CSCW 系统访问控制模型及其基于可信计算技术的实现*)

张志勇[1,3] 杨 林[2,1] 马建峰[1] 普杰信[3]
(西安电子科技大学 教育部计算机网络与信息安全重点实验室 西安 710071)[1]
(中国人民解放军总参谋部第61研究所 信息安全研究室 北京 100039)[2]
(河南科技大学 电子信息工程学院 洛阳 471003)[3]

摘 要 现有的CSCW访问控制策略模型缺少时间和约束特性,在实现上也未能较好地解决开放网络下的身份伪装和欺骗问题,以及影响安全策略完整性实施的软硬件平台可信问题。本文基于角色-活动概念提出了一种具有时间依赖和约束特征的CSCW访问控制模型Fine-grained Access Control for CSCW,从而能够定义更为精确细致的安全策略;在模型实现中给出了Trusted Computing-enabled Access Control架构以及关键的策略分发和实施协议等。该方法通过建立完整的协作实体-CSCW平台-应用信任链,构建了可信的访问控制平台,增强了协作实体的身份鉴别,并通过角色相关策略的分发和在本地协作站点上的完整性实施,减轻了服务器端集中式执行安全策略的负担。

关键词 CSCW,访问控制,可信计算,TPM,策略分发

Access Control Model for CSCW System and Implementation Based on Trusted Computing Technology

ZHANG Zhi-Yong[1,3] YANG Lin[2,1] MA Jian-Feng[1] PU Jie-Xin[3]
(Computer Network and Information Security Lab. of M. O. E, Xidian University, Xi' an 710071)[1]
(Information Security Laboratory, No. 61 Research Institute of General Staff of PLA, Beijing 100039)[2]
(Electron. Inf. Eng. Coll., Henan Univ. of Sci. & Technol., Luoyang 471003)[3]

Abstract Access control policies and models available lack of temporal characteristic, and do not well solve the question of identity disguise and cheat in open network, as well as platform trustworthy question effecting on security policies integrity enforcement. This paper presented an role-activity-based access control with time-dependent and constraints features for CSCW, called as Fine-grained Access Control for CSCW, which could define more precise security policies; Trusted Computing-enabled Access Control architecture and key policies dissemination and enforcement protocols are addressed. The method constructs CSCW trustworthy access control platform and strengthens cooperative entity identification, through creating integrated cooperative entity-CSCW platform-application trustworthy chain, as well as easing centralized policy server using partial related policies distribution and integrity enforcement in local workstation.

Keywords Computer supported cooperative work, Access control, Trusted computing, Trusted platform module, Policy dissemination

1 引言

近20年来,伴随着信息技术的进展,涌现出大量面向大规模计算机网络(网格)环境的应用,如e-commence、e-business、e-government、移动计算、普适计算、音频视频等电子数据的共享,以及企事业基于业务的Intranet构建等,使得整个互联网络得到了空前的广泛应用。由此而产生的计算环境的安全问题也面临着严峻的考验,嗅探、窃听、身份冒充、分布式拒绝服务攻击等手段以及Trojan horse、蠕虫病毒、恶意程序的入侵,致使敏感的数据信息被窃取、篡改和滥用,系统安全遭受到严重的威胁。传统的安全解决方案如防火墙、入侵检测、防病毒软件等在一定程度上减少了上述不安全隐患,但并未从根本上解决系统安全问题。可信计算(Trusted Computing,或者Trustworthy Computing)技术作为全新的安全解决方案在资源共享[1]、DRM[9]、Peer-to-Peer网络[2]等方面近年来得到了研究者的广泛关注和应用。

CSCW(Computer Supported Cooperative Work)旨在基于分布式网络环境或开放式协作环境[3]实现多用户间的协同处理和资源共享等基本任务,典型的应用环境诸如协同指挥与决策、工作流处理、协同编辑、协同设计与制造等。目前CSCW平台也同样面临着安全性隐患,这里的安全问题主要指来自计算环境内部的资源窃取与来自于外部的敌意攻击。在这种情形下,协作者之间如何安全地共享数据资源、采用何种访问控制策略模型、如何保障安全策略的完整性实施、如何对协同者进行身份鉴别和认证,这些都将成为CSCW系统安全所面临的关键问题。然而,目前CSCW访问控制研究主要集中在基于传统的计算平台和网络环境,实现基于角色的安全策略和模型。在文[4,5]中较集中地提出了基于角色的协

*)国家自然科学基金项目(No. 60573036);教育部科学技术重点研究项目(No. 03081)。**张志勇** 博士生,讲师,研究方向为访问控制策略与模型、可信计算与可信网络;**杨 林** 研究员,博士生导师,研究方向为信息安全与系统安全;**马建峰** 教授,博士生导师,研究方向为计算机可生存性与可信移动网络;**普杰信** 教授,研究方向为网络安全。

