SoC Level Security Solution for Mobile Payment

Marvell

Jialin Chen/陈家林 chenjl@marvell.com

微博：安卓安全小分队

Agenda

- Introduction
- Marvell Security Overview
- Trusted UI for Mobile Payment

Introduction

Marvell Introduction

- RIM – Blackberry
- Motorola – Ming
- Samsung
- Yulong Coopad
- ZTE
- Lenovo
- HP
- …

Team Introduction

安卓安全小分队

- 《安卓安全小分队怎么利用Bluebox Security 曝的漏洞》

http://blog.sina.com.cn/s/blog_be6dacae0101bmq3.html

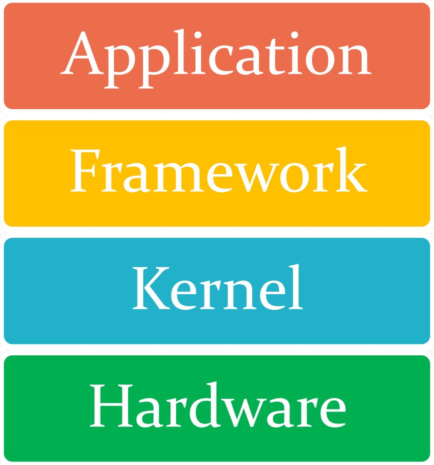
- 《安卓安全小分队发现Android新漏洞 》

http://blog.sina.com.cn/s/blog_be6dacae0101bksm.html

- 《主流安全大漏洞：隐私空间泄密》

http://blog.sina.com.cn/s/blog_be6dacae0101csrc.html

System Security DNA



Application

