第三届
全国网络与信息安全防护峰会

对话·交流·合作

XDef 2014

移动终端的安全挑战及其等级保护标准的探讨

陆宝华

国鼎网络空间安全技术有限公司
中关村诚信互联网安全数据服务产业联盟
中关村信息安全产业联盟移动计算安全工作组

对话·交流·合作

目录

- 为什么要提出移动终端的等级保护问题
- 国外移动智能终端安全标准讨论
- 国内移动智能终端的安全现状分析
- 等级保护的背景
- 移动智能终端的安全等级定义
- 移动智能终端的分等级安全要求

为什么要提出移动智能终端的等级保护要求

- 移动办公的需求分析
- 移动智能终端的特点分析
- 移动智能终端的安全需求

移动智能终端的特点分析（资产）

- 基本特点：
- a)　在手持式单机硬件平台上工作}
- b)　单人员用户使用；
- c)　支持多个管理员角色；
- d)　支持应用软件安装；
- e)　应用软件通过操作系统介导访问数据、传感器及无线通信资源；

移动办公的需求分析

- 高度的网络化
- 无线通信的发展

  蜂窝移动通信

  W—LAN网络
- 移动办公的需求

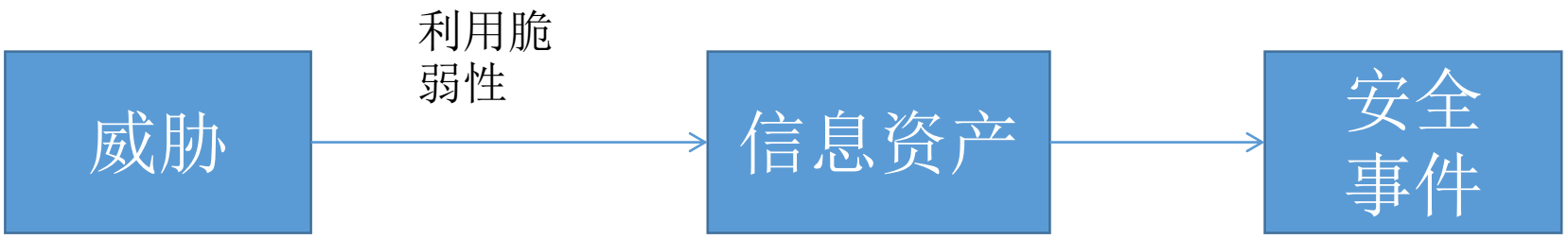
公安、海关、税务、边检

- 对提高工作效率、提高为民服务的水平

移动智能终端的特点分析

- 体积小，便于携带（易丢失）
- 存储和计算能力相对较差（不适宜太多的安全规则和工具在上面安装）
- 即作为个人的通信工具又可以作为移动办公的终端。能够通过多种方式接入Internet或其他计算机系统，并支持各种商业应用。
- 既有个人安全使用需求，也有办公安全要求
- 移动终端操作系统的特点是开放应用软件可编程接口（API)或开放操作系统源文件，由此带来的安全威胁使得安全功能成为移动智能终端操作系统必不可少的组成部分。

- 风险分析



移动智能终端的安全需求分析（资产）

- 移动终端上与用户利益直接相关的硬件

  包括:通信设 备（蜂窝移动通信设备、无线局域网设备）、终端信源传感器（麦克、摄像头、加速度计、定位导航系统）、终 端输人输出设备(红外线接口、蓝牙、USB接口、SDIO接口）等

- 与用户利益直接相关的软件包括存储

  用户信息的文件(通讯录、通信记录、短消息、电子邮件、记事本等）以及相关应用软件。

移动智能终端的安全需求分析（资产）

- 信息资产
- 在移动终端中需要保护的资产有：
- ——用户数据:包含位置信息、账户信息、通信记录、通讯录等。
- ——移动终端敏感资源：包含通信资源、外设接口，如摄像头、位置传感器等.
- ——移动终端操作系统安全功能数据:包含鉴别数据、安全属性等。

移动智能终端的安全需求分析（脆弱性）

- 使用环境的开放性
- IP信道的开放性（各类的免费Wifi，伪基站，恶意AP等）
- 语音短信通信的信道的开放性
- 网络边界的开放性(这个开放性会导致原来信息系统边界的完整性被破坏)
- 操作系统的开放性
- 各类应用软件的开放性

移动智能终端的安全需求分析（脆弱性）

- 脆弱性分析
- 易丢失
- 用户大多不具备安全技术能力或者安全技术能力薄弱，不能正确地配置安全策略。对安全事件的响应能力也较弱。
- 内置了IP网络通信协议，数据包和控制包都在一个公共信道上传送，不能将不同用户、不同用途的信息流分割到不同的独立的信道中，同时又提供“任意到任意”和“端到端”的连通性
- 操作系统和应用的安全机制薄弱，并存在漏洞、后门