同工作中需要解决的问题及基本解决方案，如角色分配与迁移等；Lang[6]采用元策略概念把访问控制策略从访问决策功能中分离出来，提出了一种灵活的安全机制，该策略能够动态地实现多安全策略。文[7]利用 XML 实现了满足动态安全需求的角色模型，但未给出模型的形式化工作；文[8]则主要集中在理论模型的创建，给出了基于角色 CSCW 访问控制模型中基本组件和普通授权规则的形式化描述。上述研究工作对于硬软件平台以及 CSCW 应用的可靠性和完整性并未考虑。安全策略是否能够完整性地实施，而不是被篡改或旁路，则是建立在对 OS 和应用程序的信任基础上[2]，但目前 OS 和应用程序的安全问题却令人担忧。近来 Sandhu[9]给出了使用可信计算实现资源共享的解决方案，他们的研究主要集中在 OM-AM（Objective-Model- Architecture-Mechanism）[10]的架构层次，并未涉及到安全模型层，因此该解决方案对于选择何种策略模型具有一定的普遍意义。

本文将试图基于可信计算技术，具体研究 CSCW 访问控制中平台可信性（软硬件和安全策略执行的完整性）以及协作实体可信性（身份鉴别）问题，结合 OA-AM 和 PEI 安全模型构建方法论（Methodology）[1]提出形式化模型 FAC for CSCW 及其架构与协议实现，并通过应用举例给出完整的协同工作访问控制过程。

2 相关研究工作

2.1 可信计算技术及其本质

可信计算的研究可以追溯至 1970 年后开始的容错计算（Fault-tolerant Computing）和 Anderson 提出的可信系统（Trusted System），以及 1980 年后 TCSEC 标准的制定与 TCB 的研究进展。这个阶段的可信系统研究主要集中在硬件设备和软件系统的可靠性上，因此也称为可靠计算（Dependable Computing）。2002 年初，正式提出可信计算的概念，从众多业界厂商加入的 TCPA 到今天的 TCG，一直致力于研究面向不同应用环境的可信计算平台及由此而衍生出来的可信网络。

可信计算平台（TCP）具有复杂的三层体系结构，包括底层的硬件、固件（TPM）到上层执行 TPM 管理和访问的软件栈（TSS），以及顶层系统软件和应用软件等，其本质是创建一个可信源（根），并通过硬件芯片和可信第三方将这个可信源不断扩大到 OS、应用软件、网络平台[11,12]。TCP 的主要特征涉及对敏感数据的保护、不同层次上的信息正确性证明以及系统完整性的度量、存储和报告，最终达到用户对平台的可信、平台上运行软硬件的可信以及平台间相互信任等，使得整个系统按照所期望的行为方式工作，并真实地报告当前状态，但不泄漏密钥和暴露身份。

2.2 访问控制策略与模型

访问控制作为传统的安全解决方案，从上世纪六七十年代便开始了对访问控制策略、模型、实现机制的研究，直到目前它仍是系统安全的基本保障手段。经典的访控策略有自主访问控制策略（DAC）、强制访问控制策略（MAC）、基于角色的访问控制策略（RBAC）和近年来提出的使用控制策略（UCON）。相对于上述策略也产生了一些代表性的理论模型，如访问控制矩阵模型、BLP 与 Biba 模型、RBAC96 和 $UCON_{ABC}$ 等。这些策略与模型被广泛地运用在操作系统、数据库系统与实际应用系统中，为它们提供了较好的基本安全保障。访问控制的本质就是通过定义安全策略来完成有效的授权（包括权限传播）和身份认证，从而确保合法用户能够得到相应的计算服务和共享资源。现有的访控研究和应用大多关注在授权的正确性上，然而对身份认证的实现相对薄弱。鉴于目前网络环境，防止敌手通过身份伪装和欺骗进入系统窃取资源和进行非法操作，使得对实体的身份鉴别变得尤为重要。

3 FAC for CSCW 形式化描述

3.1 模型思想与基本组件

FAC for CSCW 模型结合 CSCW 环境特征，在 RBAC96 基础上引入任务（Task）和活动（Activity）概念，实现协作中的访问控制授权。任务作为一次完整的工作流程，具体可细划为若干具有时序性的活动。协作角色可执行的操作由操作指派赋予，协作实体将通过角色指派获得相应的角色（集），从而在实体和操作之间建立起联系。实体-会话-活跃角色-活动之间是一一映射关系，其他则是多对多的关系。该模型主要由协作实体、角色、操作、约束规则、任务、活动和会话等七部分构成，如图 1 所示。

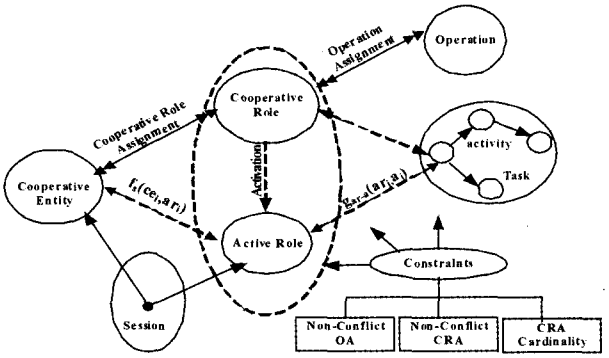

图 1 Fine-grained Access Control for CSCW 模型

3.2 FAC for CSCW 基本组件的定义

用集合论和谓词逻辑形式化描述该模型如下：定义协作实体集 CE、角色集 CR、操作集 Op、约束集 C、任务集 T、活动集 A、会话集 S。

定义 3.2.1（协作实体 Cooperative Entity） 在 CSCW 环境中参与协同工作的主动者，可以是自然人 User 或智能 Agent 等。CE 集可细化为协作发起者 Spnr 和协同者 Copr 两个子集。

