MTAA

Mobile Terminals Assurance Architecture

安自心 简随行

基于MTAA的移动安全解决方案白皮书

腾讯移动安全实验室

Tencent Mobile Security Labs

目录

第一章：摘要

随着互联网与移动通信技术的飞速发展，二者的进一步融合，以往存在于互联网中的病毒传播、网络攻击等各类不同级别的安全事件已开始向移动网络中转移，移动网络从核心交换到终端设备，都面临着前所未有的压力和挑战。特别是近年来伴随着iPhone、Android等智能手机系统平台的崛起，一系列安全问题也随之出现，移动信息安全形势不容乐观。

同时，伴随着移动终端的多样性发展和智能化演进，终端上所承载的各类应用、特别是高端商务应用业已成为移动运营商新的收入来源和核心业务增长点，如手机网上支付、电子商务、基于位置的服务等富有特色的一系列增值服务，这将极大地激发运营商、终端厂商、增值服务提供商对终端安全保障体系的关注和投入，移动终端安全已成为新的产业链。

腾讯公司作为中国最大的互联网综合服务与增值应用提供商，从用户、行业的业务需求出发，凭借多年服务海量用户而积累的丰富经验，致力于打造互联网、特别是移动互联网终端的安全保障体系。腾讯终端安全架构，（Mobile Terminals Assurance Architecture, 以下简称MTAA），以及基于MTAA的腾讯移动安全实验室，就此宣告面世。