移动智能终端的安全需求分析（威胁）

- 主要威胁：
- 非授权用户的访问、
- 授权用户的恶意访问（可能存在多个授权用户，包括维修人员、各种服务人员和开发者等理论上的可信用户。）
- 恶意应用软件的访问（开放应用软件安装）
- Inernet非授权实体的访问。

移动智能终端的安全需求分析（个人）

- 作为个人用户的安全需求（主要防范以下：）
- 数据的非授权访问
- 恶意吸费通信
- 个人物理信息的暴露
- 移动支付的安全性
- 各类传感器使用的保护
- 网络通信的保护

移动智能终端的安全需求分析（办公）

- 移动办公的安全需求

企业或政府相关解决方案的部署，确保用户自带设备办公的安全；

有可能导致办公系统的边界发生破坏。

- 审计要求的区别
- 个人物理轨迹的区别
- 对移动APP的限制要求

企业和政府行业用户的APP应用的安全性要求更高，不能允许某些APP管理员对用户数据的掠夺。

- 国外的情况简介

国外移动安全标准简介

- 美国国防部的安全要求
- GP组织的安全要求

国外的标准简介--DoD

- 美国国防部的标准
- DoD对网络空间安全的研究一直处于领先地位，同时他们考虑的是军事通信，所以首先考虑的是保密问题，从83年的桔皮书就体现了这一点。我国的专家对DoD的标准也是非常认可的，国家的第一个关于信息系统安全的标准，计算机信息系统安全等级划分准则就是桔皮书的翻版，在每个等级中加入的完整性要求。
- 在移动智能终端方面，DoD的步伐也是比较快的，出台Mobile OS Standard ，其中涉及到安全方面的要求有很多条。

国外的标准简介--DoD

- 这些标准大概可以分为这样的几个大的部分
- 访问控制要求
- 身份认证与解锁
- 审计
- 入侵防范及恶意代码防范
- 密码技术与认证证书
- 数据保护
- 安全保障要求

这些要求，与DoD的思想是一脉相承的。

国外的标准简介--GP

- GlobalPlatform（GP）是跨行业的国际标准组织，致力于开发、制定并发布安全芯片的技术标准，以促进多应用 产业环境的管理 及其安全、可互操作的业务部署。作为一个国际标准组织，其工作重心主要集中在安全单元、可信执行环境和系统消息等领域，其成熟的技术规范是建立端到端可信业务解决方案的工具，并服务于产业环境的多个成员，支持多种商业模式。

国外的标准简介--GP

- GlobalPlatform 的目标是创建一个标准化的基础架构, 加快安全应用程序及其关联资源的部署，如数据和密钥，同时保护安全应用程序及其关联资源免受软件方面的攻击。GlobalPlatform 通过发布和推进相关技术标准来实现这一目标，着重于以下三个方面:
- 1. 安全单元(SE)
- 2. 可信执行环境(TEE)
- 3. 系统消息(System Messaging)

国外的标准简介--GP

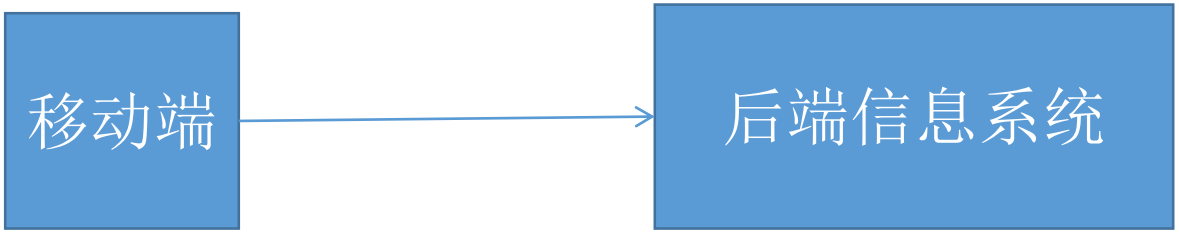
- 1. 安全单元(SE)（Secure Element）
- SE由软件和防篡改硬件组成，具有较高级别的安全性，　　GlobalPlatform 卡片技术规范支持防篡改芯片的技术实现和多应用管理，如智能卡和多种安全单元（SIM 卡，SD 卡和嵌入式安全单元）。支持在智能卡和移动设备上部署近场支付业务, 身份，医疗，交通等应用。

