“Hardening” Android: Building Security into the Core of Mobile Devices

Frost & Sullivan Analysis by Frank Dickson
Frost & Sullivan reports are limited edition publications containing valuable market information provided to a select group of customers in response to orders. Our customers acknowledge, when ordering, that Frost & Sullivan reports are for our customers’ internal use and not for general publication or disclosure to third parties.

No part of this report may be given, lent, resold, or disclosed to non-customers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the publisher.

For information regarding permission, write:

Frost & Sullivan
7550 West Interstate 10, Suite 400
San Antonio, TX 78229
United States
“Hardening” Android: Building Security into the Core of Mobile Devices

Table of Contents

Introduction ........................................................................................................... 5

Overview of Mobile Security ............................................................................. 6

What is a Threat in the Mobile World? ................................................................. 6
Contrasting Android and iOS .............................................................................. 8

Android Application Stores .............................................................................. 9

Rooting and OS Settings to Access Alternative Market ....................................... 9
Third Party App Stores ...................................................................................... 10
When Mobile Threats Are Not Black and White .................................................. 11

Good Security Hygiene Practices for Android .................................................... 13

Leveraging Hardware Technology to Improve Android Security ...................... 14

The Foundation of Security—A Root of Trust ................................................... 14
Mobile Challenges with Roots of Trust .............................................................. 15
Roots of Trust in Android ................................................................................ 15

Companies Leading Innovation ...................................................................... 16

ARM TrustZone ............................................................................................... 16
Qualcomm ........................................................................................................ 19
SecureMSM ...................................................................................................... 19
Studio/Access Technology ............................................................................... 20
Enterprise and BYOD security ........................................................................ 20

Samsung ........................................................................................................... 20
Device & Data Security .................................................................................... 20
Container Usability ........................................................................................ 20
Easy Enrollment ............................................................................................... 21
Cloud-based Mobile Device Control ................................................................. 21
Centrify for Samsung KNOX .............................................................................. 21

Intel ................................................................................................................... 21
Intel Identity Protection Technology (IPT) .......................................................... 21
Intel Device Protection Technology (DPT) for Android ....................................... 22

Boeing .............................................................................................................. 24
Blackphone ..................................................................................................... 26

The Last Word ................................................................................................. 27
“Hardening” Android:
Building Security into the Core of Mobile Devices

List of Figures

Figure 1: F-Secure Labs Mobile Threat Classifications ............................................................ 7
Figure 2: Mobile Vulnerabilities by Year (2011-2013) ................................................................. 8
Figure 3: Risk Posture of the Google Play Store ....................................................................... 9
Figure 4: Analysis of the Malware Content of Android App Store ............................................ 10
Figure 5: Mobile Malware Types Common to Sideloadig Practices ......................................... 11
Figure 6: Example Request for Android Application Permissions ........................................... 12
Figure 7: Changing Face of Mobile Threat Vectors; Malvertising Overtakes Porn ................. 13
Figure 8: ARM TrustZone Environments ............................................................................. 17
Figure 9: Attributes and Benefits of TrustZone ...................................................................... 18
Figure 10: Intel IPT Example .................................................................................................. 22
Figure 11: Intel Device Protection Technology Features and Benefits .................................... 23
Figure 12: Intel DPT Secure Containerization ........................................................................ 24
Figure 13: The Boeing Black Smartphone ............................................................................... 25
“Hardening” Android:
Building Security into the Core of Mobile Devices

Introduction

Mobile computing devices such as tablets and smartphones enable a high degree of connectivity and productivity that employees now expect in their jobs. Frost & Sullivan research demonstrates how pervasive mobile is becoming. Recent research provides the following insights:

- Nearly three out of every four organizations issue corporate-owned laptops (74%) and smartphones (71%) to their workforces; while almost half issue tablets (47%).
- Android has taken a surprising lead as the most common mobile operating system supported for organization-owned devices (at 56%); followed by iOS (41%); Windows Mobile (30%); and BlackBerry (28%). The landscape is changing dramatically in this industry.

The use cases of mobile devices result in different risk than traditional PCs. The availability of Internet-based application stores provides uniquely mobile conduits for mobile malware, with Android malware being the favored mobile attack vector. Research by the United States Computer Emergency Readiness Team (US-CERT) confirms that the majority of known mobile threats target Android devices.

In this market insight, we will:

- Provide an overview of mobile security and mobile threats
- Discuss the unique role of the application stores and what makes Android especially vulnerable
- Review good mobile security hygiene
- Discuss how hardware technology can be leveraged to improve Android security
- Elaborate on how some companies are leading innovation by using hardware technology to improve Android security

1 In preparing this report, Frost & Sullivan conducted interviews with representatives of the following companies:

- ARM – Rob Coombs, Director of Security Marketing
- Blackphone – Jon Callas, Co-founder and Board Member
- Blue Coat Systems – Timothy Chiu, Director of Product Marketing, Security
- Centrify – David McNeely, Senior Director of Product Management
- Dell SecureWorks – Tim Vidas, Sr. Security Researcher, CTU
- Intel – Vishram Dalvi, Director of Strategy & Alliances
- Qualcomm – Asaf Ashkenazi, Director, Product Marketing
- Samsung – Dr. Wonseok Back, Ph.D., Senior Manager, KNOX Business Group, Mobile & Comm. Division, Samsung Electronics
- Wave Systems – Greg Kazmierczak, CTO; Girish Bhat, Director of Product Marketing