第二章：移动终端安全：行业与用户观点

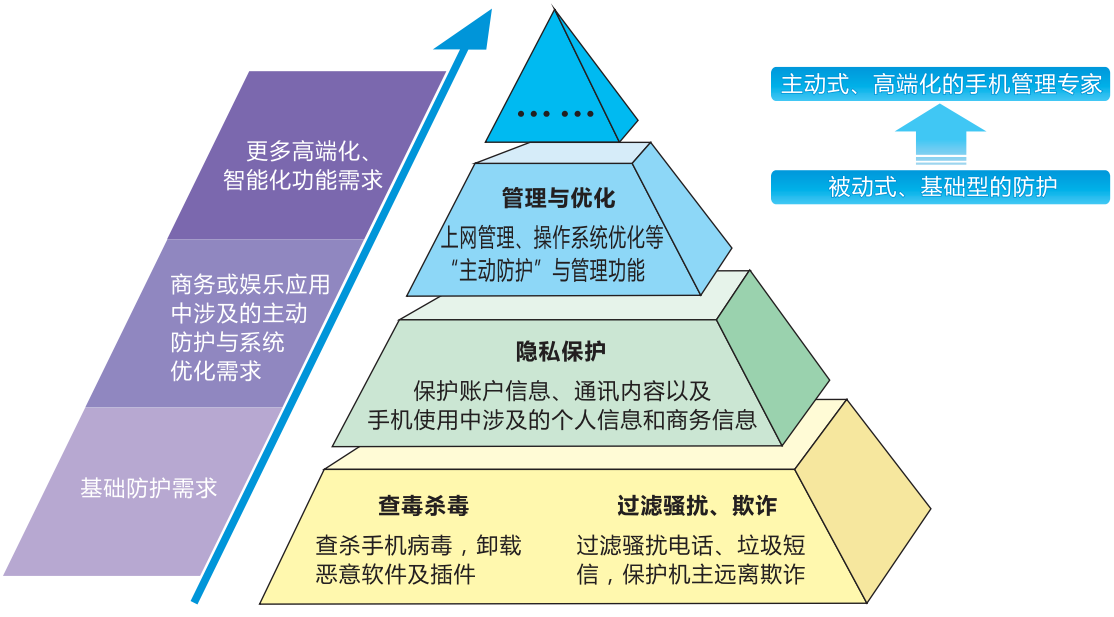
2.1 现状

国家互联网应急中心发布的《2010年互联网网络安全态势报告》指出，随着移动互联网智能终端的普及，手机恶意程序开始出现并快速蔓延。不法分子利用手机恶意程序盗取用户隐私信息，恶意订购各类增值业务或发送大量垃圾短信，危害终端用户利益和网络安全。报告指出，根据中国互联网协会反网络病毒联盟的监测数据，2010年新截获手机恶意程序1600余个，恶意程序累计感染智能终端800万部以上。其中，“毒媒”程序全年累计感染约200多万个用户手机，“手机骷髅”程序累计感染83万余个用户手机。报告同时指出，从手机操作系统平台来看，Symbian平台是手机恶意程序感染的重点对象，约有69%的恶意程序针对该平台手机，其次是J2ME平台（27%）和Android平台（3%）。

调查表明，58.8%的手机用户表示自己面临安全威胁，超过90%的手机用户遭受垃圾短信困扰，89%曾遭恶意骚扰；47%因感染手机病毒而被骗订SP业务。

2.2 行业观点

行业观点：用户对于手机安全未来需求路径



（Source: iResearch艾瑞咨询和腾讯合作调研结论）

运营商的观点认为，与电子商务相结合的手机网上支付，手机安全是首要保障，没有充分完整的手机安全保障策略，移动电子商务不会得到迅速发展。移动终端安全与PC安全策略相比较，两者既有共同点，比如两者面临的是大部分同性质的安全威胁事件；但是站在移动终端用户的立场上，对身份验证、个人隐私保护等的要求更高，技术实现难度必然更大。在网络一端，运营商可以通过强化各网络层的安全策略部署和实施，建立一个安全的体系模型，确保基础设施的安全性以及在链接、传输、与系统层面建立安全层。在此基础上通过与终端厂商和安全解决方案厂商的协同合作，达到保护应用层安全的最终目标。

业界普遍认为手机安全产品市场已经处于导入期的后期阶段，预计2012年，手机安全市场将进入高速成长期。由于智能手机用户对于手机安全产品的需求将是刚性的，智能手机用户数的飞速增长将进一步推动手机安全市场规模快速增长。预计到2014年，中国手机安全产品激活用户数将占智能手机用户数的85%，手机安全产品激活用户数将达到4.34亿。届时中国将成为世界上最大的手机安全市场。未来手机安全市场的竞争形势更加激烈，综合实力最强的手机安全厂商有望胜出。除了软件厂商外，运营商、终端厂商也开始与手机安全厂商开展合作，手机安全产业链正在形成。

