企业级系统移动智能终端访问控制技术研究

黄 健,黄建文,黄志新,梁 栋,李俊磊
(广州电信研究院,广东 广州 510630)

摘 要:设计了一种专门应用于企业级系统移动智能终端访问控制框架,拓展 DTE 安全机制,弹性动态地对重要应用进程进行预留系统资源且对其进行统一分配与管理,能够有效预防系统资源竞争而发生的冲突问题。相比传统的访问控制框架而言,该移动智能终端访问控制框架不仅保证了企业级系统敏感数据信息的机密性和完整性,同时也满足了可用性要求。

关键词:移动智能终端;访问控制框架;预留系统资源;可用性
中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2014)06-0058-04

Research of access control technology for mobile intelligent terminal

Huang Jian, Huang Jianwen, Huang Zhixin, Liang Dong, Li Junlei
(Guangzhou Research Institute of China Telecom, Guangzhou 510630, China)

Abstract: In this article, we specifically designed an access control framework for mobile intelligent terminal, expanded DTE security mechanism, the framework dynamically allowed key appiications to reserve system resource, system can allocate and manage these reserve system resource with unite, and effectively prevented system resources competition and conflict problem. Compared with traditional access control framework, the access control framework for mobile intelligent terminal can effectively ensured informational confidentiality, integrity and availability.

Key words: mobile intelligent terminal; access control framework; resource system reservation; availability

随着现代信息科技的不断进步,移动智能领域获得了前所未有的发展,移动智能终端逐渐成为人们生活中不可缺少的日常工具,如移动智能手机、商务掌中宝、个人数字助理等。由于在便携性与智能计算能力等方面得到了广泛提高,移动智能终端已开始应用于各大行业领域。与此同时,移动智能终端的安全问题也愈来愈突出,如病毒感染、恶意代码攻击、数据信息泄露、系统资源浪费、应用进程无法响应以至于死机等。企业级系统是一个国家赖以生存的支柱型行业领域,对移动智能计算的需求也逐渐提升。因此,如何保证企业级系统移动智能终端的安全性,已成为备受关注的焦点。

机密性、数据完整性以及可用性是用户对移动智能终端的基本安全需求。传统的访问控制技术只能有效地保证数据信息的机密性与完整性,对可用性并没有进行充分的考虑与完善。传统访问控制技术的应用场合一般针对于个人 PC。尽管移动智能终端的软硬件配置都在不断提高,但与个人 PC 相比还是显得不足。不良攻击型的代码应用程序更容易导致系统资源的浪费,致使企业级系统中的重要应用进程得不到及时响应,从而形成分布式拒绝服务(DDos)攻击,所以若将传统访问控制技术直接应用于移动智能终端中,移动智能终端的安全性将得不到保障。相比于个人 PC、工作服务器等平台,企业级系统移动智能终端主要包括以下几个特点:(1)移动智能计算能力与系统资源有限;(2)通信交互依赖于无线网络等公共媒介;(3)单一型用户系统;(4)易丢失、盗窃等。

企业级系统移动智能终端的各个特点对访问控制技术提出了更高标准,如可用性、实时性等。可用性是指移动智能终端[1]必须对重要的、关键的企业级系统应用进程进行及时响应;实时性是指移动智能终端应该与企业级系统进行实时交互,实现一体化操作等。

1 相关研究

迄今为止,已有一些研究学者与单位钻研于如何提高移动智能终端的安全性,也提出了众多相对应的安全解决方案与安全结构。例如可信计算组织(Trusted Computing Group)设计出一种统一的 TCG 移动智能终端安全系统结构[2],且应用平台不限于移动智能终端,也可以是个人

PC 与工作服务器。在 TCG 安全系统结构中，主要包括以下几种特点：(1)系统安全保护能力；(2)移动智能终端数据信息完整性比较；(3)一份通过完整性比较之后得到的系统安全完整性报告。在系统安全保护能力这个特点中，可信计算组织定义了一个移动智能终端访问控制机制，主要是保护那些涉及敏感数据访问的应用进程。可信移动平台(Trusted Mobile Platform)是针对移动无线平台提出的一种 TMP 移动智能终端安全系统结构，这个安全系统结构主要包括硬软件安全结构[3]以及相关规范。TMP 安全系统结构中的软件结构通过硬件特点来提升整个移动智能平台的安全性能。一般基于可信条件下的移动智能终端支持两种不同的访问控制模型，分别为自主动态模型与强制命令模型。这两个访问控制模型都建立在硬件的域分栏机制之上，以确保对数据信息与系统资源的访问都是通过合法授权的。