Please note that the insights and opinions expressed in this assessment are those of Frost & Sullivan and have been developed through the Frost & Sullivan research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

2 For more information on the latest trends in mobile, please see The Future of Mobile Devices from a Customer Perspective: United States and Europe Trends and Opportunities for Mobile Solution Providers (M9CF-65), January 2014.
Overview of Mobile Security

Mobile security cannot be viewed through the same lens or paradigm as personal computer (PC) security. The PC market began as general purpose computing platforms. Due to the evolution of the PC market, the operating system (OS) and the ecosystem of applications that run on the OS are independent. The PC application ecosystem is fundamentally open, designed that way from the start. Historically, a PC user would obtain applications from a number of sources, and install those applications, as long as the user had the proper permissions.3

Mobile, due to its evolution from tightly controlled platform, is different. For mobile devices, which are defined here as smartphones and tablets, applications are generally provisioned from an application store such as Google Play or Apple iTunes. The mobile device, the mobile device OS, and the mobile device application store are tightly coupled. As a result, mobile device security cannot be discussed without discussing the application store(s) that provision applications to the device.

What is a Threat in the Mobile World?

Malicious or compromised applications are the most significant attack vector for mobile devices, making application and application store management especially germane to mobile security. In its 3Q 2013 Mobile Threat Report,4 F-Secure Labs classifies mobile threats into two categories based on their potential for damaging the user’s device or data: ‘Malware’ and ‘Potentially Unwanted Application’ (PUA). See Figure 1 below. A key takeaway from the F-Secure Lab mobile threat classification is that mobile threats are application centric.

---

3 PC ecosystems are beginning to move toward a model similar to mobile. OSX, for example, is very close. Windows is moving there with Windows 8; and Linux distributions like Ubuntu have marketplaces for software. The issues that will be highlighted in this paper may appear in PC markets in the future.

**Figure 1: F-Secure Labs Mobile Threat Classifications**

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Malware</strong></td>
<td>A mobile application that performs actions which pose a significant security risk to the user's system and/or information. Such applications are, by default, blocked from installation.</td>
</tr>
<tr>
<td><strong>Backdoor</strong></td>
<td>A program that provides unauthorized remote access to the device.</td>
</tr>
<tr>
<td><strong>Trojan</strong></td>
<td>A program that deliberately performs harmful actions such as stealing data, hijacking device resources, interfering with the user’s control of the device, etc. Beneficial functionality, if any exists, is intended as a decoy or distraction to draw attention away from the malicious payload. Trojans may be further subdivided by the type of action they take—trojandownloader, trojan-dropper, trojan-spy, etc.</td>
</tr>
<tr>
<td><strong>Worm</strong></td>
<td>A program that creates exact or similar stand-alone copies of itself. The copies can be on the device and/or connected or removable media. A notable subset of worms sends copies of themselves over a Bluetooth connection, i.e., Bluetooth-worm.</td>
</tr>
<tr>
<td><strong>PUA</strong></td>
<td>An application or component that may be considered undesirable or intrusive by a user if used in a questionable manner, or that may inadvertently introduce privacy or security risks. If the user is aware of and accepts the implied risk(s), he/she may elect to install and use the application.</td>
</tr>
<tr>
<td><strong>Spyware</strong></td>
<td>A program that collects data about the user’s behavior patterns, such as Web browsing history and site preferences, and stores the data locally or remotely.</td>
</tr>
<tr>
<td><strong>Trackware</strong></td>
<td>A program that gathers data that could be used to identify a user or a device to a third party; for example, an app that provides device location services as theft protection.</td>
</tr>
<tr>
<td><strong>Adware</strong></td>
<td>A mobile application with an advertisement display functionality that potentially exposes the user to privacy or security risks, as well as exhibiting aggressive advertisement behaviors. Privacy concerns involve the collection or leakage of user’s or device’s personal information such as location, behavior, International Mobile Equipment Identity (IMEI) number, contacts, etc. Aggressive behavior includes changing device settings such as adding home screen shortcuts, browser bookmarks, or icons on the user’s device for advertising purposes. Security concerns involve exposure and/or redirection to unsolicited, unverified or questionable applications, Web sites or contents.</td>
</tr>
</tbody>
</table>

*Source: F-Secure Labs*
**Contrasting Android and iOS**

The current status of mobile malware is highly focused on the Android platform. However, Android does not necessarily have more or less vulnerabilities than Apple iOS (Figure 2).

**Figure 2: Mobile Vulnerabilities by Year (2011-2013)**

![Graph of mobile vulnerabilities by year (2011-2013) with details on affected products.]

Source: Dell SecureWorks

Threats, however, are overwhelmingly dominated by Android. According to the Threat Report 2H 2013 from F-Secure Labs, 97 percent of the mobile threats targeted the Android platform in 2013, including 804 new families and variants. In contrast, 2012 saw 238 new Android threats, demonstrating a huge growth in the problem of Android threats. The role of the application stores of the various mobile platforms is quite significant.

---

Android Application Stores

Taking advantage of the vulnerabilities of Android-based devices is easier than on Apple products, as Apple applications are provisioned from a “closed” or tightly controlled store, requiring application approval from Apple. In contrast, the Android marketplace is open, allowing for easier dissemination of applications with malware.

