TEE：从手机端到云端的系统安全增强

对虚拟化、ARM TrustZone和Intel SGX技术的探讨

上海交通大学 · 利文浩 / 夏虞斌 · 2015.11

什么是TEE？

GLOBALPLATFORM®

TEE (Trusted Execution Environment)

GlobalPlatform在2013年提出

与REE (Rich Execution Environment)对应

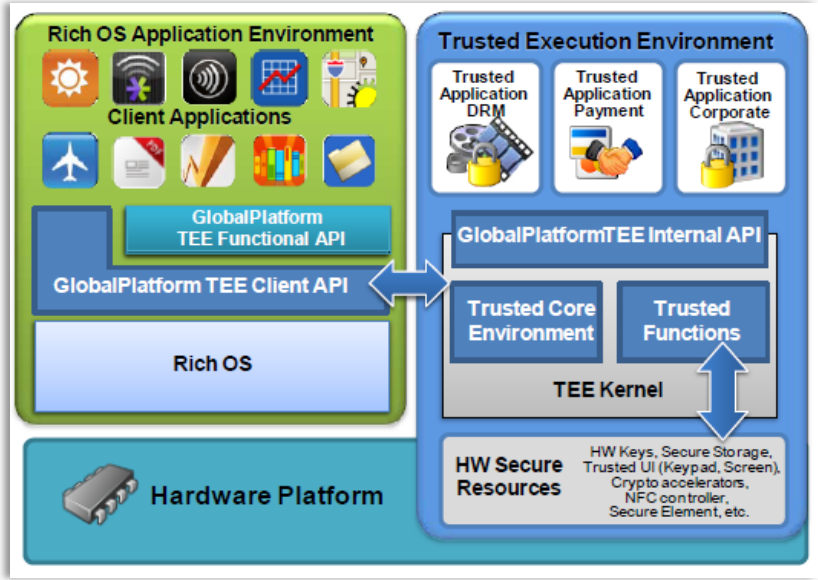
TEE通常用于运行关键的操作

移动支付：指纹验证、PIN码输入等

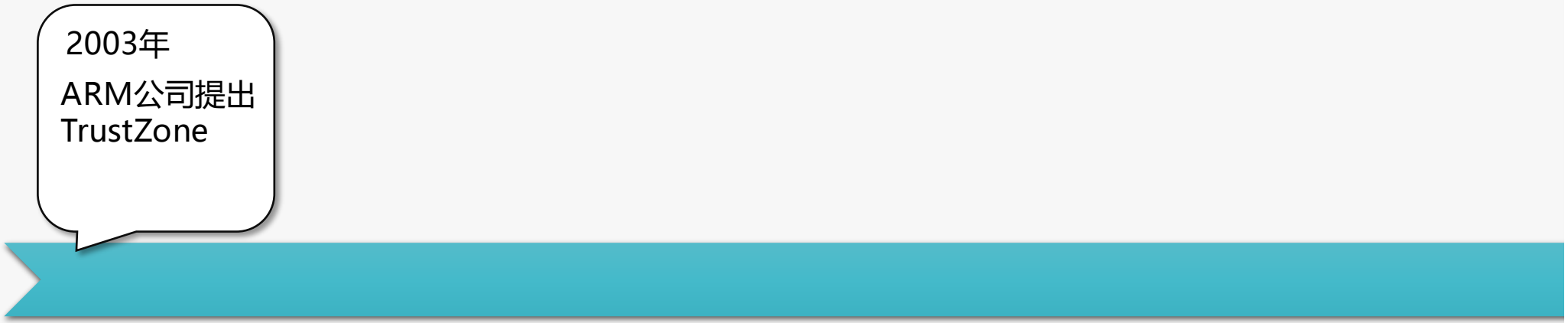
机密数据：私钥、证书等的安全存储

内容保护：DRM（数字版权保护）

…



支持TrustZone技术的部分设备一览



支持TrustZone技术的部分设备一览

支持TrustZone技术的部分设备一览

支持TrustZone技术的部分设备一览

2010年

支持TrustZone技术的移动智能设备均支持TrustZone技术

TEE与我们的生活有什么关系？

TEE已经成为生物识别设备的标配

使用TEE来隔离指纹的采集、存储、验证等过程

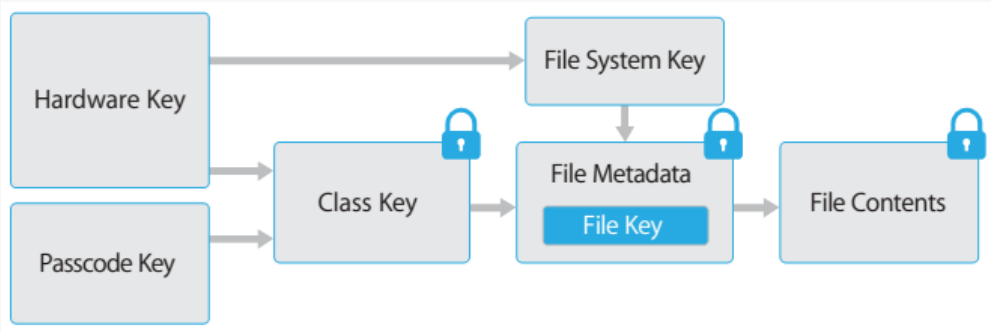
即使手机被越狱或Root，攻击者也无法获取指纹数据

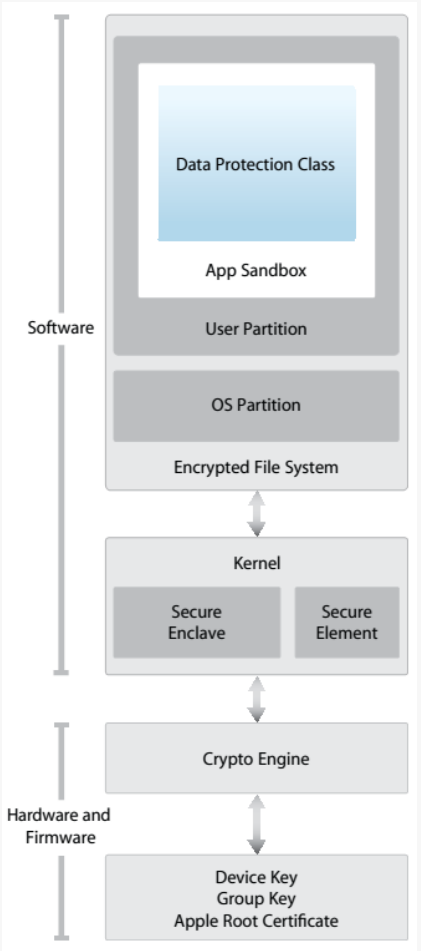
Apple：iOS Enclave

iPhone 5s 指纹识别的基础

基于TrustZone等技术实现Enclave与外界强隔离

所有指纹相关数据均通过Enclave保存和访问





* 图片引自Apple

TEE从系统软件的角度来看TEE

TEE内部运行一个完整的操作系统

与REE（如Android）隔离运行

TEE与REE通过共享内存进行交互：OS间/应用间

TEE内部也分内核态与用户态

TEE的用户态可以运行多个不同的安全应用（TA）

TEE包含：Secure OS + 中间件 + 安全应用 + 外部交互

T6：基于TrustZone的安全平台


获奖证书

上海交通大学

利文浩 华志超 梁凉 古金宇 付元 薄智元 同学：

你（们）的作品《移动平台安全操作系统T6及其应用》在第十四届“挑战杯”中航工业全国大学生课外学术科技作品竞赛中荣获

特等奖

指导老师：夏虞斌

特颁此证，以兹鼓励。

共青团中央 中国科协 教育部 全国学联 广东省人民政府


Poster:TVisor: A Practical and Lightweight Mobile Red-Green Dual-OS Architecture

AdAttester: Sec Attest

Reducing World Switches in Virtualized Environment with Flexible Cross-world Calls