$CE=\{ce \mid ce\in Spnr \vee ce\in Copr, ce\in Usr \vee ce\in Agnt\}$

定义 3.2.2（协作角色 Cooperative Role） 具有明确协作目标，承担一定协作任务的一类协同实体 ce 的抽象集合。CE 在一次协作过程中所激活的角色成为活跃角色（Active Role），记为 AR。

$CR\in 2^{CE}(ce\in CE), ar\in CR(ce)$

定义 3.2.3（操作 Operation） CE 对访问客体 Obj（共享文件、数据库、画板等）可施加的动作，记为 Op。这里的操作既可以定义为实际的读、写和执行，也可以是抽象的操作，这满足了基本安全需求中的“数据抽象”原则。例如在协同设计中，操作可以定义为图像提取、图像格式转换等。

定义 3.2.4（任务和活动 Task & Activity） CR 间协同处理所完成的一项工作称为任务；任务由若干操作组成，具有完整语义的协作步骤称为活动。活动具有动态特征和原子性，它是任务中不可再分的最小基本单位。

$\forall t(t\in T)t=\{a_1,a_2,\cdots,a_m\mid a_i\in A\}$

$\forall a(a\in A)a=\{op_1,op_2,\cdots,op_n\mid op_j\in O_p\}$

定义 3.2.5(会话 Session) 会话是实体通过活跃角色 ar 执行一次活动的过程，ce 和 ar 之间存在一一映射关系，记为 $f_s(ce,ar)$。$f_s(ce_i):ce_i\rightarrow ar_i(ce_i\in CE,ar_i\in CR(ce_i))$。

性质 3.2.1 CR 能够完成且只能完成某个协作活动，即活跃角色 ar 和活动 a 之间也存在一一映射 $g_{ar-a}(ar_i):ar_i\rightarrow a_i(ar_i\in cr_i,a_i\in T)$。

定义 3.2.6(指派 Assignment) 指派 a 是一个三元组 (x_i,y_j,z_k)，其中 z_k 为指派约束(见 3.4 节)。该三元组的语义解释在满足 z_k 的前提下可以将 y_j 分配给 x_i。当 $x_i=cr(cr\in CR)$，且 $y_j=op(op\in Op)$时，称指派 a_{op} 为操作指派 OA，这时 z_k 表示操作指派约束；当 $x_i=ce(ce\in CE)$，且 $y_j=cr(cr\in CR)$时，称指派 a_{cr} 为角色指派 CRA，这时 z_k 表示角色指派约束。指派 a 在 x_i 与 y_j 之间满足多对多的关系。

$OA\subseteq CR\times OP$ 且 $OA\neq\varnothing$

$CRA\subseteq CE\times CR$ 且 $CRA\neq\varnothing$

显然，ce 和 op 之间也隐含着多对多的关系。

定义 3.2.7(指派撤销 Assignment Revocation) AR 是指收回已指派的操作或角色的动作，即 AR 是指派的逆过程，这里分别记 $(a_{op})^{-1}$，$(a_{cr})^{-1}$ 为操作回收和角色回收。

定理 3.3.1 任意一个完成角色指派关系的协作实体至少可以参与一个协作活动。

证明：对于 $\forall ce_i(ce_i\in CE)$，由于 $CRA\neq\varnothing$，故至少 $\exists cr_j$，使得满足角色指派关系 CRA。当 ce_i 参与协作时激活 $cr_j(cr_j\in CR)$，此时 $ar=cr_j$，则满足函数 $f_s(ce_i):ce\rightarrow ar_j(ce\in CE,\ ar_j\in CR(ce))$。由于 AR 与活动 a 之间存在映射 $g_{ar-a}(ar_i):ar_i\rightarrow a_i(ar_i\in cr_i,a_i\in T)$，那么至少 $\exists a_k$，满足 $g_{ar-a}(cr_j)=a_k$，即在 ce_i 和 a_k 之间存在一一映射 g_{ar-a}。$f_s(ce_i)=a_k$，故命题成立。 □

3.3 FAC for CSCW 时间依赖特征及相关性质

定义 3.3.1(状态集 Status Set) Op 的状态集 Sta={invoke, sleep, expire}，其中 invoke 为激活态，sleep 为休眠态，expire 为终止态。

定义 3.3.2(操作时限 Operation Time Limit) Op 具有时效性，操作时限 $Op\_TL=\{x\mid x=[\tau_{bi},\tau_{ei}](i=1,2,\cdots,n)\}$，其中 τ_{bi} 为该时段的起始时间，τ_{ei} 为终止时间。

