一种基于可信计算的分布式使用控制系统

初晓博[1),2)] 秦 宇[1),2)]

[1)](中国科学院软件研究所信息安全国家重点实验室 北京 100190)

[2)](信息安全共性技术国家工程研究中心 北京 100190)

摘 要 随着互联网络等分布式环境的发展,如何控制已经分发的数据成为一个重要的安全问题.最近提出的使用控制概念和模型虽然适用于描述该类问题,但其实施机制研究仍处于起步阶段.文中给出一种基于可信计算技术的分布式使用控制系统,有效地支持和实现了使用控制模型的 3 个特点:丰富的策略决策因素、控制的持续性和主客体属性的变异性.实验证明该方案具有较高性能,是一种分布式计算环境下的行之有效的使用控制实施解决方案.

关键词 可信计算;使用控制;分布式访问控制;Linux 安全模块;可信扩展访问控制标记语言

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.00093

A Distributed Usage Control System Based on Trusted Computing

CHU Xiao-Bo[1),2)] QIN Yu[1),2)]

[1)](*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[2)](*National Engineering Research Center of Information Security, Beijing* 100190)

Abstract As the development of distributed environment such as internet, controlling usage of data after it has been released to a different control domain from its provider's becomes an important security issue. Recently proposed usage control concept and model are suitable for describing this issue but the area of usage control enforcement mechanism has not been fully explored yet. This paper proposes a novel distributed usage control system based on trusted computing technology, which could implement and support all three features of usage control model: abundant policy decision elements, control continuity and mutability of attributes. Experiments show the system enjoys good performance and can be used as an effective solution for usage control enforcement in distributed computing environments.

Keywords trusted computing; usage control; distributed access control; Linux secure module; trusted extended access control markup language

1 引 言

传统访问控制只关注在"服务端"保护数据,而现代分布式环境中出现的新问题要求访问控制的实施范围从"服务端"扩展到"客户端".即使在自己的控制域访问客体,使用者的行为仍然要受到限制.这种扩展的访问控制模型被称为使用控制[1-3],相应的策略被称为使用控制策略.当今多数的使用控制实施系统纯粹依赖于软件,容易被旁路和破坏.相比之下,可信计算技术以硬件为信任根,可以极大增强使用控制实施的可靠性和有效性.目前国内外可信计

收稿日期:2009-07-24;最终修改稿收到日期:2009-09-30.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA01Z412)、国家科技支撑计划项目基金(2008BAH22B06)资助.初晓博,男,1984 年生,博士研究生,主要研究方向为网络与系统安全、可信计算.E-mail: chuxiaobo@is.iscas.ac.cn.秦 宇,男,1979 年生,博士,助理研究员,主要研究方向为网络与信息安全、可信计算.

算标准发展迅速:国际上,可信计算组织(Trusted Computing Group,TCG)于 2003 年推出了可信平台模块(Trusted Platform Module,TPM) 1.2 版规范①;在国内,国家密码管理局于 2007 年出台了国家标准《可信计算密码支撑平台功能与接口规范》②,多家厂商推出了可信密码模块(Trusted Cryptography Module,TCM)及相关产品.

基于可信计算的使用控制实施研究尚处于起步阶段,已有的方案存在以下问题:(1)不能充分支持丰富的使用控制决策因素;(2)控制实施的持续性较差,为敌手的恶意行为留下了时间空隙.针对上述问题,本文给出一种新型的基于可信计算的分布式使用控制系统.其从策略描述语言和实施机制两个层面支持了丰富的使用控制决策因素,并监视用户所有的访问数据的操作,动态检查访问进程和系统环境的可信性,第一时间发现非法访问,为受控文件提供了持续性的保护.实验表明,系统性能良好,可以作为分布式计算环境下的行之有效的使用控制实施方案.此外我们还给出一个新式的使用控制数据分发协议,其不但提供了数据机密性,还最大限度保护了以往工作忽略的数据使用者的平台配置隐私性.

本文第 2 节介绍可信使用控制的相关工作;第 3 节定义系统构架以及威胁模型;第 4 节分数据分发系统和使用控制实施系统两个部分,给出系统框架设计和实现并讨论其如何支持使用控制模型的特性;第 5 节是对原型系统的测试与分析;最后是全文的小结和下一步工作展望.

2 相关工作

基于可信计算的使用控制实施,需要借助于完整性度量、远程证明、密钥认证和安全存储等可信计算机制.度量功能用于收集平台软、硬件配置,远程证明用于向远端报告上述配置.目前研究者已经在国内外规范的基础上给出了大量度量[4-5]和远程证明方案[6-8].特别的,文献[6]给出一种保护平台配置隐私的远程证明协议,其思想也可以用于使用控制场景下的数据分发.密钥认证是 TCM/TPM 提供的简单功能,用于可信平台向对端证明某个自身产生的密钥的信息.安全存储功能提供了封装和配置绑定等机制来保证存储的可靠性.

UCLinux[9]是目前最典型的可信使用控制实施方案,其在通用的 Linux 内核之上部署安全模块[10],提供可信的数据分发和策略实施功能.下载数据前,UCLinux 向数据提供者远程证明自身的可信配置;数据下载后,UCLinux 加密数据,封装加密密钥,并截获访问数据产生的系统调用以检查访问是否满足策略要求.该方案对现有内核的改动小,策略实施系统具备相当的安全性和不可绕过性,但同时存在下述问题:(1) UCLinux 未采用专用的使用控制策略描述语言,不能支持丰富的使用控制决策因素;(2) UCLinux 控制粒度较粗,其采用的加载时度量机制[4]动态性不足,导致控制持续性较差.此外 UCLinux 的数据分发系统以普通远程证明机制为基础,暴露数据使用者平台配置,可能带来配置歧视或攻击. TrustWorthy SELinux[11]是另一个比较典型的方案,其基本原理和优缺点类似于 UCLinux,不同的是其在本地实施控制时采用强制访问控制策略③,且存储时未使用安全存储功能.文献[12]给出了一种使用虚拟机实现可信使用控制的方案,相比 UCLinux 等其安全性和不可绕过性都有较大提高,但实现的难度很大.