中华人民共和国国家知识产权局 BP20140871P

2014年12月25日

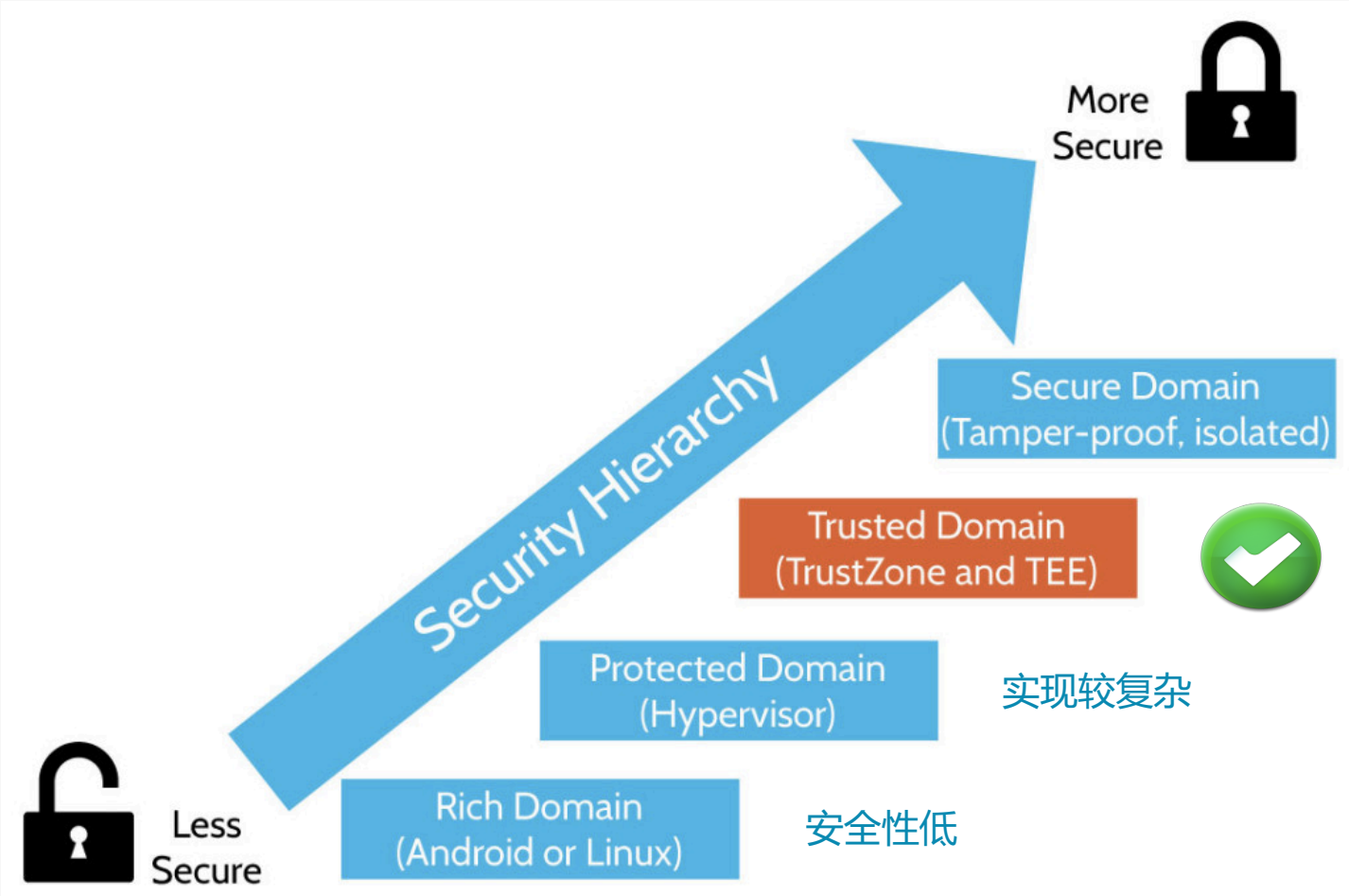
发文序号：20141222012645 70

中华人民共和国国家知识产权局 BP20140871P

2014年12月25日

T6：基于ARM TrustZone的安全操作系统与平台

移动平台可信组件的层次



ARM TrustZone技术

ARMv6版本开始的安全硬件特性

包括ARM11及Cortex A系列

目前大部分手机芯片均有该硬件特性

同时运行一个安全的OS和一个普通的OS

两个系统之间互相隔离运行

安全的OS具有更多的权限

TrustZone是一个全系统级别的安全架构

处理器、内存和外设的安全隔离

TEE 与 REE

TEE三层架构

TA (Trusted Application)层

可信钱包、TUI

TEE层

安全操作系统

对上层TA提供的库

硬件层

CPU状态隔离

内存隔离、外设隔离

TEE在工业界的实际应用：现有技术方案

Samsung TIMA

Apple: iOS Enclave

Qualcomm: Zeroth

安全支付与解锁

DRM

……

TEE，你的名字是隔离

TEE：一种基于硬件的隔离

常见的隔离方式最终都是基于硬件

应用程序的隔离	基于操作系统	基于CPU特权级（Ring-0）
虚拟机的隔离	基于Hypervisor	基于CPU特权级（VT-x）
关键代码/数据隔离	基于Flicker[EuroSys08]	基于SVM/TXT & TPM
手机指纹的隔离	基于TEE	基于TrustZone
核心源代码保护	基于物理安全	基于机房锁…

Flicker[EuroSys-08]：基于SVM的TEE

利用CPU的新指令（Intel TXT, AMD SVM）

构造出一个与之前运行状态无关的执行环境

通过TPM来保证执行环境的可验证性

缺点

需要暂停所有的CPU核，保证TEE的独占执行

性能开销大：验证密码需要约2秒

Intel SGX：加密与隔离的结合

Software Guard Extension

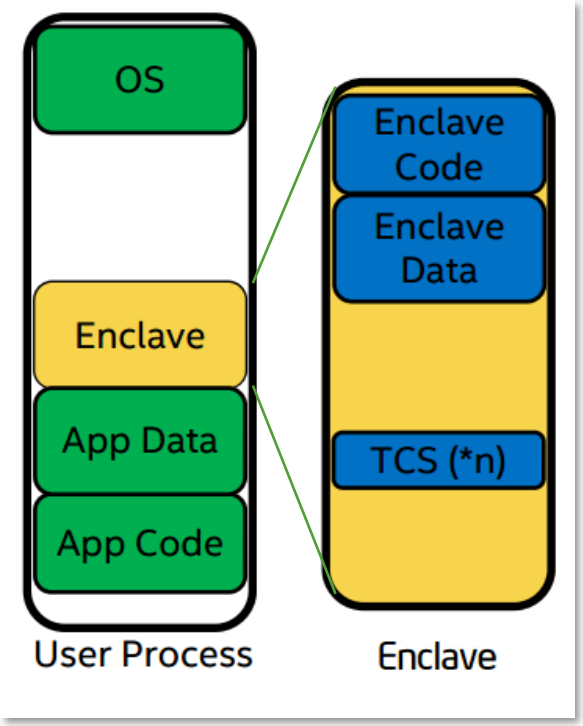
构建安全的运行环境：Enclave [1]

所有数据在内存中均加密，可防**物理攻击**

保证应用执行过程的隐私性和完整性

从XOM开始，我们的HyperCoffer

云计算安全的终极解决方案？



[1] Apple在白皮书中提到其保护指纹的机制也命名为*Enclave*

处理器加密的相关研究

XOM [ASPLOS-00]

Rogers [MICRO-07]

Bastion [HPCA-10]

HyperCoffer [HPCA-13]

…

Architectural support for copy and tamper resistant software
D Lie, C Thekkath, M Mitchell, P Lincoln, D Boneh… - ACM SIGPLAN …, 2000 - dl.acm.org
Abstract Although there have been attempts to develop code transformations that yield tamper-resistant software, no reliable software-only methods are known. This paper studies the hardware implementation of a form of execute-only memory (XOM) that allows ...
被引用次数：633 相关文章 所有 59 个版本 引用 保存 更多

Architecture support for guest-transparent vm protection from untrusted hypervisor and physical attacks
Y Xia, Y Liu, H Chen - High Performance Computer Architecture …, 2013 - ieeexplore.ieee.org
... The next sec- tion describes necessary background and related work. Sec- tion 3 describes the goals and challenges underlying Hyper- Coffer, as well as an overview of the design of HyperCoffer. Section 4 illustrates the architecture extension required by Hy- perCoffer. ...
被引用次数：25 相关文章 所有 10 个版本 引用 已保存

TEE：从移动端到服务端

	ARM	X86
移动端	TrustZone	Virtualization
服务端	?	SVM/TXT/SGX

TEE，除了指纹还有什么？

隔离带来的安全能力增强

面向安全的功能划分

对系统进行重构，将安全敏感的部分放入隔离区

例如：Flicker [Eurosys-08]、ProxOS [STC-10] 等

利用不对称权限的安全检查

从高权限区检查低权限区的运行状态

例如：VMI [NDSS-03]