国外的标准简介--GP

- 2. 可信执行环境(TEE)
- GlobalPlatform 制定了可信执行环境的标准，可信执行环境是一个驻留在所连接设备的主处理器上的安全区域， 以确保在可信执行环境中的敏感数据的存储、处理和保护；支持智能设备产业利益相关方的核心需求，如智能手机和平 板电脑应用程序开发人员和设备制造商。这种技术的发展对移动钱包，近场支付实现，内容保护和自带设备办公 （ BYOD ）等技术实现至关重要。

国外的标准简介--GP

- 3



- .系统消息(System Messaging) 这是通过定义“谁”负责“什么”以及约定统一的语言（消息）来实现的。
- 根据GlobalPlatform 的定义，消息可以通过移动网络使用无线传输（OTA），也可以通过互联网使用云环境来实现。通过此项技术，用以实现可信业务管理，发卡和个人化安全芯片以及可信执行环境（TEE）技术。

国外的标准简介--GP

- REE（Rich Execution Environment）
- 针对多功能性和丰富性创建的环境，执行诸如安卓（Android）塞班和Windows Phone OS 支持第三方下载，该环境下安全是其考虑因素，但并非最重要的因素。
- TEE（Trusted Execution Environment）

TEE是一个一Rich OS并行运行的独立环境，是由软件和硬件共同完成的，需要有可信OS内核支持。通过可信存储和可信访问来隔离敏感数据

- SE （Secure Element）
- SE由软件和防篡改硬件组成，高级别的安全性，可以与TEE一起运行。对于近距离支付相应用或官方电子签名，SE是强制的安全措施，用以安全地传输个人身份识别号码（Pin）进行大额交易，它还可以对直接存储在SE中的应用进行过滤访问。

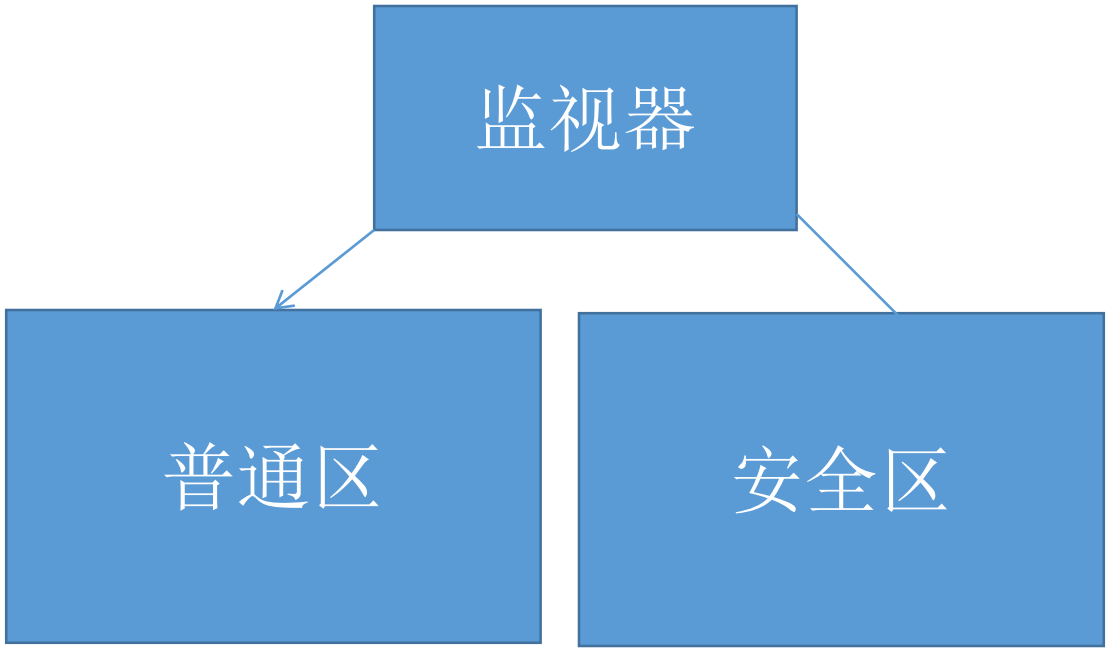
基于TrustZone技术的可信执行环境

- TrustZone技术是ARM公司提出的一套在系统范围内扩展安全特性的硬件架构。旨在提供一套可信的嵌入式设备平台，为用户提供了一个可信的执行环境。不同于其他安全解决方案，TrustZone架构可以为系统的任意部分提供安全保护，可以提供包含功能和调试单元的端到端安全解决方案。
- TrustZone技术将SoC的所有硬件与软件资源分隔为两个区域——安全区域和普通区域。安全子系统在安全区域上运行，而其他程序运行在普通区域内。

