



智能终端虚拟化及安全隔离技术

黄勇军, 金华敏, 刘国荣, 刘东鑫, 汪来富, 沈军
(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 随着智能终端能力及安全需求的提升, 在服务器和桌面机上发展起来的虚拟化技术, 也逐渐在智能终端上发展和应用。对智能终端虚拟化及安全隔离技术的应用场景、各类实现技术进行了分析探讨, 并对各种技术以及与服务端虚拟化及其安全需求进行了对比分析。

关键词: 智能终端; 虚拟化; 隔离

中图分类号: TP309.1

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018099

Virtualization and isolation technology in intelligent terminals

HUANG Yongjun, JIN Huamin, LIU Guorong, LIU Dongxin, WANG Laifu, SHEN Jun
Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: With the improvement of computing capability and security requirements for intelligent terminals, the virtualization technology has been gradually developed and applied, which is originally created in the server and desktop computer industry. The application scenarios, a variety of different implementation and security requirements of virtualization were analyzed by contrasting to the computer servers.

Key words: intelligent terminal, virtualization, isolation

1 引言

近年来, 我国移动互联网迅速发展, 并加速与经济社会各领域的深度融合。截至2017年6月, 我国手机网民规模达到7.24亿户, 网民中使用手机上网的比例持续提升, 达到96.3%^[1]。各类手机应用的用户规模不断上升, 场景更加丰富, 大大方便了人们获取信息、社交、购物、娱乐等各

类活动, 互联网理财、线下支付、网上外卖、共享出行等线上线下融合创新应用的涌现, 更进一步方便了人们的生产、生活, 使用手机进行支付、购物甚至理财已经成为主流, 手机日益成为个人信息助理和第一钱包, 成为生活中不可或缺的一部分。

另一方面, 移动安全状况仍然非常严峻。2017年第一季度, 360互联网安全中心共截获Android平

收稿日期: 2017-11-20; 修回日期: 2018-01-30

通信作者: 刘国荣, liugr@gsta.com

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No. 2015AA017205)



台新增恶意程序样本 222.8 万个, 累计监测到移动端用户感染恶意程序 5 812.7 万人次, 自 2012 年以来, 移动端从几十万跨越到千万级别恶意样本, 显示了移动恶意程序总体进入平稳高发期。山寨 App、钓鱼网站、二维码扫码诈骗等各类骗局也威胁着手机安全^[2]。

因此, 提升手机等智能终端的安全性成为迫切需要, 特别是以移动支付、移动购物、移动办公为代表的用户对安全具有更高要求。采用虚拟化及隔离技术, 将高安全要求的应用与日常应用进行隔离, 是防范安全问题的一种有效手段。

2 智能终端虚拟化及隔离技术的应用

2.1 虚拟化及隔离技术概述

智能终端隔离的主要目的是将具有高安全要求的关键应用、数据与普通应用进行分离, 并针对性地实施差异化的安全策略, 分等级保障不同应用的安全。隔离机制可在硬件、系统和应用等不同层面上实现。特别是随着智能终端能力及安全需求的增强, 在服务器和桌面机上发展起来的虚拟化技术, 也逐渐在智能终端上发展和应用。

虚拟化是指资源的抽象化, 也就是单一物理资源的多个逻辑表示, 或者多个物理资源的单一逻辑表示。移动虚拟化与服务器虚拟化一样, 都是利用管理软件, 对基础设备的各种实体资源予以抽象、转换后呈现出来, 打破实体结构间的不可切割的障碍。与服务器虚拟化不同的是, 移动终端虚拟化的主要目的在于为应用提供相互隔离、安全的执行环境, 提高资源的利用率反而在其次。

2.2 智能终端隔离应用场景

(1) 移动办公等行业应用, 提供独立可管区域

随着移动互联网和智能终端的普及, 移动互联网随时随地连接的特性推动了移动办公的兴起, 特别是移动办公 (bring your own device, BYOD), 大大提升了企业运营效率和员工工作

的便利性, 同时也降低了企业在终端上的投入成本。但 BYOD 也引入了新的风险, 与传统办公模式相比, BYOD 环境主要存在以下安全隐患: 移动网络处在一个开放的网络, 而传统重要的信息系统都是通过企业内网接入; 使用环境与传统信息化模式不同, 传统的大部分时间都在固定的办公场所, 设备丢失可能性很小, BYOD 通常使用移动智能终端, 更加容易丢失; BYOD 使用的个人设备上往往同时安装很多个人的 App, 而个人 App 市场上的恶意软件众多, 将企业数据置于安全隐患之中。由于 BYOD 终端管理涉及产权和员工个人隐私的问题, 企业也难以针对终端实施严格的管理。

采用虚拟化技术为个人应用和企业应用提供双域/双系统的解决方案, 则可很好地解决上述难题。办公应用运行在独立的工作域/系统中, 由企业 IT 管理员进行控制, 并实施相应的安全策略; 员工在个人区正常运行个人应用, 两个系统相互独立, 互不干扰, 如图 1 所示。

