

Mobile Device Management: Capability Gaps for High-Security Use Cases

Mobile Device Management (MDM) software provides IT organizations with security capabilities that support the integration of mobile devices into enterprise networks. MDM products support enterprise-owned devices, as well as user-owned devices in what is commonly called the bring-your-own device (BYOD) scenario. However, certain behavior that is highly desirable or necessary for high-security environments remains unavailable on commercial mobile device platforms and is not sufficiently mitigated by MDM products. This paper, intended for mobile device platform vendors as well as risk decision makers, provides an overview of MDM platform components and then outlines these gaps in capability.

Platform Overview

The capabilities of an MDM product fundamentally depend on the management interfaces made available to it by the underlying mobile operating system. In fact, even when an MDM vendor provides a similarly-named product for multiple mobile OS platforms, considerable differences exist between the enterprise management capabilities possible on each platform. Furthermore, neither MDM products nor any commercially-supported 3rd party software enable an enterprise to carry out arbitrary modifications to the underlying mobile OS platform. This represents a fundamental departure from the traditional managed desktop paradigm, in which 3rd party software can run highly-privileged code with power equal to that of the operating system. Yet, mobile OS platforms include very powerful security-enhancing features such as application isolation and mandatory code signing that have yet to be widely implemented on desktop or server platforms. In fact, for the general-purpose use case, it is not at all clear that the lack of some enterprise controls makes these mobile devices less secure than other platforms.

MDM products typically involve an agent on the mobile devices, a server component used by administrative personnel within an enterprise enclave, and an intermediary server operated by the platform vendor. The

on-device agent may be a hidden part of the mobile OS itself, or it may take the form of a 3rd party app distributed through online app repositories. The intermediary server maintains a continuous connection to the devices to facilitate on-demand queries such as push notifications initiated by the enterprise. Some MDM products depend on additional network infrastructure, which may compel additional risk considerations.

Gaps for Specialized, High-Security Use Cases


Most commercially-supported MDM products and the platforms on which they run are designed for general-purpose use and for compatibility with the BYOD scenario. This means that many feature trade-offs have been made that are detrimental to specialized scenarios having higher security requirements. Implementation of the following features would significantly advance the suitability of commercially-available mobile devices for more specialized, high-security use cases across government and industry.

Binding Only to Trusted Wireless Networks. The ubiquitous wireless connectivity of mobile devices is the source of much of their perceived risk to enterprise IT. This risk could be significantly mitigated by enforcing a policy that requires all network traffic from enterprise-managed devices to pass through an enterprise-controlled path, such as a secure WiFi network or VPN, which is monitored and filtered by established network defenses such as firewalls and intrusion detection systems. The need for a robust network binding capability backed by mutual cryptographic authentication is not yet suitably met by any MDM and mobile OS combination. Interestingly, some configurations support the analogous ability to connect only to particular cellular Access Point Names.

Automatic, Comprehensive VPN Connectivity. Many VPN implementations, such as those provided by “SSL VPNs,” ensure only that a subset of a device’s network communications are cryptographically protected and routed to a trusted enclave. Only when all of a device’s network layer communications transit a trusted enclave



The Information Assurance Mission at NSA



is the enterprise positioned to defend in depth against network attacks aimed at the mobile devices. Furthermore, enterprise enforcement of this configuration ensures that users are not burdened with manual setup, and enterprises have confidence in their ability to provide network-based defenses to mobile devices.

Verifiable Device Integrity. Some MDM solutions attempt to detect modification of the underlying platform, but since the MDM agent has limited privileges and is susceptible to compromise by malicious privileged software, these stand little chance of detecting a targeted attack by a capable adversary. An immutable cryptographic root of trust on the platform, available to be leveraged by MDM or other software, provides a means of countering this threat. This provides the ability for devices to credibly attest their integrity to an enterprise and also soundly carry out any local policy decisions. The availability of this root of trust to other software can powerfully complement a chain of trust which begins at boot and extends into system runtime, already available on some platforms. An additional benefit to an immutable root of trust is that it allows an enterprise to bind the unique identity of that device with other credentials to restrict enterprise access to only those devices. In effect, the device itself can become one of the factors of a multi-factor access.

Cryptographic Trust Management. Enterprise-managed devices that connect exclusively to an enterprise intranet have no need to trust many of the root Certificate Authorities that are trusted by default on the platform. To reduce the risk of compromise through fraudulent certificates, enterprises using devices in high-security scenarios should have the ability to remove root Certificate Authorities from managed devices' trust stores. Given the recent, high-profile compromises of certificate authorities and certificates, a compelling case exists for this capability in the general purpose use case as well.

Conclusion

While current MDM capabilities support the BYOD and enterprise-owned use cases, certain gaps exist for high-security use cases. Management capabilities are

limited to those provided to MDM products by the underlying mobile OS, and therefore these capability gaps cannot be closed by MDM providers alone. Ongoing cooperation between enterprise customers, OS vendors, and MDM vendors is essential to the continued advance of enterprise-level security for mobile devices. Closing these gaps will enable the deployment of commercially-available mobile devices for high-security use cases common in sensitive industry and government environments.