TrubiZone

Securing Critical Mobile Applications for Android Using ARM TrustZone

Tiago Brito
Supervisor: Prof. Nuno Santos

Instituto Superior Técnico,
Av. Rovisco Pais, 1049-001 Lisboa - PORTUGAL
tiago.de.olveira.brito@tecnico.ulisboa.pt

Abstract. With the ever-growing number of connected devices worldwide, and with a more conscious and sharing society, mobile devices are becoming interesting data banks. With such an impact in our lives, mobile developers must focus on developing secure and privacy aware applications to protect users and services. Today's mobile operating systems do not offer fully secure methods to support critical applications, such as e-Health, e-voting and e-money, by not taking advantage of secure hardware technology like TrustZone. This paper proposes a new model for the development of critical mobile applications and a system based on TrustZone implementing it.

1 Introduction

Mobile devices are becoming the predominant device. Actions previously performed by powerful desktop computers can now be easily replicated on mobile devices. A recent study [4] from early 2015, with key statistics for the U.S. market, even shows that mobile devices, such as smart-phones and tablets, dominate digital media time over the Personal Computer (PC), with the trend being to continue raising.

Present in our everyday personal and professional lives, mobile applications (apps) start to handle privacy and security-sensitive data. Most notably these apps are handling photos, health and banking information, location and general documentation. The growing role of mobile devices has the negative consequence of becoming an attractive target for attacks. Among the several mobile platforms, Android is the one which attracts much more malware attacks [3].

The health sector is an interesting market for attackers due to its information value. According to Reuters [1], "medical identity theft is often not immediately identified by a patient or their provider, giving criminals years to milk such credentials. That makes medical data more valuable than credit cards". This is way regulatory laws such as the Health Insurance Portability and Accountability

[1] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Act (HIPAA), which establishes standards for electronic health care transactions, are so important to follow when managing sensitive health data.

Valuable health care information is a motivation for criminals to perform critical attacks on hospital networks around the world, consequently leaking or stealing health records of millions of patients. In September 2014, a group of hackers attacked the network of University of California, Los Angeles (UCLA)'s Hospital accessing computers with sensitive records of 4.5 million people. According to Cable News Network (CNN) [2], among the stolen records were the names, medical information, Social Security numbers, Medicare numbers, health plan IDs, birthdays and physical addresses of UCLA's patients.

In the mobile context, data is even more exposed and vulnerable due to the inherent portability of these devices, the sharing of information to third-party advertisers by device manufacturers or mobile app developers, unregulated management of sensitive medical information, specially because regulatory laws such as HIPAA do not account for the mobile sector, and because of security flaws on medical or consumer device software.

Parallel to the growth of the mobile app market, the number of e-Health mobile app, also known as Mobile Health (mHealth), available is increasing rapidly. In 2013, Research2Guidance [2] reported the existence of more than 97.000 mHealth apps across 62 app stores, with the top 10 apps generating up to 4 million free and 300.000 paid downloads per day. According to a report from MarketsAndMarkets [1], this market is expected to grow even further, from $6.21 billion in revenue in 2013 to $23.49 billion by 2018.

To protect sensitive data on mobile apps developers rely on mechanisms such as Digital Rights Management (DRM) [5], access control mechanisms, permission refinement, security Application Programming Interface (API), privacy enhancement systems and access control hooks, either from native Android [3], iOS [4] and Windows [5] or from extensions. These mechanisms rely on ad-hoc Operating System (OS) and application-level methodologies, which in most cases depend upon a very complex Trusted Computing Base (TCB) code, and do not fully enjoy the potential of the hardware of most modern smartphones, by not taking advantage of technology such as ARM's TrustZone.

Objectivos

Restrições

Especificação do sistema

Arquitectura

[2] http://money.cnn.com/2015/07/17/technology/ucla-health-hack/

[3] https://www.android.com/

[4] http://www.apple.com/ios/

[5] http://www.microsoft.com/en-us/windows

Contribuições

The remainder of this document proceeds as follows. Section 2 highlights the related work on mobile health, mobile security and TrustZone technology. Section 3 highlights the architecture of TrubiZone.

2 Related Work

This section presents the related work for this project and characterizes the main contributions of past works and how these contributions helped in the development of this project. This section is organized is the main parts: mHealth, mobile security and TrustZone.

The first part focuses on describing the attack surfaces of mHealth apps, the most common threats and their seriousness, present a few publicly available unsecure mHealth apps as well as some compliance recommendations that app developers should follow to avoid unnecessary security risks when handling sensitive health information. The second part of this sections describes the state of the art of mobile security with a particular focus on the Android Operating System and how developers can build secure applications with a trusting OS and security mechanisms built upon the application layer. The third part of the related work describes TrustZone, a hardware technology available a most modern ARM Holdings (ARM) processors which supports executions of two isolated worlds, a hardware secure world and a normal world. Besides describing the technology this sections also presents previous work developed using TrustZone and who these previous contributions may be helpful in achieving the main goals of this project.

2.1 mHealth

As discussed above, mobile devices are increasing in number at astonishing rates and with this growth the mobile market becomes cheap and accessible. This motivates the shift from mainframe systems located in the facilities of healthcare providers to apps on mobile devices as well as storage in shared could services. This accessibility also motivates the private sector in building more healthcare applications to support both patients and healthcare agents. Thus, the mobile health market is becoming a competitive market and one which is increasingly handling with more sensitive data.

Kotz, David [7] defines a threat taxonomy for mHealth. He, Dongjing, et al. [6] analyse several mHealth applications available in Android's app store considering the most common attack surfaces, shown in table 1. This work contributes with understanding of security and privacy risk on the Android platform.

Table 1. Description of attack surface

Attack Surface	**Description**
Internet	Sensitive information is sent over the internet with unsecure protocols (e.g. HTTP), misconfigured HTTPS, etc.
Third Party	Sensitive information is stored in third party servers
Bluetooth	Sensitive information collected by Bluetooth-enabled health devices can be sniffed or injected
Logging	Sensitive information is put into system logs where it is not secured
SD Card Storage	Sensitive information is stored as unencrypted files on SD card, publicly accessible by any other app
Exported Components	Android app components, intended to be private, are set as exported, making them accessible by other apps
Side Channel	Sensitive information can be inferred by a malicious app with side channels, e.g. network package size, sequence, timing, etc.

References

1. Mobile health apps & solutions market by connected devices (cardiac monitoring, diabetes management devices), health apps (exercise, weight loss, women's health, sleep and meditation), medical apps (medical reference) – global trends & forecast to 2018. Technical report, MarketsAndMarkets, 09 2013. http://marketsandmarkets.com/.
2. Mobile Health Market Report 2013-2017. Technical report, Research2Guidance, 03 2013. http://research2guidance.com/.
3. Mobile Threat Report. Technical report, F-Secure Labs., 03 2014. https://www.f-secure.com/documents/996508/1030743/Mobile_Threat_Report_Q1_2014.pdf.
4. Digital Future in Focus. Technical report, Comscore Inc., 03 2015. http://www.comscore.com/Insights/Presentations-and-Whitepapers/2015/2015-US-Digital-Future-in-Focus.
5. OMA DRM. Open mobile alliance digital rights management.(2010). *Retrieved May*, 2, 2011.
6. Dongjing He, Muhammad Naveed, Carl A Gunter, and Klara Nahrstedt. Security concerns in android mhealth apps. In *AMIA Annual Symposium Proceedings*, volume 2014, page 645. American Medical Informatics Association, 2014.
7. David Kotz. A threat taxonomy for mhealth privacy. In *COMSNETS*, pages 1–6, 2011.