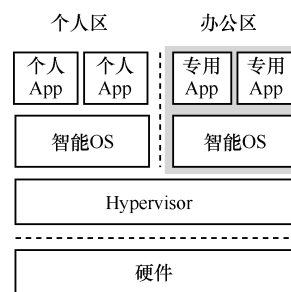


图 1 双域应用场景

(2) 移动支付等高安全要求应用, 提供隔离的安全运行环境

当前移动应用所涉及的领域逐渐扩大到各行各业, 如手机网银、移动支付、移动电子商务等, 这些应用需要更高的整体安全级别。对于移动支付等金融业务, 防御恶意软件/病毒、保障智能终端的安全是重中之重, 更是其发展的根基。

移动终端虚拟化技术可在多个层面上实现安全应用与普通应用的隔离, 满足应用的安全需求。

典型的是可信执行环境（trusted execution environment, TEE）技术，在与设备上的 rich OS（Android、iOS 等操作系统）并存的运行环境中实现独立的可信运行，并且给 rich OS 提供安全服务。TEE 有多种实现技术，典型的是基于硬件的 TrustZone，也可采用基于 Hypervisor、安全容器等软件实现，隔离出安全操作系统和普通操作系统。TEE 具有其自身的执行空间，比 rich OS 的安全级别更高。TEE 所能访问的软硬件资源与 rich OS 分离。TEE 提供了授权安全软件可信应用（trusted application, TA）的安全执行环境，同时也保护 TA 的资源和数据的保密性、完整性和访问权限，如图 2 所示。

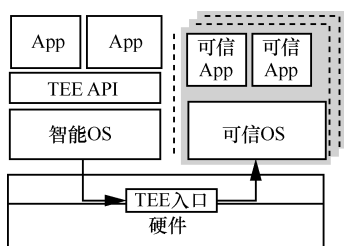


图2 可信执行环境

（3）多协议栈/多系统终端，降低系统与硬件的耦合度，降低终端研发及硬件成本

移动终端设计、生产厂商从降低系统与硬件耦合、快速将原有协议栈移植到新设计的终端，或从硬件资源复用、降低硬件成本等方面考虑，采用虚拟化技术实现隔离的多协议栈、多系统终端。本场景中，主要是终端厂商基于成本考虑，使用者在终端使用上，并不能直接感受到多系统/协议栈的存在。

- 多/旧协议栈隔离与兼容：随着技术的发展通信制式也不断演进，目前智能手机普遍要求同时支持 GSM、CDMA、WCDMA、cdma2000 1x Ev-Do、HSPA 和最新的 LTE TDD、FDD 等通信制式。在同一手机平台中继承原有稳定的协议栈，又要快速支持新的协议栈，同时避免不同

协议栈之间耦合产生的兼容性问题，是目前智能手机设计中的一大重点。用虚拟化技术，可将原有稳定的协议栈与实时操作系统（real-time operating system, RTOS）一并迁移到虚拟机上。只需要虚拟出原有 RTOS 需要的硬件环境，而对 RTOS 本身和其承载的协议软件不需要任何修改。同时根据资源分配原则使各个协议栈子系统相对独立。既可以快速继承原有协议栈，又避免了各个协议栈之间的干扰，如图 3 所示。

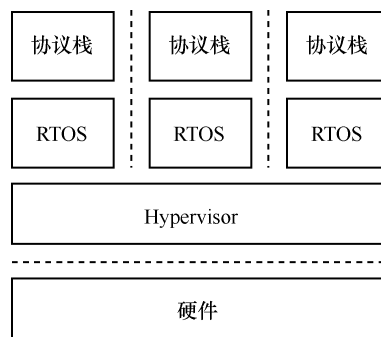


图3 协议栈隔离

- 硬件资源复用：智能手机除具备传统的通信功能外，还需运行功能丰富的应用软件。由于通信栈和普通应用具有不同的要求和特性：通信栈具有高实时性的要求、应用软件具有功能丰富的特性，现有的面向基带处理的 RTOS 和面向应用处理的智能操作系统都不能独立地满足系统需求，主流的智能机通常采用基带（base band, BB）+ 应用处理器（application processor, AP）结构，存在硬件 IP 地址的重复浪费。采用虚拟化技术，则可在单一的 CPU 上模拟两个处理器，运行两种不同类型的操作系统，从而可简化手机设计、降低硬件成本，如图 4 所示。如早在 2009 年，摩托罗拉公司就曾采用 OKL4 的虚拟化方案推出 Evoke QA4 手机。

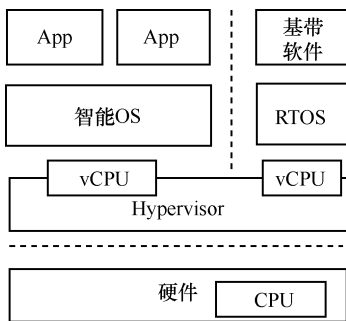


图4 硬件资源复用

3 虚拟化及隔离技术分类

针对智能终端个人化、资源紧凑等特点以及不同场景的需求差异，产业链的不同厂商分别从终端硬件、操作系统、应用以及云平台等多种层面入手，采用了差异较大的技术路线，形成了多种技术实现形式。主要的实现方式如图5所示。