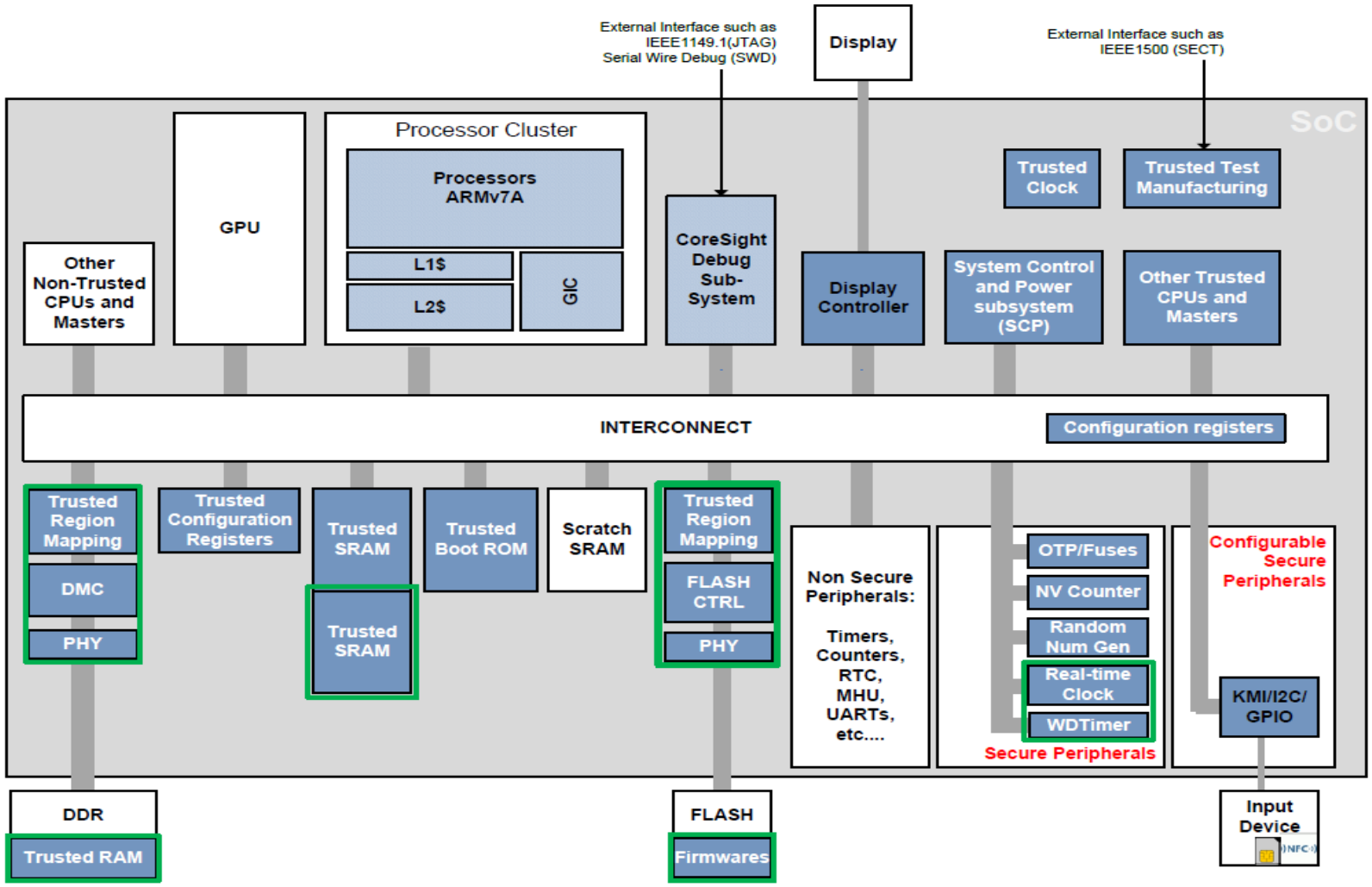
TrustZone硬件架构

- 在这个两区域内，通过支持TrustZone技术的总线架构所呈现的硬件逻辑，任何普通区域的组件都不可能访问安全区域的资源，保证两个区域之间的有效隔离。
- 在支持TrustZone技术的处理器上，通过一个新增的处理器模式——监视器模式，处理器可以有效与安全地以时间片的方式执行来自安全区域与普通区域的程序。同时TrustZone具有一个安全的调试架构，可以保证黑客不能从调试模式接入的方式访问安全区域的资源，可信执行环境硬件框图如图所示：

