

技术白皮书

SecureIT Mobile

利用移动虚拟化和其他商业成品技术，构建一款更加安全的智能手机

针对安全应用和安全通信

Rob McCammon
产品管理 副总裁
Open Kernel Labs

2010年9月

内容

简介	3
谁应该阅读本白皮书	3
安全通信领域的新兴需求.....	4
移动安全威胁	4
需求.....	5
安全移动通信	7
架构选择.....	7
虚拟架构	8
概念验证和SecureIT Mobile.....	9
安全目标	9
安全语音.....	9
安全SMS.....	12
结论.....	14
OK Labs SecureIT Mobile.....	14

简介

在公共安全和国家安全领域，员工工作的移动性通常高于公共服务和私营企业领域。无论是警察、消防员、其他救援人员，还是情报组织成员和武装力量，依靠高度专业化的安全通信设备是避免不了的。他们需要这些设备来履行职责，完成使命。

一般来说，安全通信设备包括模拟和数字射频组合，以及其他专用设备。现在，安全通信家族接纳了越来越多的定制无线设备，这些设备在民用领域扮演了移动终端的角色。然而，在满足安全性和耐用性特殊需求的同时，这些设备很难承受高额的开发和制造成本、严格的互操作性要求，以及有限的升级渠道。

在90年代初期，美国军队和在美国乃至全球的其他部门发布了一系列的“COTS举措”，旨在利用民用商业成品（COTS）技术和产品，控制制造和维护的成本。不同的“COTS举措”针对不同资产，并且涉及了零部件、电脑到航空母舰。

针对这些举措的精髓和应对新的需求，本份白皮书探讨了如何利用 COTS 硬件和软件来执行和部署安全移动通信设备。特别需要指出的是，其重点在于集成。

- 大量生产的智能手机
- 加密硬件
- 应用层移动操作系统
- 移动虚拟化方案

以上是OK Labs *SecureIT Mobile*实现的目标。

谁应该阅读本白皮书

本文主要针对移动/无线生态系统和政府IT及电子领域。同时，涉及的话题包括利用现有硬件和软件构建安全移动设备。适合阅读本文的人士包括：

- 移动设备OEM厂商和芯片供应商
- 政府承包商中的无线安全集成人员
- 市级、州级和联邦政府首席信息官（CIO）和IT架构师
- 公共安全和国家安全部门的IT管理人员

安全通信领域的新兴需求

曾几何时, 无论从现实还是理论角度而言, 移动电话都非常类似于它的前辈有线电话 —— 不过是语音通信设备而已。此外, 用户对安全通信的期望主要集中在物理安全和网络可靠性方面。而今天, 移动设备代表的是整合的数字服务, 包括语音、数据通信和应用托管。

由于这些设备性能较高, 终端用户和他们所在的企业把移动计算视为关键业务及关键任务。无线设备帮助移动工作者涉足商业、政府和公共服务活动, 执行了一系列现场任务。此外, 同样这些设备还满足了广泛的个人需求, 包括娱乐及个人理财。

期间最大的变化, 就是这些受益群体都直接或间接的表示, 希望移动设备安全传输数据, 托管服务和应用。

移动安全威胁

由于移动设备越来越接近桌面电脑和数据中心电脑, 这些设备有了同样的弊端, 公司和政府IT部门也因此苦不堪言:

- 这些设备容易遭受病毒、木马和其他恶意软件的攻击
- 支持这些设备的应用代码库和中间件不仅体积庞大, 而且不可靠也不合格。
- 运行在这些设备上的移动操作系统(OSes)和软件注定存在诸多缺陷, 也因此容易遭受频繁的零时差攻击。
- 无论对于开放操作系统, 开放源操作系统(安卓, Linux, 塞班等)而言, 还是对于在这些系统上运行的应用来说, 对质量和灵敏度截然不同的社区开发正在显现 —— 尤其是那些重视安全性的领域。
- 在智能手机上运行的移动应用, 包括通信客户端, 都容易遭受一系列的“野蛮”攻击, 尤其是针对每个进程和系统级DoS攻击。

政府机构和其他公务人员的主要顾虑包括:

- 攻击导致语音、文本信息和其他数据的泄漏, 及其他未经授权的第三方监查行为。
- 未经许可的一方干扰关键业务通信, 欺骗或伪造参与者身份及内容。

需求

对安全移动通信的需求体现在诸多方面。在美国，国土安全局和其他政府机构对IT安全性和机密性有严格要求，世界其他政府和民营机构也有着相似或是更高的移动计算安全及认证需求。