3.1 基于硬件实现的隔离

基于硬件实现的隔离，是采用硬件物理分区或者分时运行的方式实现运行环境的隔离。典型的有安全元件（secure element, SE）、移动可信模块（mobile trusted module, MTM）等独立硬件模块、可信执行环境和 TrustZone 技术等。

（1）独立硬件模块

独立硬件模块，可以有外部硬件模块和固化的内部模块两类形态。

外部硬件安全模块，是在设备中以接口的

形式外接独立的硬件模块，比如设备上的 SIM 卡、TF 卡等智能卡。这种方式的优点是智能卡具有特定的软硬件安全特性，能够保护卡内的密钥等资源，而且要攻破其防护所付出的代价很高。缺点就是与设备的接口通信速度低，而且不能保护用户界面的安全，即与用户交互的数据的安全，在交易支付方面该方案还不能提供好的保护。

内部的硬件安全模块，即把类似于智能卡的功能直接放到 SoC 里面。这种方式也只能保护诸如密钥之类的资源，不能保护用户交互数据。在 SoC 里面有两个核：一个普通的 App 核和一个安全核。两个核之间的通信速度也会比较低。而且在占用 SoC 面积、调试端口的访问控制等方面也需要很小心谨慎。

（2）可信执行环境

TEE 是 Global Platform（GP）提出的概念。TEE 是与设备上的 rich OS（如 Android）并存的运行环境，并且给 rich OS 提供安全服务。它具有其自身的执行空间，比 rich OS 的安全级别更高，但是比起安全元件（SE，通常是智能卡）的安全性要低一些。但是 TEE 能够满足大多数应用的安全需求。从成本上看，TEE 提供了安全和成本的平衡。TEE 与 rich OS 并存，所能访问的软硬件资源与 rich OS 分离^[3]，如图6所示。

TEE 提供了 TA 的安全执行环境，同时也保

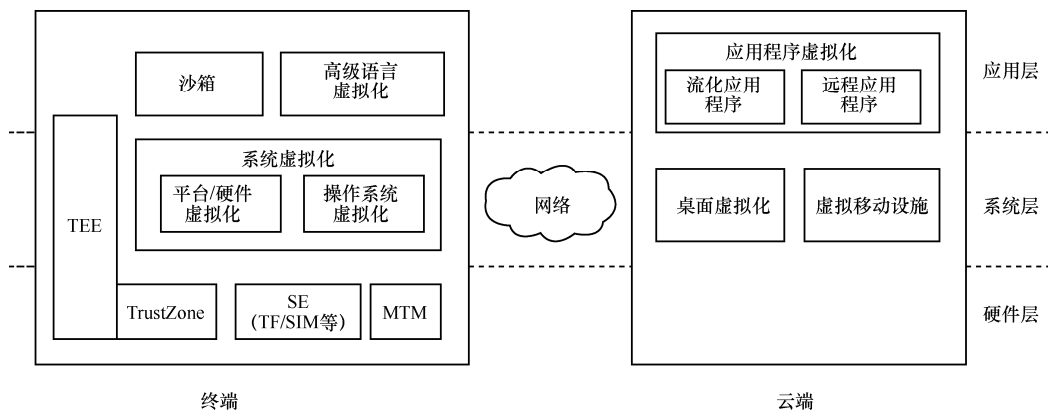


图5 移动虚拟化技术实现方式

护 TA 的资源和数据的保密性、完整性和访问权限。为了保证 TEE 本身的可信根, TEE 在安全启动过程中是要通过验证并且与 rich OS 隔离的。在 TEE 中, 每个 TA 是相互独立的, 且不能在未授权的情况下互相访问。

TEE 已经制定的基础规范有 TEE 内部 API、TEE 客户端 API, 还有一系列补充的功能性 API 规范以及应用管理、调试功能、安全保护轮廓等规范正在制定中。

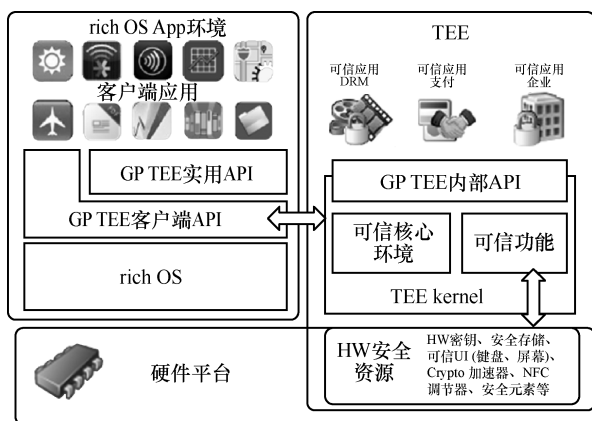


图6 TEE架构

(3) ARM TrustZone

TrustZone 的硬件架构是整个系统设计过程中的安全体系的扩展, 目标是防范设备可能遭受到的多种特定威胁。系统的安全是通过将 SoC 的硬件和软件资源划分到两个世界获得的。这两个世界是安全子系统对应的安全世界和其他子系统对应的普通世界。