定义 3.3.3(操作状态迁移 Status Migration) Op 在其生命周期内会发生以下状态转换：假定 ST 为系统时间，$\exists i(1\leqslant i\leqslant n)ST\in[\tau_{bi},\tau_{ei}]\rightarrow S=invoke$；$\forall i(i\in N)ST\notin[\tau_{bi},\tau_{ei}]\wedge(ST)\tau_{b1})\wedge(ST<\tau_{en})\rightarrow S=sleep$；$\forall i(i\in N)ST\notin[\tau_{bi},\tau_{ei}]\wedge ST)\tau_{en}\rightarrow S=expire$。

性质 3.3.1(角色时限) 如果角色 cr 拥有 m 个操作，则角色时限为指派给该角色的所有 m 个操作的时限并集，记为 CR_TL。

$\forall op_1,op_2,\cdots,op_m,cr_i(op_1\in OP,op_2\in Op,\cdots,op_m\in Op,cr_i\in CR)op_1\in OA(cr_i)\wedge\cdots\wedge op_m\in OA(cr_i)\rightarrow CR\_TL=Op\_TL_{op1}\cup Op\_TL_{op2}\cup\cdots\cup Op\_TL_{opm}=\bigcup_{j=1}^{m}\bigcup_{i=1}^{n}[\tau_{bi},\tau_{ei}](n=1,2\cdots)$

性质 3.3.2(活动时序性 Activity Time-Order) 任务中活动的执行为异步或同步，它们之间满足偏序关系，记为“$\triangleright$”。

证明：因为 $\forall t,a_i(t\in T,a_i\in A)(a_i\in t\rightarrow a_i\triangleright a_i)$，满足反身性；$\forall t,a_i,a_j(t\in T,a_i,a_j\in A)(a_i\in t\wedge a_j\in t\wedge a_i\triangleright a_j\rightarrow\rightarrow(a_i\triangleright a_j))$，满足反对成性；$\forall t,a_i,a_j,a_k(t\in T,a_i,a_j,a_k\in A)(a_i\triangleright a_j\wedge a_j\triangleright a_k\rightarrow a_i\triangleright a_k)$，满足传递性；故命题成立。 □

性质 3.3.3(活跃角色时序性 AR Run-Order) 不同实体的激活角色 AR 在执行活动中是串行或并发的，AR 之间的时序关系满足偏序关系 $\geqslant_{AR}$，其中传递性可描述为

$\forall t,ar_i,ar_j,ar_k(t\in T,ar_i\in cr_i,ar_j\in cr_j,ar_k\in cr_k)(ar_i\geqslant_{AR}ar_j\wedge ar_j\geqslant_{AR}ar_k\rightarrow ar_i\geqslant_{AR}ar_k)$

定理 3.3.1 任意一个实体所执行任务中的某个活动 a_i 和 ar_i 之间在时序上存在一一映射关系，使得两者在时序上是同构的，记作 $AR\cong A$。

证明：根据性质 3.3.2 和. 3.3.3，在一个任务 t 中的任意两个活动 a_i,a_j 满足偏序关系 $\triangleright$，并且不同实体的任意两个活跃角色 ar_i,ar_j 之间也满足偏序关系 $\geqslant_{AR}$。并且，根据性质 3.2.1，活跃角色 ar 和活动 a 之间也存在一一映射 g_{ar-a}，故 $g_{ar-a}(ar_i)=a_i$。所以，两集合 AR 和 A 在元素个数上相等，并且各自元素之间的时序关系一致，故 $AR\cong A$。

从而推论出，$\forall t,a_i,a_j,ar_i,ar_j(a_i,a_j\in t,ar_i,ar_j\in AR)(g_{ar-a}(ar_i,a_i)\wedge g_{ar-a}(ar_j,a_j)\wedge a_i\triangleright a_j\rightarrow ar_i\geqslant ar_j)$ □

3.4 FAC for CSCW 约束特征与授权撤销特性

FAC for CSCW 约束特征是加强访问控制授权的重要手段，也体现了该模型自定义安全策略的特征。特定系统可以根据实际安全需求，自定义约束规则集，从而实施更为完整的指派关系。这里的约束特征主要包括无冲突操作指派约束、无冲突角色指派约束和角色指派基数约束等，它们将构成实际 CSCW 应用系统的基本授权策略。

定义 3.4.1(冲突操作 Conflicting Operation) 如果 op_i，op_j 不能同时指派给同一角色 cr_k，则称 op_i，op_j 为冲突操作，记为 $Conf\_Op(op_i,op_j)$。

约束规则 3.4.1(无冲突操作指派约束 Non-Conflict OA) 对同一角色的操作指派中，不能包含两两冲突的操作。

$\forall op_i,op_j,cr_k(op_i\in Op,op_j\in Op,cr_k\in CR)\ op_i\in OA(cr_k)\wedge op_j\ OA\in(cr_k)\rightarrow\rightarrow Conf\_Op(op_i,op_j)$

定义 3.4.2(冲突角色 Conflicting CR) 如果 cr_i,cr_j 不能同时指派给同一实体 ce_k，则称 cr_i,cr_j 为冲突角色，记为 $Conf\_CR(cr_i,cr_j)$。

