerabilities in mobile apps or the mobile OS itself. A key reason for including MTD in a mobile security strategy is to provide visibility/detection and remediation against various "zero-day" attacks. A zero-day vulnerability is a computer software vulnerability that is unknown to those who should be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit the zero-day to adversely affect programs, data, additional devices, or a network.[14] An occurrence of this scenario took place in January 2021.[15, 16]

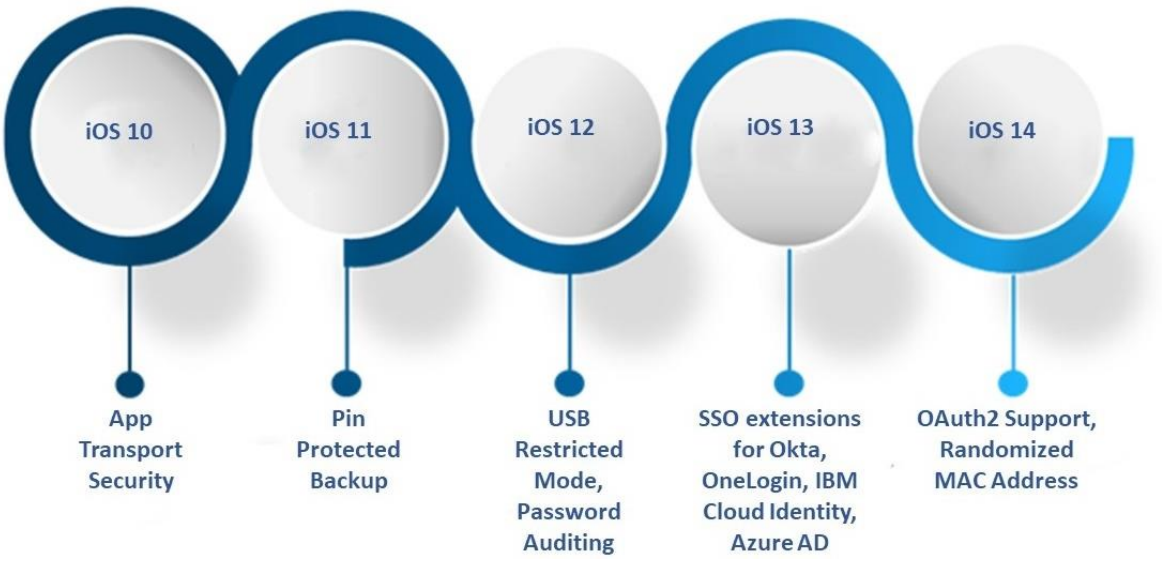
---

[10] NIST – Draft SP 800-124, "Guidelines for Managing the Security of Mobile Devices in the Enterprise", March 2020
[11] NIST – SP 1800-21, "Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)", September 2020
[12] NIST – SP 1800-22, Mobile Device Security: Bring Your Own Device (BYOD)
[13] Mobile device constantly receives unknown text/SMS/WhatsApp messages that contain links or bitly links that sends a user to a website that impersonates a real website in order to gain PII / login and other credential. MTD systems help mitigate negative consequences of a user operation (e.g., human vulnerability) by blocking access to said sites.
[14] Wikipedia - (Paraphrased) "Zero-day (computing)", May 2021
[15] TechCrunch - "iOS 14.4 fixes three security bugs 'actively exploited' by hackers", January 2021
[16] Cyber Talk - "The iOS zero-day exploit throwing journalists for a loop", December 2020

Native Mobile OS Security Functionality

The security elements of the mobile OS provide the first line of defense for the mobile device beyond what is native in mobile hardware/firmware. The most recent releases of mobile device OSes (e.g., Apple iOS, Google Android) ship with security and privacy protection capabilities that can be accessed through native out-of-the-box capability (e.g., file data encryption), security hooks exposed through application programming interfaces (APIs), or through integration with UEM products. Native mobile OS security capabilities also include app sandboxing, app provenance validation, app privacy data tracking disclosure, one-time app permissions, and warnings when visiting fraudulent websites. Mobile security program managers should adopt a posture where new OS releases can be quickly deployed across the mobile enterprise (after completion of agency/department standard testing and vetting processes). Deploying mobile device operating systems with the latest anti-exploitation features forces an adversary to spend considerable resources to bypass defenses or find new vulnerabilities. These features have the potential to make known and unknown vulnerabilities difficult or impossible to exploit. The National Security Agency (NSA) has developed an exhibit the underscores the urgency to quickly adopt new mobile OS updates/upgrades so that increased security protections can be activated on the mobile device.[17] Mobile OS vendors have taken a progressive approach to enhancing the security of their systems. Some of the major enhancements to the Apple and Android mobile OSes are illustrated below (Figure 2).

iOS



[17] NSA – "Update and Upgrade Software Immediately - page 2", September 2019.