在处理器架构上, 每个物理的处理器核提供两个虚拟核, 一个是非安全 (non-secure, NS) 核, 另一个是安全 (secure) 核, 在这二者之间切换的机制叫做监控模式。NS 核只能访问 NS 的系统资源, 而安全核能访问所有资源。普通世界的软件可以使用 SMC 指令或者通过硬件异常机制的一个子集来进入监控模式。可以配置 IRQ、FIQ、外部 data abort、外部 prefetch abort 这几个异常进入监控模式^[4]。图 7 展现了这种切换方式。

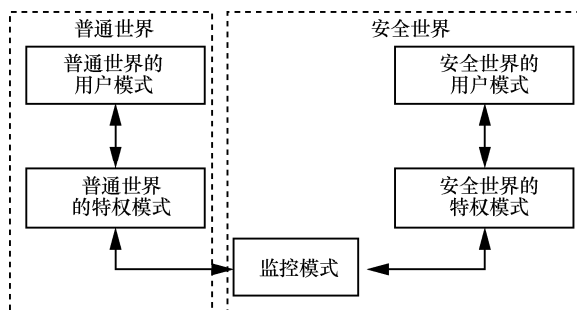


图7 TrustZone原理示意

当普通世界的用户模式需要获取安全世界的服务时, 首先需要进入普通世界的特权模式, 在该模式下调用 SMC, 处理器将进入监控模式, 监控模式备份普通世界的上下文, 然后进入安全世界的特权模式, 此时的运行环境是安全世界的执行环境, 此后进入安全世界的用户模式, 执行相应的安全服务。

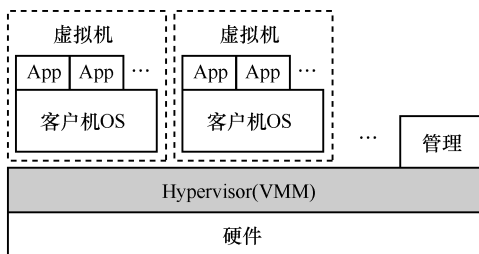
TrustZone 实现了应用在硬件物理层面的隔离, 是实现 TEE 的最佳技术, 目前大多智能终端基于该技术, 提供身份认证、支付等安全应用保障的基础, 如指纹识别、人脸识别等。此外, 也可以基于 TrustZone 实现系统虚拟化, 如在 ARM 架构支持虚拟化扩展技术前, Green Hills 的 INTEGRITY 曾利用该特性, 在安全区运行 Hypervisor 实现了双操作系统。

3.2 系统虚拟化

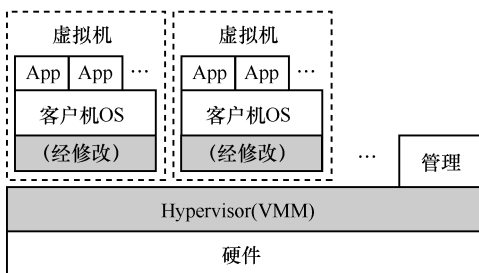
(1) 平台/硬件层虚拟化

平台虚拟化, 是通过虚拟硬件抽象层来实现虚拟机, 为客户操作系统呈现相同或相近的硬件抽象层, 通常宿主机和客户机指令集相同、其他部分如中断控制器, 设备等可以完全不同。平台/硬件抽象层虚拟化又分多个类别, 其中, 最主要的是全虚拟化 (full virtualization) 和半虚拟化 (para virtualization), 如图 8 所示。

全虚拟化, 主要是在客户操作系统和硬件之间捕捉和处理对虚拟化敏感的特权指令, 使客户操作系统无需修改就能运行, 速度会根据不同的实现而不同, 但大致能满足用户的需求。这种方



(a) 全虚拟化



(b) 半虚拟化

图8 全虚拟化与半虚拟化

式是业界现今最成熟和最常见的。半虚拟化也利用 Hypervisor 来实现对底层硬件的共享访问，但是由于在 Hypervisor 上面运行的客户机 OS 已经集成与半虚拟化有关的代码，使得客户机 OS 能够非常好地配合 Hypervisor 来实现虚拟化。通过这种方法无需重新编译或捕获特权指令，使其性能非常接近物理机。

全虚拟化的优点是客户机 OS 无需修改、使用简单，缺点是性能方面不是特别优异，特别是 I/O 方面。目前主要通过引入硬件辅助虚拟化技术来提高其性能。和全虚拟化相比，半虚拟化架构更精简，而且在整体速度上有一定的优势。但其缺点是需要对客户机 OS 进行修改，所以在用户体验方面略差。

性能问题是系统虚拟化技术发展的一大障碍，为解决该问题，ARM 从 v7 架构开始新增 Hypervisor 模式提供对虚拟化扩展的支持，该模式比非安全世界中原有的内核模式具有更高特权，使 Hypervisor 可以管理非安全世界里其他所有的模式里运行的软件，为实现硬件辅助虚拟化奠定了基础。图 9 为最新的 ARMv8 架构^[5]对该模式的支持方式。

