Honeywell

Making the Google Android™ Operating System "Enterprise-Ready"

How Honeywell Scanning & Mobility Solves the Security Challenges

Honeywell Scanning & Mobility
Mika Majapuro, Manager - Product Marketing and Daniel Yeakley, Director of Software Engineering

Executive Summary

Historically the Automatic Identification and Data Capture (AIDC) industry has been dominated by Microsoft® Windows® operating systems (OS) like Windows® CE and Windows® Embedded Handheld. However, both end-users and application developers have recently begun looking for viable alternative. Google® Android™ has emerged as the OS that most businesses and developers are evaluating primarily due to its popularity in the consumer smartphone market and the following several reasons:

- More and more AIDC end-users expect rugged hand-helds to have the same or similar user experience as consumer smartphones. The ease-of-adoption lowers the training costs associated with deployment, especially among younger workers.
- In general, the Android™ OS is considered more modern and optimized for touch applications.
- Enterprises are looking to develop applications that may be provisioned to their employees and also offered directly to consumers on their own devices.
- Some developers feel that it is faster to develop applications for Google® Android™ (although this naturally depends on the background of each particular developer).
- The Android™ Market Place has hundreds of thousands of applications that may be helpful for end-users in day-to-day activities and also provides a new route to market for Independent Software Vendors (ISVs).
- Some companies are simply frustrated with Microsoft® and don't see a clear roadmap beyond Windows® Embedded Handheld 6.5.

In spite of these motivations, some IT decision makers have voiced concerns about the security challenges that Google® Android™ presents and those challenges must be addressed before new offerings are widely accepted. In this paper Honeywell Scanning & Mobility has identified those challenges and detailed a series of solutions that enable customers to consider transitioning without putting their businesses at risk.

Device Management and the Honeywell Approach:

The ability to remotely manage an install base of devices running the Android™ OS is the foundation of Honeywell's approach to solving the associated business concerns. Currently, there are multiple third party companies that focus on building remote management and security solutions for Android™. However, in order to truly manage an Android™ offering at the level expected by corporate enterprises, remote management vendors need to get root access to the device which therefore requires close collaboration with the hardware vendors. Without this close collaboration, "off-the-shelf" remote management solutions have limited capabilities to manage Android™ devices across many mobile device OEMs. For example they are not capable of advanced activities, such as installing and uninstalling applications silently or performing advanced help desk activities.

Honeywell offers a remote device management solution - Remote MasterMind™, which leverages an OEM device management engine. Remote Mastermind addresses Android™ vulnerabilities and it greatly reduces the work and effort needed by IT support personnel to deploy and manage devices with an Android™ operating system. And because Honeywell and its partner have worked very closely during the Android™ development process, Remote Mastermind adds a host of capabilities that are not available with many "off-the-shelf" management tools. The issues presented below are not meant to be comprehensive, but instead give a quick overview of the answers that Honeywell offers. Please note, that users deploying Windows® based offerings also encounter some of the same vulnerabilities.

1. Challenge: Root-Access

Rooting, or obtaining root system access, can allow end-users to access additional functionality, tweak system performance and enhance user experience. Unfortunately, it can also reduce the level of system security. Root system access poses potential threat because changes at the root level can potentially allow malware to access private data, remove security or monitoring tools put in place by the enterprise, modify critical system settings that may impact device functionality and worst case scenario, “brick” the device.

Honeywell Solution: By locking users into a kiosk mode or locking down menus using HSM EZMenu, it is possible to prevent users from changing device settings and getting root access. Honeywell’s Remote MasterMind can detect devices that have been rooted and take pre-defined actions to respond to this risk such as removing the device from the corporate network or locking it down. Honeywell has by default disabled root access on the 7800 with Android™ and does not provide tools for rooting.

2. Challenge: Managing Permissions, Applications and Mobile Malware

Permissions management in itself is a good thing. The challenge is that it puts the burden of analyzing applications to the user. An application might state, for example, that it will access the GPS or users calendar. It is then up to the user to either proceed to downloading or to determine that the application might not be appropriate or a security risk.

Further, the various types of applications that need to be managed and sandboxed include enterprise applications, collaborative applications, commercial applications, and custom applications. Third-party applications downloaded on user devices, may not employ secure encryption functionality allowing confidential enterprise data to be easily viewed and exploited. Malware is often masked in third party mobile applications. While this threat is not unique to Android™, Android’s™ huge popularity makes it an attractive target for hackers.

Lastly, spyware and SMS trojans are the two major categories of malware targeting connected devices. Spyware captures and transfers a variety of sensitive data such as GPS coordinates, text files and surfing history. As stated above, this threat is not unique to Android™ but again, Android’s™ popularity makes it more attractive in the eyes of hackers.

Honeywell Solution: There are several ways to tackle issues related with applications and malware. First, by offering a kiosk mode end-users can be locked into an environment where they are unable to access, for example, the internet or mobile market places. Remote MasterMind can also be used to disable certain hardware features such as Bluetooth®, phone, or Wi-Fi™. These settings can be applied both on individual user and group level. Second, by using Remote MasterMind IT managers can create lists of allowed and not-allowed applications and also monitor applications installed on devices and silently removing them if needed. Finally, Honeywell has also partnered with McAfee to offer a virus and malware protection software suite.

3. Challenge: Privacy

By default some of the newer devices geo-tag photos and tweets and applications can also utilize geo-location tracking. The potential risk is that a third-party application can track this data and exploit it leading to potential privacy issues.

Honeywell Solution: When deploying units with Honeywell’s Remote MasterMind, the IT department can enable global settings that can, for example, prevent the use of GPS altogether or limit which applications can access the GPS information. Similarly a list of allowed applications can be used to tackle privacy issues.