文献[13]给出一个基于密钥认证的可信数据分发的协议.相比 UCLinux 的基于远程证明的数据分发方案,该协议不需要数据使用者封装数据加密密钥,因而拥有更高的数据机密性,但是目前包括文献[13]在内的各种使用控制的数据分发方案都无法保障数据使用平台的配置隐私.

3 系统架构

使用控制场景中,数据提供者分发数据及相应的策略,数据使用者下载数据并在本地使用.使用者可能是恶意的,其希望逃避使用控制策略的约束,非法访问、执行或传播数据.我们假设恶意使用者可以使用任意的软件攻击方法,但无硬件攻击能力.

本文给出的系统架构如图 1 所示,主要包括数据分发子系统、使用控制实施子系统以及可信引导和加载时度量两个独立模块.数据分发子系统由可信分发、接受模块以及策略生成、解析模块构成.可信分发和接收模块负责使数据提供者确认对端的可信配置、协商策略格式并安全地传输数据.策略生成

① Trusted Computing Group. http://www.trustedcomputing.org

② OSCCA. Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing. http://www.oscca.gov.cn/Doc/6/News_1132.htm

③ Security-Enhanced Linux. http://www.nsa.gov/selinux/

和解析模块支持策略协商，转换策略格式. 控制实施子系统由安全存储模块、策略判定模块和动态度量模块构成. 安全存储模块向可信接收模块提供封装接口、加密存储数据以及检查数据与策略的完整性. 策略判决模块决策是否允许对文件的访问. 策略判决时可能需要度量访问文件的进程，该功能由动态度量模块完成. 可信引导和加载时度量模块配合完成认证启动，前者在系统启动时将信任链从底层扩展至操作系统，后者在系统启动后度量和报告平台运行的所有程序，将信任链进一步扩展至应用层程序. 认证启动是保证系统安全、进行远程证明的基础.

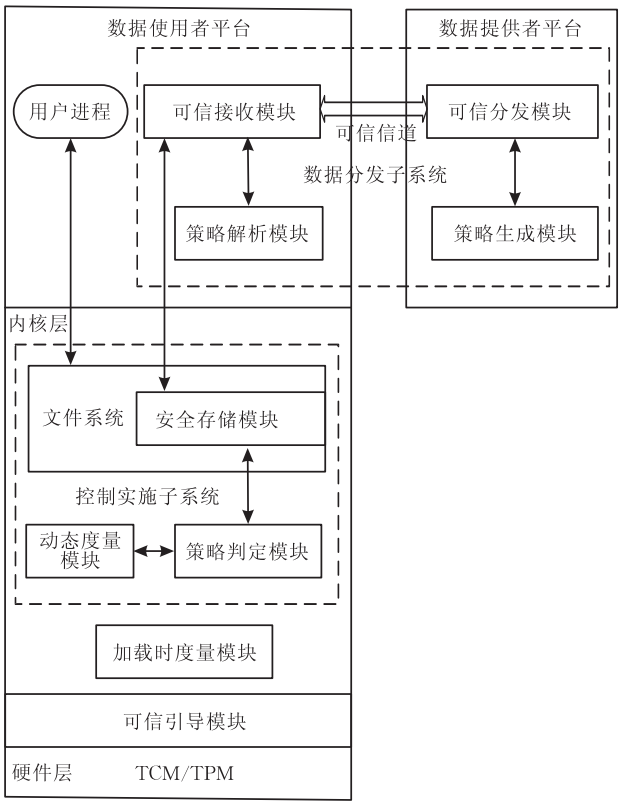

图 1　系统架构

4　系统设计与实现

4.1　数据分发子系统

4.1.1　工作流程

如图 2 所示，一次完整的数据分发过程分为 10 个步骤：

1. 可信接收模块发送下载数据请求；

2. 可信分发模块发送挑战随机数，用于保证会话的新鲜性；

3. 可信接收模块进行远程证明；

4. 双方协商使用控制策略格式以及加密数据使用的密钥(可能包含多轮交互)；

5. 可信分发模块调用策略生成模块，根据协商要求生成策略；

6. 策略生成模块返回策略；

7. 可信分发模块使用协商好的密钥传输数据及策略；

8. 可信接收模块请求解析策略；

9. 策略解析模块返回适用于本机平台的策略描述；

10. 可信接收模块调用安全存储模块，将数据文件及其策略存储于本地设备.