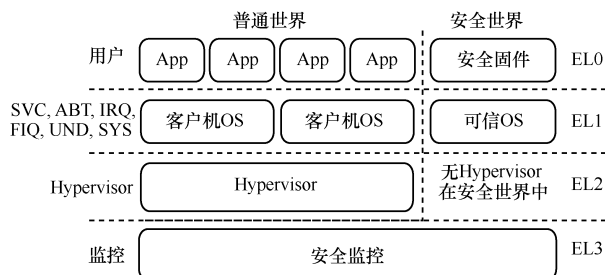


图9 ARM 虚拟化扩展

目前，在移动终端领域的虚拟化产品主要有 VMware MVP、Red Bend vLogix、OKL4 Microvisor 等，大部分采用的是半虚拟化技术，Green Hills 的 INTEGRITY Multivisor 在支持虚拟化扩展的硬件上实现了全虚拟化^[6]，如图 10 所示。

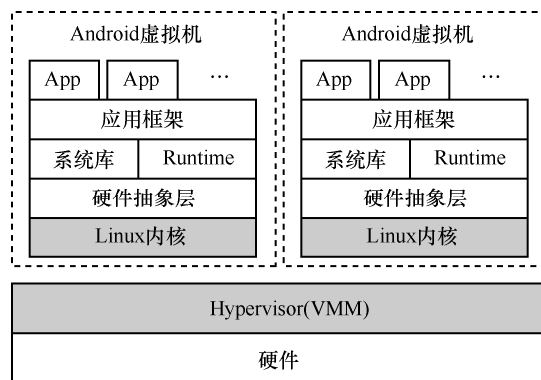


图10 Android 平台虚拟化

(2) 操作系统虚拟化

操作系统虚拟化是对操作系统本身进行虚拟化，而不是平台，如图 11 所示。在这种方式下，操作系统提供一组用户空间彼此隔离，而应用被限制在每个用户空间里面。同一个操作系统内核上运行多个实例，提供多个相互隔离的用户态实例、独立的文件系统、网络系统设置和库函数等。

操作系统级虚拟化技术是一种轻量级的虚拟化手段，虚拟机与宿主机使用同一个内核，不需要指令模拟或任何解释机制，避免了平台虚拟化和系统调用替换中的复杂性，虚拟化资源的性能开销小，在隔离的同时还提供共享机制，以实现容器与宿主机的资源共享，因此具

有高效的优点。但要求虚拟机系统与宿主机内核相同，且需要进行修改，用户态实例间的隔离性也不如平台虚拟化。

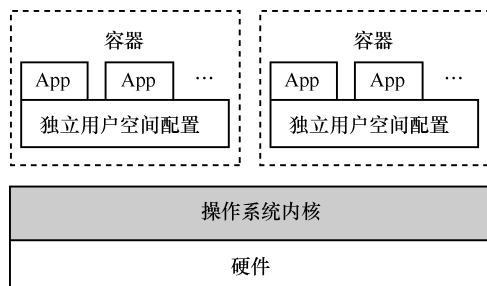


图 11 操作系统虚拟化

由于系统需要修改，操作系统虚拟化主要针对开源的 Android 系统，在 Linux 内核层面实现，通常是利用 LXC（Linux container）、namespace（命名空间）等内核技术创造多个互相隔离的进程环境，在隔离的环境分别运行服务和 App，并通过改造 HAL 和服务以公用硬件资源实现必要的 namespace 间通信。如开源项目 L4Android，可在同一个 Linux 内核上，同时运行多个 Android 实例，如图 12 所示。

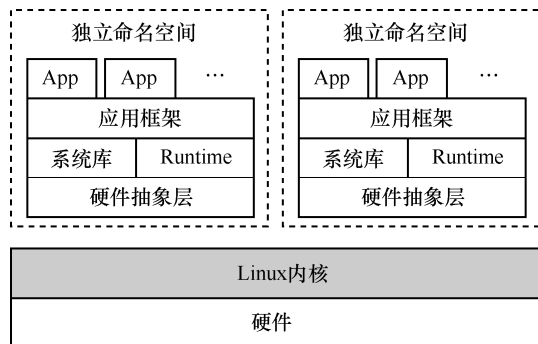


图 12 Android 操作系统虚拟化

该技术对 App 兼容性高，不需要移植，且应用隔离和资源共用可以调整，对硬件也无特殊要求。主要的缺点是针对不同硬件和 Android 发行版仍需部分系统移植，包括 HAL 的资源共享和调度等。

3.3 应用层虚拟化

应用层虚拟化是针对应用程序实施安全隔

离，包括安全沙箱、编程语言虚拟化等技术以及借助于云端实现的应用程序虚拟化。

（1）安全沙箱

安全沙箱作为一个独立的逻辑存储空间，将设备上的不同应用和存储区域划分开，限制各方数据的互相通信，从而加固重要应用的数据安全性，成为保护系统安全的有效方法，能防止未认证或不受信任的程序威胁。