2.3 终端用户观点

用户观点：被访用户对目前注重功能和未来需求的表达

1 、对于市场已有功能，用户的安全需求路径如下：

现有用户注重的功能TOP5

防骚扰电话	39.6
网络连接监控	33.8
强力卸载恶意软件	33.6
拦截垃圾短信	33.2
手机账户隐私保护	27.8

潜在用户注重的功能TOP5

手机账户隐私保护	39.6
强力卸载恶意软件	35.2
拦截垃圾短信	35.0
网络连接监控	31.7
防骚扰电话	31.5

2、 对于市场未来功能，用户的需求表达如下：

一方面，需要尽可能智能化的设置，另一方面，也要保证足够的自主空间；
一方面，要实现实时防护和及时提醒，另一方面，又要避免过于频繁的干扰。

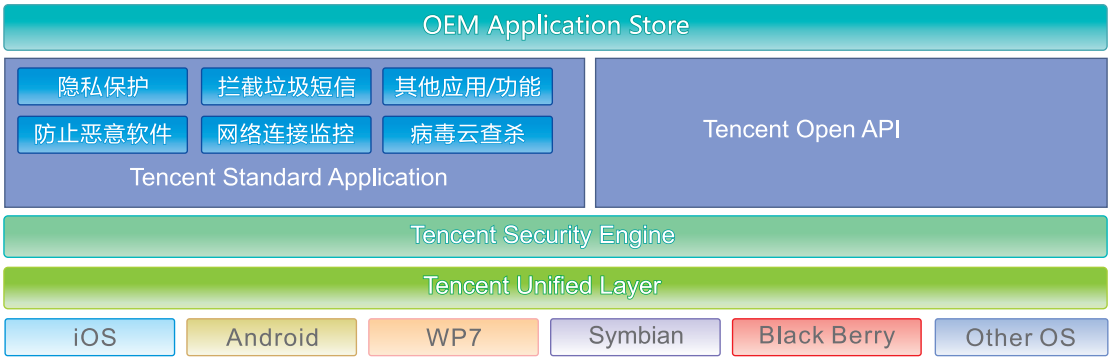
（Source: iResearch艾瑞咨询和腾讯合作调研结论）

第三章：基于腾讯移动终端安全架构（MTAA）的移动安全解决方案

3.1 目标

基于手机管家安全软件，为用户提供一站式移动终端安全解决方案服务，打造最佳用户体验；同时与运营商和广大手机厂商、软件厂商协同合作，分享最佳实践，推动整个产业链的健康发展。

3.2 MTAA的技术架构



3.2.1 Tencent Unified Layer (腾讯平台统一组件)

腾讯平台统一组件是一个中间层，负责整合所有移动操作系统（如iOS、Android、Symbian、WP7等）的差异性，向所有上层应用提供无差别的编程平台。

3.2.2 Tencent Security Engine（腾讯安全引擎）

腾讯安全引擎为所有移动安全应用，提供统一的应用程序监视、加载/释放、控制、调度等功能，并且能通过OPEN API提供给合作伙伴进行安全引擎的调用，合作伙伴不需要自己开发安全引擎，就能轻而易举地开发出专业的安全应用。

3.2.3 Tencent Standard Application （腾讯标准应用）

腾讯标准应用是腾讯在“安全引擎”基础上，向最终用户直接提供的服务，和对第三方厂商提供开发的范例。也可以允许第三方厂商在这些标准应用上直接嫁接自己的应用。

3.2.4 Tencent Open API（腾讯开发接口）

腾讯开发接口对第三方应用开放轻便易于上手的接口，合作伙伴通过标准接口，可以调用腾讯安全引擎、或者是腾讯标准应用，来开发自有的应用。

3.2.5 OEM Application Store（第三方厂商应用）

第三方厂商的应用可以在腾讯的Application Store上推广，腾讯除了与合作伙伴共享用户外，还为合作伙伴提供产品管理平台、产品展示平台、用户沟通平台。

3.3 MTAA 业务功能实现特点

3.3.1 面向多平台系统层面的高权限解决方案：

至今应用最广的智能操作平台包括Android、iOS、Symbian S60 V3、Symbian S60 V5，移动安全解决方案在系统层面优先考虑这四大智能平台。

1）Android平台深层次安全解决方案

MTAA与众多知名厂商达成深度合作，在多款手机中取得最高root权限，能在linux层，通过先进的hook和inject等技术，截获系统的大部分调用，实现主动式防御引擎，对终端实现高度融合与深层次的保护。

- 在root权限模式下，可以直接调用Android对外提供的pm命令，实现静默安装和卸载；
- 通过inject技术，把逻辑注入到在系统服务所在的进程当中，通过代理服务的方式，截获各种系统调用：
  - 代理系统的activity服务，可以监控系统各种数据库的读取，比如短信、联系人、通话记录等,同时也可以监控某个应用的开启，实现应用锁功能。
  - 代理系统的phone, sms, phoneinfo等服务，实现拨打来去电、短信收发、获取手机唯一码、地理位置等信息获取的监控；
  - 代理系统的input服务，可以在用户在输入密码和帐号时，提供实时保护。

