White Paper

Samsung on Android™

The secure, defense-grade alternative

2016 Second Edition

Samsung on Android™
The secure, defense-grade alternative

Headlines frequently warn about the growing threat from mobile malware, which is increasingly a key concern for any organization that is embracing the connected enterprise. The popularity of Android has skyrocketed in the general market, as it now powers 81% of the world's mobile devices[1]. Erroneous mobile security perceptions dating back to the early days of Android and some negative press propagated by the media and security vendors are deterring some enterprises from leveraging the Android platform for competitive differentiation and business transformation.

Enterprise mobile security is paramount to realizing the full potential of the connected enterprise. This paper presents an overview of enhancements made to the Android operating system, Google Play security services, and Samsung Knox. The paper also includes data from the *Android Security 2015 Year In Review* report. Together, these enhancements make Samsung devices running Android among the most secure mobile devices available to enterprises and government organizations alike.

Android operating system enhancements and Google Play security

Google has always implemented a multi-tiered security model to include application sandboxing and security services provided by Google Play Services. Recently, Google has made significant improvements in Android security, which include:

1) enabling deployment of full disk and block-level encryption;
2) expanding the use of hardware-protected cryptography and removing older exportable cipher suites;
3) securing the Linux kernel by requiring Security-Enhanced Linux (SELinux) to run in full enforcing mode, which requires Mandatory Access Controls (MAC) policies;
4) incorporating secure inter-process communications (IPC);
5) implementing vulnerability exploit mitigation with Address Space Layout Randomization (ASLR);
6) enabling security updates verification with the Android security patch level feature; and
7) allowing users to see, grant, and revoke permissions for applications at a granular level using the new permission models.

Also inherent in the Android security ecosystem are Google-provided security services, which went through major enhancements in 2015:

Verify Apps uses a cloud-based service to check every application prior to installation to ensure that the device is protected against Potentially Harmful Applications (PHAs). Verify Apps screens all applications for PHAs, even installations from unknown sources. It also checks all previously installed apps on a regular basis.

Safety Net validates that the device is operating as expected according to the Android security model and detects and protects against network-level attacks.

Safe Browsing (for Google Chrome on Android) protects against browser-based exploitation and websites attempting to deliver PHAs.

Android now powers
81%
of the world's mobile devices

Verify Apps performs over
400 million
security scans of devices per day and nearly cut in half the number of infected apps downloaded from non-Google Play app stores

More than
1 billion
devices are protected by Android's holistic security ecosystem

6 billion
installed apps are scanned every day by the Android holistic security ecosystem

Google delivers monthly security updates for Android to address vulnerabilities and ensure enterprise security

WebView updates are now provided via Google Play as needed to update, reduce, and remove SSL vulnerabilities.

System Integrity Check (SIC) is an on-device client that hashes the system partition and checks it against a Google cloud-based service with a collection of known good system partitions.

Anomaly Correlation Engine (ACE) monitors devices for changes in key security indicators, then examines which applications have changed since the device was in a known secure state.

The enhancements to Google Play security services have reduced the probability of installing a PHA from Google Play by over 40% compared to 2014. Within Google Play, install attempts of most categories of PHAs declined, including:

Data Collection decreased over 40% to 0.08% of installs

**Spyware** decreased 60% to 0.02% of installs

Hostile Downloader decreased 50% to 0.01% of installs

Google launched the Android Vulnerability Rewards program to encourage independent security researchers to test Android's security protections and help make the Android platform and ecosystem even safer. Google has also begun delivering monthly security updates for Android to address vulnerabilities and ensure enterprise customers get timely Android OS patching. Samsung has also committed to an aggressive update schedule for the carriers.

Google works continuously to reduce the existence of PHAs in the Android ecosystem by vetting applications offered via Google Play and expanding the set of security services for applications that run on the Android platform. All applications on Google Play are subjected to an in-depth security analysis before they are made available to the public. This includes a static analysis, dynamic analysis, heuristic analysis, third party review, and when needed, a manual review to identify and classify any potential threats. All applications in Google Play are reviewed on an on-going basis.

In 2015, the largest global threat to Android was installation of PHAs—"applications that may harm a device, harm the device's user, or do something unintended with user data"[2].

