第 32 卷 第 24 期 计 算 机 工 程 2006 年 12 月
Vol.32 No.24 Computer Engineering December 2006
·安全技术· 文章编号：1000—3428(2006)24—0129—03 文献标识码：A 中图分类号：TP309

可信计算环境下策略控制系统的研究

吴振飞，陈克非
(上海交通大学计算机科学与工程系，上海 200030)

摘 要：近几年可信计算平台发展迅速，但基于可信计算平台上的策略控制系统的研究相对落后，现有的一些策略控制系统无法满足新式的可信计算平台的需要。经过对可信计算平台关于策略控制需求的认真分析，结合最新的 XrML 技术，该文提出了一套策略控制系统，该系统的控制力度、可配置性、可扩展性更为优越，基本符合可信计算平台的需求，将其应用到了微软的 NGSCB 平台上。

关键词：可信计算；策略控制系统；XrML；NGSCB

Research on Policy Control System Under Trusted Computing Environment

WU Zhenfei, CHEN Kefei
(Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】 Trusted computing platform develops rapidly in these years, but research on policy control system under trusted computing platform is not enough. To supply the gap, this paper represents a brand new policy control solution for trusted computing which uses XrML technology. The system is fit for the requirement of trusted computing platform and it also affords more ability of control, configuration and extension. How to applie the system on Microsoft NGSCB platform is represent.

【Key words】 Trusted computing; Policy control system; XrML; NGSCB

1 概述

计算机为人们保护着有价值的数据，对于本地或者远端想要访问敏感信息的用户，需要有一种有效的机制来进行适当的控制。2002 年 12 月，多家著名 IT 企业联手创建了 TCPA(TCG)组织，并于 2003 年 4 月正式发布了它们的 TCG Spec(1.2 版本)，提出了一个新式的软硬件结合的可信计算平台。多家硬件厂商推出了适合于该平台的硬件芯片。而该平台的主要推动者微软与 IBM 公司则分别针对 Windows 与 Linux 操作系统构建出了实验所用的操作系统。

可信计算平台是一种基于信任链的安全架构平台。该平台在硬件主板上有一块专有安全芯片用来存储系统各模块的 Hash 值，并能够提供一些加解密、签名等安全运算服务。系统必须从启动时刻起就开始执行验证过程，最先进行验证的是系统 BIOS 程序，需要对其进行 Hash 运算并与先前存于安全芯片的 Hash 值进行比较，只有在相等的情况下，BIOS 程序才可以被执行。装载之后的 BIOS 被作为一个可信根，可以对其上装载的程序进行 Hash 值验证，后面的程序同样依此方式通过层层验证，来确保运行中的所有程序的可信性。

在这种新式的可信计算平台上，对资源的访问与控制有了更细粒度的需求，这样现有系统中对资源访问进行控制的策略模块将无法适应：(1)现有的策略控制系统基本全部只能基于单一操作系统平台进行控制，而在可信计算的平台下，则需要多种平台能够可以互相执行资源访问验证。(2)现有系统的资源访问策略的粒度都定位在访问者一级。以 Windows 操作系统为例，在其策略控制子系统活动目录中，只能对用户、组与计算机这 3 种实体，实施安全访问策略控制。而在可信计算平台下，程序对程序的调用同样需要进行验证，需要有相应的策略控制进行支持。在这种情况下，需要有一套更加符合可信计算平台的新式策略控制系统。本文将根据最新的 XrML 技术构建一套完全基于可信计算平台的策略控制系统。

2 策略控制系统的设计

文中设计的策略控制系统从欲控制环境的用户角色以及对应不同用户角色的使用场景进行分析，而后给出在每个场景中对资源进行访问的具体情况描述，接下来再对所有场景中涉及到的资源进行系统的整理与划分，设计出一种有效的方式来表达访问行为，在访问执行时能够对访问可行性直接进行判定。下面是具体的设计方案。