2）Symbian平台深层次安全解决方案

MTAA直接从Nokia取得最核心和最高级的权限，通过赋予的最高权限，可以紧密地在手机的内核形成有效的保护，让手机系统最核心的部分可以免受病毒的侵扰。

MTAA可实现专业而且强悍的系统防护功能：

- 深入内核，形成系统保护层，让系统文件无法被破坏。
- 专业查杀病毒，对手机系统里的文件了如指掌，病毒无所遁形，并且使用先进的杀毒技术，粉碎病毒各种自我保护机制，使得病毒被彻底清除。
- 有效的对手机资源的访问监控。

3.3.2 “云到端”的解决方案

为了弥补终端本身的处理速度、容量等的限制，MTAA解决方案还着重开发强大解决能力的云端平台。

- 云端平台实现了强大的病毒与木马云端实时检测功能，能应对普通手机终端、合作伙伴服务器、其他下载类的应用程序（如浏览器、下载器）的软件安全性检测请求。
- 终端与云端的结合解决方案：

MTAA围绕着用户使用手机的整个流程、不同的使用习惯，对不同级别的安全事件进行分布式处理。当系统开始启动，安全软件即进驻系统底层，对系统软件、内存驻留软件进行扫描。在手机使用过程中，对系统软件与应用软件的运行进行安全监控，主要包括对各种敏感操作调用过程进行监控，如发现超出安全许可的敏感操作，立即进行主动式的防御，如：防隐私信息的扫描（通讯录、短信、彩信、照片、视频、位置信息、文件文档、收藏夹、上网记录、cookies等）、防某指定程序的扫描（部分机型）、防按键捕捉，防帐号密码捕捉，防私自信息交换（短信、彩信）、防私自无线数据交换（联网、蓝牙、红外等）。用户下载软件时，能实时通过云端检测正在下载软件的安全性，防止下载高风险软件。在用户安装新软件时，对软件进行安全性扫描，防止安装高风险软件。