约束规则 3.4.2(无冲突角色指派约束 Non-Conflict CRA) 对同一实体的协作角色指派中，不能包含两两冲突的角色。

$\forall cr_i,cr_j,ce_k(cr_i\in CR,cr_j\in CR,ce_k\in CE)\ cr_i\in CRA(ce_k)\wedge cr_j\in CRA(ce_k)\Rightarrow\rightarrow Conf\_CR(cr_i,cr_j)$

约束规则 3.4.3(角色指派基数约束 CRA Cardinality) 角色 cr_i 所能够指派的最大实体数不能超过指派基数 c(c 为自然数)。

$\forall ce_1,ce_2,\cdots,ce_m,cr_i,\exists c\in N(ce_1\in CE,ce_2\in CE,\cdots,ce_m\in CE,cr_i\in CR)ce_1\in CRA(cr_i)\wedge\cdots\wedge\ ce_m\in CRA(cr_i)\Rightarrow m\leqslant c$

性质 3.4.1(角色强制撤销 System Imperative Revoke) 当系统时间 ST 超出角色 cr 最大时限后，系统将隐式或显式地强制执行 $(a_{cr})^{-1}$ 动作，即撤销协作角色 cr。这里记 Maxtime(t)为时间 t 的上限。

$Maxtime(\bigcup_{j=1}^{m}\bigcup_{i=1}^{n}[\tau_{bi},\tau_{ei}])\Rightarrow(a_{cr})^{-1}$

性质 3.4.2(管理者撤销) 当系统安全策略动态变化

时，管理者可以显式、实时地执行$(a_{op})^{-1}$和(或)$(a_{cr})^{-1}$动作，回收已指派的操作和(或)角色。

约束规则 3.4.1 和 3.4.2 解决了的授权中的操作和角色冲突问题，实现了基本安全策略中的“责任分离原则”；约束规则 3.4.3 解决了角色的指派数量问题，则满足了“最小特权原则”。

4 CSCW 访问控制体系架构与关键协议

所有安全策略、机制和实现过程都需要建立在特定的合理假设基础上，否则在一个最为普遍、抽象的情形中，研究计算机系统是否安全将是不可判定的[13]。本节所提出的基于可信计算技术的 CSCW 访问控制架构 TC-enabled AC 和相关协议集，是建立在以下合理假设基础上：服务器、各协作站点所依赖的可信硬件平台 CRTM 和 TPM 一致，它们已通过生产厂商或可信第三方 Privacy CA 认证，成为整个系统绝对可信的根。此外，本节所涉及的可信计算的基本特征，如保护能力(Protected Capabilities)、证明(Attestation)、完整性度量、存储与报告(Integrity Measurement, Storage and Report)，以及相关密钥和证书，如 TPM 签注密钥 EK 与证书、身份证明密钥 AIK 与证书等，这里将不再赘述，可参考文[10]。

4.1 TC-enabled AC 混合式架构

实现可信计算的 CSCW 访问控制架构采用服务器和协作站点的混合式结构，其中服务器负责共享资源和自定义安全策略的保密存储和访问控制等问题。地理上分布的各个工作站之间完成任务的协同工作。这里所采用的服务器和协同工作站都是基于可信计算的软硬件环境，包括 CRTM、TPM 和提供 TSS 基本服务的 Enforced Security Kernel(ESK)。此外，重要部件 AC-TCB 是实现访问控制的可信计算基(Access Control-Trusted Computing Base)，它不可被旁路，可信性由 ESK 证明和保障。AC-TCB 负责定义和管理安全策略，管理协作者，为他们进行共享数据资源的访问授权，并在协作站点访问对象时，由 AC-TCB_s 将和本次访问相关的安全策略发送到协作站点 AC-TCB_w，并安全地存储在 Sealed Store 中，此后在本地便可以执行系统安全策略。协同者的身份证书从 Cooperative Identity CA 获取，在站点登录和访问资源时将再次进行身份鉴别。TC-enabled AC 架构适合于不同时间、不同地点上的协同工作环境，如图 2 所示。

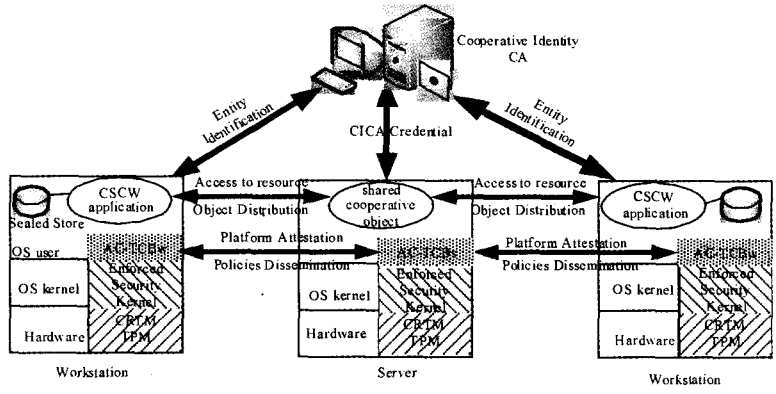

图 2 Trusted Computing-enabled Access Control 架构

4.2 关键协议描述

依据上述 TC-enabled AC 架构，实体鉴别协议、策略和对象分发协议和本地策略实施协议完成了平台之间的完整性验证以及平台与实体间的身份鉴别，从硬件底层保证了应用程序的完整性以及正确地实施安全策略，达到协作中共享资源访问控制的目标。上述协议所涉及的对象、系统函数、语义描述如表 1 所示。

