

A VA Executive's Guide to Past Notes: Mobile Security

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)



Introduction

This TS Note revisits three previous TS Notes and combines their highlights into one document. Specifically, this note addresses the challenges of mobile device security. Increasingly, both the private and public sectors utilize smartphones as institutional communication tools, providing employee access to business emails and stored confidential information. Benefits to using mobile devices include increased interoperability, expanded systems capabilities, opportunities to for cost savings in development, and a competitive advantage to drawing the best talent to VA.

As mobile phones collect an expansive quantity of sensitive data, there is a growing need to control and protect the privacy of users and the intellectual property of organizations. Smartphones are targets for security hackers and tech-savvy thieves. The TS Note series has covered three topics in Mobile Device Security: Mobile Device Management, Device Independent Development, and Enterprise Mobility Management. This TS Note will revisit these security topics and their relation to VA's IT Vision.

Mobile Device Management & Containerization

Mobile devices are not inherently secure; however that makes them no better or worse than a laptop. One solution to these risks is Mobile Device Management (MDM) policies to secure government-owned mobile devices. Strict MDM policies limit employees' choice of mobile device (often no choice at all), choice of mobile applications (simple apps like email or calendars), and freedom of use (work only). MDM employs strict rules to address mobile device risk,

hampering the benefits of mobile devices. Furthermore, often the primary security concern is not to secure the mobile device, but to secure the applications that operate on it.

Containerization offers a balance between the limitations of MDM and the security risks of mobile devices. Containerization puts all the enterprise applications you use in a "container," secured from the rest of your phone, which may reduce the usability of those apps. However, the future of containerization places apps in individual containers, allowing for usability with other apps and devices while maintaining the security of the sensitive app. The same technology can be used to develop secure mobile applications and services. Using containerization in mobile app development allows developers to build secure apps from the ground up. The result is a suite of apps that rely on customized security policies to securely share information or services between each other.

Device Independent Development

Device independent development is an important strategy for VA as it moves forward from restrictive MDM. Device independence refers to the nature of an application allowing it to run on different devices regardless of the hardware or operating system of the device. From a security standpoint, device independence emphasizes security at the application level. These applications no longer rely on a network for providing security controls. Instead, they provide their own security, such as FIPS 140-2 encryption for the data residing on and transmitted via mobile devices.

Today, numerous open standards and open source tools make it relatively easy to use local device hardware features, build "responsive" user interfaces, and implement

The TS office within OI&T's Architecture, Strategy & Design (ASD) interacts not only with the ASD pillar offices, but also with multiple stakeholders within OI&T and with strategic offices across the enterprise. TS works closely with IT and business owners to capture business rules and provide technical guidance as it relates to Data Sharing across the enterprise, specifically for interagency operability.

device-independent FIPS-compliant security with only pure HTML5, CSS, and JavaScript. Using service-oriented architecture (SOA) concepts, device-independent development decomposes resources into services, either provided externally or internally to the device. For example, developers use a platform-as-a-service (PaaS) to provide processing resources on which the application will run. Each app can rely on different PaaS implementations, further increasing the agility of the application. From the point of view of an application, then, the end-device is not seen as a static resource, but rather as a set of dynamic services.