TrustZone原理框图



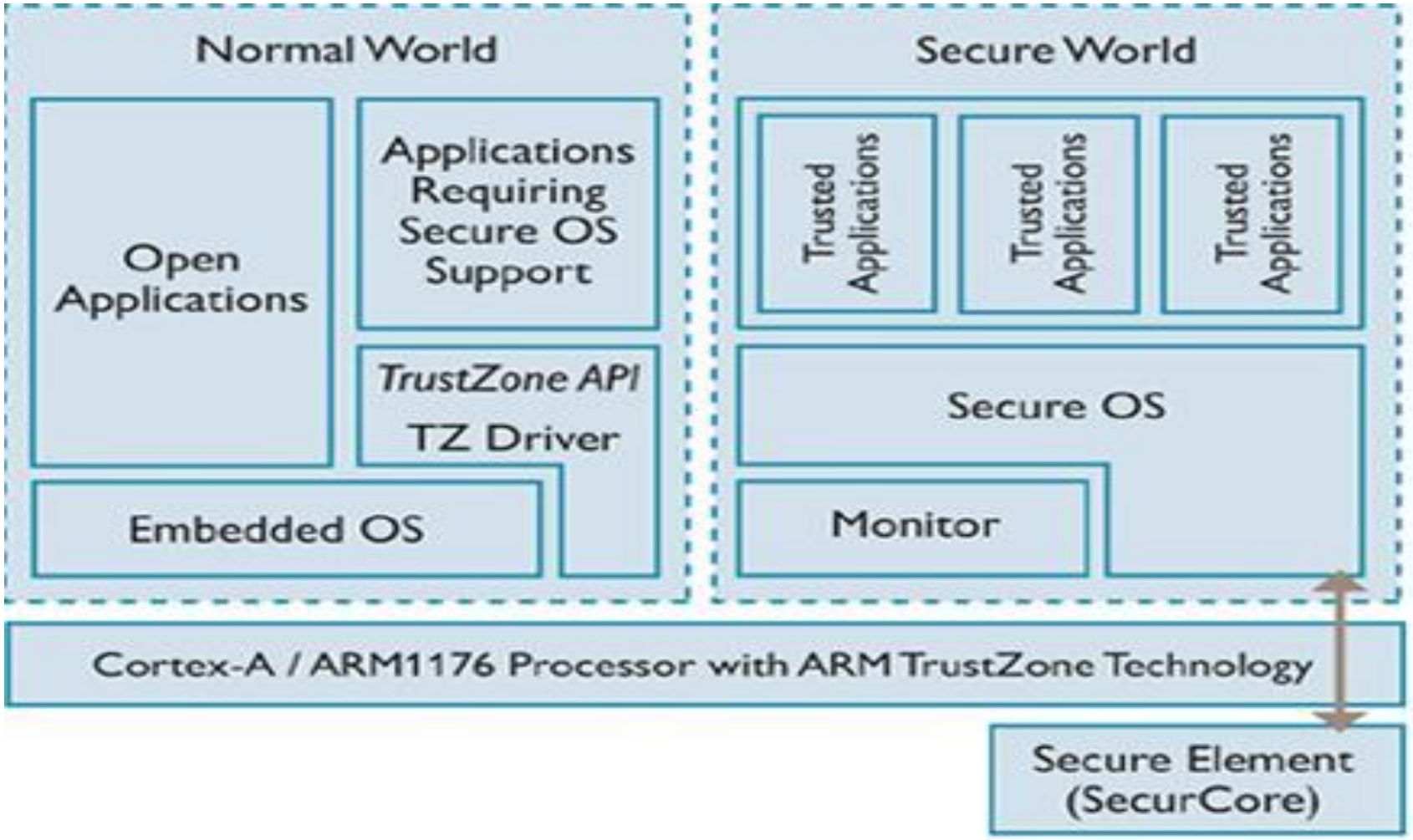
TrustZone硬件架构



TrustZone硬件架构

- TrustZone硬件架构的基础特性是在主系统总线上为每个读写通道增加一个额外的控制信号，这个比特位称为NS（Non-Secure）位，通过对这个比特位上的高低电平，来控制对不同区域的读写控制。对于普通区域，此位上的电平为高。
- TrustZone的处理器架构，相对于原有的ARM处理器，支持TrustZone技术的处理器能够提供两个虚拟核，一个是普通的，而另一个是安全的。同时新增监视器模式，可以鲁棒地在两个核之间进行上下文切换。被送往系统总线的NS位的值可以间接的从当前进行指令与数据访问的虚拟核的标示中得到。这样普通的虚拟核只能访问普通区域的系统资源，而安全的虚拟核可以访问所有的系统资源。

TrustZone软件架构



TrustZone软件架构

- TrustZone软件架构的总体框架依赖于安全区域上可用的硬件资源，安全软件利用安全区域的硬件资源和自身的软件资源（包括安全算法）向普通区域的软件提供安全操作服务。

