文章编号:1001 - 9081(2007)S2 - 0113 - 03

基于可信计算的移动设备上的软件行为控制策略

庄云鹏,陈启安
(厦门大学 计算机科学系,福建 厦门 361005)
(zhype@163.com)

摘 要:简要介绍可信移动平台的思想,在软件行为方面提出了一个基于可信平台的手机访问控制策略,并给出基于可信计算核心安全硬件可信平台模块在这个策略模型上的应用及实现方法。

关键词:可信计算;可信移动平台;可信移动平台;软件行为
中图分类号: TP309 **文献标志码**:A

0 引言

随着无线通信技术与计算机技术的不断融合,移动终端(Mobile Equipment, ME)正逐步成为与 PC 同等地位的人机接口的主要设备之一。一直以来,人们对于手机的安全不够重视,忽视了黑客或病毒入侵所带来危害。如何保护终端数据和应用程序的机密性、完整性,防止其被非法使用、篡改和拷贝已逐渐成为手机安全的研究重点,同时对手机的访问控制策略也提出了更高的要求。

传统上,电子设备的安全保护功能是由软件进行处理的,这种方式很容易遭受攻击。而且杀毒软件的更新总是迟于病毒的发作。病毒删除之后,已经造成的损失无法挽回,这就需要一种基于硬件的安全策略,这样才能更有效地阻止病毒或黑客程序对手机功能或内容的破坏或窃取。

手机和 PC 机相比有以下不同点:

1)手机作为现代人最经常使用的通信工具,其存储的信息的敏感度相当高,一旦被窃取,后果无法估量。

2) 手机一般一直处于开机状态,而且一般放置于自己不能看到的地方,并一直处于联网状态,如果遭受病毒或黑客程序入侵,在相当长的一段时间内,用户根本意识不到问题已经出现。

3) 手机病毒的传播更为迅速和有效,尤其是当智能手机处于企业应用网内时。

4) 手机用户一般是预付值的,一旦恶意程序操控手机拨打高收费的服务电话,将给用户带来巨大的经济损失。

从上面的分析中,手机中程序的运行应该得到更为严格的控制,从而使手机成为用户可信任的手机。

1 预备知识

1.1 可信移动平台

可信移动平台(Trusted Platform Module, TPM)实际上是一个含密码运算器件和存储部件的小型片上系统,存储用于验证和签名的密钥以及证明平台硬件、软件可信状态的哈希值,它是平台中重要的防篡改元件,是平台的信任根,与度量可信根的核心(Core Root of Trust for Measurement, CRTM)一起执行可信启动流程。2006 年 3 月可信计算组织(Trusted Computing Group, TCG)发布的可信计算规范[7]中给出了"信任"的定义:如果一个实体对特定的任务总是处于可预料的状态则它是可信的。以 TPM 为基础,可信机制可以通过完整性检测、检测结果的存储和报告三个方面来体现。系统启动时,对平台 BIOS 和操作系统进行完整性检测,将检测生成的哈希值传给 TPM 并存储于平台状态寄存器 PCR 中。比较检测结果与 TPM 中存储的数据看是否匹配,如果匹配则认为平台状态是安全的,否则是不安全的。

如图 1 所示,可信平台模块 TPM 的结构是一个可信硬件模块,由执行引擎、存储器、I/O、密码引擎、随机数产生器等部件组成,主要完成加密、签名、认证和密钥产生等安全功能。TPM 本身就是一个小的计算机系统,一般是一种片上系统(System on Chip, SOC),而且它应当是物理可信的。

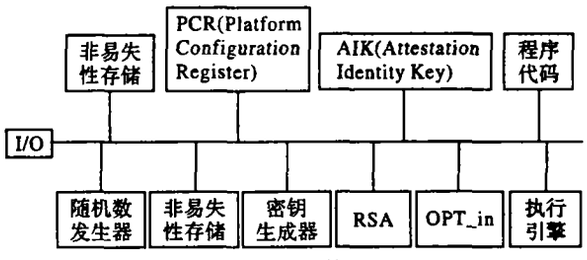

图 1 TPM 结构

I/O 部件管理信息通过总线的流通,它完成协议的编码和译码,发送消息到各个部件。

密码协处理器实现加密、解密、签名和签名验证。TPM 采用 RSA 公钥密码,也允许使用 ECC 或 DSA。算法实现要符合 PKCS#1 的规范。TPM 可以在其内部使用对称密码,但对 TPM 用户不暴露对称密码的算法。