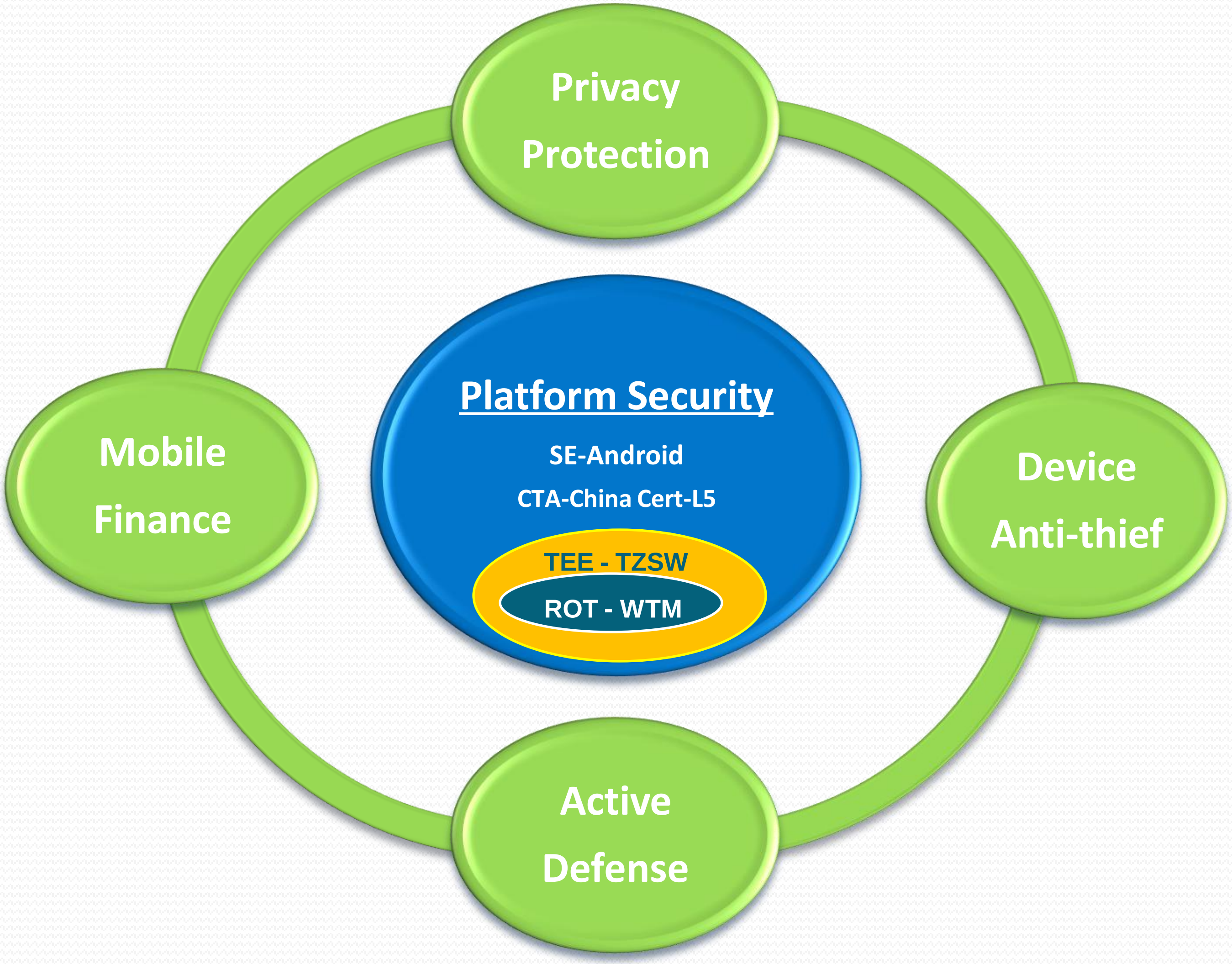
Framework

Kernel

Hardware

Marvell Security Overview

Marvell Security Overview - Consumer



Privacy Protection

Mobile Finance

Platform Security

SE-Android

CTA-China Cert-L5

TEE - TZSW

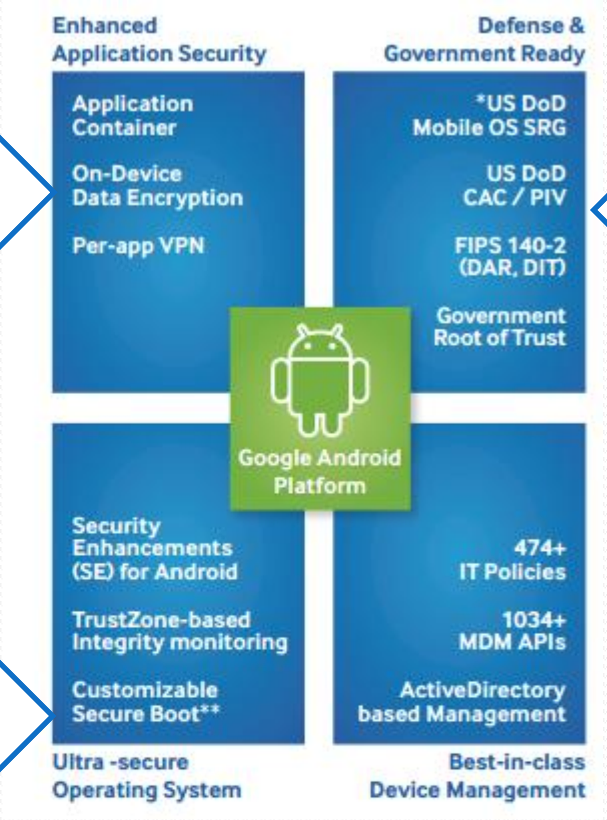
ROT - WTM

Device Anti-thief

Active Defense

Marvell Security Overview - Enterprise

TZSW TEE extensibility
-Device Unique Secure Storage in Persistent Media
- TEE assisted TIMA operations
 > Attestation / Key store
 > Kernel Protection



Enhanced Application Security

Application Container

On-Device Data Encryption

Per-app VPN

Defense & Government Ready

*US DoD Mobile OS SRG

US DoD CAC / PIV

FIPS 140-2 (DAR, DIT)