Android 沙箱针对 Android App 的安全封装，为 App 提供或替换 API，提供互相隔离的服务，实现原理如图 13 所示。

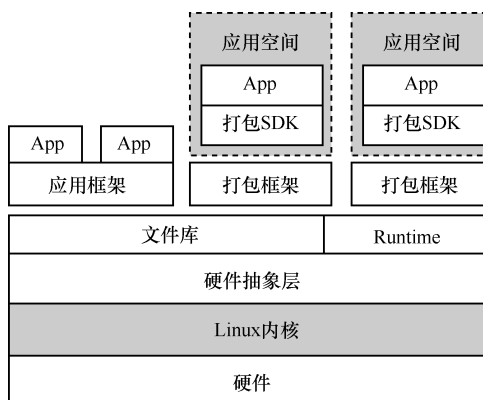


图 13 Android 应用容器

相对于平台及操作系统虚拟化，安全沙箱对操作系统要求低、无特殊硬件要求，属轻量级的虚拟化技术，缺点是存在大量共用的服务和资源、App 需改造或重新打包可能对 App 兼容性造成影响，安全性不如平台及操作系统虚拟化。

安全沙箱为移动信息化中企业应用和数据安全管理与保护提供了轻量级的安全防护方案，安全厂商通常基于安全沙箱的应用容器，为企业用户提供包括远程安全管理、终端安全运行结合的解决方案，如 MobileIron MDM。此外，安全沙箱也是实现应用加固的一种常用手段。

（2）高级语言虚拟化

高级语言虚拟化，主要思想是在应用层次上创建一个和其他类型虚拟机方式类似的虚拟机，并支持一种新的自定义的指令集（Java 中



的字节码），运行时由支持系统翻译为硬件上的机器语言再执行。这种抽象层次的虚拟化主要代表有 JVM 虚拟机。在 Android 系统中，先后采用了 Dalvik 和 ART 虚拟机，是其主要安全机制之一，每个虚拟机作为一个独立的 Linux 进程执行，可以防止在虚拟机崩溃的时候所有程序都被关闭。

3.4 云端实现的虚拟化技术

(1) 应用程序虚拟化

应用程序虚拟化包含远程应用程序和流化应用程序两种方式。

远程应用程序（也称为会话虚拟化），运行在远程服务器上，而不是客户端设备上。技术原理是基于应用/服务器（A/S）计算架构，采用类似虚拟终端的技术，把应用程序的人机交互逻辑与计算逻辑隔离开来。在用户访问一个服务器虚拟化后的应用时，用户计算机只需要把人机交互逻辑传送到服务器端，服务器端为用户开设独立的会话空间，应用程序的计算逻辑在这个会话空间中运行，把变化后的人机交互逻辑传送给客户端，并且在客户端相应设备展示出来，从而使用户获得如同运行本地应用程序一样的访问感受。

流化应用程序，将应用程序与操作系统解耦合，为应用程序提供了一个虚拟的运行环境。在这个环境中，不仅包括应用程序的可执行文件，还包括它所需要的运行时环境，应用程序的执行

由该虚拟化层控制，可以在本机上只运行部分已下载的组件，以便在无网络连接的情况下继续使用。应用虚拟化是把应用对底层的系统和硬件的依赖抽象出来，可以解决版本不兼容的问题。同时，与底层操作系统和其他应用程序隔离，其独立的计算环境可规避底层系统及其他应用的安全问题，如图 14 所示。

(2) 桌面虚拟化

桌面虚拟化是指将计算机的终端系统（也称为桌面）进行虚拟化，以实现桌面使用的安全性和灵活性。可以通过任何设备，在任何地点、任何时间通过网络访问属于个人的桌面系统。桌面虚拟化依赖于服务器虚拟化，在数据中心的服务器上进行服务器虚拟化，生成大量的独立的桌面操作系统（虚拟机或虚拟桌面），同时根据专有的虚拟桌面协议发送给终端设备。

桌面虚拟化实现桌面应用及其运行环境的模拟与分发，可以跨平台访问，通过该技术，Android、iOS 等智能终端可以访问基于 Windows 的传统办公环境。

(3) 虚拟移动设施

虚拟移动基础架构（virtual mobile infrastructure, VMI）是在云端服务器上创建 Android 虚拟机，用户手机通过网络连接虚拟服务器来实现移动桌面传输及操控，类似 Android 远程桌面。通过使用客户端程序，用户可以获取企业定制化的移动应用程序和数据，由于应用及数据都不离