3.3.3 MTAA的四大防御体系：防病毒、防骚扰、保隐私、网络防御

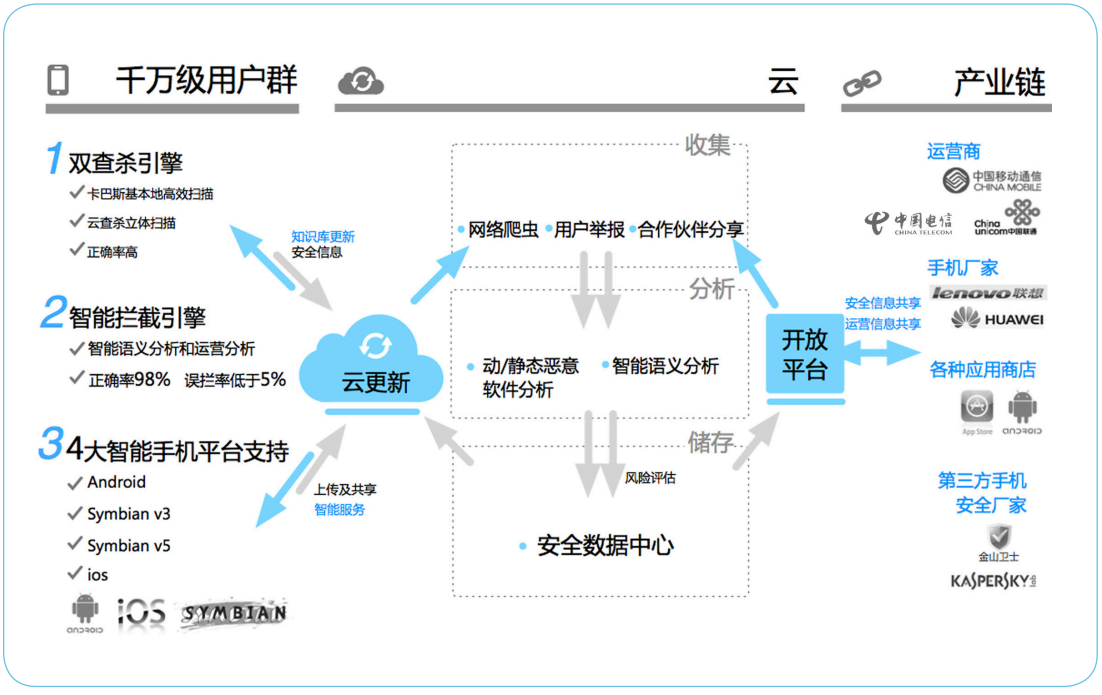
1）防病毒：

基于MTAA在Symbian、Android平台构建的移动安全软件具备强大病毒查杀能力。具体包含：

- 多引擎查杀：QQ手机管家查杀病毒引擎+卡巴斯基查杀病毒引擎+云查杀病毒引擎
  - 高性能的本地查杀引擎——QQ手机管家查杀病毒引擎、卡巴斯基查杀病毒引擎，在无需联网的情况下，可以快速的对本地已安装软件和即将安装软件进行病毒查杀，第一时间保护手机的安全。
  - 精准的云查杀引擎：在用户允许的前提下，终端会联网将本地的软件信息及行为特征上传到云端服务器，服务器根据所上传的信息进行精准的病毒扫描，将最终精确的查杀结果返回给终端。
- 病毒特征库云更新及病毒预警技术
  - 可以以最快的速度将最新的病毒特征库进行更新，从而能全面及时的保障用户手机的安全。基于“防杀结合，预防为主”的理念，系统会在截获病毒后第一时间推送病毒预警，让用户防患于未然。

- ◆ 联网行为监控
  - 用户可以清晰的观察到手机上安装的每个软件的联网行为，出现异常时可以及时进行处理。
- ◆ 强力卸载
  - 某些病毒简单的使用系统无法卸载，这时强力卸载可以帮助用户清理手机，保障手机远离病毒。
- ◆ 安全软件管理
  - 基于“以防为主”的理念，MTAA提供了安全、可靠、完善的软件管理渠道，全部软件都经过全面病毒检测，确保安全。可以满足用户大部分场景的应用使用需要，保证用户能放心的安装使用。
- ◆ 全网数据监控拦截技术
  - 通过对全网数据的抓取和与合作伙伴的资源合作，可以达到最全面数据监控，能第一时间发现病毒，并进行预警。
- ◆ 自动化检测技术
  - 采用智能的动静态检测、用户行为模拟、软件行为模型分析等技术，对软件进行自动化检测，从而发现病毒木马。

MTAA手机杀毒系统体系架构



2）防骚扰：

商家广告、诈骗、钓鱼、色情等信息被推送到手机终端，甚至还有深夜陌生人电话响一声的骚扰，这些都严重影响用户的正常生活。基于时刻为用户着想，为客户实现最大价值的理念，MTAA为用户建立骚扰防护的安全盾。 鉴于手机的最大骚扰来源于电话和短信，MTAA实现了一整套针对电话与短信的安全解决方案。

- 防电话骚扰：通过用户设置的黑白名单可以实现对黑名单号码拨打电话的时候提示各种语音信息，包括空号、关机、不在服务区、停机等，还通过本机智能判断+云平台信息共享，智能拦截“响一声”的吸费电话。

- 短信拦截：通过用户自定义的黑白名单或模式外，还依靠智能语义分析技术，实现了智能度业界领先的短信智能拦截平台。智能拦截能实现关键字语义分析，对内嵌电话号码、广告号码、客服号码、银行帐号、网址等进行智能分析拦截。

3）保隐私：

隐私问题是所有安全类问题中最备受关注的。

MTAA构架的“隐私保护”的解决方案是基于高权限用户模式下，结合手机操作系统本身的框架特点，通过先进技术，可截获系统的大部分调用，如发送短信、拨打电话、读取数据库、获取IMEI号等，来实现终端层面颗粒度极细、力度极强的解决方案。