The official Android application store, Google Play, is open. Google does not vet the applications before they are placed in the application store. Although Google has taken steps to remove potentially malicious software from Google Play, and to ensure that applications in Google Play are compliant with its policies, the process is not perfect. According to RiskIQ, the number of malicious apps in the Google Play store has grown 388 percent from 2011 to 2013, while the number of malicious apps removed annually by Google has dropped from 60 percent in 2011 to 23 percent in 2013 (see Figure 3). To arrive at its conclusions, RiskIQ combines synthetic users with a worldwide proxy network and threat data to analyze and detect malicious digital properties including copycat apps, malvertisements, and rogue Web sites.

Figure 3: Risk Posture of the Google Play Store

<table>
<thead>
<tr>
<th></th>
<th>Apps</th>
<th>Mal-Apps</th>
<th>Removed by Google</th>
<th>% Malware Apps Removed by Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>413,425</td>
<td>10,916</td>
<td>6,592</td>
<td>60%</td>
</tr>
<tr>
<td>2012</td>
<td>327,003</td>
<td>27,666</td>
<td>11,179</td>
<td>40%</td>
</tr>
<tr>
<td>2013</td>
<td>374,529</td>
<td>42,445</td>
<td>9,982</td>
<td>24%</td>
</tr>
</tbody>
</table>

Source: RiskIQ

Rooting and OS Settings to Access Alternative Market

Increasingly, security professionals are discussing methods to protect against the ‘human element’. Users are often, knowingly or unknowingly, active participants in compromising network security.

The “walled garden” design inherent in popular mobile devices limits the user experience to the specific capabilities envisioned by the device manufacturers. While this experience is suitable for many mobile device owners, others may become frustrated to learn that they cannot remove factory-installed apps, download all the apps they desire, or adjust certain device settings. Tech-savvy users overcome these limitations by “jailbreaking” or “rooting” their devices—terms that refer to the process of gaining device root access to remove security features built into the operating system. These practices enable the installation of a modified OS; installation of non-certified applications; tethering (sharing the device’s data connection with other devices); and full device customization controls. However, these practices elevate risk as they allow apps to be installed with root privileges. Essentially, devices that are rooted or jailbroken are stripped of

Users are often, knowingly or unknowingly, active participants in compromising network security.

---

6 http://googlemobile.blogspot.com/2012/02/Android-and-security.html
7 http://www.riskiq.com/company/press-releases/riskiq-reports-malicious-mobile-apps-google-play-have-spiked-nearly-400
important security features, enabling malicious apps to perform unwanted actions—such as accessing sensitive data or operating system functions, without user detection or notification.

In many instances, alternative Android markets may not require rooting the device. Accessing alternative markets can be as easy as changing a phone setting.

**Third Party App Stores**

Third-party app stores often exist for legitimate reasons, such as addressing specific regional, language or business needs. These third-party app stores can be as legitimate as the official app stores. For example, Amazon maintains “Amazon Appstore for Android,” which includes a vetting process to help insure the legitimacy of the applications in the app store. Downloading apps from third-party app stores or Web sites onto a mobile device is called sideloading.

Not all third party sites maintain as secure an approach to the market as does Amazon. Some have little or no vetting. Some alternative markets exist solely to distribute malware. Figure 4 is the result of research conducted by Timothy Vidas and Nicolas Christin, analyzing the malware content of application stores. When a point is graphed on the dotted line, the store is entirely comprised of malware.

**Figure 4: Analysis of the Malware Content of Android App Store**

![Figure 4: Analysis of the Malware Content of Android App Store](image)

Source: Vidas, Timothy, and Nicolas Christin

---

These third-party app stores provide access to “cracked apps,” harboring malware, such as spyware, that steals private data, and aids in the spread of mobile malware, as shown in the following chart.

Figure 5: Mobile Malware Types Common to Sidelocking Practices

![Pie chart showing mobile malware types]

Source: Frost & Sullivan analysis in collaboration with The Android Malware Genome Project

Sidelocking is risky, through the applications that are downloaded and also from the updates. Official app stores often check the legitimacy of updates, and distribute updates to users. Sidelocking circumvent the policing of apps by the proprietors of official marketplaces, and produce unknown and unqualified consequences. Corporate policies that ban rooted and jailbroken devices will greatly minimize an organization’s risk profile, if the ban can be enforced.

Adding to the mobile threat landscape are apps that are more ambiguous in nature, and therefore more difficult to address. For example, apps that require excessive privileges, or that surreptitiously access sensitive data such as contact information or geolocation, are considered potentially unwanted apps (PUA). This increasing amount of access is often required by advertising software.

---

development kits (which developers use in order to profit from apps that are given away for free). Many times, PUAs obscure the high-risk nature of their functionality through cleverly worded descriptions. These apps may be difficult to identify as malware because they do not explicitly violate marketplace terms. They, in essence, operate within the device manufacturer’s rules.

To ensure that apps do not perform unwanted functionality, the Google Play Store requires the user to review and accept requested permissions before installing apps. Unfortunately, excessive permissions can be easily missed, or the seriousness discounted by users as the notification text is highly static and monotone, as shown below. Also, users (and many developers) simply do not understand what a permission means. Users can easily incorrectly assume that apps that are available in official marketplaces have been thoroughly vetted. As a result, users will often accept the requested permissions without reviewing them.