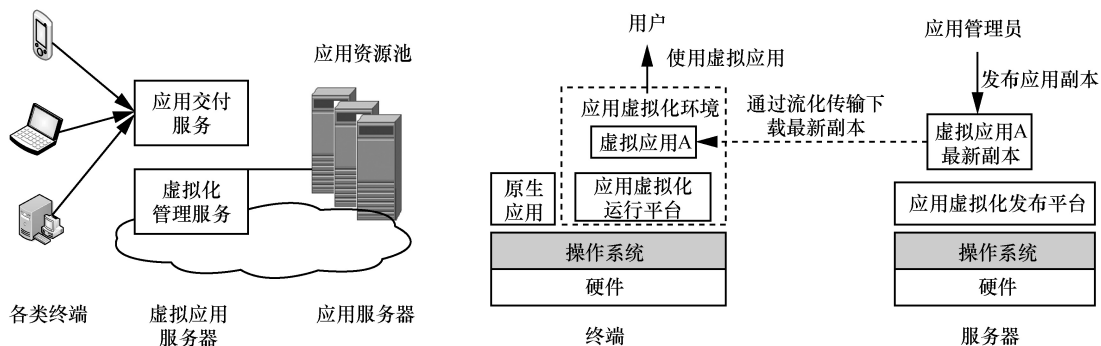


图 14 远程应用程序与流化应用程序

开数据中心,从而确保数据的高度安全性及管理的便利。

目前推出基于VMI的移动信息化产品的厂商有不少,如Raytheon、Nubo、Hypori、Virtual公司(被Citrix收购)、亚信安全、趋势科技、中兴网信等。Nubo VMI架构如图15所示。

云端虚拟化技术主要面向BYOD等企业移动信息化场景,由于应用和数据在云端统一部署,简化了应用发布、更新、安全策略统一管理。同时,由于应用运行在云端,手机端只是展示画面,网络传输的只是一些图元绘制命令,因此在网络传输和移动终端基本不涉及业务数据,安全性非常高。此外在设备兼容性、用户个人隐私保护方

面具有明显优势,无需对用户的移动设备进行严格管控,对移动操作系统也没有特别依赖,完全兼容主流的Android、iOS设备。

除VMI外,云端实现的虚拟化技术,都是在已有的PC、服务器虚拟化技术上向移动智能终端的扩展,如VMware的View和ThinApp、Citrix的XenApp和XenDesktop,支持包括PC、平板电脑、手机等在内的多种主流终端,实现移动办公的全面支持。

4 智能终端虚拟化技术比较

4.1 智能终端虚拟化技术对比

表1是对智能终端虚拟化技术的特点、典型技术/产品以及优缺点的简要对比分析。

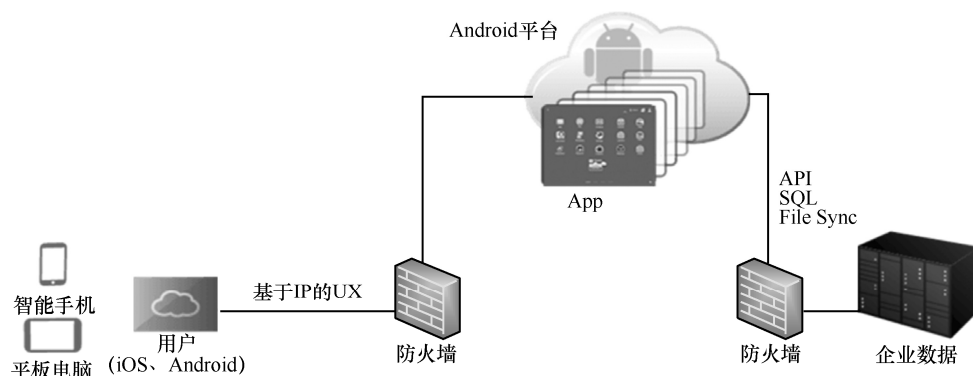


图15 Nubo VMI架构示意

表1 智能终端虚拟化技术对比

类型	特点	典型技术/产品	优点	缺点
终端侧	基于硬件隔离	TrustZone、SIM/UIM/USIM 等 智能卡	TEE	实现应用安全隔离; 需终端支持, 定制或出厂支持;
	系统平台虚拟化	Hypervisor+多内核	VMware MVP、OKL4、Red Bend/VLX、Citrix/Xen	技术门槛高;
	操作系统虚拟化	内核+多用户空间	Android container、L4Android	未标准化(除 TEE), 不同厂商技术难以互通
	应用安全沙箱	独立运行环境、数据隔离	MobileIron、McAfee 安全容器	难以防范内核攻击
平台侧	编程语言虚拟化	Runtime+中间指令	Dalvik、ART	系统、支持范围广
	应用程序虚拟化	运行环境+应用进程	VMware ThinApp、Citrix XenApp	
	虚拟移动设施	云端运行	Nubo	需平台支持
	桌面虚拟化	云端运行	VMware View、Citrix XenDesktop	



4.2 终端虚拟化与服务器虚拟化技术对比

移动终端虚拟化是在服务器虚拟化技术的基础上发展，两者都由软件实现硬件资源的虚拟化，在一台智能设备上同时运行多个不同的操作系统，因此，两者对系统的隔离性、安全性具有相同的要求，相应的，由于系统共存、资源复用，两者都面临跨虚拟机攻击等各类安全问题。

另一方面，移动终端虚拟化与服务器虚拟化也存在较大的差异，比如服务器虚拟化存在多租户的特点，虚拟机动态创建、使用和回收资源，为支持其运营，需由管理员对虚拟机镜像、资源等进行管理；而移动终端具有个人化的特点，系统出厂时统一安装，多虚拟机一般仅供个人使用，通常是一个运行普通系统的虚拟机，另一个为特定应用使用的专用虚拟机。系统使用、管理上的不同，使两者面临不尽相同的安全风险，