Government Root of Trust

Google Android Platform

Security Enhancements (SE) for Android

TrustZone-based Integrity monitoring

Customizable Secure Boot**

Ultra -secure Operating System

474+ IT Policies

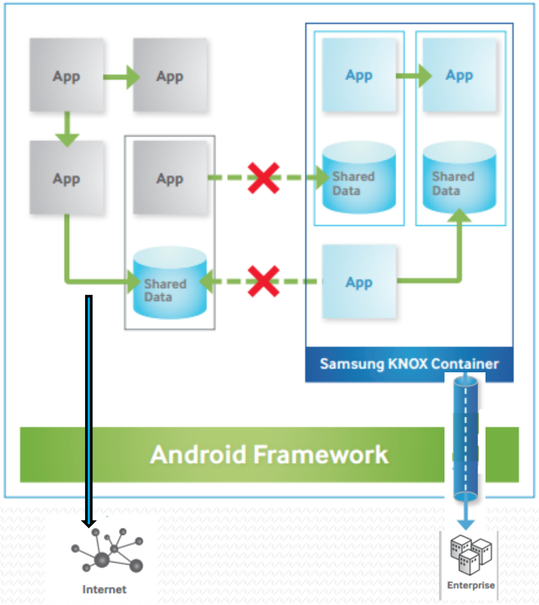
1034+ MDM APIs

ActiveDirectory based Management

Best-in-class Device Management

WTM – Root of Trust Support
- Secure Storage platform binding
- Key OTP provision
- FIPS140-2 Certified Key Mgmt
- Continuous System Integrity Monitoring
  (Linux kernel/TZSW image)

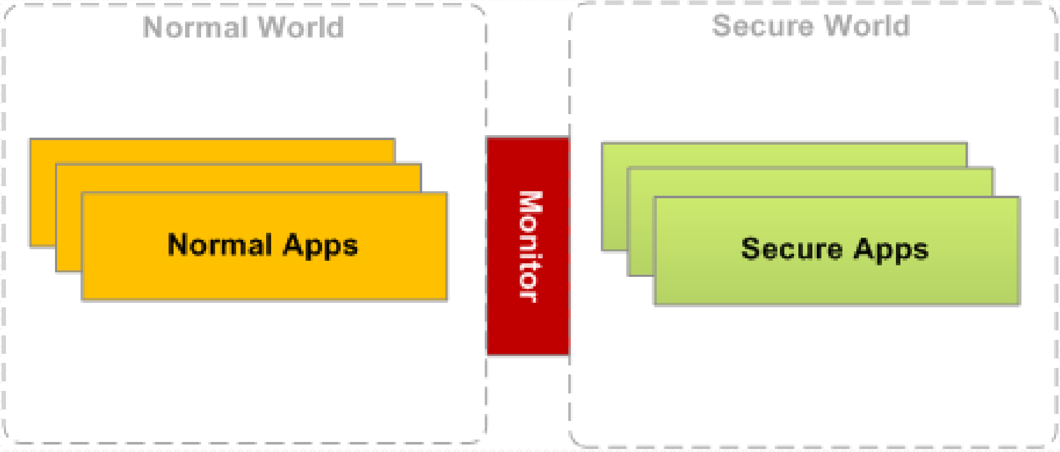
- HW-protected key
- ROMed X509 Certificate hash
- KNOX Enterprise Root of Trust
- KNOX Government Root of Trust
- Root key/certificate change upon deploy