code

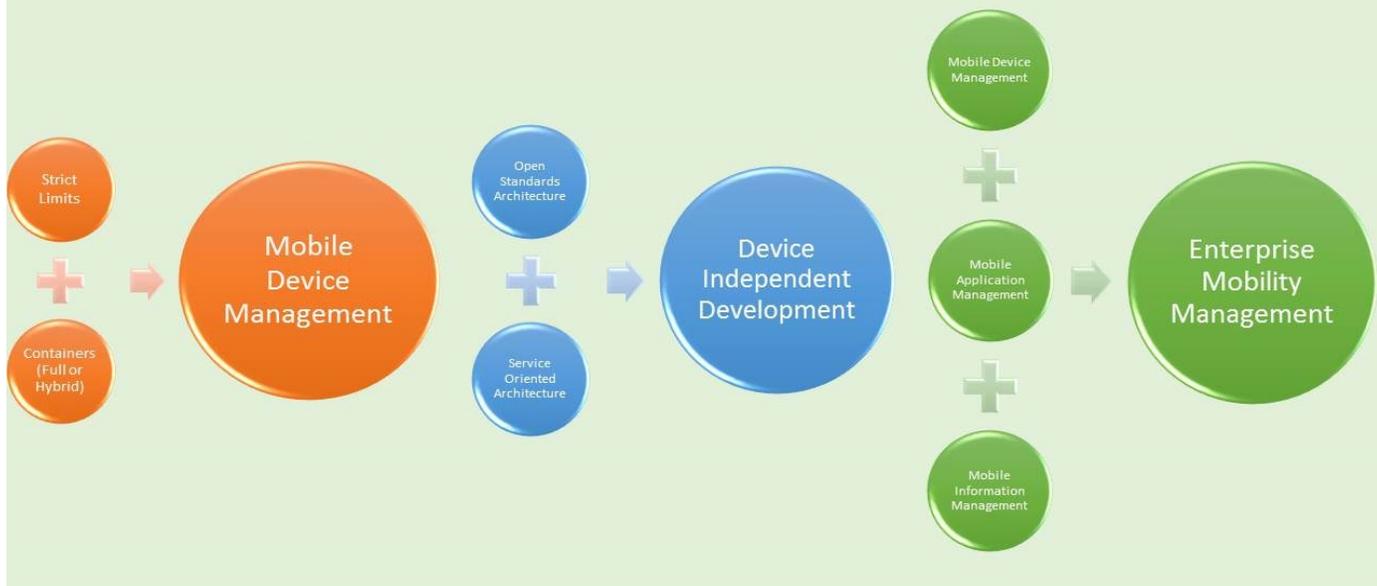
Enterprise Mobility Management

The most recent discussion surrounding mobile security concerns and providing enterprise solutions requires a critical focus on Enterprise Mobility Management (EMM). EMM is a set of systems intended to prevent unauthorized access to enterprise applications and

A VA Executive's Guide to Past Notes: Mobile Security

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)

3 Mobile Security Strategies



data on mobile devices. EMM comprises the combination of mobile device management (MDM), mobile application management (MAM) and mobile information management (MIM). These can include password protection, encryption, and/or remote wipe technology, which allow an administrator to delete all data from a misplaced device. EMM is an all-encompassing approach to securing and enabling employee use of smartphones and tablets. In addition to addressing security concerns, a strong EMM strategy also helps employees be more productive by providing them with the tools they need to perform work-related tasks on mobile devices

While each of the three systems address specific concerns, they still do not provide complete solutions for enterprise mobility security. The challenge lies in managing all three concerns with minimal over-head. As more organizations adopt enterprise mobility management, vendors have started to offer EMM products, usually by adding MAM or MIM features to their MDM products or vice versa. An enterprise app store or other application delivery and deployment technology is also a common component of EMM products.

VA's security strategy must put appropriate BYOD policies in place and ensure mobile apps are secure and device-

independent. EMM is a top solution for helping to control risks and mitigate threats for smartphones. Enterprise data protection (EDP) in operating systems, such as the block, override, and audit protection modes that are offered by Microsoft Windows 10, also help to support a solution.

Conclusion

The future of the VA workplace, as it adapts to a patient-centric operating model, relies on personal mobile devices and emerging mobile technologies. Mobile devices pose significant challenges to securing VA and Veteran information, data, and privacy. VA must focus on improving and evolving its security strategies to support a robust, customer-centric mobile application framework. Mobile applications are a key feature in VA's long-term strategy to enhance information agility and reduce lifecycle costs of IT investments. Ultimately, the growing use of mobile devices and mobile applications across VA requires device independence in order to ensure apps are interoperable and secure across any mobile device.

For more information on these topics, please check out the original TS Notes (Volume 1, Issues 5 and 7, and Volume 3, Issue 1) [here](#), as well as Enterprise Design Patterns on mobility, privacy, and security [here](#). If you have any questions about mobile security, don't hesitate to [ask TS](#) for assistance or more information.