



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

A VA Executive's Guide to Mobile Device Security

INTRODUCTION

This CTS Note discusses the increased use of mobile devices in the workplace and the many security issues raised by this trend. While there are many benefits to mobile device usage in the workplace, there are some security risks to consider. This note highlights some of the basic security concerns, as well as tools and strategies necessary to securely manage mobile devices in the workplace.

BACKGROUND

Across the healthcare industry, private and federal organizations are adapting to a new model of geographically dispersed, patient-centric services. Medical professionals and patients are encouraged to use mobile applications to track, deliver and improve healthcare. This new operational model has impacts beyond health care delivery; non-clinical VA staff and Veteran users are also increasingly using mobile devices to create, store and share personnel, administrative and benefits-related data. There are many benefits to using mobile devices:

- Mobile apps rely on Web services, thereby increasing interoperability
- Mobile apps easily plug into VA systems to provide new capabilities to staff and Veterans
- Federal agencies can engage private industry to build apps at lower cost
- Mobile connectivity is a prerequisite to recruiting and retaining the best people

For this reason, mobile applications are a key feature in VA's long-term strategy to enhance information agility and reduce lifecycle costs of IT investments. However, 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.

IS MY MOBILE DEVICE SECURE?

No. Mobile devices are not inherently secure, but that makes them no better or worse than your notebook. The trick is not to secure the mobile device, but to secure the applications that operate on it. This is the reality of securing mobile devices. There are a few key things to keep in mind when thinking about mobile security:

Popular Technologies are Popular Targets: Because mobile device sales now significantly outstrip PC and notebook sales, it is safe to assume security threats will begin to focus on mobile devices. The bad guys go where the most targets are.

From Foreign Governments to Basement Hackers in a Day: Cyber warfare proliferates with greater speed than traditional threats. A minimal threat today can become a great threat tomorrow.

Mobile Networks on the Rise: We cannot develop and use apps assuming the network is secure. Mobile applications must provide their own security both for data on the device and for communication with enterprise networks and other devices.

EVOLVING MOBILE DEVICE SECURITY

Enterprise-wide security policies and technologies have historically dealt with networks and assets that are physically or logically inside the boundaries of an organization. Attacks on networks from the outside can be deterred by securing the network through a variety of defenses (i.e., firewalls, intrusion detection systems, access control). Each application that runs on the network inherits and relies on the network's

This newly established 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 inter-agency operability.

security.

In the constantly changing mobile world, VA can no longer rely on its networks to provide all necessary security. Mobile devices evolve more rapidly than VA can afford to invest in the latest and greatest devices for staff, and the software application lifecycle will always be longer than the product lifecycle of consumer mobile products we use. There are two ways VA may take advantage of the benefits of mobile devices, while maintaining information privacy and security:

First Generation Mobile Security: Mobile Device Management

Historically, agencies have provided staff with all the devices necessary to do their jobs, like workstations, notebooks, and mobile devices. Mobile devices added another layer of risk, and agencies developed Mobile Device Management (MDM) policies to secure government-owned mobile devices. Strict MDM limits 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). However, in order to

(Continued on page 2)

A VA Executive's Guide to Mobile Device Security, cont'd

take advantage of mobile innovation, organizations have opened up their MDM policies.

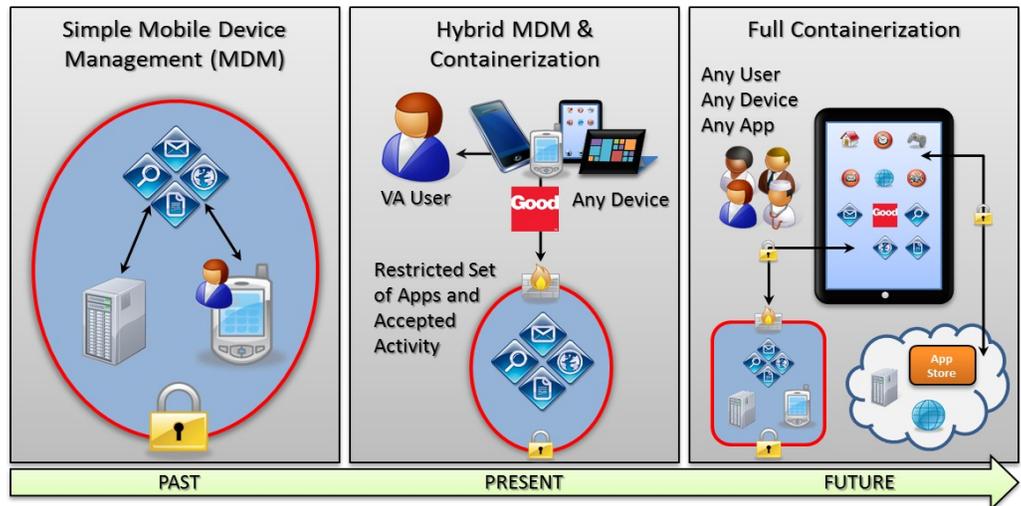
Bring your own device (BYOD) policies (see Figure) allow employees to use any personal device, access enterprise or third party apps, and combine personal and work use on a single device. Initially, strict MDM policies combined with BYOD policies allowed staff to bring their own devices, but still severely limited freedom of use. Further, since the government did not own every device, there was an amount of risk in allowing staff to store sensitive information or applications on personal devices.

The first generation of BYOD security policies to address these challenges focused only on one-off solutions for basic apps like email. VA mobile users may be aware of Good, a mobile security tool for use on personal devices that uses basic containerization. Today, 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, containerization technology has moved on from simply segregating mobile applications. The future of containerization places apps in individual containers, which allows for usability with other apps and devices while maintaining the security of the sensitive app.

Second Generation Mobile Security: Device-Independent Apps

In a mobile world, we can access the banking, gaming, and music apps we use in our personal time on any mobile device running any mobile operating system. This is what makes the mobile app so useful and flexible in a constantly changing marketplace of technologies. VA recognizes we are no longer in a facility-centric world, and the number of personal mobile devices that connect to VA networks is growing. VA has also recently entered into mobile app development with Veteran-focused apps that assist in activities like healthcare management. In order to meet the pace of the mobile marketplace and adapt to a patient-centric business model, VA must begin building device-independent applications.

From a security standpoint, device independence emphasizes secu-



The figure shows how older MDMs only allowed an internal mobile device and apps. The center shows how VA users may have any device, but the MDM restricts apps and accepted activity. The right portion shows full containerization where the MDM allows any user, any device, and any app on the device.

ity at the application level. These applications no longer rely on a network for providing security controls. They may communicate over the mobile network back to an enterprise network, but these channels exist outside VA firewalls. Therefore, device-independent apps must provide their own security, such as FIPS 140-2 encryption for the data residing on and transmitted via mobile devices.

Additionally, containerization does not stop at securing the corporate workplace on a mobile device. The same technology can be used to develop secure mobile applications and services. Using container technology 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.

The future of the VA workplace, as it adapts to a patient-centric operating model, relies on personal mobile devices and emerging mobile technologies. VA's security strategy must put appropriate BYOD policies in place and ensure mobile apps are secure and device-independent.

If you have any questions about mobile device security, don't hesitate to ask CTS (askCTS@va.gov) for assistance or more information. Check out earlier CTS Note editions [here](http://www.blog.va.gov/OIT360) (www.blog.va.gov/OIT360).