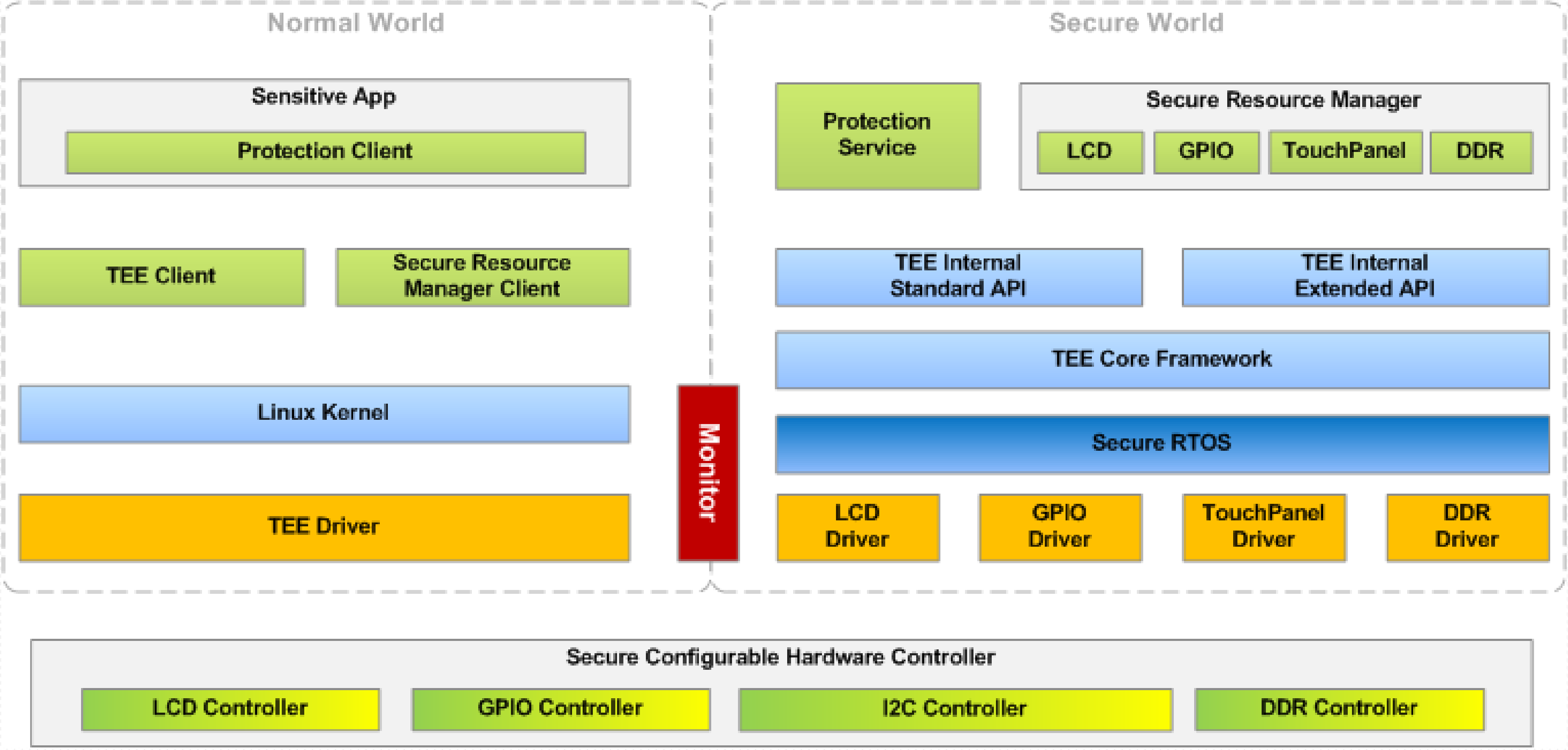
Trusted UI for Mobile Payment

ARM Trust Zone

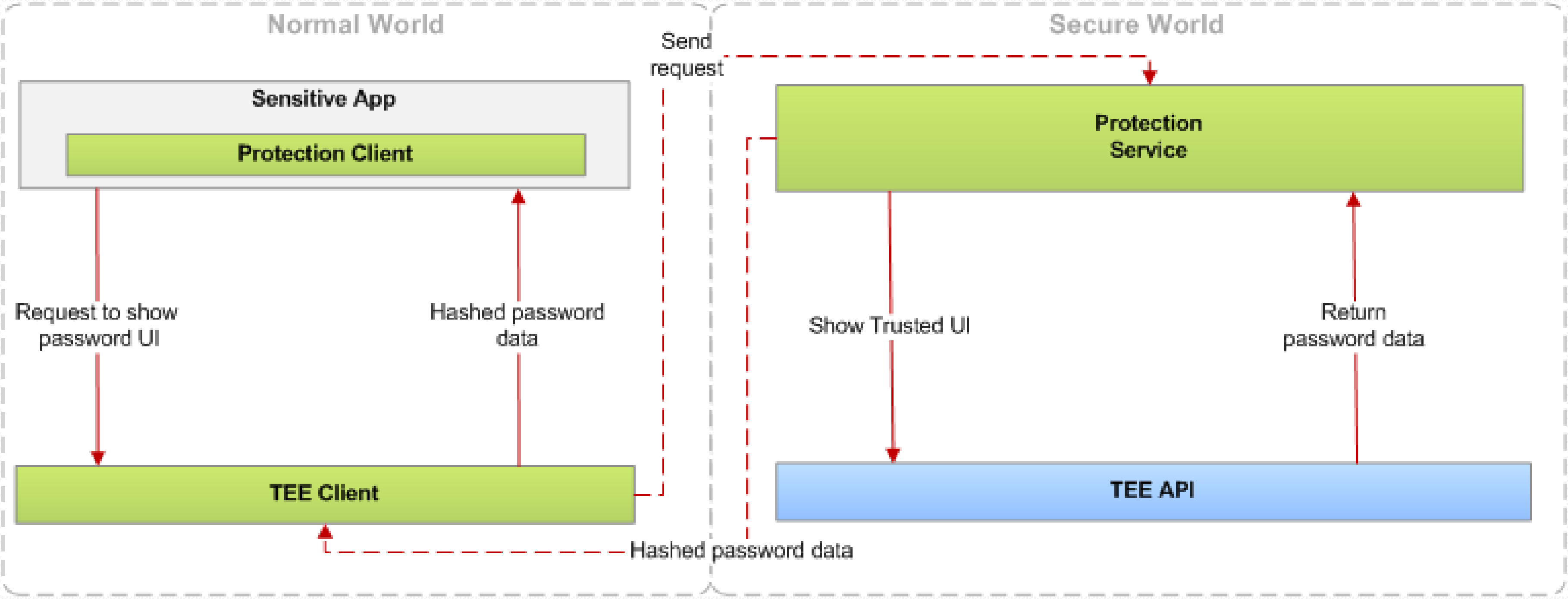
- Hardware isolation
- Minimum impact to power, performance and die size
- Target for secure payment, DRM, enterprise services



Architecture



Example: Password Input



Key Difficult - Summary

Hardware:

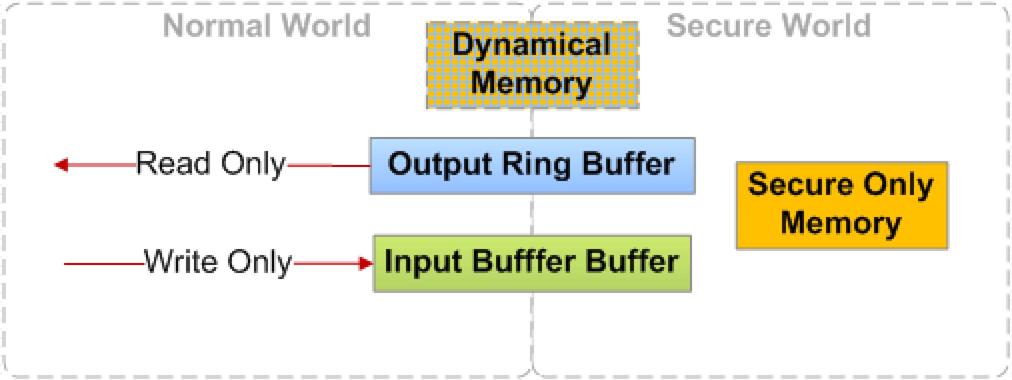
- SoC Support
- Dedicated Security Engine: Root of Trust

Software

- TEE(Trusted Execution Environment): Secure RTOS
- Normal OS Support

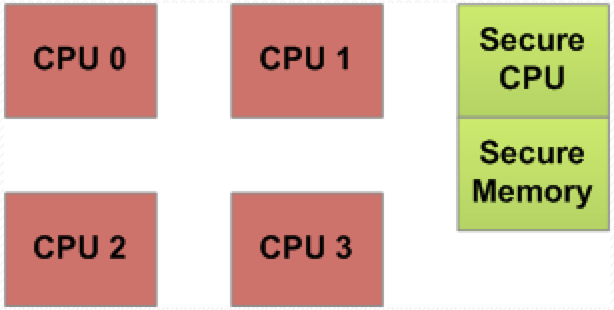
Key Difficult – SoC Support

- BUS
- Memory: support security region
- Peripheral: support security controller
  - Touch, Keypad, LCD, GPIO
- Subsystem: GPU, VPU, Audio
- Debugging vs Security