**Figure 6: Example Request for Android Application Permissions**

![Figure 6](image)

Source: Google Play

The PUA category also includes apps that push advertisements (called adware), send costly SMS messages, or place calls to premium numbers. In a recent study, Web root research found that approximately 23 percent of scanned Android apps, from March through August of 2013, were malicious in nature; and a greater percentage was classified as PUAs.

In fact, malvertising has overtaken porn as the leading threat vector (please see Figure 7), according to Blue Coat Systems Mobile Malware Report for 2014. Pornography, once the dominant threat vector, has declined six percentage points from November 2012 to February 2014. One in every five times that a user was directed to mobile malware, it was through the Web, reflecting the increase of Web traffic on mobile devices.

---

For security product vendors, IT organizations, and end users, the challenge is in identifying which apps present a true threat. Identifying a true threat can be difficult when malicious apps blur the lines between useful features and excessive or exploitative functionality.

Figure 7: Changing Face of Mobile Threat Vectors; Malvertising Overtakes Porn

Good Security Hygiene Practices for Android

Mobile security hygiene in a good first step in preventing mobile threats. Security professionals need to be especially vigilant on controlling and monitoring Android-based devices that are accessing corporate data and the corporate network. Employees should be aware of problems created by obtaining content from alternative marketplaces.

Mobile security services are not a panacea, but should be included as a part of current enterprise security planning. Capabilities to be considered in a comprehensive mobile security solution include:

- **Anti-malware**: identify, block, and remove malicious programs or applications including computer viruses, worms, Trojans, rootkits, and spyware.
- **Content filtering**: filter traffic from known malicious Web hosts.
- **Call and message filtering**: block unwanted calls and short message service (SMS) and multimedia messaging service (MMS) communications.
- **Remote wipe and lock**: user or administrators can remotely erase data or lock a mobile device that is lost or stolen.
• **Anti-loss and anti-theft**: remotely locate a lost or stolen mobile device. This feature may sound a loud audible siren or enable Global Positioning System (GPS) tracking.

• **Content controls**: monitor and limit user access to Web sites, messaging and calls based on location, time, or content maturity level.

• **Mobile Virtual Private Network (VPN)**: enable secure VPN connections and session persistence over wireless and mobile networks.

• **Encryption**: secure files on the device and data exchanged with the device.

• **Application reputation scanning**: identify common app risks, such as access to privacy settings, insecure network connections, and malicious code.

• **Jailbreak and root detection**: provide protection through methods such as application wrapping or software development kit integration.

• **Enterprise app store**: provide employees with easy access to company-approved public and custom-built internal applications.

• **Mobile device management**: address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console.

---

**Leveraging Hardware Technology to Improve Android Security**

Implementing good security hygiene has its limitations. Although the security tools can have high efficacy and are a critical element in an organization’s security policy, even the best tools can be challenged in overcoming the ‘human element’ issues. Users still remain the most commonly leveraged attack vector.

Innovative companies are looking to implement measures that “harden” Android, essentially making mobile devices more secure. Hardening goes beyond network or software solutions: it utilizes security embedded in semiconductor devices. As the security industry has clearly been challenged to protect mature operating systems, such as Microsoft Windows, expecting Android to be more secure is improbable.

Security embedded in semiconductors is not a new concept. The SIM card, which is found in many cell phones, utilizes embedded security, which is recognized for its inherent security.

**The Foundation of Security—A Root of Trust**

A critical component of hardened Android-based systems is a root of trust. Roots of trust are software components that are inherently trusted and secure by design, and ideally implemented in hardware. In general, roots of trust perform one or more of the following functions:

• Measure or verify software, ideally in the boot and launch environments such as BIOS, OS Loader, and virtual machines (VMs).

• Protect cryptographic keys

• Perform device authentication
Mobile Challenges with Roots of Trust

Roots of trust are hardly new concepts. They have been in existence in server environments for some time. However, mobile devices present unique challenges that do not exist in server environments. The risk of physical attacks is much greater as the devices are inherently portable, making hardware protections even more critical. Mobile devices are inherently open systems, with multiple processors and interfaces to protect, including central processing units (CPUs), baseband radio, near-field communication (NFC), multiple cellular technologies, Wi-Fi and Bluetooth. Additionally, power and space constraints force the sharing of system resources, such as processing and memory.

Roots of Trust in Android

Essentially, the root of trust provides a “known good” position to assess the integrity of the mobile device, its OS, and its components. The root then enables a secure comparison of software during the boot and launch sequences to known good software components, preventing the launching of unrecognized software, and enforcing known good software configurations. After a root of trust and a known good condition is established, verification of security to other components of the system is extended, such as sealing and protecting memory, and providing attestation of system configuration.

In providing for a root of trust-based foundation for Android devices, the root of trust should provide a cryptographically protected identifier for each approved software component that will be launched, and then provide hardware enforcement mechanisms to block software that cannot be verified. Providing the root of trust in silicon is critical in establishing the foundation on which trusted platform solutions can be built to protect against malware attacks.

For an Android-based system, the root of trust and associated security component should provide the following services:

- **Boot firmware protection** – Protects and isolates the boot firmware from being accessed by the system. This functionality is ideally “hardwired” in the mobile processor, unable to be accessed by the user.

- **Validated system boot** – Verifies and enables a known good state. System changes are detected through cryptographic measurements.

- **Application control** – Creates and implements enforceable lists of “known good” or approved software, application, and executable code.