2.1 用户角色与场景描述

在可信计算平台下，大致可以把用户角色划分为以下 3 类：

(1)程序开发人员。他们需要识别他们编写的代码段应该具有什么权限，以便在某些适合的策略下运行。

(2)IT 管理员。他们需要能够对企业施行的策略进行设置或修改。

(3)终端用户。他们需要知道如何设置或修改他们本机的策略以及如何下放权限给其信任的实体。

可信计算最基本的一个要求是进程的隔离性。为了做到这一点，对内存页的访问需要进行细致的控制，比如可读、可写、可清空或者任意组合，这就是一个标准的用户场景描

作者简介：吴振飞 (1981－)，男，硕士、助教，主研方向：可信计算；陈克非，教授、博导

收稿日期：2006-03-13 **E-mail：**wuzhenfei@sjtu.edu.cn

述。像上述这样的用户场景有很多，一个完善的策略控制系统需要对他们分门别类地逐一列举。本文限于篇幅只将用户场景简单分成几个大类：程序访问场景(包含可信远程桌面连接可信终端服务器，自定义的网络连接程序等)，IT 管理员管理场景(包括对安全计数器的访问、颁发证书等)，终端用户访问场景(包括对加密组件的访问以进行签名操作等)以及一些通用的场景(包括多个进程的隔离性控制等)。

2.2 场景到对资源访问的映射

有了对用户角色与场景的划分后，需要将每一类场景映射到对各种资源对象的访问上来。下面以 IT 管理员管理场景为例，给出了一张映射列表，如表 1 所示。

表 1 映射关系

用户需求	对象类型	行为	缺省
运行	可信子系统装载器	Load	None
		None	
访问信号量	可信子系统/系统线程		
保护内存页	可信子系统/内存管理器	R、W、X，它们的任意组合或者 None	R
对可信输出设备的访问	可信输出设备	None	None
		W	
对网络的访问 (走 IP 协议族的网络)	网卡	是否可以发送消息与母系统沟通	Can't
对数据的访问	可信程序之间	None	None
	与母系统间的传输	Read	
	物理内存页	Write	
	剪贴板	Destroy	
对封闭内存的访问	封闭的内存	None	None
		Read	
		Write	
对密钥数据	身份私钥	Read	Read
		None	
颁发证书	密钥	Off	Off

2.3 对资源分类并定义操作类型

由第 2.2 节的映射列表，可知场景可以转变为各种资源以及对特定资源执行的不同操作的类型。

在可信计算平台的环境下，资源可以分成下面几类：(1)系统级资源：进程/线程；(2)IPC 资源：信号量/事件/传输信道；(3)数据资源：容器/数据流；(4)沟通资源：窗口/密钥/其它设备/网络；(5)状态资源：计数器。

接下来需要针对上述这些资源分别定义不同的操作类型，限于篇幅原因只以 IPC 资源为例，表 2 呈现了 IPC 的各项资源分别对应的操作类型。

表 2 操作类型

行为	对象管理器的操作类型
信号量等待	IPC_SEM_WAIT
信号量发出信号	IPC_SEM_SIGNAL
销毁一个信号量	IPC_SEM_DESTROY
设置一个事件	IPC_EVENT_SET
事件重置	IPC_EVENT_WAIT
事件触发	IPC_EVENT_PULSE
传输信道读取	IPC_XPORT_READ
传输信道写入	IPC_XPORT_WRITE

2.4 使用 XrML 证书进行策略管理

有了资源的划分以及对资源的操作类型的定义，需要有一种有效的方法表达对资源访问的行为，包含待访资源说明，执行何种类型操作以及执行操作时附加包含哪些信息(比如私钥)等，并在访问执行时能够对访问操作进行判定。XrML 策略证书就是能完成上述任务的一种非常好的技术。

