Mobile Security Best Practices for Federal Agencies in the Post-COVID World

Key Highlights from the May 2022 Roundtable

White Paper

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with **Zimperium**, the global leader in mobile security, industry experts from various Federal agencies discussed the challenges that agencies encounter with mobile security and incorporating new technologies into a Zero Trust Architecture. Panelists shared strategies and best practices to adapt and adjust mobile security to fit the needs and applications of digital modernization, while also meeting new reporting requirements and cybersecurity goals set by the government.

Mobility in Post-COVID Working Environments

The panelists discussed the post-COVID working environment through two primary lenses. The first perspective is for agencies to look inward and focus on the organization's ability to support and protect its employees from mobile security threats. The second and larger focus is how agencies can protect not only the agency's mission but also private individuals and businesses that interact with the agency online.

While some federal agencies have operated successfully under flexible remote and telework policies since as early as 2015, much of that was enabled by government-issued and managed devices connecting to on-premises networks. This worked well until the increased ubiquity of and reliance on mobile devices and cloud infrastructure. Now agencies are faced with new security challenges as employees utilize their own devices, a concept referred to as Bring Your Own Device (BYOD).

> BYOD in mobile context requires significant user trust due to fewer checkpoints on
>
> - How users enter an environment
> - What applications are downloaded
> - Inadvertently shared information
> - Security of network connections

Personal devices are managed by the owner, which makes it difficult for agencies to rely on every device owner to update to the latest OS, patching critical security flaws. Agencies must ensure all OS and applications are up to date as new updates are released, and it is critical that employees leverage encryption to protect sensitive data on all devices that employees are working on, including mobile devices. For unclassified connectivity, agencies must ensure their mobile threat defense (MTD) system can monitor updates to systems and notify users of device risk. There are many aspects of mobile security that agencies must consider (e.g., threat forensics, zero-day detection capabilities, network attack detection and prevention, etc.) to ensure that remote users understand security policies and remain compliant. Allowing employees to BYOD requires significant user trust as many security policies can be overlooked.

In a non-traditional endpoint environment such as mobile, agencies have limited visibility and threat forensics over how users utilize their device, what applications are downloaded, what information is inadvertently shared, or how secure their network connections truly are. Threats today are evolving tremendously as adversaries are looking at mobile devices as new avenues of entry to gain access to sensitive data through on-device, network, malware, and app attacks. With the lines

between mobile and traditional endpoints beginning to blur, security teams must incorporate MTD solutions to provide increased visibility and attest and secure access to agencies from a modern endpoint terrain. Doing so also adds an additional mix of security issues and challenges.

Modern Technologies and Mobile Security Trends

Mobile technology is the future that is arguably already here. Mobile devices are used and relied upon by most individuals, especially at work. As such, mobile security needs to be a predominant focus for agencies at all levels of government, as well as private businesses regardless of size. Of the many security aspects to consider, panelists agree that identifying the many touch points of mobility and understanding advanced mobile threats on-device, network, malware, and app attacks are key to developing a comprehensive mobile security strategy.

First and foremost, robust mobile device management is a key component of mobile security for managed devices, however, when used in conjunction with an MTD, security teams can fill even more security gaps without over controlling a device. Agencies should consider MTD as its own area of investment when it comes to securing mobile devices, especially if additional security apps or monitoring are required. On the contrary, existing security monitors and sensors may not integrate with MDM solutions. Management should also identify which devices are connecting with certain networks and are utilizing software or applications, as users may not be aware of benign-looking applications that are developed in China or Russia with the sole intent of capturing information. Panelists suggest that a best practice for robust mobile security requires agencies to consider an MTD that offers rich telemetry, active monitoring, and most importantly, offer on-device remediation.

Key components of mobile security strategy:

- Identifying the many touch points
- Robust mobile device management
- Embedded vs add-on security code
- Integration of existing security monitors and sensors
- Supply chain security – from device, source code, and network standpoint
- User education on phishing scams

Another aspect of mobile security to consider is the supply chain. Not only should agencies be monitoring where devices are developed and whether they include source code, but agencies must also consider supply chain security from an application standpoint. Mobile devices connect to and download risky apps from third-party app stores that the government has no control over. Agencies should be concerned with rogue wi-fi networks that can pose as potential points of sensitive communications exposure such as a Man-in-the-Middle (MiTM) attack. Additionally, agencies should educate users on mobile device awareness security and look out for phishing scams as they become more sophisticated and evolve into ransomware exploits.

Panelists agree that the use of testing environments is an important step when integrating new technology. Taking new concepts out and testing them in the wild is the truest test to determine exposure risk and identify vulnerabilities. As there are many components to mobile security, testing environments along with vulnerability management, allow agencies to test integration between devices, endpoints, and networks as well as mitigation and response efforts.

Mobile Security, Zero-Trust, and Zero-Day

Roundtable participants shared some of the challenges with meeting Zero Trust mandates in the mobile environment. Agencies must approach Zero Trust in the mobile environment from multiple layers, focusing on resource protection and the premise that trust is never granted implicitly. Organizations operate in multi-cloud environments with data stored with multiple service providers in different locations, and users accessing secure networks in non-linear ways. Authenticating both users and devices on a continuous basis, is of critical importance to ensure a secure mobile environment.