通过上述归纳分析，虽然已有多种移动智能终端安全解决方案与安全结构，但始终未从移动终端的硬件条件与水平以及企业级系统的角度出发，致使在基于有限的系统资源的条件下无法确保企业级系统重要的应用进程及时得到响应与交互。本文设计的基于企业级系统移动智能终端的访问控制框架，不仅能够保证数据信息的机密性与完整性，同时也满足了可用性要求。

2 系统访问控制框架

企业级系统的移动智能终端是单一型用户系统，系统中主动操作访问控制的主体是应用进程。受到保护的客体主要分为以下几种：(1)动态系统资源：移动智能系统中动态调度与管理的资源，如物理内存页面、时间消耗量以及 CPU 处理时间等。(2)静态系统资源：移动智能系统中静态或固定存在的资源，如敏感数据信息、软硬件接口等。

关于静态系统资源的访问控制机制已有较为成熟的访问控制框架模型，其中 DTE 安全机制[4]由于各种优于其他访问控制机制的特点而受到关注，如简单灵活多变、结构功能强大等，且多用于 Linux、Unix 等操作系统中。因此选择 DTE 安全机制作为企业级系统的移动智能终端访问控制框架的雏形模型，用于控制对静态系统资源的访问与应用，且依据企业级系统的不同安全需求对 DTE 安全机制进行配置与完善。在企业级系统数据信息的机密性与完整性得到保证的条件下，弹性地对 DTE 安全机制进行拓展，提高其移动智能终端的可用性。此外，提出一种系统资源预留的相关概念，在其访问控制框架中引入了动态系统资源控制功能，为企业级系统实时交互的重要应用进程预留系统资源，防止与其他应用进程产生资源竞争与冲突，从而确保系统及时响应关键应用进程。

如图 1 所示，在企业级系统的移动智能终端访问控制框架中，在基于可信[5]的整体系统环境下，主体(主动进程)向安全服务器提交对客体(被保护)的访问请求，

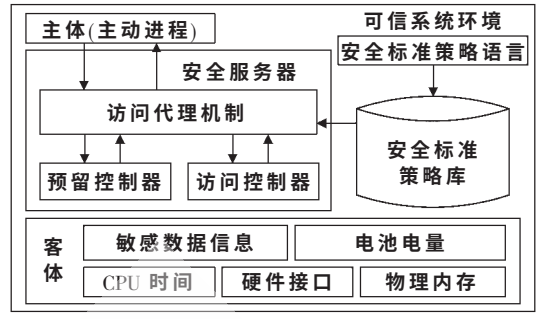

图 1 企业级系统的移动智能终端访问控制框架

访问代理机制在安全服务器中截取到相关访问请求，以安全标准策略库为依据，从中获取对应的安全标准策略信息，按照被保护客体的类型将访问请求与对应的安全标准策略一同提交到预留控制器(动态预留系统资源)以及访问控制器(静态访问系统资源)中，然后通过它们得到相关的访问决策信息，最后将一系列的最终结果回馈给访问代理机制，且将访问决策信息通知主体。

3 功能实现与详细设计

3.1 访问代理机制

主动进程向安全服务器发出相关的访问请求，然后由访问代理机制获取其访问请求信息，且从安全标准策略库中取得相对应的安全标准策略信息。依据不同类型的访问请求信息，访问代理机制将其访问请求以及其对应的安全标准策略一同发给预留控制器与访问控制器，通过它们的结果回馈给访问代理机制，最终由其访问代理机制将结果回复给主动进程。具体操作流程信息如下：(1)访问代理机制，获取相关的访问请求信息；(2)从移动智能终端系统中得到相对应的安全标准策略信息；(3)安全标准策略信息可以区别为预留策略信息与访问策略信息；(4)依据访问请求的不同类型，将其各个策略信息相对应地交付给预留控制器与访问控制器；(5)从预留控制器与访问控制器中读取相关裁定信息；(6)访问代理机制，对裁定信息进行处理，并将相关结果通知主动进程。