将基本的策略语句以签名的 XrML 文档 – XrML 证书的形式进行传输非常方便。一个 XrML 证书可以表示一段程序拥有什么权限。如果一个权限没有在 XrML 证书中显式标明，那么访问将会被拒绝。反之，将会授予该程序段相应的访问权限。下面的例子演示如何将“运行”权限授予所有包含给定签名的程序段。

```
<license licenseId="One">
  <grant>
        <forAll varName="Object"/>
        <grant>
  <!--下面是一个细粒度的基于最基本的受保护对象的授权-->
              <principal varRef="Object"/>
              < NX_THREAD:THREAD_CREATE/>
              <prerequisiteRight>
                    <principal varRef="Object"/>
                    <possessProperty/>
                    <group:ISV/>
                    <trustedIssuer>
                          <keyHolder>
                                <!--指明谁必须担保这个关系，比如说某公司的密钥-->
                          </keyHolder>
                    </trustedIssuer>
              </prerequisiteRight>
        </grant>
  <grant>
        <!--下面是对一组对象的授权 -->
              <principal varRef="Object"/>
              <NX_PROCESS/>
              <prerequisiteRight>
                    <principal varRef="Object"/>
                    <possessProperty/>
                    <group:ISV/>
                    <trustedIssuer>
                          <keyHolder>
                                <!--指明谁必须担保这个关系，比如说某公司的密钥-->
                          </keyHolder>
                    </trustedIssuer>
              </prerequisiteRight>
        </grant>
  </grant>
  <issuer>
        <keyHolder>
              <!--签名；指明谁制定此策略-->
        </keyHolder>
  </issuer>
</license>
```

将 XrML 证书作为策略控制方式引入可信计算平台后，分布式环境中的系统间访问有了更细粒度更严密的访问控制。对于异构的操作系统之间进行策略的访问控制在可信计算环境下变得尤为重要。保存策略控制信息的 XrML 证书可以在各个系统间进行信息无损的沟通，这种方法彻底弥补了原有特定于不同操作系统的策略控制系统无法向其他系统移

植的弱点。

本文设计的策略控制系统具有极强的松散耦合特性，可以在多种可信计算平台的实现中得以实施。下面以微软公司设计的 NGSCB 平台为例，演示一下它如何被应用到可信计算环境中。

3 策略控制系统在 NGSCB 平台上的实现

3.1 微软 NGSCB 平台介绍

为了满足可信计算的安全需求，新的平台需要在原有平台上实现比如封闭的内存区域(Sealed Storage)，认证性(attestation)等许多新的安全特性。然而考虑到现有操作系统已经过于庞大，并且已经为其提供的功能性与性能进行了优化，在现有设计的操作系统中添加新的安全启动模块与安全保证模块将非常困难。基于这种情况，斯坦福大学、达特毛斯大学等研究机构提出了一些新式的类似于虚拟机的解决方案方向[2,3]。同时，微软公司也沿着这种思路设计出了NGSCB平台[1]。在NGSCB平台上，机器分区通过采取在同一套硬件系统上同时运行两个或多个操作系统的方式来解决需求上的冲突。其中的一部份依然是传统市场上使用的操作系统，管理着绝大多数的硬件以及原有的应用程序。一个或多个新式的拥有高可信度安全的操作系统也同时被应用在同一硬件系统上，可以用来提供一个需要高信度的可信计算环境。

图 1 给出了 NGSCB 的架构，左半边显示的是传统的操作系统运行着非可信安全的应用程序。右半边则为一个小型的高可信度的系统内核，称为 Nexus，上面运行专供可信计算应用的 Agent 组件，可满足用户一些与安全、可信相关的一些系统服务的调用。左右两个系统内核之间则依靠系统监控器来进行数据的传输与协调。NGSCB 硬件平台可以允许任何软件引导、运行。然而在可信系统平台 Nexus 下执行的受策略控制的操作会严格地保护宿主程序、其它应用程序以及操作系统之间的隔离性。NGSCB 对于可信系统的初始化与启动过程也给出了严密的步骤。