HMAC 引擎实现 HMAC 的计算,其计算根据 RFC2104 规范。

SHA-1 引擎实现 SHA-1 的计算。

Opt-in 是一组选项开关。

非易失存储器主要用于存储嵌入式操作系统和其文件系统,存储密钥、证书、标识等重要数据。

密钥产生部件用于产生 RSA 的密钥对和对称密码的密钥。

随机数产生部件是 TPM 的随机源。TPM 采用所产生的随机数作为当前量、密钥或签名中的随机数。

电源检测部件管理 TPM 的电源状态和平台的电源状态。TCG 要求 TPM 能检测到所有的电源变化。

执行引擎包含 CPU 和嵌入式软件,通过软件的运行来执行接收到的命令。

易失存储器主要用于 TPM 的工作存储器。

收稿日期:2007 - 04 - 06;**修回日期**:2007 - 06 - 29。

作者简介:庄云鹏(1984 -),男,福建泉州人,硕士研究生,主要研究方向:软件工程、嵌入式系统、计算机网络、人机界面设计; 陈启安(1962 -),男,福建永安人,副教授,主要研究方向:嵌入式系统软件、信息电器、计算机网络、人机界面设计。

1.2 移动可信模块

TCG 组织于 2006 年 9 月 12 日发布了移动可信模块(Mobile Trusted Module,MTM)规范草案 V0.9。MTM 包含 TPM 规范 V1.2 的一个子集,并针对移动平台的特性,添加了一系列新的命令和数据结构。可以在这个基础之上建立基于可信手机的服务,比如手机钱包,手机票务等。MTM 引入了参照完整性度量(Reference Integrity Metrics,RIM)概念,并为它建立了相应的结构体。RIM 主要度量实体的完整性,如硬件、应用程序的可信性等。MTM 的主要目的是如何保证 RIM 的可信性。

1.3 MTM 定义的软件使用

1) 每个应用程序都有其被允许访问的数据对象,当程序启动时,平台操作系统就初始化这些数据。在这种情况下,该程序被限制只能访问这些数据,有利于防止恶意代码的执行。

2) 每个软件包含有被允许执行的功能列表。程序启动,操作系统就初始化这个列表。这种情况下,该程序只能执行这些功能。

3) 在移动设备上安装程序后,如果发现该程序有 BUG,该程序就应当不再被允许执行。如果不适当地限制一个含有缺陷的程序的执行,就有可能影响移动设备的其他功能,并导致设备的某些服务无法运行,甚至会影响到移动网络。

4)所有被取消运行资格的缺陷程序被包含在一个列表中,这个列表可被称为撤回程序列表。该列表有可能为每个缺陷程序提供相应的解决方法,比如说移除、更新或仅仅是阻止程序的运行。

1.4 基于可信计算的智能平台

基于可信计算的智能平台是一个双设备体系,即 MTM 设备与智能设备。智能设备操作系统与 MTM 设备通过认证代理互相访问。但智能设备不能向 MTM 设备写入数据,MTM 由用户来操作。如图 2 所示。

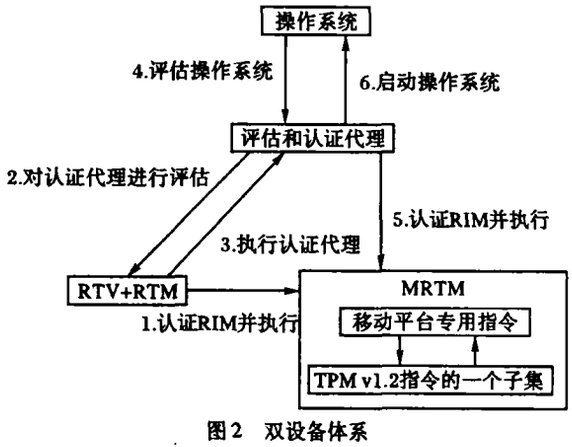

图2 双设备体系

2 基于可信计算的应用程序体系

可信移动平台规范中指出访问控制策略的制订基于两个基本原则[8]:责任分离和最小特权。只允许经认证和授权的主体(用户、进程或服务等)访问资源,从而使需要保护的资源在合法范围内被使用,不同的主体具有不同的访问权限。访问控制策略中不仅要明确访问者的身份,访问的时间和方式,在有特殊条件限定的情况下还需指定访问的条件。

基于可信计算的软件行为控制重点从以下两个方面对移动设备进行安全保护:

1)访问设备中存储的数据:手机存储卡可以存储大量数据,根据使用者具有的权限等级确定可以访问的数据。这些数据包括应用程序本身的文件。

2)访问设备的各种硬件功能:手机本身提供了不少应用功能,如最基本的拨号等。根据应用程序的权限等级确定可以访问的硬件功能,以防止不必要的损失。

定义智能平台的各种基本应用:网络访问、通信功能、图形、扬声器、SIM 卡访问、存储区域访问等。这些基本应用在手机出厂的时候是基本固定下来的,因此厂家可以根据自己的需要,制定自己的策略。比如制定手机的资源列表等。

2.1 体系描述

软件行为规约是软件运行时必须遵守的准则,软件行为规约定义如下:

1)基本应用访问。软件是否被允许访问手机的基本功能,如拨号、蓝牙等基本应用。

2)存储区的访问。软件有其被允许访问的存储区范围。

3)内存及 CPU 使用限制。

每个软件都运行于独立的应用程序域,软件所遵守的约束也同样适用于相对应的应用程序域。如果该软件调用了系统服务,该项系统服务也必须遵守这些约束。借鉴传统操作系统的角色分类的概念,定义以下四个基本的应用程序访问级别:

1)系统级:OS 提供的各种功能函数(如 Explorer 等)以及操控硬件的函数。这个级别的进程可访问各种硬件。

2)可信任级:可使用大多数硬件,如拨号、声音、网络等。可访问所有密级信息(如微软自己提供的 Outlook 程序等),而且同级别及以下的程序不能对程序本身文件进行操作。

3)半信任级:只可访问本身的密级信息。硬件功能限制。

4)非信任级:系统内核会开辟一段独立的内存空间和闪存空间,仅在该范围内可以访问。CPU 使用率也受限制,功能性硬件全封闭,关键系统应用封闭。

这些级别信息存储于 MTM 中,并供操作系统实时调用。用户也可以定义新的访问级别。MTM 同时维护一个访问控制矩阵,该矩阵包含各个程序的访问级别、数字签名及可访问的资源列表。

2.2 关键过程描述

程序启动过程如图 3 所示。该过程从两个方面限制了程序的运行:

1) 程序必须在 MTM 上注册过,才能访问智能平台的各种设备和使用智能平台的各种功能。

2)程序的数字签名必须和它注册时的数字签名一致。如果病毒感染程序文件后,该程序的数字签名验证就不会被通过,当然也不会被允许运行。

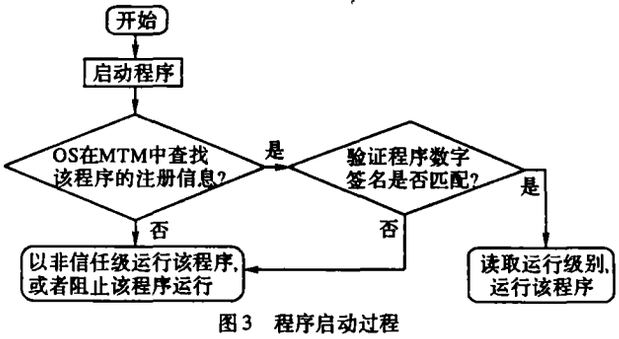

图3 程序启动过程

2.3 算法设计

主要用到的符号及其含义如下:

Capp 为应用程序数字签名;
DAapp 为应用程序数据区;
Mapp 为应用程序内存区,主要是大小限制;
Dapp 为应用程序描述;
Rapp 为应用程序所需资源列表;
CIapp 为 MTM 第一次获取程序信息时所生成的数字签名;
CRapp 为实时生成的程序数字签名;
Eapp 为应用程序运行环境。

应用程序安装并初始化控制矩阵过程:

应用程序安装后,MTM 从操作系统中读取应用程序信息 Dapp,并为它生成初始的数字签名 CIapp,储存到 RIM 中,同时也读取该应用程序所需要的资源列表 Rapp,加入 MTM 的访问控制矩阵中,等待用户进行认证。具体步骤如下:

```
1.  Read Dapp, Rapp
2.  CIapp = H( Dapp)
3.  Write CIapp, Rapp to MTM
4.  wait for user's Authentication
```

程序运行时,当在其需要资源,程序向操作系统的资源调度算法申请资源。资源调度算法接收程序的请求,并查找该程序的资源范围,如果资源被允许为该程序访问,则把资源分配给该程序,否则拒绝。具体步骤如下:

```
1.  Receive Apply ( R) from App
2.  lookup R in Eapp
      If ( Find)
        allocate
      Else reject
```