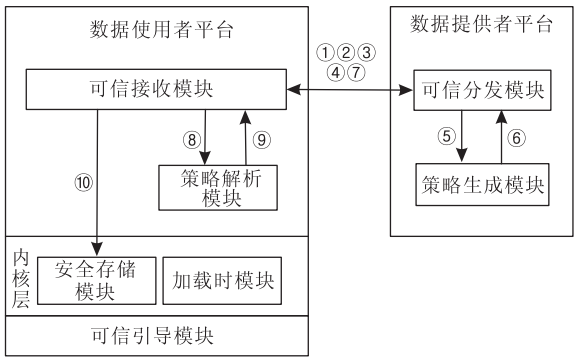

图 2　数据分发子系统架构

4.1.2　系统实现

4.1.2.1　策略生成和解析模块

我们采用可信扩展访问控制标记语言 TXACML[14] 来描述和交互使用控制策略. TXACML 扩展自 XACML，易于构建和解析，互操作和通用性强. 而且相比以往工作[9,11] 的相关部分，TXACML 支持的使用控制因素更加丰富，不但可以描述用户标识和角色等传统访问控制信息，还支持使用控制场景常见的环境条件、系统义务以及使用时间、次数限制等. 具体地，本文系统的策略主要由以下内容构成：

(1) 进程属性. 作为主体的进程的属性，例如进程标识和合法进程的标准度量值；

(2) 用户属性. 作为主体的用户属性，例如用户标识、角色和权限等；

(3) 资源属性. 作为客体的文件资源属性，例如文件名和标准度量值等；

(4) 策略管理. 可用于更新的使用控制信息，例如使用时间限制、次数限制和目的限制等；

(5) 环境属性. 访问发生时应满足的环境条件，例如操作系统、杀毒软件和防火墙版本等.

TXACML 描述的使用控制策略示例如图 3 所示.

```
〈TXACML version="1.0" encoding="UTF-8"?〉
〈Policy PolicyId= Rule Combining AlgId="Deny-Overrides"〉
〈Rule RuleId="Rule01" Effect="Permit"〉
〈Target〉
〈Subject〉
 〈Subject MatchId =
        "urn:oasis:names:tc:xacml:1.0:function: MatchTP"〉
  〈Attribute Value DataType="SecAttrPlatform Type"〉
  ……
  〈/Attribute Value〉
  〈Subject Attribute Designator
  AttributeId="urn:oasis:names:tc:xacml:1.0:environment:"
  DataType=" "/〉
 〈/Subject Match〉
〈/Subject〉
〈Resource〉
〈Resource MatchId=
        "urn:oasis:names:tc:xacml:1.0:function: MatchTP"〉
〈Attribute Value DataType=" "〉
……
〈/Attribute Value〉
〈Resource Attribute Designator
AttributeId="urn:oasis:names:tc:xacml:1.0:Resource:"
DataType=" "/〉
〈/Resource Match〉
〈/Resource〉
〈/Target〉
```

图 3 使用控制策略示例

策略必须与数据绑定才能发挥作用. 类似于文献[9]方案,我们将策略存储于 Linux 文件扩展属性中,利用文件与其扩展属性的天然绑定性实现了数据与其策略的绑定. 可信接收模块在接收到数据和策略后,将数据及策略分别存储于文件及其扩展属性中. 用户进程查询和修改策略时,只需要针对数据文件的扩展属性执行操作即可. 由于文件与扩展属性的绑定是纯粹的操作系统功能,故这种绑定方式与应用程序无关.

4.1.2.2 可信分发和接收模块

可信分发和接收模块最重要的工作是进行远程证明,而远程证明又以认证启动为基础. 我们在普通的操作系统加载器的基础上增加信任链建立、报告功能,开发了可信配置的可信引导系统 LoisGrub[15]. 平台系统启动时,主引导记录(MBR)和操作系统内核文件等被依次度量,结果被扩展至 TCM/TPM 的平台配置寄存器(PCR)中. 系统启动后,处于内核层的加载时度量模块将度量和报告所有加载入内存的可执行文件以及动态库等. 系统远程证明采用简明的证明身份密钥(AIK)方式进行,证明内容是系统启动后所有影响系统状态的软、硬件情况,即 LoisGrub 和加载时度量模块的度量结果.

为了保证图 2 所示的步①~④和步⑦交互的安全,我们采用安全传输层协议 TLS v1.0① 为消息提供机密性和完整性保护. TLS 是一种成熟的被广泛采纳的互联网安全通信标准,可提高系统的在不同平台和环境下的通用性.

4.1.3 保护配置隐私的新型数据分发协议

数据分发子系统的步①~④和步⑦实现了一个简单的数据分发协议,其思路直观、实现简便、效率较高,但是也存在暴露数据使用者配置隐私的问题. 本节非常简要地给出另一种能够保护数据使用者配置隐私的新型数据分发协议. 此协议需要 TCM/TPM 增加新功能(认证密钥承诺,协议中抽象化为命令 TCM_CertifyKeyCommitment)而暂时未实现,但其通过保护隐私有效解决了配置歧视和针对特定配置的攻击等现实且愈发突出的安全问题,目前的 TCM/TPM 已具备增加新功能所需的全部运算模块,因而不久的将来实现该协议是必要和可行的.

由于着重考虑配置隐私保护问题,我们假设协议的传输内容(例如数据加密密钥,下文中的 K)的机密性和认证性已经由安全信道进行保护,安全信道可以使用上文所述的 TLS 等成熟技术实现. 另外,该协议不区分数据和相应的策略,统一将其作为数据进行传输,具体的策略解析以及策略绑定等工作由数据使用者接收到数据后完成.

4.1.3.1 协议流程

假设数据提供者和使用者已经事先协商好可信平台配置集合 $PC=\{pc_1, pc_2, \cdots, pc_N\}$,数据分发协议一方面要保证只有处于可信配置的使用者平台才能够访问数据,另一方面应确保协议结束后,提供者确信使用者平台的配置 $pc_{\mathrm{DU}} \in PC$,但却不清楚 pc_{DU} 的具体配置.

类似于文献[13],该协议采用密钥认证而非常规的远程证明方式确保访问发生时数据使用者平台的可信配置,进而保证数据的机密性. 密钥认证通过 TCM/TPM 签署的密钥信息承诺[16] 以及使用者平台签署的环签名[17] 完成,不会暴露具体配置. 具体的环签名方案、承诺方案以及其配合使用分别借鉴了文献[6,16-17].