虚拟机自省：Virtual Machine Introspection

VMI的优势

不用修改客户虚拟机

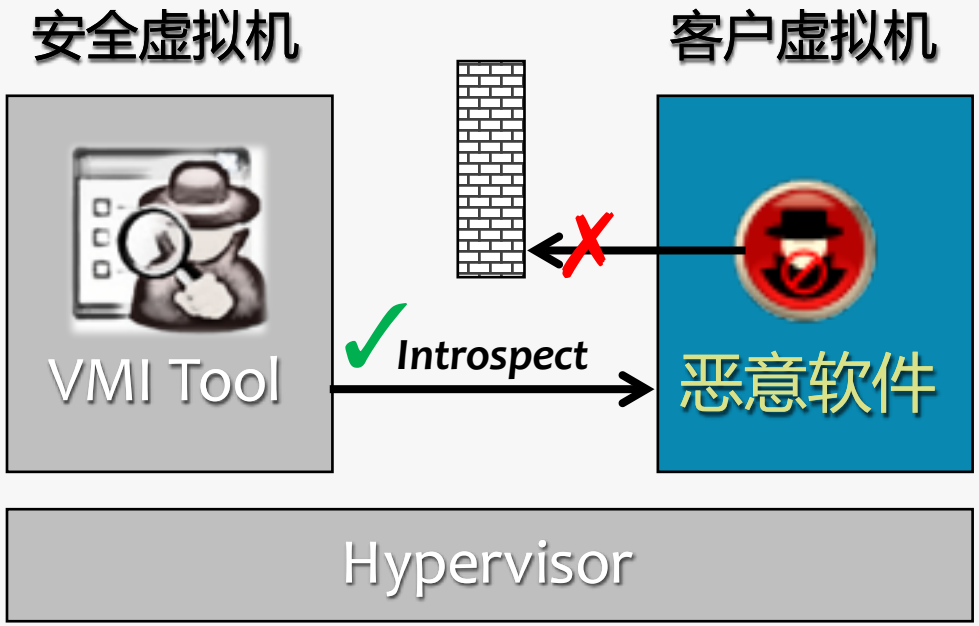
保证杀毒软件自身的安全

新的恶意软件检测技术

性能损失小

在学术界已有十多年积累

已集成在VMware套件中



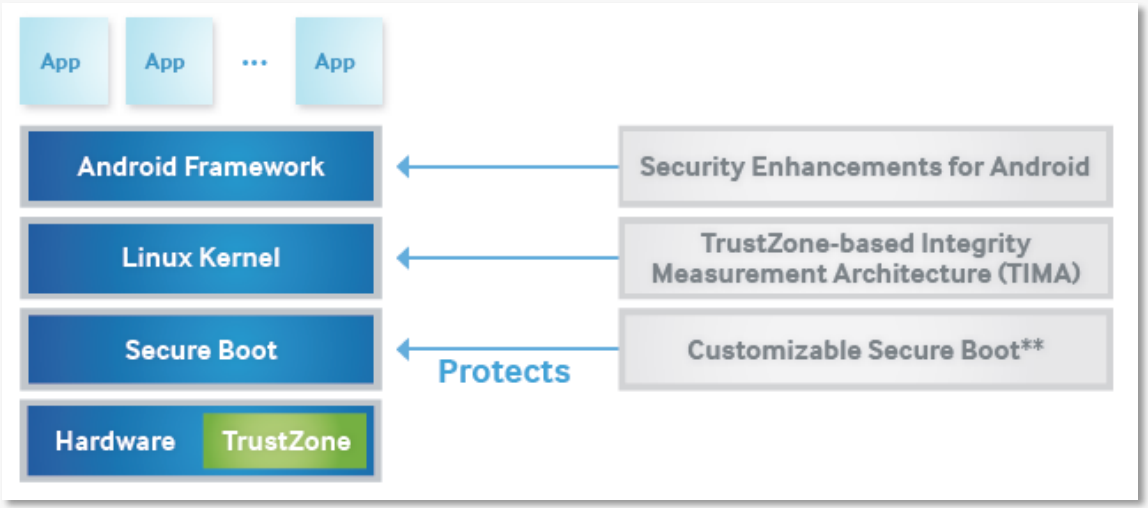
T. Garfinkel, M. Rosenblum *et al.*, "A virtual machine introspection based architecture for intrusion detection." in *Proc. NDSS*, 2003.

三星KNOX：基于TrustZone的内核保护

动态内核完整性保护

TIMA: TrustZone-based Integrity Measurement Architecture

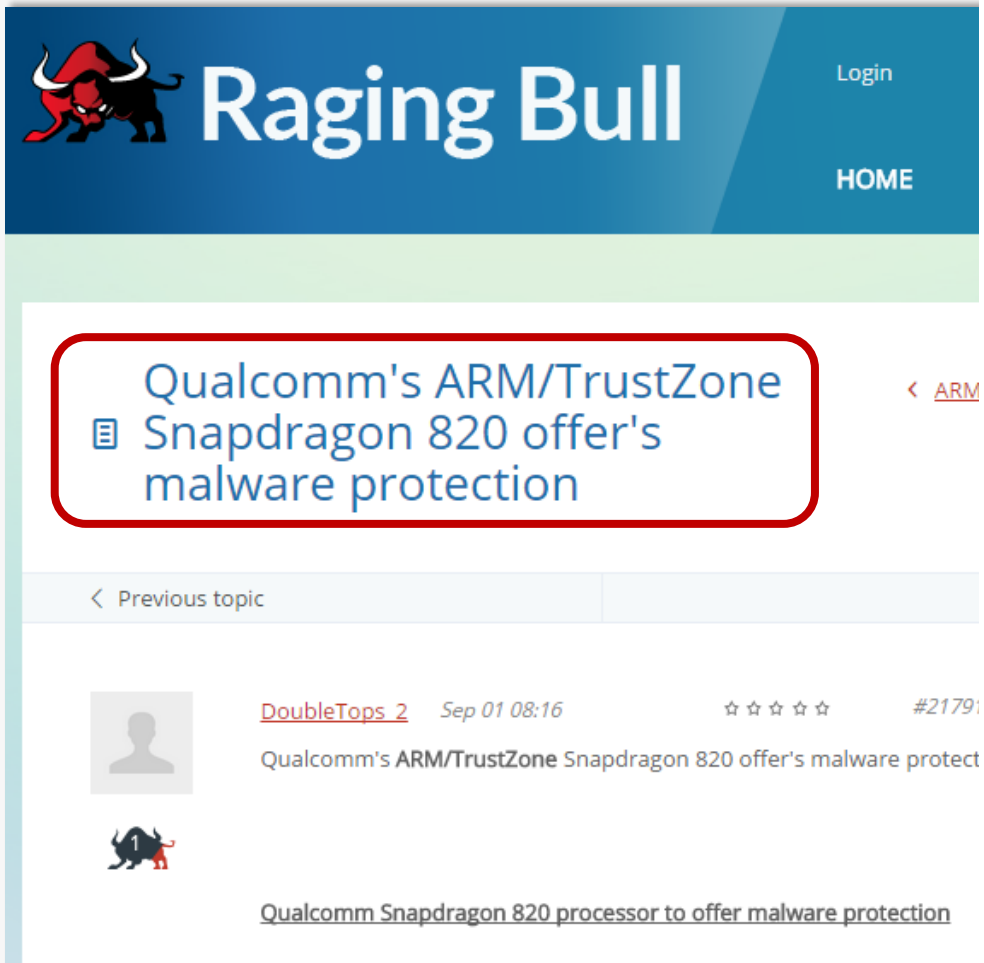
定时检测内核代码段和关键数据的完整性



高通：基于TrustZone的恶意软件查杀

杀毒？杀毒！

- 高通Zeroth芯片级恶意软件查杀
- 利用终端的NPU硬件进行本地分析
- 基于**异常行为**进行恶意软件查杀
- 与杀毒软件厂商进行协作
- 部署在骁龙820芯片
- 高通Haven软件套件



