ISSN:0975-9646

Maya Krishnan/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3965-3967

Survey on Security Risks in Android OS and an Introduction to Samsung KNOX

Maya Krishnan

Department of Computer Science, CMRIT
Bangalore, India

***Abstract*— Android is currently the world's most popular and widely used operating system in smartphones. While the power of Android comes in the form of its openness and easy to learn and implement nature, it obviously exposes the eco system to certain level of security risks to the end users. These issues could range from the client side injection, improper session handling, broken cryptography, insufficient trasport layer protection to insecure data storage. This survey aims to discuss various android specific risks and vulnerabilities and how the global leader in Android smartphone, Samsung, handles some of these key concerns in their securoty module launched in the KNOX platform. Being able to handle both the software and hardware side of things, Samsung has made the best use of both in building a powerful enterprise security platform needed for the modern day smartphones.**

***Keywords*— Android, Knox, ARM, TEE, SDK**

I. INTRODUCTION

Operating System in mobile devices has come a long way in the last twenty years. Starting with a Palm OS in 1996 to Windows pocket PC in 2000 to Symbian OS and then to the modern day Blackberry / Windows / Android / IOS platforms, mobile OS has pushed its limits to deliver complex functionalities and great user experience to a growing demand. It is undoubtedly one of the challenging and fast growing technologies in the world of computing. Introduced in 2005 and releasing the first smart phone in October 2008, the Google backed Android OS has now become the leading mobile development platform. Android's open source licensing and easy to implement nature along with its compatibility to support various smart phones from different manufacturers has made it one of the most sought after OS used for building the modern day apps. Devices that support Android OS are mainly based on ARM architecture platform. Android apps are written in java programming language and uses Linux kernel and custom virtual machine named Dalvik for execution.

Google play store lists close to 1.5 million android apps as per the statistics available in mid Feb 2015. The million dollar question would be are all thee apps safe and secure? Balancing the needs of openness and providing a tight security is a difficult problem to solve. Today's devices must not only meet both the functional and security requirements of various stakeholders, but also allow for "opening up" the device to cater to complex use cases. Everyone wants to be able to integrate the latest available softwares, download applications, and customize look and feel, but without being exposed to security risks such as privacy invasion, device intrusion or asset stealing. . Information about final paper submission is available from the conference website.

II. THREAT SCENARIOS IN ANDROID

Below are some of the aspects of Android programming which could pose security threats to end users. It is important to note that some of them are exclusive to mobile platforms due to their use cases and usage environments.

A. Open Source Governance

Due to the open source nature of the project, it allows a larger developer community to provide upgrades/enhancements to Android SDKs; wherein developers may spend little time to understand the impact on the stability and security of the platform while adding new features to solve complex problems. Years 2013, 2014 showed an array of focussed attacks originating from off device sources, including attacks on SSL protocol and CA infrastructure which was based on the technical know-how of how android internals function.

B. Poor Authentication And Authorization

Since the platform allows extension of out of box authentication and authorization SDKs, developers tend to explore new ways of handling the same and things could go drastically wrong ending up hackers to gain access to sensitive information and account details. Developers may not implement the right transport security which means the login credentials are exposed to a hacker. Inappropriate integration to authorization stores could also end up in system getting compromised.

C. Privacy

Today's smart phones carry an array of personal information such as contacts, messages, photos, video clips and even sensitive data like passwords, bank details, etc. Very little the end users know that these data elements are often not correctly encrypted in data stores and a lost or stolen phone could pose a severe security threat of hacking into the personal information thereby resulting in undesired events. The central Android logging service could also end up in a security risk if apps tend to write sensitive information into the logs. Several GPS apps end up writing geo-coordinates to the logging service there by exposing an information leakage when hacked.