3.2 访问控制器

在企业级系统的移动智能终端中，访问协调控制不仅需要考虑安全性，而且也需要顾及到易用性，从而便于用户进行相关管理与配置。访问控制器采取了一些策略机制(如 DTE 安全策略)，如图 2 所示。主要包括如下一些关联对信息：

(1)客体/型关联对

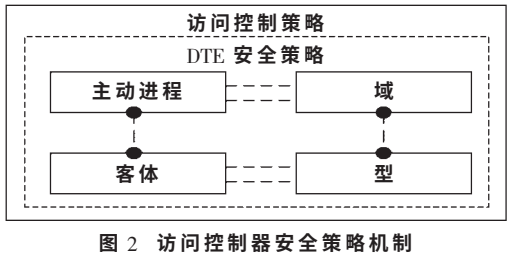

图 2 访问控制器安全策略机制

企业级系统移动智能终端中的客体依据不同需求信息可以分为 4 种不同级别的型，分别是与硬件接口相同级别的 X_Interface 型、与企业级系统敏感信息相关的 X_Sensitive 型、与企业级系统中的文件与操作数据相关联的 X_System 型和与其他客体信息对应的 X_Other 型。

(2)主动进程/域关联对

企业级系统移动智能终端中的主体(主动进程)一般分为 Y_Trusted、Y_UnTrusted、Y_Certified 3 个域。出厂就内嵌在移动智能终端中的固定应用进程与基本功能，一般属于 Y_Trusted 域，此域中的主动进程权限最大，可以访问移动智能终端中所有客体信息与系统资源。经过第三方验证才能使用的应用进程与功能程序属于 Y_Certified 域，此域中的主动进程权限中等，可以访问 X_Interface、X_Sensitive、X_Other 等型中的客体信息。未经过第三方验证的应用进程与功能程序都属于 Y_UnTrusted 域，此域中的主动进程权限最低，仅能够访问 X_Other 型中的客体信息。

3.3 预留控制器

(1)预留分类

①电池使用量预留：依据不同的应用进程与功能程序，采用不同的电池使用量模式，如省电模式[6]、标准模式等。

②CPU 处理器时间预留：CPU 处理器时间预留指的是主动进程所花费在移动智能处理器中的固定预留时间。移动智能终端为每一个主动进程在某个阶段都预留有一定数量的 CPU 时间段。对于预留请求信息主要包括计算时间量与周期数量。计算时间量表明预留阶段内的持续时间是多少；周期数量则表明某一次预留理论上能够持续多少个阶段。

③网络通信带宽预留：网络通信带宽预留表明在某些应用设备与网络程序上所预留的执行时间，单位为固定网络发送接收包传送个数。

④物理内存预留：此类型代表了一些物理内存页面，主要是一些闲散系统资源，因此需要预留控制器满足一些闲散资源的预留功能。

⑤资源预留库：预留资源库指的是几种管理与调度主动进程中的某些类型的系统资源，可以包括至少一种已定义的不同类型预留。如资源预留库 SET_i 可以表示为：$SET_i=\{Power\_L_i, CPU\_Time\_L_i\}$。

(2)预留管理

预留管理机制主要包括准入裁定、预留调度、预留执行 3 个不同的环节。准入裁定环节是对预留请求信息是否被允许进行裁定；预留调度是基于不同的预留调度模式对移动智能终端的系统资源进行最大限度的使用；预留执行是指确保主动进程可以使用其预留的系统资源。这 3 个环节都是互相关联的，如使用不同的准入裁定，都会对预留调度的安全策略与预留执行流程产生影响。

①准入裁定环节：对于企业级系统移动智能终端的每个不同类型的主动进程域中，只有属于 Y_Trusted 域的主动进程才能预留系统资源，其余主体域提交的预留请求信息将会被作废或者拒绝。

②预留执行环节：预留控制器必须保证主动进程可以使用移动智能终端为其预留的系统资源，然而主动进程则可能耗尽其预留系统资源之后继续执行下去。依据不同预留系统资源的不同类型分析，预留执行环节主要是把主动进程正在使用的预留系统资源的相关情况告知预留调度器，然后通过预留调度器中的安全策略对主动进程是否继续执行做出指示。下面以一个预留执行示例(CPU 处理器时间预留)进行详细分析。如图 3 所示。