一款安全的移动通信设备

一款高标准的安全设备应该是：

- 基于标准、成品移动终端 — 商业成品iPhone, 黑莓或Droid-设备（且非专用设备）
- 尽可能的部署现成平台和应用级软件(安卓, Linux, 塞班等)
- 支持常规通信和应用，满足低安全标准应用（例如个人通信、社交网络等）
- 在功能相似设备和/或兼容设备之间营造一种或多种安全通信环境（例如客户间通话，和/或访问数据中心的关键信息）。

现实和理想中的个案

在现实生活中，类似的设备是“奥巴马黑莓”，一款RIM黑莓手机，经过了最少的技术改良，却可以让美国总统在美国特勤特甚至可能是国家安全局的允许下，使用自己熟悉的设备进行安全办公通信¹。

在美国福克斯电视台播放的“24小时”²美剧，一种虚构的安全移动通信手段备受世人的瞩目。男主角Jack Bauer和他的反恐组织就是依靠成品安全移动设备，传达关键任务信息和行动指令。

1 了解“奥巴马黑莓”详情请登陆 <http://www.crunchgear.com/2009/01/16/obama-to-keep-hisblackberry/>

2 美剧“24小时”官方网站 <http://www.fox.com/24/>

关键需求

最后，主要应用场景都要汇总到以下简单而又很难实现的需求陈述里：

基于开放软件的成品移动设备，在开放网络上实现安全通信

让我们来进一步研究每个需求细节：

安全通信

“安全通信”是指常规应用——3G语音、VoIP、SMS、MMS和视频等，在这些应用上，客户端可以在安全环境下运行，并且可以对数据流进行加密。

开放网络

使用COTS硬件和软件，还意味着利用普遍的3G、WiFi和其他公共网络来实现个人安全通信。随着GPRS, CDMA, 802.11等给出了各自的安全定义，本白皮书假设的条件是：单凭这些措施无法满足安全合格的系统需求。

成品设备

本白皮书中安全通信的目标基于COTS硬件，但内容不一定与通过传统运营商和零售商渠道获得的大众市场手机相关。安全通信设备是以下多方共同协作的结果：

- 手机制造商
- 第三方集成商和/或政府承包商
- 售后硬件加密设备（SD卡等）供应商，和/或加密软件的供应商，这种加密软件专指在移动芯片上独立运行或利用现有功能的软件。

另一个必要条件，是这些技术的集成必须针对维护和升级提供可行的方案，并且避免传统定制硬件软件的昂贵锁定限制。

开放软件

对于适合执行安全通信任务的智能手机和其他设备而言，安卓, Linux,等开放系统和/或开放源操作系统呈现出了越来越大的吸引力。因此，一款安全通信方案不会试图取代这些软件平台，相反，则会利用安全合格的软件，提升、完善和提炼这些平台。

安全移动通信

架构选择

尽管本白皮书强调了安全移动通信的COTS方法, 在研究一些候选架构时, 白皮书也探讨了安全通信面临的挑战:

单点方案

虽然移动安全需求是一种普遍和系统级的要求, 但是安全移动通信方法依然倾向于单点方案。这样的单点方案一般都需要构建和部署安全和/或合格的应用、中间件和加密数据流, 以及专门的通信渠道。虽然限定范围有利于设计和工程, 但对于更接近于桌面电脑而非手持射频装置的现代移动/无线设备来说, 效果并不是很理想。不幸的是, 通过破坏一个已保存的或是运行中的应用镜像, 或是阻断这些应用的计算资源(DoS), 这些单点方案会在应用层受到一定的损失。

专用硬件

隔离软件最有效最安全的途径是在硬件的不同区域运行程序。一些移动芯片通过独有的协处理器, 加速图像、视频、音频, 有时甚至负责加密。然而, 这些专用的协处理器作为从属外围设备配置, 不提供足够的环境来运行整个通信栈和语音、信息客户端。理论上来说, 虽然在SD卡和其他来自二级市场的接口可以集成更多有效资源, 但在不额外更改COTS操作系统和程序栈的情况下, 通过其他非安全设备, 则无法保证发送和接收安全数据流。

多核架构

这一代高端手机和下一代设计越来越倾向于在多核应用处理器上集成两个或者更多的 ARM 处理器内核。理论上来说, 一个(或者更多的)核可专门用于安全移动通信, 提供与开放操作系统和开放应用环境的强大隔离能力。