- **Secure storage** – Includes trace data protection, which removes residual data at an improper shutdown, protecting against memory-snooping software and reset attacks. Trace data protection is implemented in hardware.

- **Attestation** – Validates platform credentials to complete the trust verification process and support compliance.
Companies Leading Innovation

Several companies are leading innovation in the area of hardening Android. Some of the leading solutions are highlighted in this section.

**ARM TrustZone**

The idea of building security into the heart of the system is not a new concept. ARM launched TrustZone in 2003. TrustZone’s motivation is to provide intellectual property (IP) resources to system-on-chip (SoC)\(^\text{11}\) designers so they can embed security into the heart of application processors, which would provide the hardware isolation to protect critical code and data from software attack.

ARM TrustZone is a SoC-based approach that provides the security foundation for a Trusted Execution Environment (TEE) that runs alongside the main OS at the highest level of privilege. Applications such as payment protection technology, digital rights management, and authentication can run on the TrustZone-protected TEE, and are referred to as “Trusted Applications.”

TrustZone technology is integrated tightly into ARM Cortex-A processors, the foundation CPU core for the vast majority of mobile processors on the market. The embedded security is enabled throughout the entire mobile processor SoC using the AMBA AXI bus and specific TrustZone system IP blocks. This approach enables the securing of system peripherals such as secure memory, crypto blocks, keyboard, and screen from software attack. To help SoC developers design the right security features, ARM provides a free-of-charge program called “TrustZone Ready” that maps high-level security requirements to SoC requirements.

Similar to the manner in which virtualization is used in servers and networking infrastructure, TrustZone uses system-wide, hardware-based, security virtualization to create a separate environment for Trusted Applications, as illustrated in Figure 8. TrustZone technology provides a secure world mode for the processor that separates small amounts of trusted code and data from the gigabytes of normal OS and application code found on typical consumer devices. The separation of the trusted environment from the rich OS application environment enables much greater security.

\(^{11}\) Please note that this Market Insight will extensively use the acronym “SoC” to refer to the semiconductor product category of system-on-chip. “SOC” is a commonly used acronym to refer to a security operations center, a centralized center that manages network security. To avoid confusion, security operations centers will not be referenced in this Market Insight.
Samsung has recently launched KNOX 2.0 security platform that uses a TrustZone-based TEE to provide enhanced security; for example, by providing checks that critical code has not been compromised (attestation); or providing a secure storage mechanism for crypto keys. At Mobile World Congress 2014, companies such as Symantec (Authentication) and Good Technology (Dual Persona) were showing Trusted Applications working on Samsung devices that made use of TrustZone.

The TEE has the same capabilities as the normal domain, while operating in a separate memory space. A Secure Monitor within the TEE acts as a virtual gatekeeper, controlling migration between the TEE and the normal domain.

The attributes and benefits of TrustZone are provided in Figure 9 below. The key takeaway is an appreciation of the rich intellectual property toolset that ARM has provided to SoC developers, to enable mobile devices with robust security.
## Figure 9: Attributes and Benefits of TrustZone

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Processor Security Controls Limit Access and Cannot be Bypassed | - TrustZone Monitor provides a single point of entry into the Trusted World which cannot be bypassed, acting as a gatekeeper and can control the interaction between the two worlds  
- Mechanisms to enter into the secure state are well defined  
- Within the Trusted World, Privileged and User states exist, and can have separate page tables from the Normal world so Trusted Applications within the Trusted World need not necessarily have access to all secure peripherals allowing a further hierarchy of control |
| Direct Memory Access (DMA) is Limited and Controlled | - Access to secure peripherals by bus masters is limited to only on-chip bus masters  
- Bus masters can be restricted to be non-secure only by configuration, preventing their access to secure assets  
- The process of deciding which peripherals and bus masters are capable of being within the Trusted World is an important aspect of the system design and directly influences the robustness of the security design |
| DMA from External Devices is Additionally Protected | - The AXI secure control signal is not carried off chip, thereby protecting on-chip Trusted World assets from external attack |
| Controlled Central Processor Access | - Only secure bus masters can access Trusted World assets |
| Processes Consuming Platform Resources can be Identified and Controlled | - Resource allocation can be securely controlled and supervised by a Trusted Application running within the TEE  
- Alternatively, a Trusted Application can be used to monitor and supervise the OS in arbitration of system resources |
| Secure Debug | - TBSA requires debug be correctly managed in production devices |
| I/O Control | - Secure I/O can be controlled from within the Trusted World. All secure peripherals can be selectively chosen to be secure or non-secure as required  
- Secure paths for video, audio and user input can be configured by the Trusted World depending on operation |
| Secure Device Identity | - The Trusted World can be used to securely store keys, and to protect secure identification assets such as serial numbers for IMEI or MAC addresses  
- This allows strong authentication at the application layer, or when network drivers are placed in the Trusted World; it can also allow secure authentication lower down the network stack, and prevent spoofing of unauthorized identification numbers |
| Secure Credential Storage | - The Trusted World can be used to securely store private keys. Cryptographic operations can then occur within the Trusted World by applications in the Normal World, without compromising the security of the keys |
| Measured/Verified Boot | - The Trusted Base Boot Requirements specification (TBBR) recommends how to construct a Trusted Boot sequence  
- In addition, a Trusted Application executing within the Trusted Execution Environment can provide a secure means to store measurements to provide virtual TPM functionality. This can be used in booting the Rich OS, to secure it’s boot process |
| Secure Update/Recovery | - Secure Firmware update is specified as part of the Trusted Base Boot Requirements specification (TBBR) |
| Control Flow Integrity | - The ARM C Compiler/DS-5, provides stack checking functionality for protecting the integrity of system and application software  
- The MMU provides an XN/eXecute Never bit, to ensure data pages cannot be executed |
| Security Primitives | - The ARMv8 architecture provides additional instructions for AES and SHA-1 and SHA-256  
- TBSA specifies RNG |