4. Challenge: Lost or Stolen Devices

Whenever a device is stolen or lost there is a risk that an outsider can access personal or corporate information. Several data breaches have been reported when mobile devices have gone missing.

Honeywell Solution: With Honeywell Remote MasterMind, IT departments can wipe, kill, and pull data from stolen or lost devices. In addition, Remote MasterMind can be used to enforce the use of complex passwords that will make it difficult to take an advantage of a lost or stolen device.

5. Challenge: Operating System and Device Fragmentation

As Android™ is an open source platform, Google® has allowed developers and OEMs to modify and customize the core Android™ software kernel per the OEM’s discretion to enhance or add new capabilities to their devices. Google® is also releasing new Android™ versions rapidly thus making the fragmentation issue worse. For companies the issue becomes how to manage all the different devices and operating system versions. If an update becomes available for Android™, it is up to the OEM to distribute software updates and security fixes to the OS. This can lead to delays in deploying functionality upgrades to the device. Fragmentation also makes it very difficult for ISVs to create applications that run seamlessly across all devices.

Honeywell Solution: Honeywell will own and support its own Android™ version that has been modified to support AIDC use-cases. Honeywell will always match the operating system and device life-cycles and therefore eliminate the risk of OS not being available. In addition, Honeywell's Remote MasterMind can be used to manage not only Honeywell Android™ devices but competing Android™ AIDC offerings and consumer smartphones as well. Honeywell will also work towards common hardware platforms and common SDKs in order to tackle fragmentation.

6. Challenge: Exchange ActiveSync

Although Microsoft® Exchange ActiveSync has become the de facto standard for email on smartphones and tablets, management and security features are usually inconsistently implemented across different Android™ devices. Many companies desire a solution to limit employee access to corporate email and restrict what they may do when granted access. Some capabilities are provided in leading mobile device management solutions or a third-party solution such as TouchDown from NitroDesk, Inc. may be required to provide robust Exchange Email support via a configurable sandbox.

Honeywell Solution: Remote MasterMind's secure email access adds a second factor of authentication to the email authentication system provided by Exchange. While Exchange verifies the user's name and password, Remote MasterMind verifies the actual device, the user will not be able to receive their email from the non-trusted device until the admin grants permission. Similarly, IT administration can enforce the requirement that users must be enrolled before they can access their corporate email.

Should a greater level of Exchange Email control be desired, a complimentary third-party solution, NitroDesk TouchDown, may be purchased. This solution allows advanced configuration Exchange Email settings and provides a configurable sandbox where corporate email settings can be enforced and data loss prevented.

7. Challenge: Remote Installation

Enterprises need to be able to manage which applications are installed or allowed to be installed on their rugged hand-held computers. With Android™, the only way to remotely install applications is through the app stores such as Google® Play or via uploading them via a flash memory card, which are not a working solution for most IT departments.

Honeywell Solution: Remote MasterMind includes a tool called Package Studio which allows IT administrators to quickly and easily create packages of software/data that can be deployed to mobile devices. The wizard includes options to automatically install or uninstall APK files, as well as to automatically execute and process other types of files on the mobile device. In addition, users have the option of adding scripts that get automatically executed at various points during the installation or uninstallation of the package.

8. Challenge: Wireless Internet and Unprotected Networks

Devices running on older unprotected Wi-Fi networks are open to attacks. Malicious hackers and applications can find users on the network pick up the sign-in credentials and logins of the users and collect information enabling identity theft and corporate espionage.

Honeywell Solution: Remote MasterMind's Configuration Profile Manager is an interface that allows IT managers to create, edit and delete configuration profiles. The profile includes initial configuration like Wireless ZeroConfig, Summit Wireless settings, Fusion settings, Devicescape Wireless settings, Static IP, Cellular connection (APN) settings and Remote MasterMind's Device Agent settings for Windows® Mobile and Windows® CE powered devices that will be managed by Remote MasterMind.

9. Challenge: Data Storage

Although full file system encryption is part of more recent Android™ OS versions, device manufacturers do not consistently apply this feature. Data stored on a memory card (usually an SD card) is not isolated by the underlying Linux kernel and can be freely accessed by any application while still in the device.

> **Honeywell Solution:** Since Android™ 2.3 does not support device level encryption, it is recommended that the ISVs rely on application level encryption. Using Remote MasterMind it is also possible to enforce the use of complex passwords that will prevent hackers from accessing stored data in case a device is lost or stolen.

Conclusions:

The AIDC industry and its operating system landscape is continuously evolving. While Windows® CE and Embedded Handheld used to dominate the market, some customers and ISVs are looking at Android™ as a new opportunity to enhance the user-experience and to offer differentiated software applications. As explained in this paper, Android™ doesn't, however, come without its challenges and Android™ offerings and remote management software solutions simply are not created equal.

When choosing a Honeywell offering with an Android™ operating system, customers don't have to worry about the operating system becoming obsolete: Honeywell will match the life-cycle of both the hardware and software. Moreover, with Honeywell's Remote MasterMind, deploying and managing Android™ offerings is straightforward as IT managers can help close the gaps inherent in making Android™ suitable for enterprise deployment, for example, remotely upgrade software, lock or kill stolen or lost devices all via a simple console that can also be used to manage not only Windows® based devices but scanners and even consumer smartphones as well.

Contact Honeywell with any hardware, software, or services related questions. We're here to take your business to a new level.

For more information visit:
www.honeywellaidc.com

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
800.582.4263
www.honeywell.com

Honeywell