在大多数情况下, 集成商甚至是 OEM 厂商会强制释放一个完整的 CPU 内核用于安全移动通信处理, 这样就会影响到设备整体的性能。此外, 即使有专用的 CPU 内核运行安全通信调用, 共享的物理内存还是容易遭受开放应用 OS 上运行的内容核带来的攻击。

虚拟架构

构建安全移动平台的最全面且直接的方法就是引入移动虚拟化技术。移动虚拟化与其在数据中心的服务器虚拟化兄弟一样，都是运行在“纯硬件”芯片上，管理一个开放式应用 OS 和软件栈，利用一个或更多隔离的安全区域（虚拟机）在不同的环境里驻留安全软件，利用其他区域（按需）来保存设备驱动等选择性共享资源。

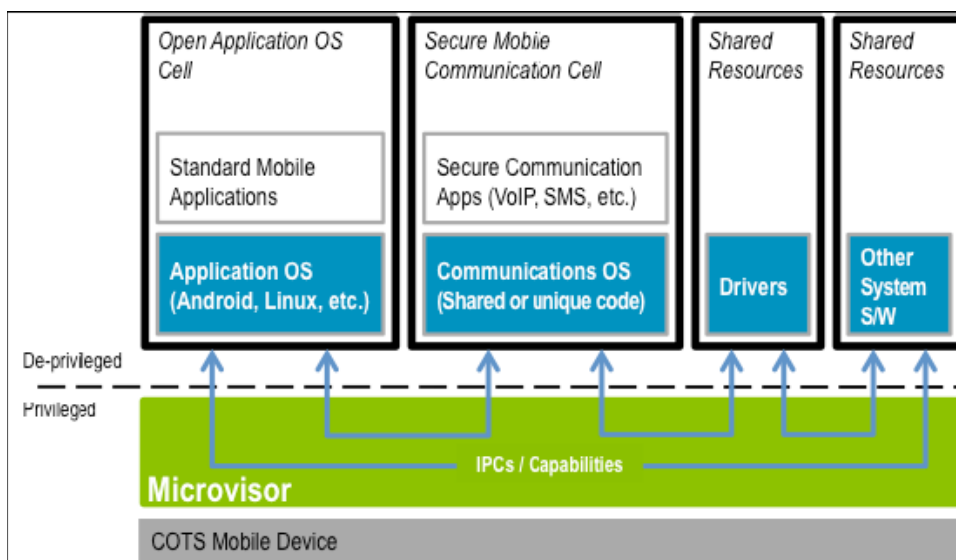


图1 —— 采用microvisor的Secure移动通信理论架构

这一架构的优势在于：

- 可信计算库的占用空间小（只有底层microvisor），便于认证，减少攻击频率
- 部署在相互独立区域里的现有成品开放操作系统和软件栈不需要进行部署调整
- 为了满足某个安全体系和其对应的支持技术特殊需求时，集成商可以灵活地增加新的区域
- 基于性能的安全性提供了充分灵活的动态保护管理，包括动态授权。
- 抵制恶意软件，通过隔离和使用受限的区域间通信(IPC) API，保证各区域的安全 —— 透明的开放操作系统即使遭受攻击失去作用，其他区域的安全通信软件也不会受到影响。
- 针对高性能操作的进程间高速通信（IPC）体系
- 通过在不同区域监控、排列优先级和平衡负担，抵御DoS攻击

概念验证和SecureIT Mobile

为了说明安全移动通信, OK Labs公司设计了两个概念验证(PoC)系统, 这两个系统的基础都是现成的硬件和软件。这些PoC并不是纯粹的概念 —— 而是复制了由一家主流手机OEM厂商针对安全语音, 以及另一家认证软件供应商³针对安全SMS而构建的相关配置。

这些概念验证都是基于OK Labs公司的安全移动通信方案, SecureIT Mobile来构建。

安全目标

两个概念验证体系和现实应用设备有着同样的安全目标:

- **隔离:** 安全软件必须完全独立于非可信开放操作系统和软件。非可信操作系统和软件栈即使遭受攻击, 也不能访问敏感数据和安全移动软件。
- **相互独立:** 非可信操作系统和安全移动环境之间必须做到互不依赖
- **TCB空间最小:** 为了使可信度最大化, 安全移动软件的可信计算基础必须在容量和范围上达到最小
- **不可伪造:** 必须有针对安全移动通信软件的运行状态进行安全鉴定的方法, 例如安全通话或文本对话正在进行或者可以开始进行的显示。