TEE，面临越来越多的威胁

TEE的CVE已经开始增加

华为Mate7发布会直播：指纹支付号称全球最安全

2014-09-04 *编辑：yoyo* *来源：网络* 评论(1)

华为Mate7发布会直播：从iPhone5s带来指纹识别功能之后，各大厂商也逐步跟进为自家的新旗舰配备起这么一个功能，华为Mate7也不例外。华为Mate7采用的是按压式指纹传感器，一次触摸便可轻松解锁。

“指纹支付宝”是由支付宝钱包和华为Mate7新旗舰联合推出的一项全新的支付功能，指纹识别技术与手机移动支付相结合的高科技产物。目前全球能够实现指纹支付的手机有两款，分别是华为Mate7和iPhone6，而国产手机中，华为Mate7是唯一首创。

华为Mate 7跪了

黑客能否攻破所谓的“可信”环境中？

奇虎360安全研究员申迪（音译）将通过华为Ascend Mate 7手机向大家展示“利用TrustZone攻击你信任的核心”

虽然说TrustZone技术支持可信执行环境（TEE），其中指纹扫描等功能要求高信任度（如非接触式支付）运行，而且Ascend Mate 7手机使用自己定制环境的软件和华为Hisilicon Kirin 925处理器，但黑客依然有办法破解。申迪将在大会上谈谈关于TrustZone的开发、如何在不可靠的可信执行环境中运行shellcode以及如何Root设备和禁用最新Android SE。

SLASHGEAR REVIEWS COLUMNS FEATURES HUBS

Trending Cars Galaxy Note 5 Windows 10 Apple Watch

Hackers able to steal fingerprints from Galaxy S5, other Android phones

42

Adam Westlake - Apr 25, 2015

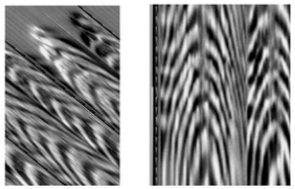
Tweet 151 Like 120 +1 28

Fingerprint readers have quickly become commonplace on our smartphones, and while they are touted as offering some of the best security, it seems that may not be true across the board. A group of researchers at FireEye have reported a flaw in certain Android phones like the Galaxy S5 that could allow hackers to steal fingerprint data. Now, before you start panicking and preparing to set your fingerprint-based phone on fire in the name of security, know that this can only take place in extremely limited situations, and as for Android itself, the loophole was already patched with the release of Lollipop.

HTC caught storing fingerprint data in unencrypted plain text

By Joel Hruska on August 10, 2015 at 4:24 pm | 40 Comments

One example is the HTC One Max — the fingerprint is saved as /data/dbgraw.bmp with 0666 world permission (world readable). Any unprivileged processes or apps can steal the user's fingerprints by reading this file. Other vendors store fingerprints in TrustZone or Secure Enclove, but there are still known vulnerabilities for attackers to leverage... To make the situation even worse, each time the [HTC] fingerprint sensor is used for auth operation, the auth framework will refresh that fingerprint bitmap to reflect the latest wiped finger. So the attacker can sit in the background and collect the fingerprint image of every swipe of the victim.