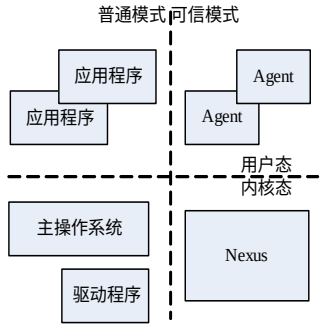

图 1 NGSCB 架构

3.2 策略控制系统在 NGSCB 上的实现

在 NGSCB 系统上使用 XrML 策略证书机制需要对其存储、读取、使用、配置等多方面进行定义。图 2 给出了一种简略的实现方式。对 XrML 策略证书进行存储的组件可以是一个运行在主操作系统上的应用，比如一个数据库程序。当然 Nexus 可信计算内核需要有一种手段，通过一个 Gate Keeper 来对其存储在 TPM 的 Hash 值进行校验，以确保策略证书存储的安全性、可靠性。对策略证书的读取需要在可信模式的用户态下提供一个用于进行策略配置的 Agent 组件来进行。同时这个 Agent 组件将会对读取到的 XrML 策略证书解析，来进行策略的设置或改动。策略配置器这个 Agent 组件作为一个管理员的角色来运行，并且在系统运行期间不可以被停止服务。只有操作系统的 Admin 才可以对此 Agent 组件进行访问，这条元策略需要在可信系统启动时直接进行加载，与其一起进行加载的还应有一些预定义好的策略模版。

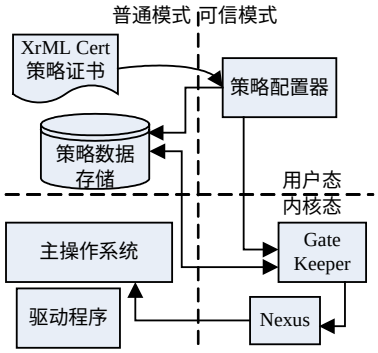

图 2 实现方式

下面给出一个策略配置器需要实现的特性如下：(1)设置/修改策略：NGSCB 发布时会有一系列缺省策略直接被进行配置，策略控制器需要能够对策略配置进行设置以及可以修改策略的相关性约束。(2)导入/导出策略：用户应该有能力利用策略配置器对签名的 XrML 策略证书进行导出，以及可以将在其他系统配置好的 XrML 策略证书直接导入。(3)根密钥安装/删除：策略配置器可对根密钥进行设置，以支持系统重置等操作。

4 总结

可信计算平台的发展将会不断深入，对可信计算各种细粒度的策略控制的需求也会不断加强。构建一个完善的、可灵活扩充的、平台无关的策略控制系统将作为可信平台建设的一个主要任务。本系统基本符合上述的需求。它具有完备的表义功能，对策略控制的各种信息都能很好地捕捉，提供了方便的扩充机制，使平台的设计者可以方便地对整个系统的策略进行调整。使用 XrML 证书技术，能够保证该策略控制系统完全的平台无关性，在分布式环境中，这种无损的信息交流使异构系统之间能够有效地利用可信计算技术提供的安全特性。

本文对整个策略控制系统的设计进行了阐述，给出了演示实例，讨论了其在微软公司的 NGSCB 试验平台下的实现过程。文中的策略控制系统在不同可信计算安全平台上的具体实现的细节，还需进一步分析讨论。

参考文献

1 England P, Lampson B, Manferdelli J, et al. A Trusted Open Platform[J]. Computer archive, 2003, 36(7).

2 Garfinkel T, Rosenblum M, Boneh D. Flexible OS Support and Applications for Trusted Computation[C]. Proc. of the 9th Workshop on Hot Topics in Operating Systems, 2003-05.

3 Marchesini J, Smith S W, Wild O, et al. Open-source Applications of TCPA Hardware[C]. Proc. of the 20th Annual Computer Security Applications Conference, 2004-10.