安全语音

PoC与配备相似的设备建立了安全的VoIP联系

硬件描述

普遍开放的移动电话硬件通常不容易获取。因此, 安全语音PoC使用的是流行、开放、低成本, 并拥有以下特征的BeagleBoard

CPU	OMAP3530 (ARM Cortex-A8 单核) @ 600 MHz
内存	256 MiB DRAM, 256 MiB NAND Flash
网络	基于Ethernet Moschip的 10/100 Ethernet Dongle
外围设备	USB 键盘, 鼠标. 扬声器. 麦克风. DVI 外部显示

图 2. —— 安全语音 PoC 硬件描述

³ OK Labs公司合作伙伴, Sirrix AG 安全技术公司

安全区域架构

如图3显示，安全语音PoC中有六个不同的OKL4 Microvisor安全域（虚拟机），驻留专用和共享的功能组合，并且通过使用对应的IPCs进行互相连接：

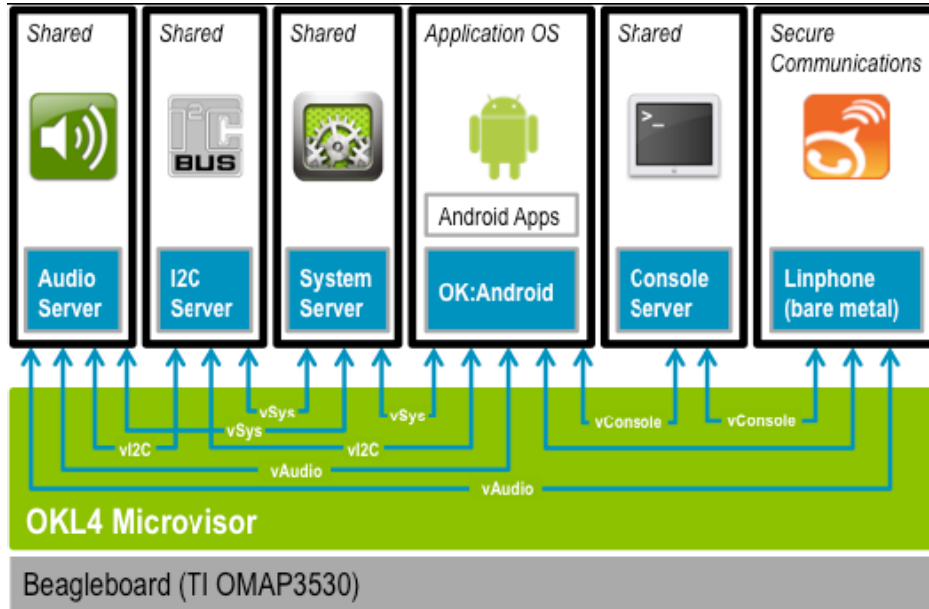


图 3 —— 安全语音 PoC 架构

音频服务器域	音频服务器通过在轻量虚拟机上运行，通过输出两个虚拟音频设备，实现了音频编解码器的安全共享。在概念验证里，只有一个虚拟音频设备在发挥功能，并且是用于Android平台运行下的安全音频或应用音频。
I2C服务器域	OMAP3530 I2C 总线用于连接多个BeagleBoard外围设备，包括带有USB物理层接口（PHY）和音频编解码器的多功能设备。为了确保Android平台和安全区域之间的隔离，PoC采用了一款I2C服务器
系统服务器域	系统服务器管理不同区域需要的时钟、电源管理和其他系统设备。通过输出一个低端应用程序接口（API），系统服务器实现了对这些设备的同步访问
应用OS域	该区域托管终端用户可见的Android操作系统。OK:Android为半虚拟化产品，负责大部分外围设备的本地运行
控制台服务器域	为了向Android平台和安全区域提供调试和命令行控制，控制台服务器对一个UART进行复用
安全通信域	该安全域上托管有Linphone VoIP客户端，以及OKL4上本地化运行的有关数据库（通过使用OK:RTX0 APIs）。此外，该区域还包括一个虚拟的以太驱动器和一个轻量级TCP/IP协议栈。

分析

安全语音概念验证涉及:

- OKL4 Microvisor负责启动系统, 调用和启动这六个安全域(客户虚拟机)
- 主要的移动操作系统(OK:Android)启动和运行的方式和在一般Android手机上的方式一样, 用户可以进行语音通话、运行应用程序等
- 在一个实际的手机或类似设备里, Android应用至少包含一个安全通信客户端, 用于安全VoIP和SMS等系统的启动。就PoC而言, Linphone命令行实现了IP语音的安全通信
- 在运行Linphone时, 音频编解码器专门为安全移动通信提供语音输入/输出。在完成安全VoIP通话时, 编解码器会自动让位给常规Android应用。
- 以太网TCP/IP实现了VoIP通信。通过使用标准Linux网络, 网络连接任务是在Android平台上执行, 并共享/桥接到安全域上。

安全和性能考虑

加密

PoC并不涵盖加密, 也不会保障IP语音流的安全。在这样的设计中, 确保VoIP和其他通信流安全的是SD卡和软件上的现成旁路加密硬件。

针对Android平台的攻击

Android平台上的应用很容易引发DoS或其他攻击。针对这一点, OKL4优先级和负荷平衡能力可以减少DoS攻击的影响, 并且严格的数据隔离和受限的IPCs会阻止其他攻击。通过限制DMA访问物理内存的范围, 使用OMAP“防火墙”可以巩固这一隔离。

系统和网络性能

OK Labs正在努力通过OKL4移动虚拟化使成本降到最低。Netperf benchmark的研究结果表明, 在某些情况下, 通过半虚拟化的Android平台和抽象的TCP/IP处理, OKL4可以提高PoC3-5%的网络吞吐量, 降低CPU使用率高达8%。

安全SMS

本概念验证将加密的SMS信息与相类似的设备进行交换

硬件描述

CPU	OMAP3430 (ARM Cortex A8 单核) @ 600 MHz
	Cache L1 32KiB 数据/ 32 KiB 指令
内存	256 MiB DRAM, 32 GiB NAND Flash
网络	GPRS/GSM, 802.11b/g
外围设备	键盘, 触摸屏, USB, 蓝牙

图4. – 安全 SMS PoC硬件描述

安全域架构

如下图5显示， SMS PoC里的OKL4安全域只有两个主虚拟机，因此，其架构和配置比安全语音PoC的更为简洁和小巧：



图5 —— 安全 SMS 架构和诺基亚N900上的SMS客户端截图

应用 OS域 该区域托管着用户可见的Linux OS（OK:Linux上的Maemo）。OK: Linux 为半虚拟化产品，负责大部分外围设备的本地化运行

安全并且通信域 该安全域运行安全的SMS客户端。当执行操作时，SMS客户端接管显示器和键盘，在应用OS管理的GPRS调制解调器上，利用OKL4 IPCs发送加密SMS信息。

分析

安全移动 SMS 概念验证涉及

- 如图5所示, OKL4 Microvisor负责启动系统, 调用和启动这两个安全域(客户虚拟机)
- 应用OS(Maemo Linux)的启动运行方式和在Nokia N900原型机上的方式一样, 用户可以进行语音通话, 运行应用程序等。
- 利用本地Linux应用启动安全SMS功能, 本地Linux应用在安全域里负责启动文本向执行代码转换的功能
- 安全SMS客户端掩饰了自己的用户界面(UI), 在执行和输入驱动器任务时接管了键盘和触摸屏。在一个产品设备中, 用安全域运行共享的帧缓存和输入驱动器, 或者在自己的安全域里运行一个小型X11服务器, 都是更好的方式。
- 在PoC 里, 通过使用一个安全OKL4 IPC, SMS 客户端和应用OS可以共享GPRS调制调解器。其他可行的方法还包括直接运行GPRS调制调解器, 或利用一个安全域运行一个调制调解器服务器
- 当安全SMS程序运行时, 在Nokia N900上的LED指示灯会从红色变为绿色, 表明现在“处于安全通话中”(该设置无法伪造)

结论

这两个概念验证说明, PoC并不仅仅是构架上的空中楼阁。现在, OEM厂商和其合作伙伴基于移动虚拟化, 以及成品移动硬件和软件, 已经开始着手进行原型设计、开发和部署应用于现实生活的安全移动设备。

OK Labs SecureIT Mobile

为了帮助OEM厂商和集成商更快更有效的把安全设备投入市场, OK Labs公司已经设计出了 *SecureIT Mobile*, 一款配备以下设置的工具包和方案:

- [OKL4 Microvisor](#)
- [OK:Android](#), 一款现成的半虚拟化Android平台
- 样品驱动器和通信代码
- 用于集成和定制的服务

请通过电话+1 312 924 1445或邮箱info@ok-labs.com了解详情