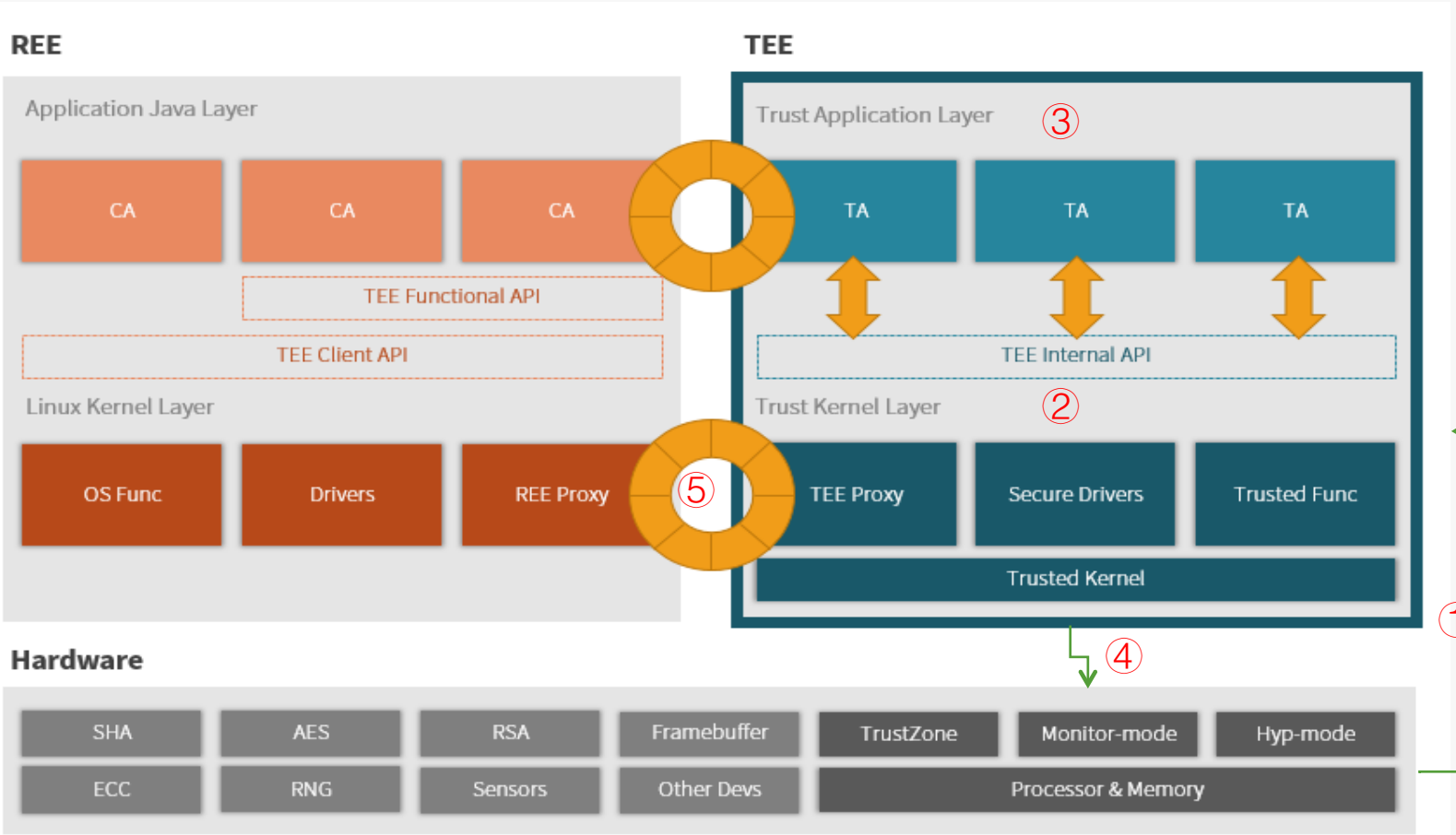


(a) (b)

Figure 5: Fingerprint bitmap obtained from HTC One Max. Both the raw bitmap (a) and the re-aligned version (b) are shown. We only pasted a small portion of the images to protect the fingerprint owner's anonymity.

http://www.extremetech.com/mobile/211985-htc-caught-storing-fingerprint-data-in-unencrypted-plain-text

TEE攻击面分析



①安全启动

②TEE内核自身

③TA安全性

④硬件操作与隔离

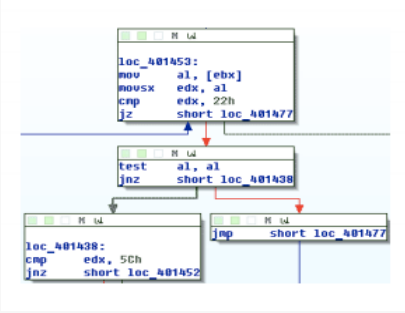
⑤TEE与REE交互部分

攻击者的Toolkit

REE侧工具

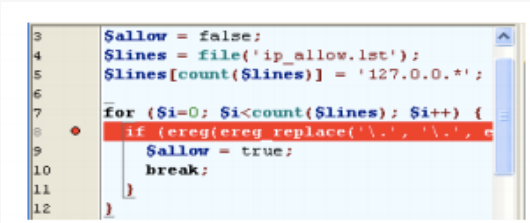
Root工具（如KingRoot）

Decompiler（如JEB）



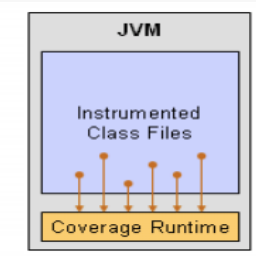
Disassembler（如IDA）

TEE侧工具



Debugger工具（如GDB）

Introspection工具
（如Androguard）



Instrumenting