[2]Google (April 2016), Android Security 2015 Year in Review. Retrieved on September 23, 2016. https://goo.gl/kDc3gM
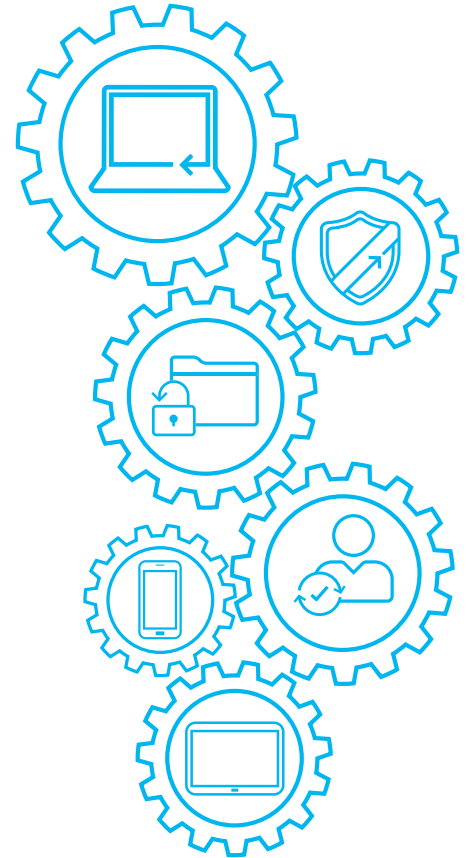
The majority of devices with PHAs installed have unknown sources enabled and have installed applications from outside of Google Play. On average, less than 0.5% of devices had a PHA installed during 2015 and devices that only installed applications from Google Play averaged less than 0.15%[3]. Devices that allow apps from outside of Google Play are around 10 times more likely to have PHAs than those that only install from Google Play. Enterprises can effectively manage the proliferation of PHAs through security policy and controls.

The Google report *Android Security 2014 Year in Review* showed that devices located in Russia that had applications installed from outside of Google Play were over 5 times more likely to install a PHA than the worldwide average; in early 2015, this device population region was identified as "at risk." Russia and Southeast Asia continue to represent the most at-risk devices. Stronger security for at-risk devices in these regions was applied to reduce the occurrence of PHAs. Some of the changes to the default configuration of services to enable stronger protection included:

1) increasing the frequency of device-wide security scans;
2) aggressive blocking of PHAs; and
3) working with a company that provides OTA update infrastructure and OTA updates as
   a service in Southeast Asia to develop a better security process to scan the applications.

As a result of these enhancements in the standard Android operating system, and in conjunction with the in-depth, continuous application review process, there are now over 1 billion devices protected by the Android holistic security ecosystem, which performs security scans of 400 million devices and 6 billion installed apps every day.

Samsung Knox platform–
## customizable, defense-grade, hardware-based security out of the box

In addition to Google's enhancements to the standard Android operating system, Samsung incorporates Knox, a defense-grade mobile security platform, which protects Samsung devices from the hardware level up, starting at boot-up and running throughout the entire device lifecycle. It is a combination of platform-level security safeguards as well as a suite of companion products and services that leverage the secure platform. This platform-level protection is standard on all of the latest Samsung flagship smartphone and tablet devices. Samsung Knox 2.6 received the most "strong" ratings of any mobile security platform in the report *Mobile Device Security: A Comparison of Platforms[4]*.

Samsung smartphones and tablets running Knox employ Secure Boot, Trusted Boot, Security Enhancements for Android (SE for Android), and ARM® TrustZone®-based Integrity Measurement Architecture (TIMA).

Secure Boot and Trusted Boot verify both the authenticity and integrity of the bootloader modules and the Android kernel. This is now a mandatory implementation required by Compatibility Definition Document (CDD) and Compatibility Test Suite (CTS) from Google.

TIMA Periodic Kernel Measurement (PKM) performs continuous monitoring of the kernel to detect if legitimate kernel code and data have been modified unexpectedly.