表 1 关键协议及函数

主要对象	系统函数	基本语义
Entity,CICA AC-TCBw	Identification(enti, role, CICA, ac-tcb_w): credential	实体 Enti 向 CICA，ac-tcb_s 请求身份验证和协作角色； CICA 颁发 credential，并由 ac-tcb_w 绑定角色(集)。
AC-TCB_w AC-TCB_s	Dissemination(enti, obj, cred, ac-tcb_w, ac-tcb_s):policies|obj}	Enti 使用 credential 通过 ac-tcb_s 请求访问 obj，ac-tcb_w 验证 ac-tcb_s 完整性后，并发送 policies 和 obj。
AC-TCB_w CSCW-App	Enforcement(enti, role, obj, ac-tcb_w, app): Boolean	ac-tcb_w 验证 app 完整性，保障 policies 实施和 enti 使用 role 合法地访问 obj，并返回是否成功的布尔值。

协议 1(协作实体认证与角色指派) 在工作站上参与协作的实体身份需要经过可信第三方 CICA(Cooperative Identity CA)的认证，这类似于可信计算平台的 AIK 需要经由 Privacy CA 认证后颁发；CICA 认证实体后，将认证证书发往 AC-TCB_w，然后 AC-TCB_w 再申请相应的协作角色，服务器端的 AC-TCB_s 将根据申请和系统安全策略 Policies，决定是否授予角色(集)，然后在证书上绑定所指派的角色，发往 AC-TCB_w。协议完整过程如图 3 所示。

(1)协作实体的公钥被 AC-TCB_w 的私钥加密，AC-TCB_w 的完整性测量 SHA(AC-TCB_w)和自身被 ESK 私钥加密的公开密钥，以及被 TPM 的 AIK 私钥加密的 ESK 公钥等，一起发送到 CICA；

(2)CICA 验证 AC-TCB_w 和 ESK 的公钥合法性以及完整性测量值，如果正确，将用 CICA 的私钥签名实体的公开的密钥证书，然后再重新发往 AC-TCB_w；

(3)实体把获得的公钥证书，连同平台完整性信息及申请的协作角色(集)，一同发给 AC-TCB_s，请求角色指派；

(4)AC-TCB_s 验证实体证书和平台完整性后，根据安全

策略 Policies 为实体指派角色(集),并绑定到实体证书;在角色指派过程中,AC-TCB$_s$ 须满足角色约束规则,最后将绑定角色(集)的公钥证书使用 AC-TCB$_s$ 私钥签名后发给 AC-TCB$_w$。至此,实体便获得了相应的角色和身份证书,作为今后参与协作访问资源的凭据。

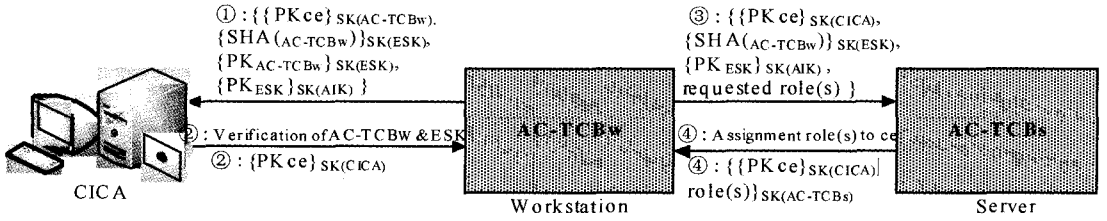

图 3 协作实体认证与角色指派协议

协议 2(Role-related Policy 与 Object 的分发) 在协议 1 的基础上,协作实体使用所获得角色请求访问 Server 上的对象,进行协同工作;AC-TCB$_s$ 需要验证 AC-TCB$_w$,然后将与该角色访问请求相关的 role-related policies 和对象发往 AC-TCB$_w$,此后在协作站点本地实施安全策略。该协议双方交互过程如图 4 所示。

(1)协作实体通过 AC-TCB$_w$ 用私钥 SK_{ESK} 签发一个包含访问对象 obj$_i$,访问角色 role$_j$ 和应用 app 完整性测量值的访问请求串,以及 ESK 被 AIK 签名的公钥和 ce 的公钥证书等发送给 AC-TCB$_s$;

(2)AC-TCB$_s$ 获取实体身份和相应请求角色,进行合法性鉴别;如果存在问题,也可将 ce 公钥证书发往 CICA,配合鉴别身份是否有效;

(3)当实体身份与角色通过一致性验证后,AC-TCB$_s$ 还需验证 app 的完整性;如果满足要求,则向实体所在平台发出验证挑战(Attestation Challenge);