Android

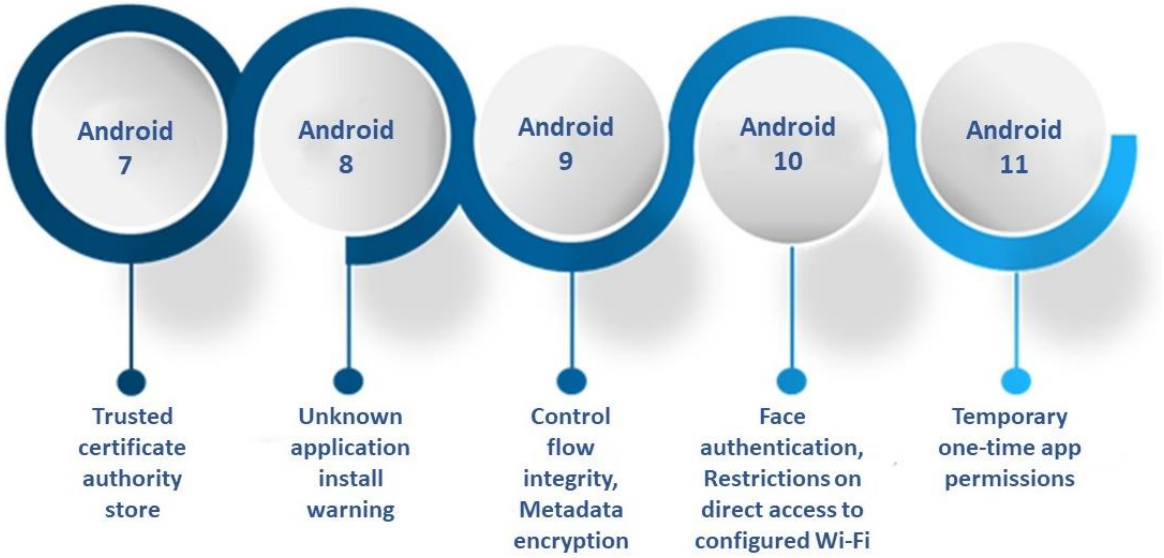


Figure 2. Examples of Progression of Security Features in Mobile OS Releases

Mobile App Vetting (MAV)

The goal of MAV is to detect software or configuration flaws that may create vulnerabilities or violations of enterprise security or privacy policies. (see Figure 3 below). Mobile apps may be developed by mobile device manufacturers (e.g., Apple's apps for iOS), the mobile OS vendor (e.g., Google Maps for Android), third-party providers, or in-house enterprise developers. App developers and OS developers, as well as enterprise administrators, may make mistakes when designing or building an app. They may also intentionally insert malicious functionality that may impact the security or privacy of the mobile user or the enterprise.

As shown in Figure 3 below, app vetting may be employed throughout the mobile app lifecycle:

a) Integrated into the initial development of an app with Continuous Integration/Continuous Delivery (CI/CD);

b) Used during the vetting and review of an app provided by internal or external sources, and,

c) Used to perform continuous app vetting after deployment.

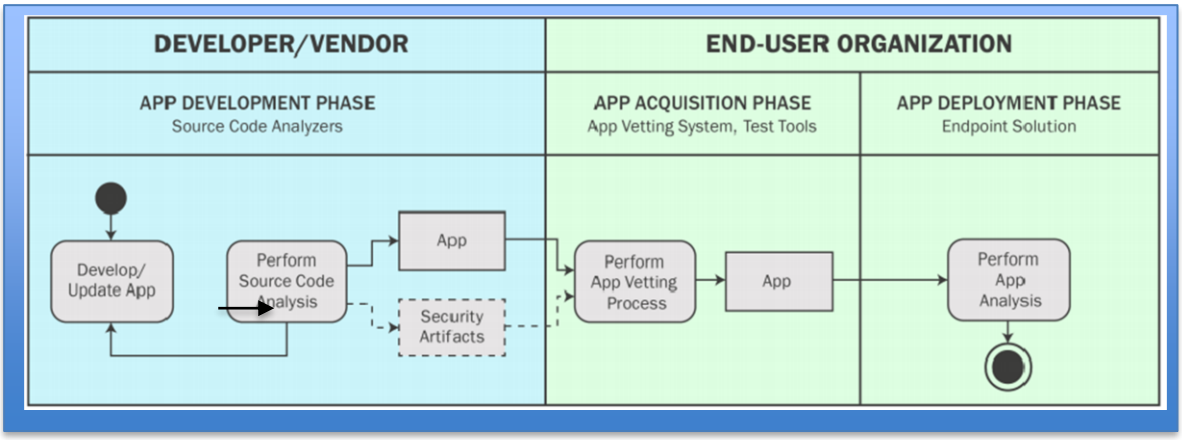


Figure 3. Software Assurance during Mobile Application Lifecycle[18]

