

A VA Executive's Guide to Mobile Security

Office of Technology Strategies (TS), Architecture, Strategy & Design (ASD)
A VA Executive's Guide to IT Service Management

Introduction

This TS Note addresses mobile security - the protection of mobile devices, such as smartphones, tablets, and laptops, and their connected wireless networks - to prevent vulnerabilities that pose a threat to the security of information assets. Also known as wireless security, mobile security has become an increasing concern in recent years, as the number of employees who log in remotely and complete work-related tasks on mobile devices has increased significantly. More and more, employees with mobile devices are connecting to corporate and government networks, using their personal devices to manage their organization's email; or using the mobile devices issued to them by their institutions to complete work outside their secure network. This note will highlight mobile security concerns and provide enterprise solutions, including a critical focus on Enterprise Mobility Management (EMM).

Overview

Now that [64% of American adults](#) own a smartphone of some kind, up from 35% just four years ago, mobile security has become ever more important to mobile computing. Increasingly, both the private and public sectors utilize smartphones as institutional communication tools, providing employee access to business emails and stored confidential information. 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. Attacks exploit the weaknesses of the

telecommunication media that supports mobility, such as Short Message Service (SMS or texting), Multimedia Messaging Service (MMS), Bluetooth, and GSM, the de facto global standard for mobile communications. Wi-Fi networks that are not secure allow nearby hackers to intercept data. There are also attacks that exploit software vulnerabilities from web browsers and operating systems. Finally, there are forms of malicious software, known as malware, that rely on the limited knowledge and high-risk behavior of average users.

Challenges

Whenever smartphone users activate their devices, they can be exposed to several threats that can disrupt the operation of the phone, and transmit or modify user data. The applications users deploy from their smartphones should guarantee the privacy and integrity of the information they handle. There are three prime targets for attackers:

1. **Data:** Smartphones are devices for data management; most contain sensitive data like credit card information, account access, or proprietary information.
2. **Identity:** A mobile device is customizable and therefore, most of the information on it is associated with its owner. This makes the owner vulnerable to identity theft.
3. **Availability:** Hacking into a smartphone gives access to tons of information, but it also can limit owner access to the device and deprive the owner of the service.

Top Mobile Security Concerns

There are several ways that mobile security can be compromised. Among the top five are:

- **A Lost Device:** Employees who misplace mobile devices put sensitive data, such as employee personal identity, customer



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.

- information, corporate intellectual property, or government classified data, at great risk.
- **Mobile Applications:** Some mobile apps can request too many privileges, including access to data sources on the device (e.g., analytics tracking by advertising networks). Another concern is malicious or Trojan-infected apps that are designed to look like platforms, in order to secretly upload sensitive data to remote servers.
- **Device Data Leakage:** New mobile business applications can tap into a variety of enterprise data sources beyond just email and calendars, if the enterprise accepts the risks. This increases the draw of cybercriminals, who use malware to target both the device and its back-end systems.
- **Malware Attacks:** The vast majority of mobile malware are SMS Trojans, designed to charge device owners with premium text messages. Experts say Android devices face the biggest threat,

A VA Executive's Guide to Mobile Security

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

A VA Executive's Guide to IT Service Management

- but other platforms can attract financially motivated cyber-criminals if they adopt Near Field Communications and other mobile payment technologies.
- Device Theft: Phone theft is a common problem for owners of highly coveted smartphones such as the iPhone or high-end Android devices. Sensitive data, such as credentials or email access, can fall into the hands of a tech-savvy thief.

A Solution: Enterprise Mobility Management (EMM)

There are several ways to better protect our mobile devices from these threats. These include establishing security within operating systems, using security software, incorporating network or manufacturer surveillance, and promoting user awareness. For the purpose of this TS Note, we will focus on Enterprise Mobility Management (EMM).

EMM is a set of systems intended to prevent unauthorized access to enterprise applications and data on mobile devices. These can include password protection, encryption, and/or remote wipe technology, which allows 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. EMM comprises the combination of mobile device management (MDM), mobile application management (MAM) and mobile information management (MIM).

- MDM: Mobile device management is a type of security software used by an IT department to monitor, manage, and secure employee mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems.
- MAM: Mobile application management is the delivery and administration of enterprise software to the business and personal devices of end users.
- MIM: Mobile information management is a device-agnostic security strategy that involves keeping sensitive data encrypted and allowing access and transmission only from approved applications.

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 overhead. 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.

Conclusion

Device management systems are programmed to support and cooperate with application programming interfaces (APIs) from various device makers to increase security compliance. For many such systems, security policies can be centrally managed and enforced. The mobile devices used in organizations with "bring your own device" (BYOD) policies, however, are often used for both personal and professional purposes. In these cases, IT departments have less control over data loss and damage due to the existence of malware. With mobile devices now used each day by millions, organizations and their employees must be cautious with the information they store and the apps they employ on their vulnerable mobile phones. 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.

If you have any questions about mobile security, don't hesitate to [ask TS](#) for assistance or more information.