D. Corporate Targets

Unlike a closely monitored employee workstation or laptop which is behind a firewall, under the corporate policies and up to date security patches, a mobile device carried by an employee for official purpose is one of the biggest threats for medium to large sized enterprises in terms of data security. Corporate supplied smart phones are often less well monitored and their inappropriate usage by an employee or the weak design of the app itself could result in data breaches wherein an attacker could copy confidential contracts, product designs or sensitive company info through a compromised smart phone.

E. Online Banking

On an infected smart phone, it is easier to capture the login credentials for online banking portals entered by the device owner and can be forwarded easily to an external party. Due to the open usage model of the Android market, malicious apps cannot be avoided completely. Especially the pirated apps or multimedia content in popular demand targeting user groups with typically low awareness levels are predestined to spread to many devices before being identified by Google as malware[6][3].

F. Rooting

It is a process of allowing users of smart phones, tablets and other devices running the Android operating system to attain privileged control (known as root access) over various Android's subsystems. Rooting an Android device gives administrative permissions on Linux kernel and could be used to alter any system parameter/setting. While Rooting provides various benefits like customization of theme/graphic [1], download of any app regardless of the app store they're posted on, extended battery life and added performance, etc, if not done properly, it can create havoc. Even if the rooting is done properly, if the phone doesn't have a proper antivirus protection onboard, rooting leaves device open to all sorts of malware. Gaining root access also entails circumventing the security restrictions put in place by the Android operating system. Malwares could access phone data and forward the information to hackers who could use it to their advantage.

Your paper must be in two column format with a space of 4.22mm (0.17") between columns.

III. SAMSUNG KNOX – A CASE STUDY

Several leading companies are already investing in tightening the Android security by building custom security layers around the android sdks which is being used in their products. But it is not easy to keep up pace with new SDK releases and also cannot be a main area of focus for such companies. This is where Samsung has launched their enterprise secure platform for enabling the third party apps to deploy and operate in a secure environment. Samsung KNOX is a suite of mobile enterprise security solutions that provides device protection, management and development options for handling security at multiple levels. A standard Knox architecture is shown below

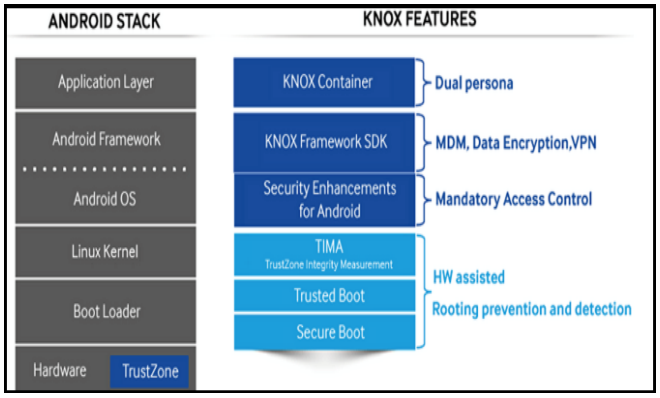

Fig. 1 KNOX Architecture

A. Platform Security – Trusted Execution Environment (TEE)

Trusted Execution Environments are being chosen to execute sensitive tasks on mobile devices. TEE is a secure area that resides in the main processor of a mobile device and ensures that sensitive data is stored, processed and protected in a trusted environment. Samsung KNOX 2.0 security platform 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.[2][3]. Samsung is an ARM licensee, and uses TrustZone technology to support embedded security. KNOX technology uses a Secure Boot protocol that requires the device boot loader, kernel, and system software to be cryptographically signed by a key whose root of trust is verified by the hardware. Commercially sold Samsung devices will have Samsung-issued root certificates.

B. Application Security

Apart from securing the platform, Samsung KNOX provides the security needs for an individual applications focussing on application Containers, On-device data encryption and VPN Support. Samsung KNOX Container is a virtual Android environment within the mobile device with its own home screen, launcher, applications, and widget. Applications and data inside the container are isolated from applications outside the container, that is, applications outside the container cannot use Android inter-process communication (IPC) or data-sharing methods with applications inside the container and vice versa.