When explaining the concept of Zero Trust, one can think of a user entering a castle, or the network. In the past, someone entered a castle and was authenticated at the gate and then again at certain designated points within the castle. Now, a user enters the castle and is not only authenticated before they enter the gate but also anytime they want to access or move within the castle. The idea of continuously assessing explicit risk and trust levels based on identity and context is the goal of Zero Trust. Continuous authentication is challenging in practice due to a myriad of factors, including not being a turn-key solution, it requires ongoing management, and can disrupt productivity

Panelists shared that they want to take mobile security one step further, by ensuring applications are protected, so regardless of where apps are running, agencies have monitoring and security capabilities in place to eliminate third-party risk. BYOD is particularly challenging, especially for staff facing services that provide access to sensitive data, while trying to maintain productivity. Currently, authentication is not elegant because most of the devices are not aligned with Zero Trust initiatives. However, conditional access, machine identity management, Zero Trust network access and identity-based segmentation such as biometric authentication is a way to combat this.

From a policy standpoint, panelists shared that agencies should approach mobile security and Zero Trust first by looking at each aspect with a verify before trust mentality. By eliminating all access to the network to only those who really need access, agencies can begin to define what their Zero Trust strategy looks like. Ultimately, the migration to full Zero Trust will require phases starting with a solid identity foundation.

By taking steps toward a comprehensive MTD and Zero Trust strategy, agencies can be more prepared to address zero-day, or never before seen, exploits. Agencies are having to evolve their overall threat detection capabilities faster than ever because flash to bang is now more harmful than ever. It is critical to leverage tools to reduce the time it takes to identify, contain and mitigate zero-day exploits before it is too late. While validating identities is critically important, device attestation is a key element for a successful mobile security and Zero Trust strategy.

> Taking steps towards Zero Trust helps be better prepared to address zero-day exploits. Threat detection capabilities need to evolve because flash to bang is now faster than ever. It is critical to cut the time it takes to identify, contain and mitigate zero-day exploits.

Another challenge in the mobile security environment is asset management. Not only do agencies need to manage devices and equipment, but also the apps and capabilities that are extended and running on the mobile device. Even in a classic cybersecurity model, device monitoring is a challenge that agencies must overcome to eliminate a host of unforeseen vulnerabilities and challenges.

OMB 21-31 and BOD 22-01 Requirements

Panelists were asked to share how their agencies are approaching the new FY 2022 Federal Information Security Management Act (FISMA) reporting requirements and the Office of Management and Budget (OMB) Memorandum 21-31, and what strategies agencies are deploying to address Binding Operational Directive (BOD) 22-01 and related software bills of materials (SBOM) risks and concerns.

The recent OMB 21-31 is fairly broad, but directly ties back to section 8 of the Executive Order on Improving the Nation's Cybersecurity to address requirements for logging and information sharing. Notably, mobile threat defense is included in the critical 1 category in the memo. Critical 1 elements must be reported to the executives of each agency, which highlights the importance of accurate logging.

Logging is critical to the visibility and fidelity of what is happening on devices. The information collected in logs can help to inform mobile security of the entire mobile fleet. Mobile traverses a large landscape and having insight into as many threat vectors as possible is critical. But just logging system logs is not enough. Agencies must log and analyze print jobs, mobile device usage, and any aspect that connects to an agency's secure environment.

Logging is especially important for categorization in order for agencies to compare like things to like things. Categorizing helps agencies identify widespread threats or exploits and more easily develop and deploy mitigation packages. When all agencies are working from a similar construct and logging the same way, identifying and mitigating threats becomes more efficient.

In discussing SBOM, panelists shared that agencies should be aware of where materials and components are sourced. Agencies have access to a list of banned companies that produce unreliable or potentially malicious devices and software. However, some of these banned companies are not only producing hardware and software, but they are also providing open source code.

Often, agencies are unaware that the open source code is produced by a banned company. For mobile app development, open source code can be very problematic if security strategies are not implemented during the code development process. In the case of SBOM, agencies should understand whether applications are developed with security codes already in place.

BOD 22-01 provides directives to Federal agencies to reduce the significant risks of known security vulnerabilities. Panelists provided many resources for agencies looking for additional information on known vulnerabilities, including CISA. Both BOD 22-01 and OMB 21-31 direct agencies to log accurately and share information widely between agencies to better defend against widespread cybersecurity threats. Roundtable participants closed the panel by imparting the importance of developing and relying on partnerships. As one panelist stated, cybersecurity is a team sport.

Resources for Mobile Security Integration

- CISA.gov has a tremendous number of resources about mobile security and Zero Trust, including mobile device security checklists for organizations, resources on authentication, protecting devices, and protecting network communications

- The National Institute of Standards and Technology (NIST) 1800-22 on Mobile Device Security: Bring Your Own Device (BYOD)

- The Federal Mobility Group (FMG) recently published a white paper on mobile security, developments in mobile ecosystems, and test environment evaluations and has Working Group meetings twice a month

- ATARC FISMA Mobility Group

- The International Telecommunications Union provides resources and best practices on cybersecurity and critical and emerging technology

- The Zimperium 2022 Global Mobile Threat Report provides a critical and timely view of mobile endpoints and applications' risks, impacts, and threats. The report is based on insights collected by the Zimperium team and survey responses from global technology leaders

- Download Zimperium's Guide: The Government IT Leader's Guide to Securing BYOD to learn how IT and security administrators protect information and connected systems on a device that often lives outside the policies, procedures, and security systems that have traditionally protected the agency's information

- Zimperium Mobile Security Solutions for Government & Federal Agencies