- 国内的情况简介

- 国内情况

国内的标准体系

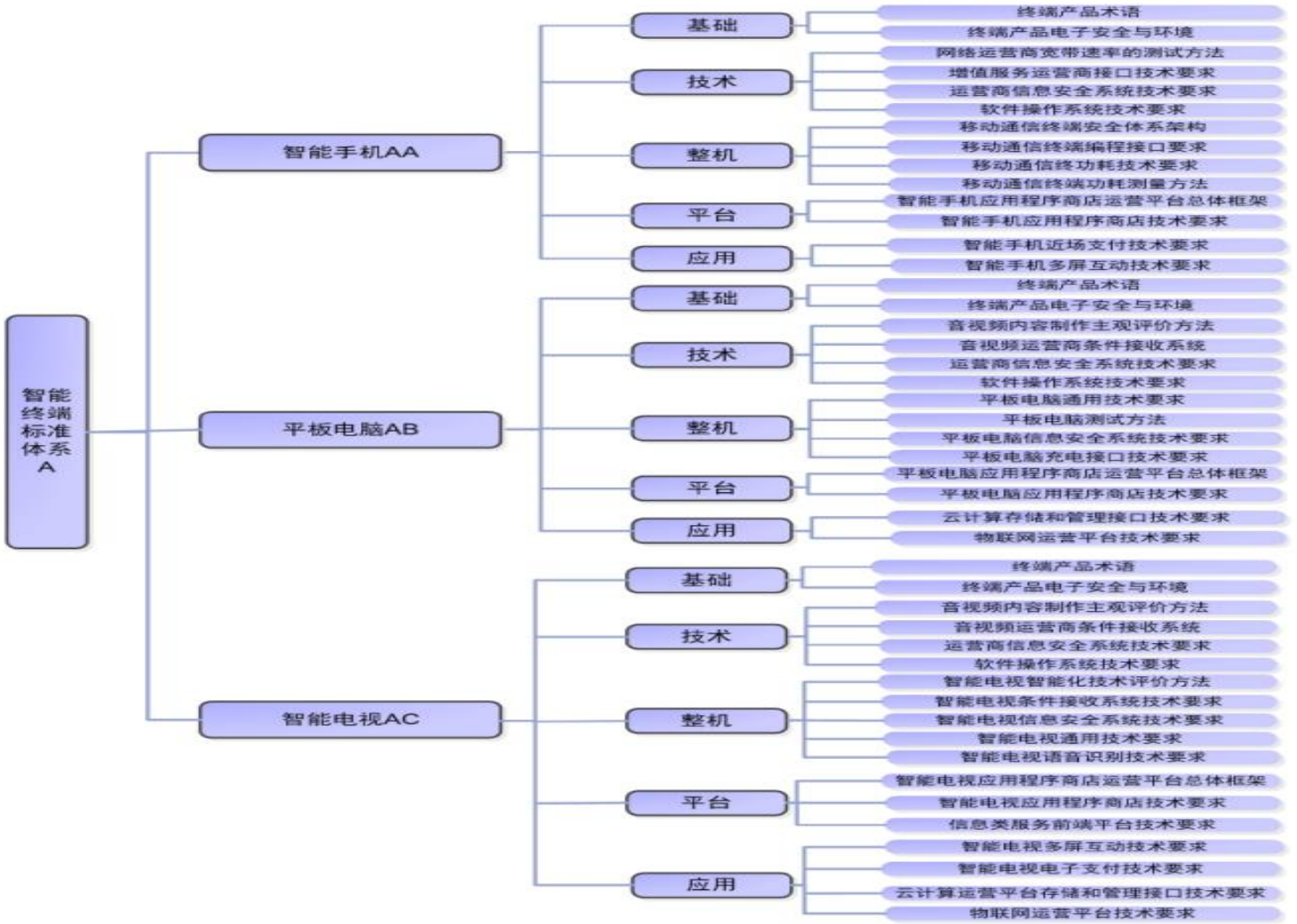


图 10 智能终端标准体系框架

国内的标准体系

- 基本分为了五大类
- 基础
- 技术
- 整机
- 平台
- 应用

在这里涉及安全的内容并不多，主要还体系和应用。

国内的情况的简介

- 国标GB/T30284-2013移动通信智能终端操作系统安全要求（EAL2级）
- 行业标准YD/2407--2013移动智能终端安全能力技术要求
- 行业标准YD/2408—2013移动智能终端安全能力测试方法

- 这些标准能适合于我国的等级保护要求吗？
- 能适合于自带设备办公吗？

国内的情况的简介

- GB/30284—2013
- 基于CC的思想，与CC标准是一脉相承的
- 安全功能不分级，对于较低安全要求的来说，一些安全功能是不必要的，会带来使用上的麻烦
- 而对于较高安全级别来说，EAL2，显得要求过低。
- 不能完全适合于等级保护体系。