One aspect of app vetting that receives a lot of attention is "Code Vetting". Code vetting allows for code review when an organization owns or has control of the source code for the app. In this instance the code must not be encrypted so that it can be subjected to the vetting process. Code vetting is appropriate for code being developed using the DevSecOps lifecycle model. MAV processes have also been developed to accommodate higher security use cases, such as to support national security and/or law enforcement organizations. These higher security use cases involve more involved app vetting that covers a broader set of threats in greater detail, with the expectation that apps must be designed to meet requirements for higher levels of security assurance.

Figure 3 above (taken from NIST SP 800-163) shows the software assurance processes that are foundational within the mobile app vetting lifecycle. For more in-depth information, NIST SP 800-163 Rev 1, "*Vetting the Security of Mobile Applications*", provides definitions and standards for app vetting. Specifically, guidance is provided on planning/implementation, developing security requirements, identifying appropriate testing tools, and standards for mobile app acceptance/suitability for deployment.

The Department of Defense's (DoD) NSA has worked with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Mobile Security Research and Development Program to develop semi-automatable testing criteria for app vetting based on NSA's National Information Assurance Partnership (NIAP) Protection Profile for Application Software.[19] [20] These criteria include tests for how apps interact with platform resources, how they defend themselves from exploitation, the cryptographic libraries they use, what permissions they request, and many others. The Additional Resources section of this paper has additional information on the NIAP protection profile.

[18] NIST - SP 800-163 rev 1, "Vetting the Security of Mobile Applications", April 2019.
[19] DHS – "Automating NIAP Requirements Testing for Mobile Apps", June 2020
[20] NIAP – "Requirements for Vetting Mobile Apps from the Protection Profile for Application Software", March 2019

An Integrated Ecosystem for Mobile Security

A deployment scenario that combines the security capabilities of the four pillars (UEM, MTD, Native Mobile OS, and Mobile App Vetting) can provide a robust security posture for mobility. Current releases of mobile operating systems have APIs that can be leveraged by UEM and MTD products. For example, a UEM might leverage a mobile OS API to configure and enforce protected Domain Name System (DNS) and provide encrypted DNS services. UEM and MTD products can provide complementary security protections based on the capabilities and strengths that each brings to the table. For example, an MTD product may employ multiple sensors to detect real-time threats on the mobile asset and provide that information to a UEM product, which then acts as a policy enforcement point (PEP)[21] to block access to local app data or enterprise resources based on severity of the assessed risk. Additionally, the UEM and MTD products may share threat intelligence data that can be fed to SIEM solutions. Finally, MAV products can screen mobile apps for vulnerabilities before they are deployed and can also integrate with UEMs to obtain a list of installed apps from managed devices and scan those apps for threats and vulnerabilities.

We hope this review of the mobile security ecosystem aided those planning and managing federal mobile program projects and deployments. The links provided in this document can provide additional insight and guidance for specific subject areas.

[21] NIST - SP 800-207, "Zero Trust Architecture", August 2020

Additional Resources

.govCAR

.govCAR represents an evolution in managing cybersecurity. DHS Cybersecurity and Infrastructure Security Agency (CISA) developed .govCAR to take a threat-based approach to cybersecurity risk management—an advancement over traditional consequence (compliance) and vulnerability (cyber hygiene) based approaches. This next generation approach looks at cybersecurity capabilities the same way an adversary does to directly identify areas where mitigations should be applied for best defense.

.govCAR is vendor agnostic and does not evaluate specific vendors or products. CISA designed .govCAR recommendations to communicate the most critical findings and actionable guidance resulting from analysis performed by CISA using the .govCAR methodology.

Key takeaways from .govCAR Spin 5, Mobile Cybersecurity, are summarized below.[22]

The .govCAR analysis identified a range of capabilities that can be deployed to increase threat mitigation coverage. The major finding indicates that to provide maximum coverage against mobile threat actions, organizations must deploy **Enterprise Mobility Management (EMM)**, **Mobile Threat Defense (MTD)**, and **Mobile App Vetting (MAV)** capabilities together as an *integrated solution*, and not as a series of standalone products. **Note:** although integration and interoperability of these three capabilities are key, this solution does not require organizations to source each of the capabilities from a single vendor.