隐私安全问题，具体到手机平台，主要是指用户电话号码、短彩信记录、通话记录、联系人、帐号密码、地理位置、浏览器书签、手机唯一码等私密信息的保护问题。

针对一般的智能手机，可以通过截获系统的消息广播和监听系统数据库变化的方式，为用户提供一个隐私数据的保护空间。在隐私空间里，保存着用户的所有隐私信息，如收发的短信、通话记录等。其本质思想，就是通过创建另外一个数据源，把用户认为隐私的数据从系统数据抽离出来，并通过数据加密技术进行二级保护。

而针对已经破解的智能手机，除了可以实现上述隐私数据保护功能之外，还可以实现主动防御式的隐私保护，并形成功能上的互补。一般来说，一个应用的权限，是在安装的时候就已经提示给用户的。但用户往往会忽略掉这个权限提示列表，而直接安装应用。针对这种情况，主动防御系统可以截获某个应用的隐私数据访问（如读取系统短信、系统联系人等），并询问用户是否允许操作。同时，主动防御系统也会根据用户的选择，进行智能分析学习，更好的保护用户的隐私。

4）网络防御：

目前无线互联网高速发展，智能手机上网的安全隐患也日益突出。一些恶意软件偷偷联网产生大量流量资费，甚至收集用户隐私信息，给用户造成损失。MTAA上网监控功能能够实现：

- 实时流量监控。由于是直接读取系统信息文件，因此流量统计更加精确，当本月使用的流量接近用户设置的限额时，会弹出提示让用户关闭网络连接。

- 采用先进的IPTABLE防火墙技术实现联网黑白名单功能，用户可以自由设置信任的程序列表，非信任程序则无法联网，从而可针对特定的程序的联网行为进行监控，除了避免产生不必要的流量外，还可以控制恶意程序联网带来的高风险。

- 根据手机的状态智能调整监控行为，从而达到最佳用户体验和省电目的。通常用户使用蜂窝制式（如3G）通道上网才会产生流量资费，因此当手机处于网络关闭状态（包括休眠状态）或者在WIFI环境下将关闭上网监控，节约用户的电池使用成本。

- 网站访问监控与提示：通过云平台进行恶意网址的监测，以及本地平台对网页的恶意代码的监控，达到网站访问监控与提示，使用户上网时远离恶意网站与钓鱼类网站，为用户打造一个安全、无忧的上网环境。

3.4 MTAA定制化服务：针对不同行业、合作伙伴与终端用户的具体需求，MTAA有不同的策略与合作侧重点

3.4.1 移动运营商

在产业链中，移动运营商是移动网络的建设者，也是移动应用的规则制定者之一，许多网络的扣费也是内置于移动终端SIM卡中，由移动运营商代收取；某些移动支付的方案是移动SIM卡相关的；所以，MTAA非常注重与运营商进行深层次的合作。

- 运营商关注手机安全，关注用户手机号、短信等私隐信息的安全性、代收费的安全性、移动电子商务的安全，以及关注垃圾信息对用户的骚扰、诈骗信息与吸费电话等可能对用户存在的潜在经济损失威胁。

- MTAA的解决方案专门针对运营商关注的问题，提供从终端到云端的全方位安全解决方案，为手机用户切实防范潜在安全威胁，从根本上防止产生经济损失。其它的，如针对扣费病毒木马的主动扫描防御、针对手机运用中各种帐户与密码的保护、对应用程序的访问以及权限控制、对各种私隐信息的主动保护，对垃圾短信、诈骗短信、吸费电话的智能拦截，等等，所有这些，都致力为运营商提供终端安全的全面支撑。

3.4.2 移动终端厂商

与移动终端商，比如NOKIA、MOTO、联想、华为等进行战略合作，在其推出的智能平台手机中全面预置手机管家，为用户提供安全的手机应用环境，并通过移动安全实验室作为技术支撑，共同提升整个产业链的价值合作。