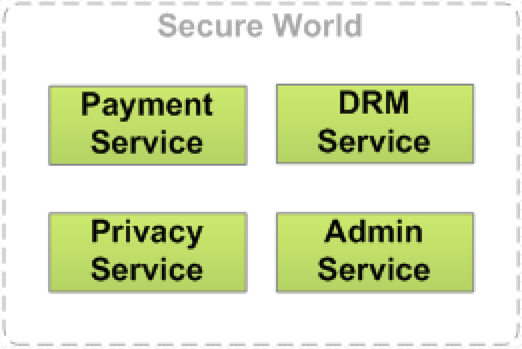
Key Difficult – Security Engine

- Physical Isolation
- Isolated encryption/decryption
- Root Key Storage: FUSE Block



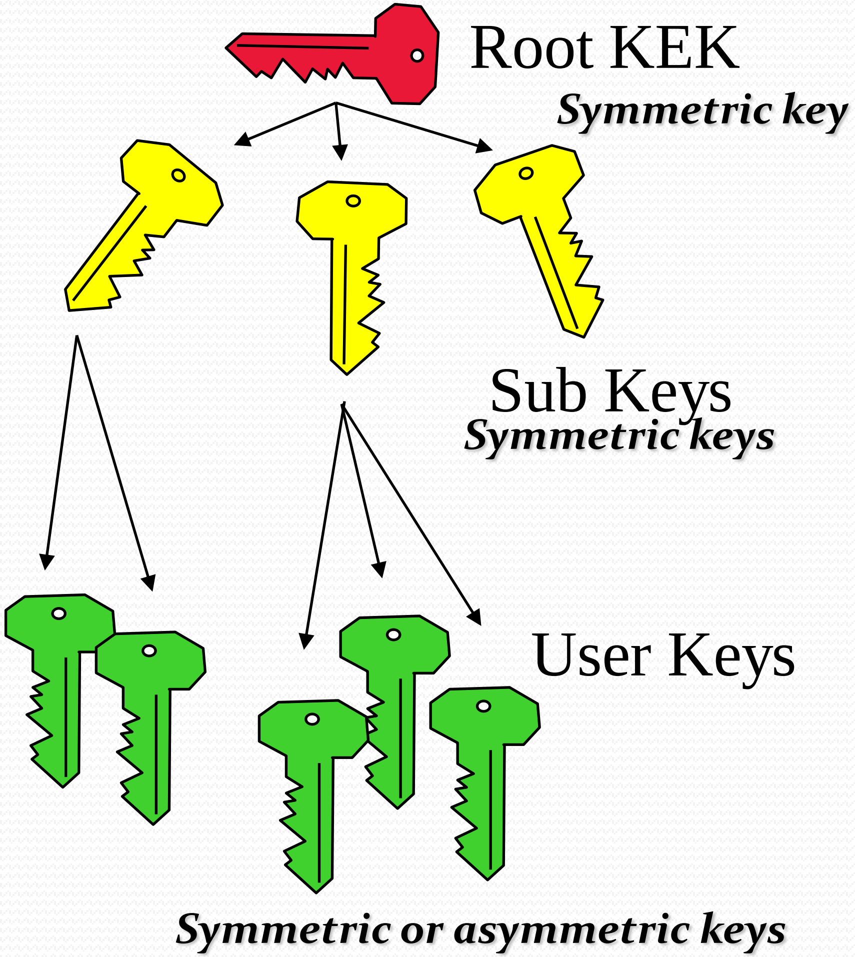
Key Difficult – Secure RTOS

- Process/Thread
- Scheduling
- Switching between Normal and Secure
- How to handle normal world event
  - Incoming Call
  - Notification
  - Alarm
- Isolation between service
- Support device driver