国内的情况的简介

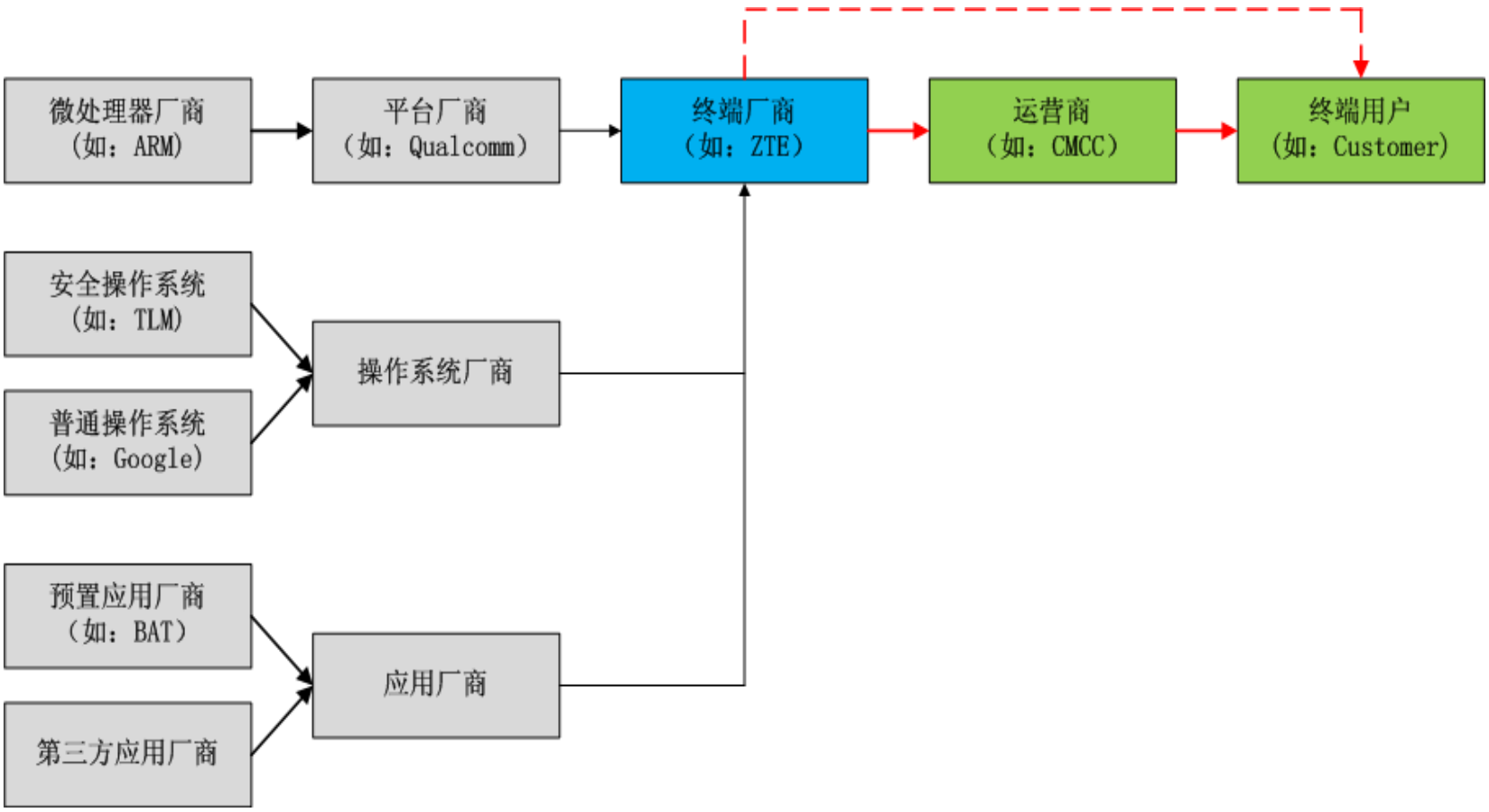
- YD/T2407—2013虽然给出了五个安全等级，但是这个标准保护目标是个人用户的，还不能适用于行业用户。按照这个标准设计和生产的移动智能终端，是很难满足企业和政府的自带设备办公的安全要求的。

国内的情况的简介

- 中办推广保密手机
- 多个厂商推出了所谓的安全手机
  （华为、中兴、阿里与公安部一所等）

还有小米
E人E本
等等

中兴通讯移动智能终端安全产业链




4G时代下的省钱利器
流量监控
云标记智能拦截
骚扰拦截
一键清除后台进程，
让手机“飞”起来；
深度清理手机内存，
让系统更加干净顺畅
手机加速
掌心管家
隐私空间
权限管理
无需root即可进行
Android系统权限的
管理
防止通话记录、短信、
照片、视频泄密
病毒查杀
业界领先的云杀毒功能