Source: ARM
Qualcomm

Qualcomm is enhancing the security enabled in its Snapdragon family of processors. Referred to as Snapdragon Security Solutions, the goal of Snapdragon is to leverage security that is embedded in the silicon, to provide more secure mobile computing platforms.

Snapdragon Security Solutions are based on three pillars of security. They are:

1. **SecureMSM** – Embedded hardware and software foundations for security services
2. **StudioAccess Technology** – DRM enabling technology to protect premium video content
3. **Enterprise and BYOD security** – Platform designed to enhance the security and performance of third-party products for the enterprise segment

**SecureMSM**

All Snapdragon processors are SecureMSM-enabled. SecureMSM has three primary components. These components are congruent with the feature enabled by ARM’s TrustZone. Qualcomm is a licensee of ARM technology.

The first component is SecureBoot. SecureBoot is an on-chip, tamper resistant, ROM-based boot-up process that verifies the authenticity and integrity of critical code and data stored in flash memory. The secure boot process controls the system immediately after reset by executing a known code resident in on-chip Read Only Memory (ROM). This code is the system’s root of trust, and authenticates the code used by the device.

The second component is a trusted execution environment. Utilizing ARM’s TrustZone technology (described earlier), the trusted execution environment is a controlled and separated environment that allows trusted execution of code. This code is executed independent of the device’s operating system to prevent, isolate, or monitor possible damage due to viruses, Trojans, and rootkits. Additionally, direct hardware access control of key device resources such as touchscreen, camera and fingerprint reader is provided to prevent access or monitoring by malware.

The final component of the SecureMSM is hardware-based cryptographic acceleration. Clearly, encryption is a critical element of today’s security. Encryption and decryption in software can hinder performance and be a power hog for energy-sensitive mobile devices. Snapdragon’s hardware data encryption is a critical element to enhance the performance and security of cryptographic operations in mobile devices. The high-speed cryptographic accelerators are capable of handling multi-data channels, while maintaining context separations; they also connect to a 256-bit secure hardware key that cannot be accessed by software running on the device.

Qualcomm has an architectural license from ARM, which provides Qualcomm with flexibility that may not be afforded to other ARM processor vendors. Much like the way that Qualcomm designs and customizes its CPU cores, Qualcomm does the same with Qualcomm security. In implementing TrustZone technology, Qualcomm has designed its secure boot as independent Qualcomm proprietary technology that is independent of TrustZone. TrustZone code integrity is protected by secure boot, and is part of the chain of trust; however, it is not the secure boot itself. In the manner in which Qualcomm implements TrustZone, Qualcomm secure boot is the root of trust, and, without it, TrustZone code cannot be trusted, as TrustZone code could be easily modified by unauthorized parties or hackers. TrustZone hardware capability is licensed from ARM, but all the TrustZone support hardware and code is unique to Qualcomm.
StudioAccess Technology

Snapdragon StudioAccess Technology provides a content security platform that gives premium content owners such as “Hollywood studios” confidence that the digital rights management (DRM) controls placed on their content remains secure. Confidence in the efficacy of DRM allows the premium content owners to expand content distribution while protecting content rights. Snapdragon StudioAccess Technology leverages the secure foundation provided by the SecureMSM.

At the heart of the StudioAccess Technology is the Content Protection Zone, an execution environment which isolates video streams and protects DRM keys protected with hardware secure storage. StudioAccess supports multiple flavors of DRM including Microsoft PlayReady, Google Widevine, CPRM, HDCP, and SDB-T. The following processors support the Snapdragon StudioAccess feature: Snapdragon 805, 801, 800, 615, 610, 602A, 600, 410, 400.

Enterprise and BYOD security

Qualcomm is not providing an end-to-end enterprise solution. Snapdragon-based solutions provide the “hooks” or application programming interfaces (APIs) that mobile device management (MDM) vendors can leverage. Qualcomm focuses on its core competency of devices, enabling those that provide network security tools with the ability to improve the overall efficacy of their solutions.

Samsung

Samsung KNOX is Samsung’s initiative to penetrate the market for secure smartphones—a market that has been historically dominated by BlackBerry devices. Samsung is looking to provide a complete security smartphone solution by supplying not only the phone but also the supporting security services. KNOX is a suite of products with the following marketing messages:

- Device & Data Security
- Container Usability
- Easy Enrollment
- Cloud-based Mobile Device Control

Device & Data Security

Samsung is an ARM licensee, and uses TrustZone technology to support embedded security. The device and data security features of Samsung KNOX include:

- **Trusted Boot** – Verifies and authorizes software that can run on the device.
- **ARM TrustZone-based Integrity Measurement Architecture (TIMA)** – Provides a trusted environment and continuously monitors the integrity of the Linux kernel. The violation of the integrity of the Kernel or the boot loader can trigger the disablement of the Kernel and the powering down of the device.
- **Security Enhancements for Android (SE for Android)** – Supports platform security of third-party container solutions in addition to the KNOX container

Container Usability

Samsung KNOX container provides data security by creating a secure area on the device for corporate applications and encrypted enterprise data. The container is isolated and secured, with its own home screen, launcher, applications, and widgets. Applications and data inside the container are isolated from applications outside the container.
Easy Enrollment

Devices are registered through the Samsung Enterprise Gateway cloud server and the Universal MDM Client, a preloaded application on Samsung GALAXY devices. The MDM client communicates with the Samsung Enterprise Gateway to download and install the MDM application. The MDM application automatically authenticates user credentials by communicating with MDM server.