C. One Device – Two Profiles

Samsung Knox provides security features that enable business and personal content to coexist on the same

handset. The user can switch from Personal to Work profile and vice versa within minutes with out a reboot. KNOX provides a dedicated secured container to install all work related apps and thereby handling them in a secured environment. A KNOX container is also administrator controlled since it is a cloud based SaaS model thereby enabling ability to remotely find, lock or wipe device in the event of loss or theft. All data inside container is completely encrypted, providing a secure and productive way to access confidential email and apps.

D. Perfect Blend of Hardware And Software Capabilities

Since KNOX is enabled on Samsung manufactured devices, it makes the hardware controls customized to work with various SDK apis. Samsung has really taken advantage of this situation and built a highly configurable ecosystem for running apps in the most secured way. KNOX provides SDKs to customize the device controls and user access to various resources there by restricting flows not required in a business enabled work profile. Kiosk mode option is another powerful feature provided by the SDK to run an app in full screen which doesn't allow end user to switch to any other app or access other resources.

E. TrustZone Based Integrity Measurement (TIMA)

KNOX utilizes SE for Android (Security Enhancements for Android) to enforce Mandatory Access Control policies to isolate applications and data within the platform. SE for Android relies on the assumption of OS kernel integrity. If the Linux kernel is compromised, SE for Android security mechanisms could potentially be disabled and rendered ineffective. TrustZone-based Integrity Measurement Architecture (TIMA) was developed to tackle this vulnerability. TIMA is as a unique feature on Samsung mobile devices and uses ARM TrustZone hardware and provides continuous integrity monitoring of the Linux kernel. The ARM TrustZone hardware effectively partitions memory and CPU resources into a "secure" and "non-secure" world. TIMA runs in the secure-world and cannot be disabled, while the SE for Android Linux kernel runs in a non-secure world. When TIMA detects that the integrity of the kernel or the boot loader is violated, it takes a policy-driven action in response. One of the policy actions disables the kernel and powers down the device [8].

IV. CONCLUSIONS

Google's security services for Android increased protection for users and improved visibility into various attempts to attack Android based applications. While it couldn't curb the problem in entirity, significatnt efforts have been made to handle security right from the playstore where an app gets downloaded. Last year, the Android platform also made numerous significant improvements in platform security, including enabling deployment of full disk encryption, expanding the use of hardware protected cryptography, and improving the Android application sandbox with an SE Linux based Mandatory Access Control system (MAC). Developers were also provided with improved tools to detect and react to security vulnerabilities. The google survey released in Feb 2015 states that delivery of potentially harmful applications continued at low levels throughout2014. Due to the open usage model of the Android market, malicious apps cannot be avoided completely. A lot still depends on design and implementation of the application to make sure the app is offered in a secured way. This is where relevance of enterprise securoty platforms like Samsung KNOX makes a difference. KNOX addresses most of the the shortcomings of the open source Android platform with its security model and industry leading device management capability.

From the facts presented in this survey, I would like to conclude that most of the malicious attacks in the recent past can be attributed to a bad app design. It is also important to note that users need to consistently upgrade the SDKs with major and minor releases; negligence of which could result in potential securoty attacks. If you like to handle security at an enterprise level, it makes a lot of sense to invest in platforms like Samsung KNOX where a lot of the security headache is moved to the platform allowing the developer to focus on the real business problem.

REFERENCES

[1] Security Threat Report 2013: New Platforms and Changing Threats, tech. report, Sophos, 2013, sophossecuritythreatreport2013.pdf.
[2] www.samsung.com/enterprise
[3] www.samsung.com/knox
[4] www.google.com
[5] Rafael Fedler, Christian Banse, Christoph KrauSS, and Volker Fusenig, *Language-Based Security on Android*.
[6] Avik Chaudhuri, *Android OS Security:Risks and Limitations A Practical Evaluation*
[7] www.sophos.com
[8] http://www.samsung.com/es/business-images/resource/white-paper/2014/02/Samsung_KNOX_whitepaper-0.pdf