The results of .govCAR analysis strongly suggest that organizations consider all three dimensions of risk (threat, vulnerabilities, and consequences) and use the following lifecycle model:

- **Stage One – Device Selection:** Organizations should first understand their supply chain risk and select devices they can trust. Depending on their risk profile, organizations may want to develop their own APLs or consult third-party APLs before acquiring new mobile devices.
- **Stage Two – Deployment Model Selection:** Next, organizations should determine whether to use a Corporate-Owned, Personally Enabled (COPE) or an Enterprise-Enabled, Owned by the Agency device deployment model.
- **Final Stage – Mobile Cybersecurity Capabilities Integration:** Finally, to achieve maximum effectiveness of available mobile cybersecurity capabilities, .govCAR recommends organizations invest in and deploy **Enterprise Mobility Management**, **Mobile Threat Defense**, and **Mobile Application Vetting** capabilities together, as an integrated solution. The .govCAR analysis demonstrated that coverage against all adversarial threat actions greatly improve only when all three capabilities were integrated (i.e., there was no improvement to the cumulative effectiveness scores of any individual capability).

For more information on the .govCAR methodology, contact CyberLiaison@hq.dhs.gov for the "What is .govCAR" fact sheet. For inquiries about CISA cybersecurity programs, please contact CyberLiaison@hq.dhs.gov. For detailed technical reports on .govCAR spins, contact CyberLiaison@hq.dhs.gov for the .govCAR Technical Annexes and Spin Summary.

[22] .govCAR Recommendations: Mobile Cybersecurity. Resources for Federal Government | CISA

Mobile App Vetting and Related NIAP Protection Profiles

This section outlines NIAP Protection Profiles for developing generalized mobile app security requirements. Organization-specific app security requirements may be drawn from the enterprise's respective security policies.

> "The NIAP Protection Profiles specify an implementation-independent set of security requirements for a category of information technology (IT) products that meet specific federal customer needs. Specifically, the NIAP PPs are intended for use in certifying products for use in national security systems to meet a defined set of security requirements."[23]

The Protection Profile for Application Software includes functional requirements for mobile app vetting, which are outlined in the table below, reproduced from NIST 800-163r1[24] (Table 1):

Table 1 - NIAP Functional Requirements.

Functional Requirements
Access to Platform Resources
Anti-Exploitation Capabilities
Cryptographic Key Functionality
Cryptographic Operations
Encryption of Sensitive Application Data
Hyper Text Transfer Protocol Secure (HTTPS)
Integrity for Installation and Update
Network Communications
Protection of Data in Transit
Random Bit Generation
Secure by Default Configuration
Software Identification and Versions
Specification of Management Functions
Storage of Credentials
Supported Configuration Mechanism
Transport Layer Security Operations
Use of Supported Services and Application Programming Interfaces
Use of Third-Party Libraries
User Consent for Transmission of Personally Identifiable Information
X.509 Functionality

[23] https://www.niap-ccevs.org/ NIAP – "Approved Protection Profiles", May 2021
[24] NIST – SP 800-163r1, "Vetting the Security of Mobile Applications", April 2019

Additional mobile app security guidance may be found through the Open Web Application Security Project (OWASP), which maintains multiple useful resources concerning mobile app testing and security.[25] OWASP's Mobile Application Security Verification Standard (MASVS) (v1.2) is a detailed model for mobile app security that can be used to provide baseline security requirements for a government organization. Like the NIAP PP, the MASVS defines a set of declarations concerning the structure and behavior of an app. However, the MASVS also defines three verification levels:

- Standard Security (Level 1)
- Defense in Depth (Level 2)
- Resilience against Reverse Engineering and Threats (Level 3)

References/Resources

- CISA Cybersecurity Division
  https://www.dhs.gov/cisa/cybersecurity
- Resources for Federal Government | CISA, Resources to Protect, .govCAR Recommendations: Mobile Cybersecurity.
- National Information Assurance Partnership (NIAP), Protection Profile for Mobile Device Fundamentals (PP_MD), Version 3.1, June 16, 2017
  https://www.niap-ccevs.org/Profile/PP.cfm
- NIAP Protection Profile for Application Software, Version 1.3, March 1, 2019.
- Requirements for Vetting Mobile Apps from the Protection Profile for Application Software, Version 1.3, March 1, 2019.
- National Security Agency/Central Security Service's (NSA/CSS), Commercial Solutions for Classified Program (CSfC)
  https://www.nsa.gov/resources/everyone/csfc/
- High Security Mobile Protection: National Security Agency (NSA) - Mobile Device Best Practices
  https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

[25] OWASP – "Mobile Security Testing Guide", May 2021