Cloud-based Mobile Device Control

Cloud-based MDM simplifies the mobility management solution, eliminating on-premise infrastructure and associated adoption and implementation issues. Devices are managed through an Admin Portal with Active Directory (AD) support. Through this portal, IT administrators can remote wipe, reset passwords, remote lock, encrypt device storage, restrict use of jailbroken or rooted devices, restrict use of camera, and report location.

Centrify for Samsung KNOX

Samsung has not developed all the technology in-house. Partners have been brought into the fold to supply portions of the technology. For example, Centrify features are bundled with Samsung KNOX devices via an OEM partnership. Mobile Zero Sign-On and single sign-on are available, leveraging AD credentials and role-based authorization. Active Directory-based KNOX container and device management using Group Policy is also available.

Intel

Similar to ARM, Intel has taken the approach of embedding security features into SoCs. The manner of embedding the security is different, though. ARM includes TrustZone as part of its IP cores that integrated into SoCs. Intel instead embeds security in its processors as a separate intellectual property (IP) block. Known as Intel Trusted eXecution Environment (Intel TXE), this IP block is a unique and separate environment for security, complete with unique microcontroller core, memory and operating system (OS), and completely embedded within Intel SoCs. This environment is a platform on which many security services may be implemented.

A significant difference between the Intel approach and the ARM approach needs to be recognized. In implementing TrustZone, ARM works with and through ecosystem partners to provide embedded security. The manner in which TrustZone is implemented is decided by SoC providers such as Qualcomm and Samsung (discussed earlier in this paper). As a result, TrustZone implementations may vary from vendor to vendor. Intel, as a result of both developing the intellectual property and the SoC, has a consistent security offering across all its processors. Given its market share in personal computing devices, this consistency provides advantages to system developers, allowing Intel to take a holistic system design approach that may not be possible when the intellectual property vendor and the SoC vendor are different entities.

Intel TXE provides two features relevant to improving security in mobile devices. Intel Identity Protection Technology enables strong authentication. Intel Device Protection Technology for Android improves system security.

Intel Identity Protection Technology (IPT)

Intel IPT encompasses a suite of products, providing built-in, hardware-level security to protect against identity theft. Intel IPT is embedded in all fourth generation Intel Core processors, Intel
Core vPro processors, Intel Atom processors, and select previous generations of Intel Core processors. IPT is currently targeting Ultrabook applications.

IPT enables strong authentication, often in a multi-factor scenario. IPT, in practice, generates secure one-time passwords (OTPs). IPT protects the OTPs by leveraging the TXE secure environment. As IPT is embedded within a protected area in Intel microprocessors, IPT is independent of the operating system, using special digitally signed applets. Individual Ultrabooks and mobile devices can be associated with a particular online service account if the service supports IPT. The account holder utilizes IPT to generate a one-time password to log in to the account.

Although not currently available for Android-based mobile devices (Atom), additional security functionality is enabled for Core- and Atom-based products running Microsoft Windows. In function, a tamper-proof window that only the user can see is used to enter sensitive data such as username, password, credit card number, and transactions details. As IPT provides a window only users can see for confidential information, IPT provides an additional benefit of providing defense against key-logging and screen-scraping—methods cyber thieves use to obtain access to online accounts. This additional benefit is provided utilizing a protected display overlay that cannot be captured by screen scrapers. The mouse input coordinates are also meaningless with the decoder.

**Figure 10: Intel IPT Example**

---

**Intel Device Protection Technology (DPT) for Android**

Intel DPT for Android was announced at CES 2014. DPT will be integrated into Intel architecture-based Android platforms beginning in the first half of 2014. Intel Device Protection Technology will
also be available on Atom processor Z3xxx platforms (Bay Trail) with the Intel-optimized Android 4.4 release.

Intel is providing a set of software extensions on Intel-enhanced Android platforms that integrate with mobile device management to deliver proactive protection for mobile devices. The extensions support:

- dynamic whitelisting
- malware scans

**Figure 11: Intel Device Protection Technology Features and Benefits**

![Intel Device Protection Technology Features and Benefits](image)

Intel provides comprehensive, secure containerization and extended mobile device management capabilities for enterprise manageability. As a result, personal and corporate environments are separate and independent. Applications can be encapsulated from any app store, and content locked down. Applications may be installed from corporate IT or from a public application store, depending on administrator preferences. The secure container can be remotely locked or wiped, still allowing user access to the device and personal data stored outside of the corporate container. Additionally, the container protects corporate information from data leakage; and personal data on BYODs from being mingled with work data on a managed device. Data in a container is only accessible to users who log in to the container, and cannot be copied electronically from the container. As of March 2014, the announced vendors supporting these capabilities include AirWatch, Citrix, and McAfee.
Boeing