（如ADBI）

TEE SDK

旁路分析、嗅探工具

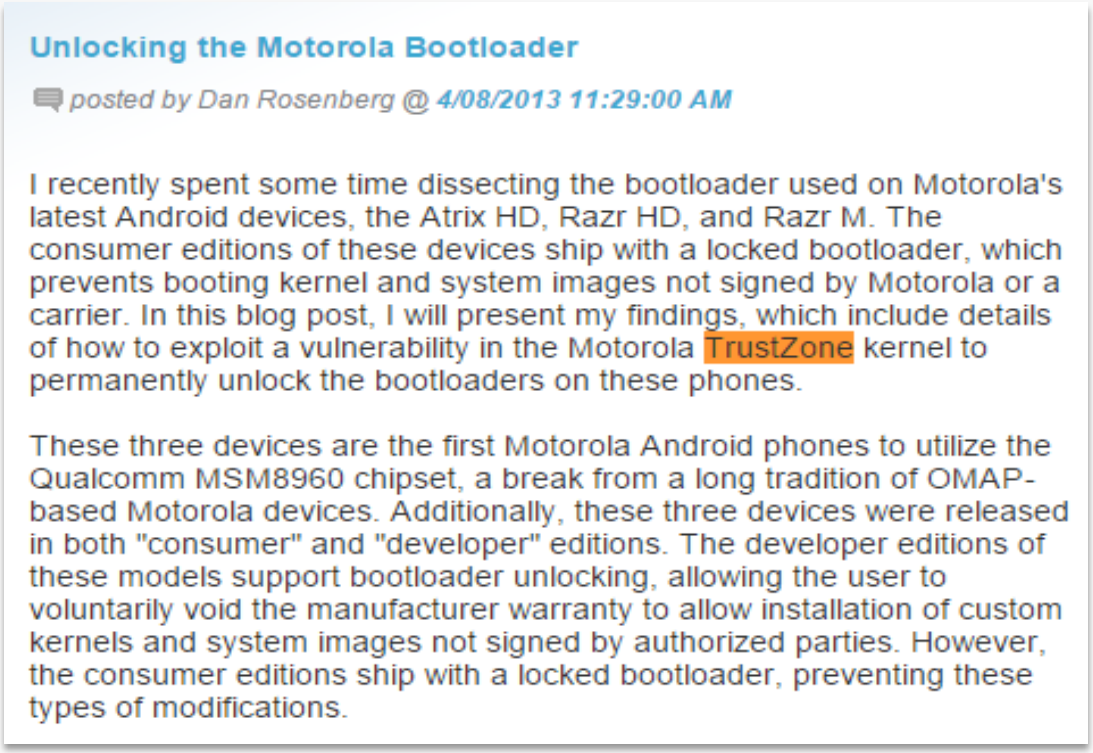
实际攻击：针对TEE安全启动

Moto、三星部分手机

2013年

TrustZone内核被破解

可解锁Bootloader，加载任意系统



Unlocking the Motorola Bootloader

posted by Dan Rosenberg @ 4/08/2013 11:29:00 AM

I recently spent some time dissecting the bootloader used on Motorola's latest Android devices, the Atrix HD, Razr HD, and Razr M. The consumer editions of these devices ship with a locked bootloader, which prevents booting kernel and system images not signed by Motorola or a carrier. In this blog post, I will present my findings, which include details of how to exploit a vulnerability in the Motorola TrustZone kernel to permanently unlock the bootloaders on these phones.

