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 remaining of this project will focus on the e-Health mobile application (app) market, also known as Mobile Health (mHealth). 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.

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".

Such valuable information as lead 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 because of the portability inherent to mobile devices, unregulated management of sensitive medical information, the sharing of information to third-party advertisers by device manufacturers and mobile app developers and security flaws on medical or consumer device software.

To protect sensitive data, apps 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. Unlike most popular mobile platforms based on Android [3], iOS [4] or Windows [5], which have a TCB comprising of a full featured OS and system libraries with millions of lines of code (LOC), a small, dedicated runtime is easy to ensure the absence of exploitable code vulnerabilities. The difficulty in developing a runtime comprised of a small, secure TCB is the limit it imposes upon the mobile apps supported. By removing complexity one removes functionality such as networking, I/O and compatibility with most used platforms.

2 Related Work

TEXT HERE
TEXT HERE
TEXT HERE

2.1 mHealth

TEXT HERE
TEXT HERE
TEXT HERE

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

2.2 Mobile Security

TEXT HERE
TEXT HERE
TEXT HERE

2.3 TrustZone

TEXT HERE
TEXT HERE
TEXT HERE

Genode
TEXT HERE
TEXT HERE
TEXT HERE

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.