Knox Real-time Kernel Protection (RKP) performs ongoing real-time monitoring of the operating system from within TrustZone or the hypervisor (depending on the device model) to prevent tampering with the kernel.
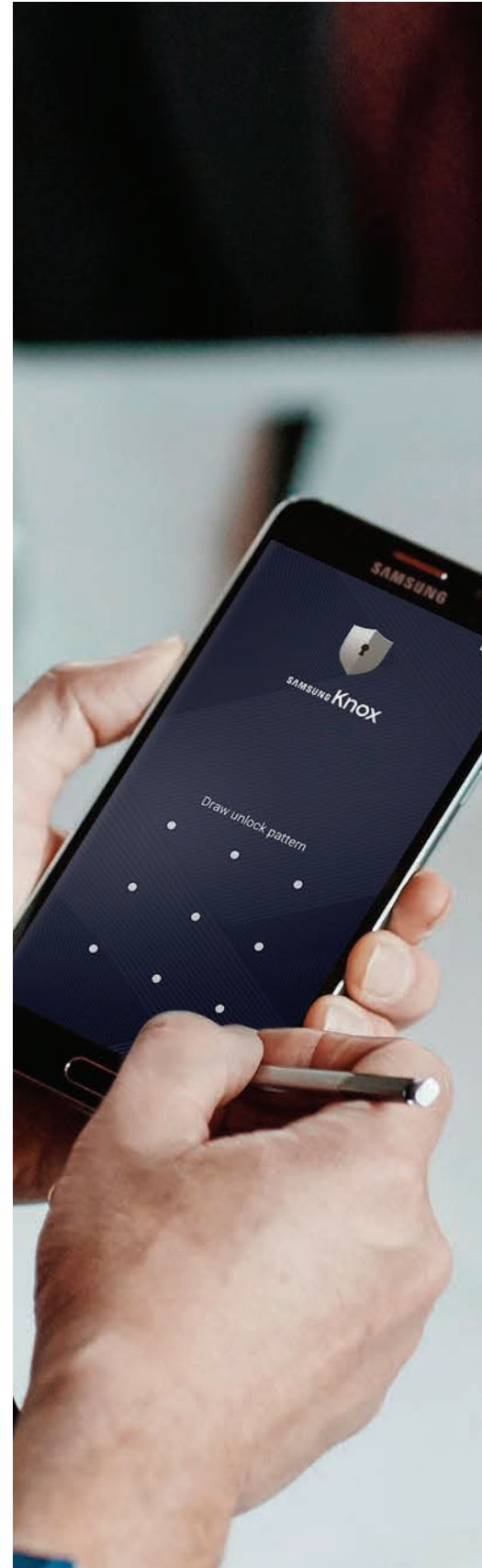
[3]*Google (April 2016), Android Security 2014 Year in Review. Retrieved on September 23, 2016.* https://goo.gl/KmUzSb
[4]*Hevesi, Patrick (April 2, 2016), Mobile Device Security: A Comparison of Platforms. Retrieved on September 23, 2016.* http://gtnr.it/2danRNr

In addition to the standard Samsung Knox features, enterprises can enable enhanced Knox capabilities to create an experience appropriate for the organization's needs.

Samsung Knox Workspace establishes a protected environment for enterprise applications and data. It is an independently certified, defense-grade, hardware-anchored, dual-persona solution. Workspace is designed to separate, isolate, encrypt, and protect enterprise data from attackers.

Samsung Knox Customization provides purpose-built solutions that can both secure data and incorporate a set of tools and services to address specific industry requirements.

Samsung Knox Enabled App is a transparent, secure container for individual applications.

Knox 2.7 has vastly enhanced the core kernel security by adding Control Flow Protection defense to protect against code reuse attacks such as Return Oriented Programming (ROP) and Jump Oriented Programming (JOP).

Samsung Galaxy devices based on the Knox platform are the first consumer mobile devices that are NIAP validated and approved for U.S. government classified use. Samsung provides enterprises the most secure devices out of the box with the Samsung Knox platform.

Conclusion

Samsung, the world's largest electronics OEM, and Google have undertaken a number of initiatives in the areas of building security into the core Android operating system, providing robust application screening and provisioning, and delivering innovative hardware-based security platforms. Together, these enhancements have positively affected perceptions of Android security and underscore Android's enterprise worthiness.

Google's ongoing commitment to providing monthly Android security patches, robust security services, and diligent application vetting processes, combined with Samsung Knox device-based security features, position Android-based, Samsung devices as the secure and logical choice for enterprises and government agencies wishing to realize the full potential of the digital enterprise.

Additional Reading

Find additional Samsung Knox platform resources, including white papers, videos and more at http://www.samsungknox.com/en/knox-technology.

To read the Google report *Android Security 2015 Year in Review*, visit https://goo.gl/kDc3gM.

For information on Android open platform security, visit http://goo.gl/YRN3vX.

For additional information about security, go to the Samsung blog at http://security.samsungmobile.com/.