协议准备. 数据使用者 DU 与数据提供者 DP 协商一个可信配置集 PC,选定一系列的密码学参数,包括大素数 P、P 上的一个 Q 阶子群的生成元 h 和子群的成员 g,并保持 g 的阶的机密性. DU 使用 TCM 生成用于加密的、不可迁移且与某配置 $pc_{\mathrm{DU}} \in PC$ 绑定的密钥 K. 由此,密钥的信息记为 $KI_{\mathrm{DU}}=$

① The TLS protocol: Version 1.0. http://www.ietf.org/rfc/rfc2246.txt

$\{K, ES\_SM2, non\text{-}migrabtable, pc_{DU}\}$. KI 中 K 表示密钥明文，即如果加密密钥是对称的，则 K 为密钥值，如果加密密钥是非对称的，则 K 为公钥值；EM_SM2 和 $non\text{-}migrabtable$ 是两个抽象标记，表征密钥的用途和迁移情况.

协议流程.

1. DU 请求下载数据 D；

2、3. DP 发送挑战随机数 N_{DP}；DU 以 N_{DP} 和加密密钥 K 的句柄(依 TCM 规范习惯，使用密钥之前必须加载该密钥，使用时以句柄指代该密钥)为参数，调用新命令 $TCM\_CertifyKeyCommitment$，请求 TCM 对密钥信息 KI_{DU} 进行认证；

4、5. TCM 选择承诺密钥为 r、计算密钥信息的承诺 C 以及对该承诺进行签名 σ_{TCM}，最后返回 C、σ_{TCM} 和 r；

6、7. DU 根据密钥 K 和可信平台配置集 PC，计算 n 个密钥配置信息 KI_i；再根据 KI_i 计算 $y_i (i=1,2,\cdots,n)$，并以 $y_i (i=1,2,\cdots,n)$ 和其它密码学参数为公钥，承诺密钥 r 为私钥，计算对 N_{DP} 的环签名. 最后发送 K、ES_SM2、$non\text{-}migratable$、C、σ_{TCM} 和 σ_{DU}.

7、8. DP 先验证 TCM 对承诺的签名，再以和 DU 同样的方式计算环签名公钥并验证环签名；如果全部都能通过则以 K 加密数据发送给 DU.

1		DU	⟶ DP	$Request\ Data\ D$
2		DU	⟵ DP	N_{DP}
3	TCM ⟵	DU		$TCM\_CertifyKeyCommitment(N_{DP}, H_K)$
4	TCM			$r \in Z_Q^*, C = g^{KI_{DU}} h^r \bmod P, \sigma_{TCM} = Sign_{TCM}(SK_{TCM}, (C, N_{DP}))$
5	TCM ⟶	DU		$C, \sigma_{TCM}, r;$
6		DU		根据K与PC,得到$KI_i = \{K, ES_SM2, non\text{-}migratable, pc_i\}$ $y_i = C/g^{KI_i} \bmod P (i=1,2,...,n)$ $\sigma_{DP} = RingSign(r, \{y_i\}, N_{DP})$
7		DU	⟶ DP	$K, ES\_SM2, non\text{-}migratable, C, \sigma_{TCM}, \sigma_{DU};$
8			DP	$Ver_{TCM}(PK_{ID}, \sigma_{TCM}, (C, N_{DP}))$ 根据K与PC,得到$KI_i = \{K, ES_SM2, non\text{-}migratable, pc_i\}$ $y_i = C/g^{KI_i} \bmod P (i=1,2,...,n)$ $Ver_{RING}(\{y_i\}, \sigma_{DU}, N_{DP})$
		DU	⟵ DP	$Enc(K, D)$

图 4　数据分发协议

协议执行后提供者对使用者平台配置的信心源自于两点：(1) TCM/TPM 的签名确保了 TCM/TPM 确实刚刚签署了有关密钥信息的承诺，(2) 环签名确保了承诺确实可以表达为 $C_m = g^m h^r \bmod P$ 的形式，其中 $m = KI_{DU}$，而且伪造这样一个签名是困难的.

在该方案中，数据离开数据提供者控制域后始终处于密钥保护之下，且只有处于可信配置的数据使用者平台才能使用密钥解密. 如果密钥认证机制和加密算法可靠，则数据机密性得到保证. 平台配置的隐私性，由上述协议的步 2～8 保证.

4.1.3.2　安全性分析

数据分发协议的目标是保证数据机密性和使用者平台配置的隐私性，故我们分别对这两种安全性质进行讨论.

数据机密性分析. 恶意的数据使用者 A 希望破坏数据机密性，即在不安全的平台配置下访问受控数据. 这只能发生在 A 生成了密钥 K 并使数据提供者相信 K 与某可信状态 $pc_{DU} \in PC$ 绑定，但 K 实际绑定的是 $pc_{NT} \notin PC$. 类似于文献[6]，我们采用游戏序列的方法①，证明敌手在各游戏中获胜的概率之差均为可忽略量，进而证明破坏数据机密性是困难的. 在游戏序列当中，$Game_0$ 为基本游戏，表征证明目标，各游戏 $Game_{i+1}$ 是对 $Game_i$ 的变型. 与 A 交互的是代表协议诚实参与方(数据提供者)模拟器 S，每个游戏中都会引入一个“失败事件”F，如果在 $Game_{i+1}$ 中发生 F，则 S 退出游戏，A 攻击失败；如果不发生 F，$Game_i$ 和 $Game_{i+1}$ 将永远一致的运行下去，即事件 $(Win_i \wedge \neg F)$ 和 $(Win_{i+1} \wedge \neg F)$ 等价(其中 Win_i 表示 A 赢得 $Game_i$ 的事件)，进而可推出 $|Pr[Win_{i+1}] - Pr[Win_i]| \leq Pr[F]$. 具体证明过程如下：