程序启动时,MTM 读取程序的实时信息,生成程序的实时数字签名 CRapp,并与 RIM 中的数字签名进行比较,两者相同时,操作系统才允许运行该程序,并读取其资源列表。具体步骤如下:

```
1.  Read Dapp
2.  CRapp = H( Dapp)
3.  Read CIapp from MTM
4.  if ( CIapp == CRapp)
      Initial Eapp
    Else reject
```

2.4 安全性分析

操作系统有自我保护功能。对基于 MTM 的智能平台而言,如果操作系统被破坏,在启动时其数字签名与 MTM 中的操作系统的数据签名不一致,操作系统就不能正常启动。这种方法其实不尽如人意。一个好的方法是在运行时保护好系统内核,不让它遭受破坏,防止恶意程序操纵操作系统的文件,其他非系统程序只能读取操作系统所在文件夹,不能对它进行修改。

每个程序的运行都有严格的限制,这些限制包括 CPU 使用率上限、存储区隔离、硬件访问等。如果系统中了木马,在这种情况下,未授权前木马无法读取机密信息,也无法使用平台的功能,如网络、拨号等,这样就能保护智能设备不受木马的影响。病毒也无法破坏机密信息,即使它把自己嵌入到其他程序中(在 MTM 的保护下,这种情况也不会出现,因为只有系统级或程序本身才能操纵程序文件夹里的文件),程序的实时验证也无法通过。

2.5 应用开发平台的拓展

开发平台为每一个软件维护一个资源申请列表,该列表是自动生成的。软件开发时,调用库文件的时候,平台会检测这个功能会用到哪种资源,然后把在资源申请列表中登记。在软件安装的时候,操作系统会读取这个列表以便与 MTM 交互。

3 结语

本文介绍了基于可信计算的移动设备应用程序控制策略。该策略应用可信安全硬件 TPM 及其提供的完整性检测、密封存储等功能来保护移动终端的数据及硬件安全,防止其被非法使用。

到目前为止,手机安全有两种保护手段:1)用传统的软件保护,多数安全厂商已经进入智能手机领域,但这种方式已经被事实证明不够可靠;2)使用芯片,有些公司开发基于闪存的芯片来保护数据。但现有的安全手段都不能达到可信计算的要求。因此,研究开发能与可信计算平台相结合的操作系统成为可信计算发展工作中的重点。

参考文献:

[1] TCG Mobile Trusted Module Specification version 0.9 Revision 1.00 [S]. 2006.

[2] REID J, DAWSON E. Privacy and Trusted Computing[C]//Proceedings of the 14th International Workshop on Database and Expert System Application. Prague: Computer Science, 2003: 383 - 388.

[3] Trusted Mobile Platform Protocol Specification Document , Revision 1.2[S]. 2006.

[4] PERELSON S, BOTHA R. An investigation into access control for mobile devices[EB/OL]. [2004 - 04 - 01]. http://www.infosecsa.co.za/proceed2ings2004/035.pdf.

[5] MURMANNT, ROSSNAGEL H. How security are current mobile operating systems[EB/OL]. [2004 - 03 - 20]. http://sec.isi.salford.ac.uk/cms2004/Program/CMS2004final/p2a2.pdf.

[6] 钟晓军. 我国拥有可信计算核心技术. [EB/OL]. [2007 - 01 - 18]. http://www.cas.ac.cn/html/Dir/2005/04/15/7473.htm

[7] Trusted Computing Group (TCG) Main SpecificationVersion 1.2 [EB/OL]. [2006 - 03 - 01]. http://www.trustedcomputinggroup.org.

[8] Trusted Mobile Platform Software Architecture Description, Revision 1.2[S]. 2006.

[9] Trusted Mobile Platform Hardware Architecture Description, Revision 1.2[S], 2006.

(上接第 109 页)

参考文献:

[1] 周永彬,冯登国. RFID 安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581 - 589.

[2] DUBNER A D. Securing the pharmaceutical supply chain — the authenticated RFID platform[Z]. MIT Auto-ID Center, 2003.

[3] FINKENZELLER K. RFID handbook: fundamentals and applications in contactless smart cards and identification[M]. 2nd ed. New York: John Wiley & Sons, 2003.

[4] LIOY A, MARIAN M, MOLTCHANOVA N, *et al*. PKI past, present and future[J] . International Journal of Information Securtiy, 2006, 5 (1): 18 - 29

[5] SCHNEIER B . Applied cryptography : protocols , algorithms , and source code in C[M]. 2nd ed. New York: John Wiley & Sons, 1999.

[6] MENEZES A J, van OORSCHOR P, VANSTONE S. Handbook of applied cryptography[M]. New York: CRC Press, 1996.