国内的情况的简介

- 这些所谓的安全手机，操作系统本身的安全水平如何？
- 操作系统安全是一个计算机系统的安全的基础，没有操作系统的安全作保障，一切的安全措施都是建立在砂子上的。尽管使用加密技术，但是，仍然是“铁锁套在纸环上”
- 安全的操作系统必须具备两方面的基本要素

  一是强力的安全机制；

  二是没有漏洞。

  隔离与控制从来都安全的基本思想和手段。

- 关于等级保护

国家等级保护背景简介

- 1994年提出了等级保护的概念，
- 1999年发布了第一个等级保护强制标准（GB17859--1999）从安全水平能力上提出五个安全等级
- 2004年出台66号文，从安全需求上提出5个安全等级
- 2006年发布了等级保护的系列标准（20271系列共5套，20269--20273）作为17859的配套标准。
- 2007年出台等级保护实施办法，从安全需求的角度进一步明确了五个安全等级。
- 2008年发布了等级保护定级指南和基本要求（GB/T22239—2008 和GB/T22240--2008）

信息系统安全等级划分的原则

	一般	严重	特别严重
个人或小组织	一级	二级	可三级
社会秩序和公众利益	二级	三级	四级
国家安全	三级	四级	五级

五个安全等级的移动智能终端

- 依据国家等级保护的标准，提出对应于移动智能终端的五个安全等级
- 一、软件加固级移动智能终端
- 二、增强型加固级移动智能终端
- 三、安全手机
- 四、加固级安全移动智能终端
- 五、增强型安全移动智能终端

安全移动终端的五个等级

- 第一级 软件加固级移动智能终端
- 简称软加固机。是指仅在采用基本操作系统的移动智能终端上通过软件提升安全水平的移动智能终端。适用于个人用户和对安全需求不高的行业用户。对应于等级保护第一级，用户自主保护级。此类移动智能终端一般不能作为已经确定为二级的信息系统中的移动办公的终端使用。

包括增加了对移动支付的功能的移动智能终端，也只能是这个级别。目标用户主要是个人用户，而不是移动办公。

安全移动终端的五个等级

- 第二级增强型加固移动智能终端
- 简称强加固机。是指在第一级的基础上增加了审计功能，和针对行业用户特殊需求而设计的移动智能终端。不仅适用于个人用户，还适用于有一定安全要求的行业用户。可以作为安全性要求不高的行业用户作为移动办公的终端使用。对应于国家等级保护第二级。在这一级中应考虑访问控制的要有更细的粒度，所以在这一等级应该考虑隔离分区的作法。
- 审计保护级。

安全移动终端的五个等级

- 安全移动智能终端
- 简称安全机。是指采用了安全操作系统的移动智能终端。安全操作系统是指达到（GB17859-1999）规定的标记保护级的操作系统。并且，应用程序安全要求达到了国标（GB/T22239-2008）的第三级的安全要求。可以适用于安全要求较高的行业用户。访问控制的粒度应该等于或者高于二级要求。一些隔离措施是必要的。
- 可作为已经确定为三级信息系统作为移动办公之用。

安全移动终端的五个等级

- 加固型安全移动智能终端
- 简称加固安全机，是指采用了结构化设计的安全操作系统的移动智能终端，达到了（GB17859-1999）规定的结构化保护级的要求，并且应用程序达到了国标（GB/T22239-2008）的第四级的安全要求。可以用于安全性要求很高的行业用户，作为移动办公的终端。但不适用于存储、传输和处理绝密级信息。也不允许作为个人使用的通信终端。
- 其隔离措施必须依赖于硬件，并且能够证明这个机制是不能被绕过的。

安全移动终端的五个等级

- 增强型加固安全移动智能终端
- 简称强加固安全机。是指达到了访问验证保护级（GB17859-1999）规定的第五级的安全要求，操作系统及所有的应用程序的安全性均达到了可以验证的安全水平，可以适用于安全性要求极高的行业用户，作为移动办公使用。但不能允许用于个人通信。

标准制定的原则

- 1、满足安全需求
- 2、将所有的资源都作为客体来管理
- 3、仍然以访问控制为核心的保护技术
- 对于低安全等级的强调用户自身的认可（自主访问控制）
- 对于高安全等级强调强制访问控制
- 4、仍然强调操作系统的核心地位
- 5、与现有的等级保护制度一致
- 6、兼顾目前的隔离技术和可信计算

- 谢谢！