$Game_0$. A 生成密钥 K，K 实际绑定的配置为 $pc_{NT} \notin PC$，但敌手成功地使 S 相信，K 是与某可信状态 $pc_{DU} \in PC$ 绑定的，即 A 向 S 提供的承诺和签名三元组(C，σ_{TCM} 和 σ_{RING})经过了 S 的验证. 记 A 在 $Game_0$(也即破坏数据机密性的活动中)成功的概率

① Shoup V. Sequences of games: A tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. http://eprint.iacr.org/2004/332

为 $Pr[Win_0]$.

$Game_1$.$Game_1$ 与 $Game_0$ 基本相同,唯一的区别在于:S 刻意记录了已经使用过的挑战随机数 N_{DP},如果某次协议运行时随机选择得到的 N_{DP} 为已经使用过的随机数,S 就立即中断游戏.这种情况下,"失败事件" F_{NONCE} 定义为发生随机数碰撞,事件 $(Win_1 \wedge \neg F_{NONCE})$ 和 $(Win_0 \wedge \neg F_{NONCE})$ 等价,因而根据概率差异引理(即游戏序列的方法)有如下结论:

$$|Pr[Win_0]-Pr[Win_1]| \leq Pr[F_{NONCE}] \quad (1)$$

$Game_2$.$Game_2$ 与 $Game_1$ 基本相同,唯一的区别在于:S 拥有一个 TCM 签名 Oracle 来获取当前协议运行时 TCM 给出的真实签名(不管 A 是否实际请求 TCM 进行签名,我们假设 TCM 在每次协议运行时都对 A 要证明的密钥 K 的信息产生了签名,并将签名值报告给 Oracle),同时 S 也从 A 处获取 TCM 签名,一旦发现两个签名不符(即 A 伪造了 TCM 签名)则立即中断游戏."失败事件" F_{TCM} 定义为 A 成功伪造 TCM 签名,类似于 $Game_1$,有如下结论:

$$|Pr[Win_1]-Pr[Win_2]| \leq Pr[F_{TCM}] \quad (2)$$

$Game_3$.$Game_3$ 与 $Game_2$ 基本相同,唯一的区别在于:S 拥有一个敌手信息告知 Oracle,每次运行协议时数据提供者都能从该 Oracle 获知 A 是否真的知道对应于某个环签名公钥 y_i 的私钥 r_i,一旦发现 A 并不知道(即 A 无签名私钥的情况下伪造了环签名),则立即中断游戏."失败事件" F_{RING} 定义为无签名私钥的情况下成功伪造环签名.类似于 $Game_2$,我们给出如下结论:

$$|Pr[Win_2]-Pr[Win_3]| \leq Pr[F_{RING}] \quad (3)$$

如果 A 能够赢得 $Game_3$,则说明其面对新鲜的随机数挑战,既未伪造 TCM 签名,又未(在无环签名私钥的情况)伪造环签名.因此,为了给出能够通过 S 验证的环签名,A 必然设法拥有了对应于某个配置 $pc_i \in PC$ 的承诺密钥 s,使得 $g^{PS_i} h^S = C = g^{PS_{DU}} h^r$,因而有 $LOG_h(g)=(pc_i-pc_{UI})/(s-r)$,即 A 可成功求解出协议中 g 关于 h 的离散对数.因此,有如下结论:

$$Pr[Win_3] \leq Pr[F_{DLOG}] \quad (4)$$

其中 F_{DLOG} 表示求解 h 关于 g 的离散对数成功的概率.

根据式(1)~(4),我们可以得出结论:

$$Pr[Win_0] \leq Pr[F_{DLOG}]+Pr[F_{NONCE}]+Pr[F_{TCM}]+Pr[F_{RING}].$$

根据安全假设,上述不等式右方的 4 个概率均为关于安全参数的可忽略量,因而概率多项式敌手破坏数据机密性是困难的.值得注意的是,虽然目前所有证明均在标准模型下完成,但是环签名的安全性证明在随机预言模型下完成,因而我们的证明结论也仅在随机预言模型下成立.

配置隐私性分析. 恶意的数据提供者 A 希望获知数据使用者的平台配置.类似于文献[6],我们采用反证的方法:使用模拟器 S 来模拟诚实的协议参与方与 A 交互,并证明如果 A 破坏了协议的配置隐私性,则 S 可以破坏协议中的承诺方案的完美隐藏性[16]或者环签名方案的签名者模糊性[17].记 S 和 A 交互构成的游戏为 $Game_{PRIV}$,在两种情况下分别进行此游戏.