(4)实体平台接到验证请求后,准备被签名的平台完整性信息,重新发给服务器,接受平台正确性验证;

(5)服务器通过检查,AC-TCB$_w$ 的完整性散列值来验证协作站点,并生成一个 obj 的访问密钥 K_{obj},然后将需要在协作站点实施的角色相关 policy$_k$ 和 K_{obj} 加密的 obj$_i$ 利用 AC-TCB$_w$ 的公钥再次加密后,发给 AC-TCB$_w$;到达协作站点后,AC-TCB$_w$ 使用自己的私钥解密,便可获得 policy$_k$ 和 obj$_i$,并将其安全地封存在 Sealed Store 中,从而完成了安全策略和对象的分发。

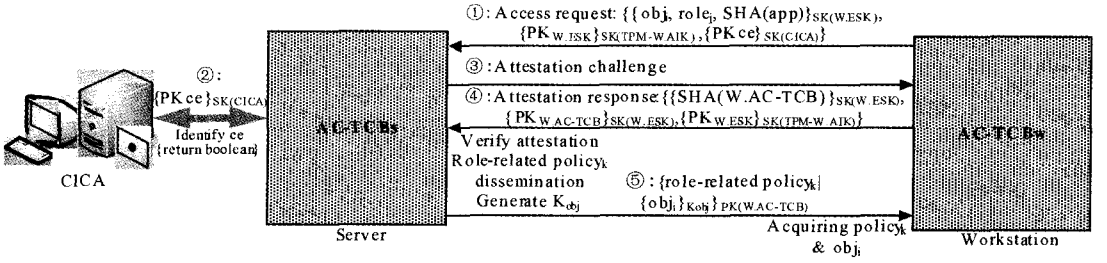

图 4 策略与对象分发协议

协议 3(本地应用验证与策略实施) CE 使用 CSCW-App 进行协同工作,AC-TCB$_w$ 需验证 app,保证它能够正确地、完整地实施安全策略,从而达到控制实体访问共享资源的目的。协议交互过程类似于协议 2,AC-TCB$_w$ 需要验证被 ESK 私钥签名的 app 完整性测量,并生成一次性会话秘钥 K_s,然后使用该会话秘钥加密 obj$_i$,和 role$_j$ 相关策略 policy$_k$ 后发给 app,由 app 实施安全策略中该角色有关的访问操作。该协议中本地应用的完整性证明类似于面向终端的可信计算中的证明过程,这里将不再赘述。

5 应用举例

本节依据上述架构与协议集,给出一个协同处理(签发)包含有敏感数据文件 F 的访问控制过程。这里假定该任务由四个角色协作完成:文件拟定角色 R_1、文件审核角色 R_2、文件签署角色 R_3、文件发布角色 R_4。在系统自定义安全策略中,这四个角色之间协作具有一定的时序要求,并且存在着某些冲突关系,如 R_4 在 R_2,R_3 之后执行,R_1 和 R_2 存在角色指派冲突等。下面以 Alice 行使 R_2,R_4 为例,描述一次完整的访问控制过程。

(1)预备过程:服务器端 CSCW 系统管理员根据安全需求,在 AC-TCB$_s$ 上定义完整的安全策略 Policies,包括角色-操作指派,角色时序限制、角色冲突约束等;

(2)协作者 Alice 从可信第三方和 AC-TCB$_s$ 获取绑定了角色 R_2 和 R_4 的身份证书;角色指派时如果存在冲突约束,则由 AC-TCB$_s$ 完成;

(3)Alice 在协作站点须首先激活 R_2(时序限制导致不可能是 R_4),以 R_2 身份请求 F,AC-TCB$_w$ 将平台完整性信息发给 AC-TCB$_s$ 接受验证;证明通过后,AC-TCB$_s$ 将分发与 R_2 相关的 policies 和 F,协作站点收到后使用 Sealed Store 存储它们;

(4)Alice 在本地启用协作应用程序 CSCW-App 访问 F,这里由 AC-TCB$_w$ 验证 CSCW-App 的完整性,保障策略 R_2-related policies 的实施。假设 policies 中定义 R_3 的周期时间为(13:00-13:45,14:15-15:00),当系统时间不在此范围时,App 则拒绝 Alice 访问 F,否则他可以使用 R_3 所包含的操作,如阅读 F,审查 F 等对文件进行相关处理;

(5)此后,Alice 如果需要发布 F,可以再激活 R_4 行使职

(下转第 124 页)

R_{14}、直接购买商 L_{11} 至 L_{13} 的信息；提取相关的间接供应商 R_{21} 至 R_{28}、间接购买商 L_{21} 至 L_{26} 的信息；……；直至提取到其最终产品的终端零销商信息、初始原料的源头提供商信息为止。②根据所提取到的各级供应商信息、购买商信息，进行构图。图中→代表供应渠道，箭头指向购买方，每条渠道又载有其运输成本费用、产品交易希望价格等相关信息。

