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.

Keywords:
TrubiZone, Security, Privacy, e-Health, Mobile Devices, Android, TrustZone

1 Introduction

According to a Comscore's whitepaper [3] from early 2015, with key statistics for the U.S. market, mobile devices, such as smart-phones and tablets, dominate digital media time over the Personal Computer (PC), with the trend being to continue raising. This shows a future where mobile devices might be the predominant device.

Present in our everyday personal and professional lives, mobile applications (apps) start to handle privacy and security-sensitive data, notably photos, health and banking information, location and general documentation, thus becoming an attractive target for attacks.

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.

Thus, the goal of this project is to fill the security gap in the mobile application market by proposing TrubiZone, a development system with a small, dedicated TCB which, by using ARM TrustZone technology, allows app developers to execute parts of the application logic in a trusted environment isolated from the OS, which in turn supports the development of secure mobile applications independent from a full blown platform and its inherent vulnerabilities.

To avoid the limitations referenced above the final implementation must guarantee the following requirements:

Assure Security Policies
TrubiZone must guarantee the fundamental security properties of confidentiality, integrity and authenticity, on which every high level security application can be built on.

[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

I/O Support
To allow the development of realistic mobile applications I/O interaction must be supported, while trying to maintain a small, compact TCB.

Support for General Applications
The implementation should run general applications instead of dedicated and specifically crafted apps. To support this restriction TrubiZone must execute applications built using modern high-level languages with components such as garbage collection and strong typing.

Developer Friendly
Developers must be able to easily specify the security properties required and the security-sensitive app logic to transparently run in the trusted environment. This allows developers to focus on the logic and design of said application rather than mobile security mechanisms.

TrubiZone will be based on Genode [6] running along side Android and implemented upon a Freescale i.MX53 START development board [7], which supports ARM's TrustZone. To illustrate TrubiZone's functionality a mHealth will be implemented.

*** Aqui terá uma breve descrição da arquitectura do sistema. ***

In summary this work expects to contribute with:

- The design of a novel security system, based on TrustZone, for development of secure mobile applications.
- Implementation, on a development board, of a prototype of this new security framework.
- Implementation of a mobile health application using the prototyped framework.
- Assessment of the prototype and mHealth app.

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

TEXT HERE
TEXT HERE
TEXT HERE

[6] http://genode.org/index
[7] http://www.freescale.com/products/arm-processors/i.mx-applications-processors-based-on-arm-cores/i.mx53-processors/i.mx53-quick-start-board:IMX53QSB

2.1 mHealth

TEXT HERE
TEXT HERE
TEXT HERE

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. 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.