$Game_{PRIV}1$. 假设环签名方案具有无条件签名者模糊性[17].S 在 $Game_{PRIV}1$ 中模拟数据使用者,其得到一次协议运行中的对密钥信息的承诺 C,试图获取 C 对应的被承诺值 KI_{DU}(其中配置部分 $pc_{DU} \in PC$)、承诺密钥 r 以及 TCM 的签名 σ_{TCM}.如果 S 拥有无限计算能力,则可以计算出协议中 g 相对于 h 的离散对数 α,并给出 l 满足 $C=h^l=g^{CS_i+\alpha S_i}$,$S_i(i=1,2,\cdots,n,n$ 为 PC 集合包含的元素个数),其中任意 $S_i(i=1,2,\cdots,n)$ 均可作为环签名私钥,因而 S 可以给出相应的环签名 σ_{RING}.由此,S 根据承诺 C(虽然不清楚被承诺值和承诺密钥)给出了完整的、可通过验证的证明三元组 $(C,\sigma_{TCM},\sigma_{RING})$.敌手 A 得到该三元组后,输出索引值 i,表示断定 TCM 承诺和签名的密钥信息中包含的是配置 pc_i. S 也给出和 A 同样的输出.如果 A 可以破坏配置隐私性,即 $Adv=|Pr[i=DU]-1/n|$ 为不可忽略量,S 就同样以不可忽略的概率猜测出平台配置的情况.在已经假设环签名方案具有无条件签名者模糊性的情况下,这相当于破坏了承诺方案的完美隐藏性.

$Game_{PRIV}2$. 假设承诺方案具有完美的隐藏性[16].在 $Game_{PRIV}2$ 中 S 拥有环签名 Oracle,可对任何消息签名.不同于 $Game_{PRIV}2$,S 在 $Game_{PRIV}1$ 中除了模拟数据使用者外还模拟 TCM,因此它自己随机选择 l,并给出承诺 $C=g^l$ 以及相关签名 σ_{TCM},然后 S 请求环签名 Oracle 给出 σ_{RING}.敌手 A 接收到证明三元组后,输出索引值 i,表示断定 TCM 承诺和签名的密钥信息中包含的是配置 pc_i.S 也给出和 A 同样的输出.如果 A 可以破坏配置隐私性,即 Adv 为不可忽略量,S 就同样以不可忽略的概率猜测出平台配置的情况.在已经假设承诺方案具有完美隐藏性的情况下,这相当于破坏了环签名机制的

签名者模糊性.

4.2　控制实施子系统

4.2.1　工作流程

如前所述，控制实施子系统开始运行前，数据及相应的策略已经加密存储于本地存储器，加密密钥封装于可信配置. 当用户进程试图访问数据时，控制实施子系统将执行以下工作流程，如图 5 所示：

1. 用户进程发起数据访问请求，该请求被内嵌于文件系统的安全存储模块截获；

2. 安全存储模块调用策略判决模块，判断此次访问请求是否符合与数据关联的使用控制策略；

3. 如果策略规定了进程状态、环境因素等需要动态度量模块执行的内容，则策略判决模块将调用动态度量模块，对用户进程进行完整性状态度量；

4. 动态度量模块将返回度量结果；

5. 策略判决模块根据动态度量结果以及其他信息（例如环境因素、用户角色），进行请求判定并返回结果；

6. 如果允许访问，安全存储模块调用 TCM/TPM 解封密钥（解封时平台的状态必须与密钥封装绑定的状态一致）并解密数据. 如果拒绝访问，则返回出错信息给用户进程.

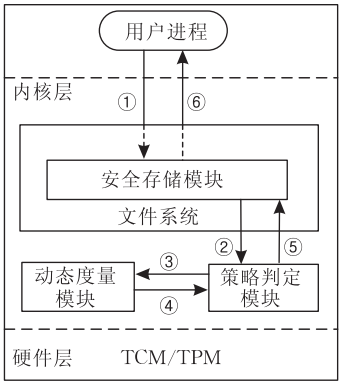

图 5　控制实施子系统架构

4.2.2　系统实现

4.2.2.1　安全存储模块

我们以修改 Linux 内核函数的方式实现安全存储系统. 具体地，为读写文件及其扩展属性的 Linux 虚拟文件系统函数（包括 *vfs_write*()、*vfs_read*()、*vfs__setxattr*() 和 *vfs_getxattr*()）增加加解密和完整性检查功能. 加解密算法是速度快、使用灵活的流密码体制. 数据和策略的完整性标准值存储于数据文件的扩展属性项，除非主体是特定进程，否则所有修改标准值的操作都将被拦截. 此外安全存储模块包装了 TCM/TPM 的封装功能，支持可信接收模块封装密钥. 封装功能置于内核层而不是由可信接收模块在应用层直接完成，提高了系统的安全和可靠性.

4.2.2.2　策略判决模块

策略判决模块以 Linux 内核模块的方式实现并为安全存储模块调用. 具体地，我们利用 Linux 安全模块（LSM）[10] 技术安插在 *vfs_write*()、*vfs_read*()、*vfs__setxattr*() 和 *vfs_getxattr*() 中钩子函数，包括 *inode_permission*()，*file_permission*()，*inode_setxattr*() 和 *inode_removexattr*()，来截获文件打开、读文件、写文件、写扩展属性和移除扩展属性的请求，同时调用策略判决模块. 策略判决模块首先根据文件的扩展属性判定当前处理的是否为本文系统所控制的文件，所有该类文件的扩展属性都将以字符串“*linux.tcwg.tuc*”进行标记；然后调用动态度量模块获取访问文件的用户进程的状态；最后结合其它环境、时间限制和使用次数限制等信息给出策略判决结果. 需要注意的是，目前我们只允许特定进程操作扩展属性，进程的杂凑值是判决扩展属性操作请求的唯一条件.