图 3 CPU 处理器时间预留执行

在 CPU 处理器时间预留的一个周期过程中，主动进程使用本身预留的系统资源阶段称之为强预留。在强预留阶段中，某个主动进程仅仅允许优先级比自身高的主动进程抢夺一定的预留系统资源，计时器 A 告知预留调度与处理阶段结束。若移动智能终端的预留系统资源已经耗尽，通过使用其他主动进程预留的系统资源，某个主动进程继续执行下去，这个阶段称之为弱预留，此时某个主动进程可以被预留系统资源的主动进程或优先级比自身高的主动进程抢夺其预留系统资源，计时器 B 告知预留调度与处理阶段结束，若无法使用预留系统资源，将会同一般的主动进程一样加入调度库中进行处理。

③预留调度环节：在一般的系统资源预留模型中，主动进程与预留系统资源进行绑定，确保某个主动进程需要预留的系统资源时不会因为有其他主动进程相互竞争其系统资源而发生冲突。然而由于移动智能终端的现实情况，即系统资源限制性等原因，使用主动进程与预留系统资源绑定的形式将会致使过于剩余的预留系统资源，从而影响其终端系统的整体性能。企业级系统的移动智能终端是一个单一型用户系统，在固定的时间节点只能有一个主动进程与用户进行数据信息交互。由于预留的系统资源可以由多个主动进程进行共享获取，所以可能存在并发访问。系统需要对不同的主动进程进行不同类型安全策略地调度与处理。预留控制器一般是使用基于优先级的安全调度策略，高优先级的主动进程具有抢夺预留系统资源的高权限，低优先权的主动进程只能排列在等待队列之中，等待高优先级的主动进程使用完成为止。

3.4 安全标准策略语言

DTE 安全策略机制主要是由描述性的策略语言进行定制使用，用户可以很灵活、便携地管理和配置其策

略。在企业级系统的移动智能终端中，安全策略文件与数据信息一般将其编译成二进制类型，然后在终端系统开启时加载到其安全标准策略库中，从而确保安全服务器使用正常。

安全标准策略语言示例描述如下：

```
#Domain Definitions
/ bin/ phone = Y_Trusted
/ usr/ bin/ mpIayer = Y_Certified
#Type Definitions
/ ect/ network = X_System
/ usr/ IocaI/ abc. mpe = X_Sensitive
#Access ControI Materix
(Y_Trusted, X_System, all)
(Y_Certified, X_Sensitive, rw)
#Constraints
(Y_Certified, X_Sensitive,
TimeintervaI! 4:00! 19:00)
#Reservation Definitions
CPU_Time_L1=10ms, * * *
Memory_L1=50
Power_L1= strict
Set1 ={CPU_Time_L1, Memory_L1}
Set2 ={Power_L1}
/ bin/ phone 70
```

本文提出了一种基于企业级系统的移动智能终端访问控制框架，通过拓展 DTE 安全机制，弹性动态地为重要应用进程预留系统资源且对其进行统一分配与管理，有效预防系统资源竞争而发生冲突的问题。相比传统的访问控制框架而言，基于企业级系统的移动智能终端访问控制框架不仅保证了企业级系统敏感数据信息的机密性、完整性，同时也满足了其可用性要求。

参考文献

[1] 辛阳，杨义先.移动终端安全模块技术研究[J].通讯与电视，2005，31(11)：23-27.

[2] LAMPSON B W.Protection[J].Operating System Rev，1974，8(1)：18-24.

[3] SANDHU R，COYNE E J，FEINSTEIN H L，et al.Role-based access control madels[J].IEEE Computer，1996，29(2)：38-47.

[4] Badger L，STERNE D F，SHERMAN D L，et al.Practical domain and type enforcement for UNIX[C].In：IEEE Symposium on Security and Privacy，OakIand，1995.

[5] 李涛，胡爱群.可信模块与强制访问控制结合的安全防护方案[J].东南大学学报(自然科学版)，2011，41(3)：234-238.

[6] SCORDINO C，LIPARI G.Using resource reservation techniques for power-aware scheduling[C].In：Proc.of the 4th ACM Intl.Conf.on Embedded Software，Pisa，2004.

[7] 刘伟，梁洪亮.移动终端系统的访问控制框架[J].计算机科学，2006，33(6)：299-304.

(收稿日期：2013-12-20)

作者简介：

黄健，男，1976 年生，工程师，主要研究方向：通信智能卡和手机终端，安全访问控制。