3.4.3 MTAA还覆盖与产业链的下游厂商合作。包括，电子市场、论坛、下载网站、手机专卖店、手机卖场等。

主要有两方面的合作：

- ◆ 与电子市场、论坛、下载网站进行软件认证合作：电子市场、论坛、下载网站通过接口把软件传输到MTAA云查杀平台，云查杀平台对这些软件进行多方位的安全检测，并给出可靠的软件安全结论。
  - 技术实现：合作伙伴通过接口把软件传送到MTAA的云检测平台，云检测平台经过静态、动态、人工三重检测，确保结果的可靠性，并把结果反馈给合作伙伴，力求让合作伙伴能向用户提供安全的软件下载。
- ◆ 与有下载功能的软件进行云查杀合作：包括浏览器类、搜索下载类，使这些软件的用户在下载的过程中就能知道下载文件的安全性。
  - 技术原理：合作伙伴在用户下载的时候，把下载文件（主要是应用安装包）的URL提供给云检测平台，云检测平台在云端实现下载文件（主要是应用安装包）进行云检测，把检测结果实时同步到合作伙伴，力求提供给合作伙伴的用户，在下载的时候就能得到软件的安全性建议，判断是否进行下一步的安装。

第四章：MTAA 部署与实施：腾讯移动安全实验室介绍

4.1 腾讯移动安全实验室是基于MTAA的策略，为腾讯无线安全产品的开发与技术实现提供测试、验证的平台，并向业界以及合作伙伴提供和分享面向应用的最佳实践，是一个开放、增值、孵化产业链生态的坚实平台。

4.2 腾讯移动安全实验室战略合作模式

- 在信息安全领域中，与移动运营商、电信网络解决方案供应商以及全球领先的安全解决方案提供商进行战略合作，在数据安全保护、终端安全、云安全等方面进行深度合作，实现平台共享。
- 与我国域名注册管理机构和域名根服务器运行机构进行战略合作，通过腾讯移动安全实验室的技术平台，为合作伙伴提供移动安全领域的数据支持，携手权威发布中国互联网安全领域的相关统计信息，并共同制定移动安全行业的相关标准。
- 与金融领域的大型银行进行战略合作，帮助银行、证券等金融机构进行与用户资金交付相关的支付平台的信息安全建设，以及完善支付平台各项功能。
- 与移动终端商，如NOKIA、MOTO、联想、华为等进行战略合作，在其推出的智能平台手机中全面预置手机管家，为用户提供安全的手机应用环境。

同时，腾讯移动安全实验室将：

- 向第三方软件提供统一安全认证服务；
- 向第三方软件提供全方位安全测试服务；
- 与优秀个人开发者合作，为其提供全方位的支持和服务。

术语列表

MTAA：腾讯终端安全架构（Mobile Terminals Assurance Architecture）

J2ME：Java 2 micro Edition

API：应用程序编程接口(Application Programming Interface)

Root：Root是Linux系统中唯一的超级用户，具有系统中所有的权限，如启动或停止一个进程，删除或增加用户，增加或者禁用硬件等等。

Hook技术：计算机术语，一般是指对正在运行中的函数地址进行重定向，达到截获函数调用的目的。

Inject技术：计算机术语，一般是指对一个正在运行中的进程注入片段，并通过修改进程运行地址，达到运行被注入代码的目的。

Pm指令：Android平台上提供的一个命令，可以直接用安装包进行操作，如删除，安装等。

Activity服务：Android平台上的一个本地服务，负责各个APP的数据读写、服务开关、界面跳转等功能。

Sms服务：Android平台上的短信服务。

Phoneinfo服务：Android平台上的话机信息服务。

Input服务：Android平台上的输入法服务。

Cookies：指某些网站为了辨别用户身份、进行session跟踪而储存在用户本地终端上的数据。

IMEI码：是国际移动设备身份码(International Mobile Equipment Identity)的英文缩写，是由15位数字组成的"电子串号"，是每台手机在全世界的唯一标识码。

IPTABLE技术：指静态防火墙技术，对进出计算机的数据包进行过滤的技术。


Tencent 腾讯