4.2.2.3　动态度量模块

动态度量模块以 Linux 内核模块的方式实现. 其度量的对象既可为应用层进程，也可以是系统内核. 对象为应用层进程时，度量模块首先解析进程名称，获取其在内存中的程序段等各段信息；然后将段的线性地址转换为物理地址，并将该进程的段内容映射至度量模块自己的地址空间；最后使用 TCM/TPM 对段内容进行杂凑计算和签名. 我们没有度量进程的数据段，因为该段会在进程生命期内变化而很难确定标准值. 对象为内核模块时，需要先确定包含了模块重要信息的名为 Module 的结构体的情况，后续步骤与度量普通进程时相同. 动态度量模块本身的安全性依赖于两点：一是基于 TCM/TPM 的认证启动对包含动态度量模块的内核进行的检验，二是操作系统自身的安全性. 由于结合了软、硬件度量方式的优点，动态度量既具有较好的安全性，同时实现较简单，易用性和扩展性较强.

4.3　讨　论

下面我们说明本文系统如何支持和实现了使用控制模型的 3 个特点：丰富的决策因素、控制的连续性以及主客体属性的变异性，并讨论提高使用控制系统效力的一些考虑.

我们采用的策略语言 TXACML 不但能描述用户角色等传统访问控制因素，还可表达用控制场景常见的环境条件、系统义务以及使用时间、次数限制等. 同时，策略判定模块和动态度量模块可以随时获取系统环境状态，忠实实施策略. 如此本文系统在策

略和实施机制两个层次均支持了使用控制模型的第1个特点:丰富的决策因素.通过钩子函数,我们截获了与使用文件有关的请求,包括打开文件、读写文件、设置扩展属性和删除扩展属性,用户对文件的任意操作都受到使用控制系统的监控.策略判决的粒度从传统的以访问会话为单位,细化至以原子操作为单位,任意不符合策略规定的文件使用都将在第一时间被发现.如此本文系统实现了连续控制.我们将主客体属性(例如可以播放特定音乐文件的次数)作为策略的一部分存入数据文件的扩展属性中,并允许特定的进程对其进行修改(例如播放一次音乐文件后,用户剩余播放次数减1),实现了主客体属性的变异性.

为了防范数据使用者的行为,除了检查策略涉及的、与访问直接相关的因素,还必须监视策略未涉及的数据使用者所在平台的运行状况,限制可能带来攻击的用户权限.如果忽略上述第2点,恶意的使用者(特别是拥有不受限权力的系统管理员)可能通过非常规的手段直接绕开策略实施机构.例如某用户首先正常访问数据,然后复制内存中的已经解密的数据明文,就可以得到不受控的数据副本,设置在系统调用处的策略实施机构将无能为力.虽然根本上杜绝上述情况必须限制系统用户能力(UCLinux就严格限制了管理员可以开启的程序的范围),但这种办法必将极大降低系统可用性,在当前条件下不具备可行性.本文系统并未显式限制管理员(事实上我们尽量避免使用控制系统影响平台整体的使用感受),而是采用认证启动、启动后的加载时度量以及将密钥封装至特定平台状态的方式对平台运行状态进行监视,一定程度上限制了用户的恶意行为,在系统可用性和安全性的权衡中倾向了前者.

5 性能测试及分析

根据以上系统设计,我们初步实现了基于可信计算的分布式使用控制系统,并对系统的控制实施子系统的性能进行了测试.实验环境(数据使用者平台配置)为Intel P4 3.2GHz CPU;1GB内存;Ubuntu7.10发行版操作系统,自行编译Linux2.6.20内核.实验场景为:文档(.txt格式)的使用次数受到限制,用户进程访问文档时控制系统对文件的剩余可访问次数进行检查.这是对数字版权管理和隐私保护领域中典型应用的模拟.

图6[18]展示了上述场景下,读取受控文件的时间增量(相比正常系统相同操作的运行时间)与文件大小的关系.实验结果表明,文件较小时访问时间增量/文件大小约为4.5ms/M,文件逐渐增大时单位时间增量有所减小.由于控制系统被调用次数基本正比于文件操作的系统调用的执行次数,而后者与文件大小存在近似线性关系,故时间增量与文件大小存在图示的增长关系.从实验可知,在典型场景的控制系统性能处于用户可接受的范围内.

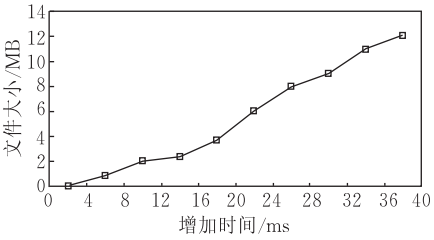

图6 读取受控文件性能

6 结束语

针对分布式环境中日益突出的使用控制问题,本文给出一种基于可信计算技术的使用控制实施系统.可以有效支持使用控制模型的特性.实验证明,本文系统性能良好,可以作为一种通用的使用控制实施解决方案.此外,我们给出一个新式的数据分发协议,可以同时兼顾数据机密性和平台配置的隐私性,解决了以往方案暴露平台配置而带来攻击或配置歧视的问题.

未来的工作主要集中于以下几个方面:(1)进一步完善现有系统,提高文件操作性能;(2)尝试限制系统管理员的部分权限,如直接拷贝内存页中数据,防止其利用正常的系统功能偷窥数据;(3)研究新的策略实施构架,例如将实施结构置入虚拟机监控层,在方案设计层面获得更高的自我保护和不可绕过性;(4)研究更加完善的策略描述语言,支持更加丰富的使用控制需求.

致 谢 感谢信息安全国家重点实验室的汪丹、周玲丽在可信接收和分发模块,聂晓伟在策略生成和解析模块以及实验部分,李昊在安全存储模块,于爱民在策略判定模块,胡浩、刘孜文在动态度量和加载时度量模块的工作!