Boeing had recently launched its Boeing Black Smartphone. This smartphone is designed to serve the ultra-secure needs of the U.S. defense and security communities. The specifications of the device include:

- **Display**: 4.3” qHD (540 x 960 pixels)
- **Weight**: 170g
- **Battery**: Lithium-Ion 1590 mAh
- **Dual SIM Supported Bands**:
  - LTE 700/1700/2100
  - WCDMA 850/1900/2100
  - GSM 850/900/1800/1900
- Bluetooth v2.1 + EDR-enabled connectivity
- Dual 1.2 GHz ARM Cortex-A9 CPUs
- Storage: On-board + microSD
- Expansion Ports: micro USB, PDMI, Modular 24-Pin Connector

**Figure 13: The Boeing Black Smartphone**

Security is so paramount that the phone is sealed; and any tampering or attempted disassembly of the phone would destroy the device. The phone is manufactured as a sealed device with both epoxy and screws, and with a tamperproof covering around the casing. Breaking open the casing will trigger functions that completely wipe the device’s contents.

Boeing refers to the system security as the PureSecure architecture. Similar to the functionality provided by ARM’s TrustZone, PureSecure is built upon layers of trust from embedded hardware and operating system policy controls. The device’s hardware roots of trust and trusted boot ensure that the device starts in a trusted state. Hardware encryption and configurable inhibit controls are embedded to protect the device, its data, and the transmission of information. Finally, the Black is compatible with leading mobile device management systems.
Blackphone

Blackphone is another Android-based handset that has a focus on security. Launched at Mobile World Congress 2014, the phone is the product of SGP Technologies, the joint venture of Silent Circle and Geeksphone. Geeksphone specializes in the development of mobile devices based on open source OS. Silent Circle specializes in encrypted voice, video, text, and file transfer on mobile devices. The core competencies of the two companies resulted in Blackphone being comprehensively optimized for security: device, OS, and application suite.

Blackphone comes out of the box set up for privacy. Blackphone has pre-installed privacy tools, including the Silent Circle suite of apps (Silent Phone, Silent Text, and Silent Contacts); anonymous search, private browsing, and VPN from Disconnect; and secure cloud file storage from SpiderOak. In addition, Blackphone is equipped with a remote-wipe and device recovery tool. Finally, the Blackphone Security Centre analyses individual app behaviors to see what they’re accessing, and to give users the ability to block certain actions at the individual app level.

One additional nifty feature is its Wi-Fi manager. Understanding that Wi-Fi is leveraged for various malicious exploits, the Wi-Fi manager identifies safe locations, such as work and home. If the user is not in the range of a safe Wi-Fi environment, the manager switches Wi-Fi off to strengthen privacy and security.

From a pricing standpoint, the Blackphone offers additional pre-paid services over the list price of the phone; including five service-years of Silent Circle (one two-year subscription and three one-year subs); storage from SpiderOak; and private browsing, search, and VPN from Disconnect. The $629 phone has almost $900 worth of available services.

In contrast to other secure Android implementations, control of the security of the device is firmly in the hands of the user, rather than the enterprise. Rather than being optimize to work with Enterprise MDM systems, users have control of the security and privacy of the device. The ideal Blackphone customer is an individual who cares about privacy and security, and does not know where to start.

Blackphone’s emphasis is on optimizing the phone for secure operation. Although the solution is elegant and well designed, it does NOT leverage a hardware-based root of trust. Frost & Sullivan would not classify the phone as having “hardened” Android. If SGP Technologies hopes to address the high-security government and corporate segment, this is a feature that will need to be added.

The Blackphone profile is to provide an example of a higher security device using a software configuration approach. Even though it does not include a hardware root of trust, it is an innovative approach, especially considering that the Blackphone is a first generation device. SGP Technologies is looking at ways to use TrustZone and other hardware approaches. Adoption of hardware-based approaches is most likely contingent on market interest.
The majority of the security risk with Android resides with the mobility use case of the platform and the risks introduced by users acting as unknowing participants in compromising Android-based systems.

Good security hygiene is always recommended. Comprehensive mobile security is a required component for enterprise security planning, providing services such as anti-malware, content filtering, remote wipe and lock, anti-loss and anti-theft, VPN, and encryption.

A complete solution needs to include a robust and secure client with security not just layered on top of existing devices but with security built into the device.

Android devices need to be “hardened,” with security built into the device. A critical component of hardening Android-based systems is a root of trust. Roots of trust are components that are inherently trusted and secure by design, ideally implemented in silicon. Essentially, the root of trust provides a “known good” position to assess the integrity of the mobile devices, its OS and its components. Beginning with this known good position, additional security services can be provided such as boot firmware protection, validated system boot, application control, secure storage, and attestation.

Momentum is clearly behind the hardening of Android-based devices. With the growing sophistication of malware, individuals, businesses and security professionals are looking for security tools to improve the security efficacy of Android-based devices. Hardware-based security has benefits that simply cannot be ignored. Clearly, the discussion is not about whether Android-based devices will be hardened, but rather the speed of that process in the market.

---

**Frank Dickson**

Industry Principal – Information and Network Security
Frost & Sullivan
frank.dickson@frost.com
About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan’s Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.frost.com, dial 877-463-7678, or e-mail inquiries@frost.com.