These three devices are the first Motorola Android phones to utilize the Qualcomm MSM8960 chipset, a break from a long tradition of OMAP-based Motorola devices. Additionally, these three devices were released in both "consumer" and "developer" editions. The developer editions of these models support bootloader unlocking, allowing the user to voluntarily void the manufacturer warranty to allow installation of custom kernels and system images not signed by authorized parties. However, the consumer editions ship with a locked bootloader, preventing these types of modifications.

来源: http://blog.azimuthsecurity.com/2013/04/unlocking-motorola-bootloader.html

实际攻击：针对TEE自身安全

高通 QSEE内核整型溢出 CVE-2014-4322

- drivers/misc/qseecom.c文件存在漏洞
- 没有判断offset和length的正确范围
- 可能导致攻击代码提权或DoS攻击

华为RTOSck内核任意代码执行 CVE-2015-4422

- 内核无ASLR、NX

实际攻击：针对TA安全

HTC指纹数据直接明文存放在Android侧

HTC caught storing fingerprint data in unencrypted plain text

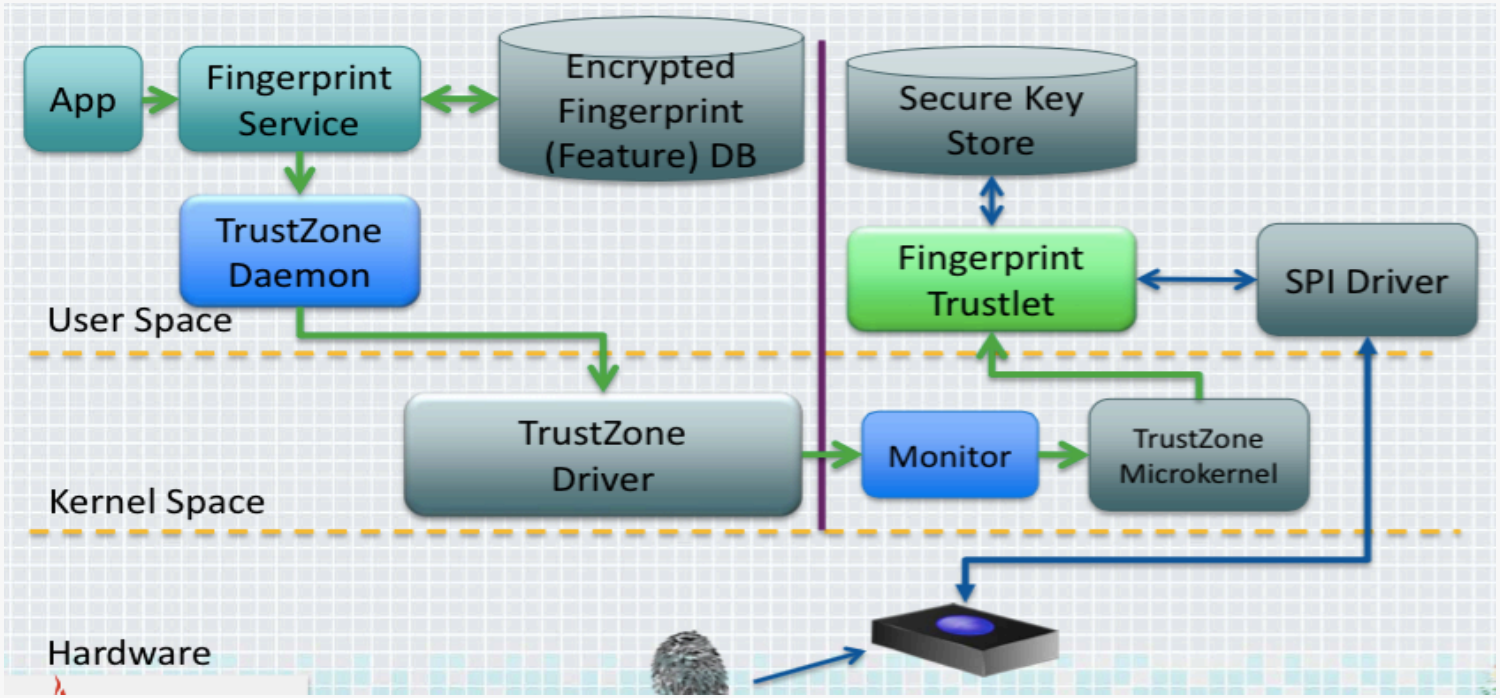
By Joel Hruska on August 10, 2015 at 4:24 pm | 40 Comments

Share This article

For the past few years, both Apple and the various Android manufacturers have been pushing the idea of fingerprint readers, typically on the dubious grounds that biometric security is a better choice compared to a good passcode. New research from the security firm FireEye seems to blow that claim wide open, however. According to FireEye, multiple Android manufacturers protect your fingerprint so poorly, it can be read by plugging the phone into a computer and knowing which folder to access.