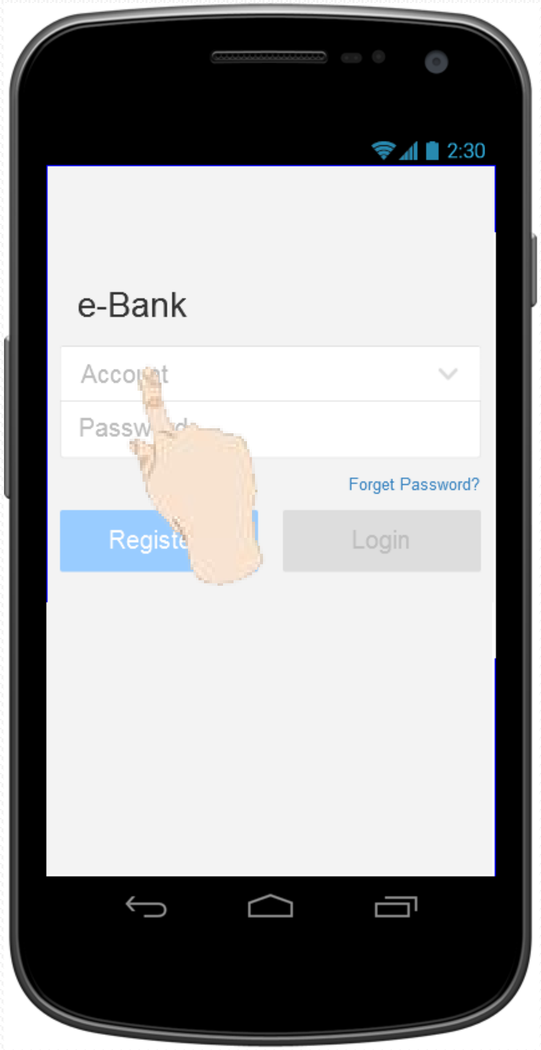
Key Difficult – Normal OS Support

- Trust boot
- Key Management
- Lock/Sync in driver
- SE Linux

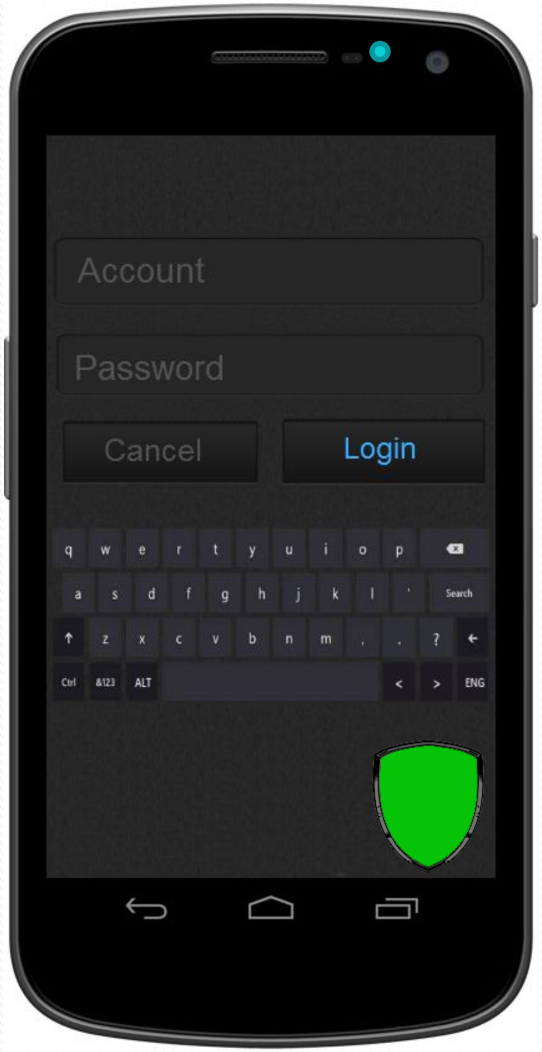


Demo

Normal World



Secure World



Thanks!