参 考 文 献

[1] Park J, Sandhu R. The UCONABC usage control model. ACM Transactions on Information and System Security,

2004，7(1)：128-174

[2] Hilty M，Pretschner A，Basin D，Schaefer D，Walter T. A policy language for distributed usage control//Proceedings of the European Symposium on Research in Computer Security (ESORICS). Dresden，2007：531-546

[3] Pretschner A，Hilty M，Basin D. Distributed usage control. Communications of the ACM，2006，49(9)：39-44

[4] Sailer R，Zhange X L，Jaeger T，Doorn L V. Design and implementation of a TCG-based integrity measurement architecture//Proceedings of the 13th USENIX Security Symposium. San Diego，2004：223-238

[5] Jaeger T，Sailer R，Shankar U. PRIMA：Policy-reduced integrity measurement architecture//Proceedings of the 11th ACM Symposium on Access Control Models and Technologies (SACMAT). Lake Tahoe，2006：19-28

[6] Chen L Q，Lohr H，Manulis M，Sadeghi A R. Property-based attestation without a trusted third party//Proceedings of the Information Security Conference (ISC). Taipei，China，2008：31-46

[7] Brickell E，Camenisch J，Chen L Q. Direct anonymous attestation//Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004). Washington. D. C.，2004：132-145

[8] Chen L，Landfermann R，Lohr H，Rohe M，Sadeghi A，Stuble C. A protocol for property-based attestation//Proceedings of the 2006 ACM Workshop on Scalable Trusted Computing (STC)，Alexandria，2006：7-16

[9] Kyle D，Brustoloni J C. UCLinux：A Linux security module for trusted-computing-based usage controls enforcement//Proceedings of the 2007 ACM Workshop on Scalable Trusted Computing (STC). Alexandria，2007：63-70

[10] Wright C，Cowan C，Smalley S，Morris J，Hartman G K. Linux security modules：General security support for the Linux kernel//Proceedings of the 11th USENIX Security Symposium. Berkeley，2002：17-31

[11] Alam M，Seifert M P，Li Q，Zhang X W. Usage control platformization via trustworthy SELinux//Proceedings of the 2008 ACM Symposium on Information，Computer and Communications Security (ASIACCS). Tokyo，2008：245-248

[12] Berthold A，Alam M，Breu R，Hafner M，Pretschner A，Seifert J P，Zhang X W. A technical architecture for enforcing usage control requirements in service-oriented architectures//Proceedings of the 2007 ACM Workshop on Secure Web Services. Alexandria，2007：18-25

[13] Sevin P E，Strasser M，Basin D. Securing the distribution and storage of secrets with trusted platform modules//Proceedings of the Workshop in Information Security Theory and Practices (WISTP). Heraklion，2007：53-66

[14] Nie Xiao-Wei，Feng Deng-Guo. TXACML—An access control policy architecture based on trusted platform. Journal of Computer Research and Development，2008，45(10)：1676-1686(in Chinese)
(聂晓伟，冯登国. TXACML——基于可信平台的一种访问控制策略框架. 计算机研究与发展，2008，45(10)：1676-1686)

[15] Xu Zhen，Shen Li-Hong，Wang Dan. LOIS Grub：A configurable trusted booting system. Journal of the Graduate School of the Chinese Academy of Sciences，2008，25(5)：626-630(in Chinese)
(徐震，沈丽红，汪丹. 一种可配置的可信引导系统. 中国科学院研究生院学报，2008，25(5)：626-630)

[16] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing//Proceedings of the International Cryptology Conference (CRYPTO). Santa Barbara，1991：129-140

[17] Abe M，Ohkubo M，Suzuki K. 1-out-of-n signatures from a variety of keys//Proceedings of the Annual International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT). Queenstown，2002：415-432

[18] Nie Xiao-Wei. A study of access control based on trusted platform[Ph. D. dissertation]. Graduate University of Chinese Academy of Sciences，Beijing，2009(in Chinese)
(聂晓伟. 可信平台访问控制研究[博士学位论文]. 中国科学院研究生院，北京，2009)

CHU Xiao-Bo，born in 1984，Ph. D. candidate. His research interests include network and system security and trusted computing.

QIN Yu，born in 1979，Ph. D.，associate researcher. His research interests include network and system security and trusted computing.

Background

This work is supported by the National High-Tech Research and Development Plan of China under grant No. 2007AA01Z412 and National Science & Technology Pillar Program of China under grant No. 2008BAH22B06.

The subject focused on in this paper is how to implement a practical usage control system using trusted computing technology. So the work extends across both the access control and trusted computing research area. Usage control, which is an extension of traditional access control, is an emerging security issue that has not been fully addressed yet. Though this concept has been proposed for several years, most researches are still limited to describing concept and abstracting usage control model. Implementations of usage control system, especially those enjoy good performance and security properties, are still rare. Traditional digital right management (DRM) systems in multimedia industry and some privacy protection systems using for medical purpose can be seen as usage control system. But all these systems suffer from an essential problem that they usually based on pure software, including operating system and some system software etc, which means software attacks on these systems can always successful in theory. It is just this problem that lags the forward step of usage control research and research on usage control implementation has reached its bottleneck yet. Unlike traditional implementation technology, trusted computing employs the virtue that all security assertions and trust relationships are based on hardware among which trusted platform module (TPM) or trusted cryptography module (TCM) plays a key role. TPM or TCM act like a supervisor who monitors data users' actions and cannot be easily tampered. This feature provides so effective means to resist common malicious behavior that the system security can be greatly enhanced. Specifically, in this paper the authors examine what trusted computing technology can brings to usage control. Though previous work has posited potential application of trusted computing on usage control, they do not halt on that point, namely try the best to support features of usage control. Another fundamental factor that differentiates their work with previous is that the practicability and performance of system have been attached much importance on.