实际攻击：针对硬件操作安全

Blackhat’ 15: 三星S5可在Android侧读取指纹设备数据

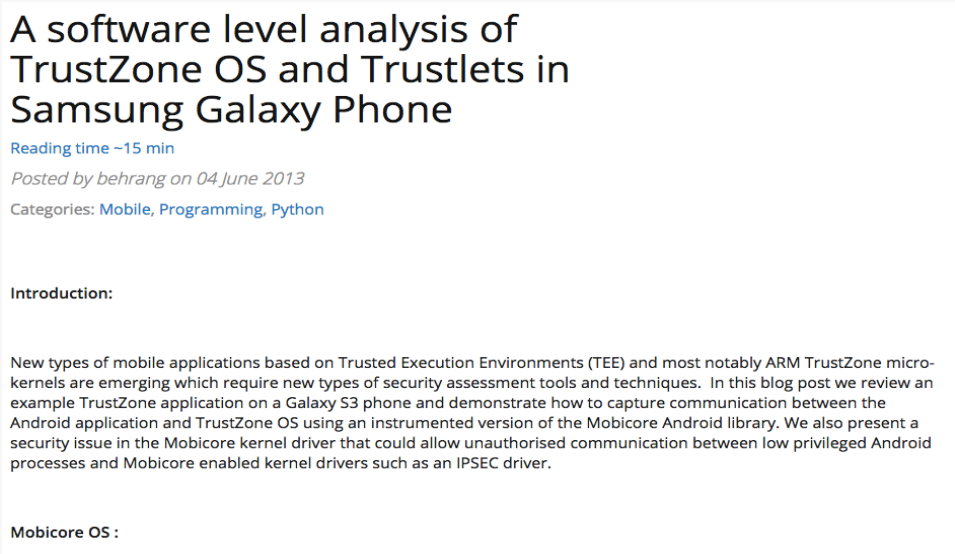


实际攻击：针对TEE与REE交互部分

TEE Driver提权漏洞 CVE-2015-4421

代码边界检查不正确

Samsung手机TEE内核MITM分析



A software level analysis of TrustZone OS and Trustlets in Samsung Galaxy Phone

Reading time ~15 min

Posted by behrang on 04 June 2013

Categories: Mobile, Programming, Python

Introduction:

New types of mobile applications based on Trusted Execution Environments (TEE) and most notably ARM TrustZone micro-kernels are emerging which require new types of security assessment tools and techniques. In this blog post we review an example TrustZone application on a Galaxy S3 phone and demonstrate how to capture communication between the Android application and TrustZone OS using an instrumented version of the Mobicore Android library. We also present a security issue in the Mobicore kernel driver that could allow unauthorised communication between low privileged Android processes and Mobicore enabled kernel drivers such as an IPSEC driver.

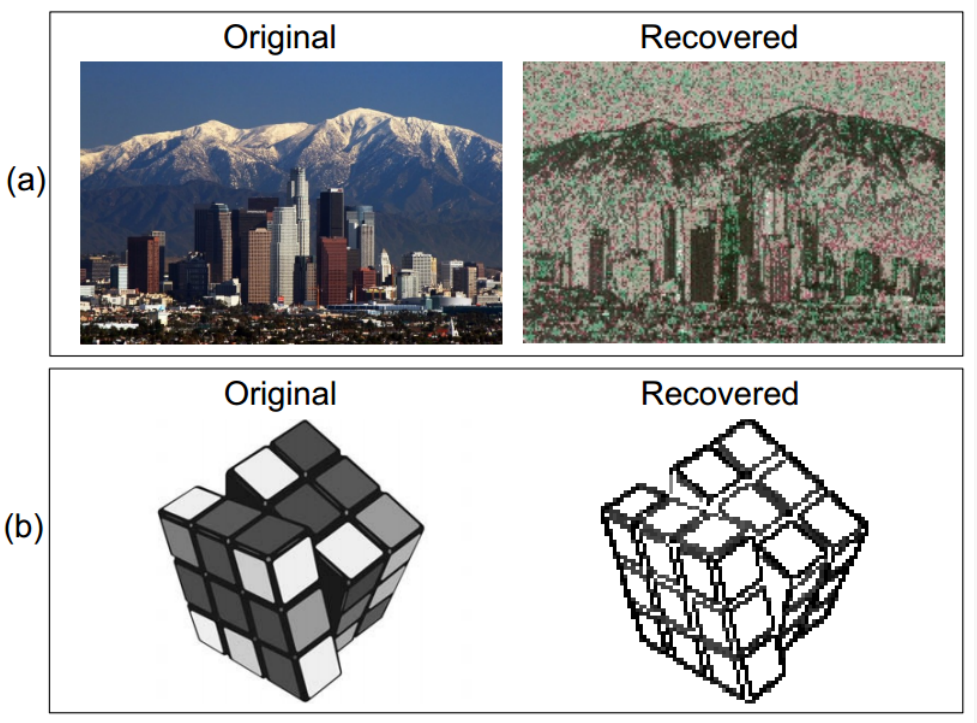
Mobicore OS :

微软对SGX的Side Channel攻击 [S&P'15]

对SGX的侧信道攻击

恶意OS通过缺页信息，结合应用的算法，反推出SGX中处理的数据

虽然无法100%精确，但依然可以泄露一定程度的信息



只有硬件安全隔离还远远不够

TEE与上层安全应用自身的安全性更需要重视

需要从整体设计与安全评估进行TEE安全增强

现状与趋势	问题与挑战
1、芯片厂商的TrustZone硬件隔离实现机制各异	如何保证不同TEE方案的安全性？
2、大多TEE与手机厂商更关注功能性	如何确保TEE自身安全性？
3、TA不断增加，带来新的安全隐患	如何更有效地将TEE与TA隔离开？
4、TEE无法应对物理攻击	如何提高TEE防御的层次？

总结

TEE并不仅仅是指纹保护

指纹目前是TEE推广的强大动力

解锁、手机支付是主要应用场景

可以做的更多，如恶意软件查杀

TEE并不仅仅在手机端

从手机端到云端都有TEE

ARM：TrustZone

X86：VT-x和SGX

TEE并不是全新的概念

本质就是一种基于硬件的隔离

基于隔离的安全研究有了用武之地

工业界正在不断寻找新的机会

TEE并不是100%都安全

关于TEE的CVE开始出现

各家实现的TEE良莠不齐

高回报，成为黑客的下一个目标

TEE并不是一个全新的开始，也不是一类问题的结束

谢谢！

THE