见表 2。

5 结束语

采用虚拟化技术在终端中隔离多个运行环境是解决移动安全问题的一个有效手段，业界发展出来的多种技术为解决不同场景的安全问题提供了灵活的选择，同时，这些技术也与其他安全技术融合发展，如指纹/人脸识别、MDM、MAM，满足个人、企业应用安全的不同需求。

参考文献：

- [1] 中国互联网信息中心. 第 40 次《中国互联网络发展状况统计报告》[R/OL].(2017-08-04) [2017-10-20]. <http://www.cac.gov.cn/2017-081041c-112142278.htm>. CNNIC. Fortieth statistical report on the development of china internet network[R/OL].(2017-08-04) [2017-10-20]. <http://www.cac.gov.cn/2017-081041c-112142278.htm>.
- [2] 360 互联网安全中心.《2017 年中国手机安全风险报告》

表 2 服务器虚拟化与移动终端虚拟化对比

	服务器虚拟化	移动终端虚拟化	对安全的影响/差异
使用目的	资源复用为主	安全隔离为主	为增强安全隔离效果，可部分牺牲资源使用效率
使用场景	多用户、多系统；对外提供服务	个人化、双/多系统	移动终端使用者、场景固定，双/多系统安全需求存在差异，可根据使用场景进行资源分配、安全增强；可用性要求相对低
设备及虚拟机管理	内部管理员统一管理，可获取虚拟机快照、绕过虚拟机安全防护机制	一般不提供对虚拟机文件管理；提供系统更新、设备调试等管理接口	服务器虚拟机文件备份、恢复存在数据泄露、篡改甚至镜像文件替换的风险，需采取机制防范管理风险；移动终端虚拟化存在远程升级、终端调试风险
虚拟机使用	动态创建、使用和回收	虚拟机固定安装	服务器虚拟化中，攻击者可通过在同一物理机上新建虚拟机实施各类攻击，如侧信道攻击；移动终端不能新建虚拟机，但仍可能通过其中一台虚拟机攻击另一台
虚拟机通信	作为服务器，具有强通信需求	仅作为通信客户端；虚拟机间一般不需建立网络连接	移动终端虚拟化层的通信隔离相对简单
硬件设备	支持 x86、x86_64、IA64、PowerPC、MIPS 以及 ARM 等架构	ARM 架构	安全特性受硬件架构的影响；移动虚拟化可利用 ARM TrustZone 技术增强安全性
	服务器与存储系统间存在多种连接关系；存储设备隔离问题复杂	单一终端共用存储，采用 FAT 格式的外部存储设备存在隔离问题	移动终端可针对应用场景进行存储设备的隔离，普通应用场景的安全性不降低
操作系统	支持 Windows、UNIX/Linux 等主流操作系统	目前主要支持 Linux 内核/Android 系统	操作系统虚拟化可针对 Android 系统安全机制进行优化

[R/OL]. (2017-05-12) [2017-10-20]. <http://bbs.360.cn/thread-14972358-1-1.html>.

360 Internet Security Center. 2017 China mobile phone safety risk report[R/OL]. (2017-05-12) [2017-10-20]. <http://bbs.360.cn/thread-14972358-1-1.html>.

- [3] 全球平台. Global Platform 卡片规范[S/OL]. (2017-04-10) [2017-10-20]. <http://www.globalplatform.org/specificationscard.asp>. Global Platform. Global Platform card specification[S/OL]. (2017-04-10)[2017-10-20]. <http://www.globalplatform.org/specificationscard.asp>.
- [4] Security on ARM Trustzone. SoC and CPU system-wide approach to security [EB/OL]. (2017-02-10) [2017-10-20]. <http://www.arm.com/products/security-on-arm/trustzone>.
- [5] Security in an ARMv8 System V1.0[EB/OL]. (2017-03-17) [2017-10-20]. https://static.docs.arm.com/100935/0100/security_in_an_armv8_system_100935_0100_en.pdf.
- [6] INTEGRITY Multivisor. Virtualization architecture for secure systems[EB/OL]. (2017-10-02) [2017-11-20]. https://www.ghs.com/products/rtos/integrity_virtualization.html.

[作者简介]



黄勇军 (1970–), 男, 中国电信股份有限公司广州研究院副院长、高级工程师, 国务院特殊津贴专家, 长期从事通信网络发展规划、新技术应用研究等工作, 主要研究方向为 IP 网技术、云计算和网络安全。



金华敏 (1972–), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为 IP 网、云计算、大数据安全和网络安全。



刘国荣 (1978–), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为移动互联网安全和云计算安全。

刘东鑫 (1985–), 男, 中国电信股份有限公司广州研究院工程师, 曾获得 CCIE、CISSP 和 CISA 等认证。主要研究方向为网络与信息安全、大数据安全。

汪来富 (1976–), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向 IP 网、云计算、大数据安全和网络安全。

沈军 (1976–), 女, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为云计算安全、移动互联网安全及 SDN/NFV 安全等。