结论 本文的研究表明：首先，多 Agent 技术可以应用于电子商务技术的供应链匹配系统架构设计，并提高其性能与品质。其次，给出了一种基于多 Agent 技术的供应链自动匹配管理平台系统模型，阐明了它的整体组成架构及其各单 Agent 的具体功能，阐述了平台系统模型中的两项关键技术——数据挖掘(包括基本任务与任务扩展)与供应链网络图构建，实现了供应链自动动态匹配管理；从而，可达到"消费者需求能得到积极满足，而供应链上不同环节众多经营商能实现互利共赢"的双向目标。

参 考 文 献

1 周启海，张元新，吴红玉. 一种基于多 Agent 的双向智能自动匹配系统模型[J]. 计算机应用，2006(7)
2 魏修建，严建援，王焰. 电子商务物流[M]. 北京：人民邮电出版社，2001
3 魏修建. 电子商务物流管理[M]. 重庆：重庆大学出版社，2004
4 刘业政，李亚飞，杨善林. 电子商务环境下基于移动 Agent 的 Web 数据挖掘[J]. 计算机工程，2004，20：107～109
5 高翔，林杰，张炜. 基于 Agent 的供应链仿真模型设计与实现[J]. 计算机工程与应用，2005，32：183～186

(上接第 113 页)

缩率。

表 3 非前缀查询 Q3

选择率	0		(0—0.3)	
统计参数	0	0	0.022	0.006
Star Schema	62962.8	2894.7	73453.4	2311.7
MidxTable	116.1	99.2	1960.0	596.0
ChunkedTable	31.2	40.4	506.1	143.2

以上实验结果表明，我们提出的基于混合 OLAP 的多维层次分块聚簇策略，能有效提高多维数据的压缩效率和基于维层次的多维选择效率。

6 相关研究

文[4,5]虽然对数据立方进行分块存储，但既不是按维层次分块，也不是按维层次聚簇的，因此对于基于维层次的操作，将不可避免地读取无用的数据单元。文[2]是通过将来自不同维的路径编码进行位交错，将多维数据线性化，然而它不是按层次分块的，而且这一实现方式完全基于关系技术，难以获得更高的压缩率和查询效率。文[7,8]介绍了一个面向 OLAP 的多维聚簇模式，但这一聚簇模式不是按多维"层次"聚簇的。虽然这一聚簇模式对多维数据进行了分块，但此分块是"物理"块，而不是本文介绍的按层次划分的"逻辑"分块。

结论 为提高基于维层次的多维存取效率，本文利用 ORDBMS 所特有的可扩展性，实现了一个同时基于"关系"和"多维"的混合型层次聚簇存储模式。基于 OLAP Benchmark 的初步实验表明，比纯粹基于"关系"技术的层次聚簇模式，具有更好的存储效率和查询效率。进一步取得更为全面的实验数据，以及根据具体的查询载荷设计层次聚簇模式，将是我们下一步的研究工作。

参 考 文 献

1 Pendsen N. What is OLAP? 2003. http://www.olapreport.com/fasmi.htm
2 Markl V, Ramsak F, Bayer R. Improving OLAP performance by multidimensional hierarchical clustering. In: Proc. Int Conf. on Database Engineering and Applications Symp(IDEAS), 1999. 165～177
3 Stonebraker M, Olson M A. Large Object Support in POSTGRES. ICDE, 1993. 355～362
4 Sarawagi S, Stonebraker M. Efficient Organization of Large Multidimensional Arrays. ICDE, 1994. 328～336
5 Zhao Y, Deshpande P M, Naughton J F. An array-based algorithm for simultaneous multidimensional aggregates. In: SIGMOD'97, Tucson, Arizona, May 1997. 159～170
6 PostgreSQL. http://www.postgresql.org
7 Padmanabhan S, Bhattacharjee B, Malkemus T, et al. Multi-Dimensional Clustering: A New Data Layout Scheme in DB2. In: SIGMOD 2003, San Diego, USA, 2003
8 Bhattacharjee B, Padmanabhan S, Malkemus T, et al. Efficient Query Processing for Multi-Dimensionally Clustered Tables in DB2. In: Proc. Intl Conf Very Large Data Bases (VLDB), 2003

(上接第 121 页)

责。基于 CSCW 平台的完整信任链，Alice 可以信任 F 已被 Bob(拥有角色 R_3)签署，而不是被其他人冒名行使了 R_3 的权利。

结束语 本文基于可信计算技术，结合 CSCW 系统访问控制的具体特性，提出形式化的访问控模型 FAC for CSCW 和体系架构，最后通过应用举例描述了完整的访控过程。该模型实现了基于角色具有时间依赖和约束特征的协同工作，并通过可信计算技术实现了 CSCW 环境中的实体身份鉴别和安全策略完整性实施，从而保障了整个系统资源的秘密性、完整性和可用性。如何基于 TC 实现 CSCW 中的委托授权传播与访问，使其更好地适应分布式协同工作环境将作为进一步的研究方向。

参 考 文 献

1 Sandhu R, Ranganathan K, Zhang X. Secure Information Sharing Enabled by Trusted Computing and PEI Model. In: Proc. of ASIACCS06, Mar, Taipei, Taiwan, 2006
2 Sandhu R, Zhang X. Peer-to-Peer Access Control Architecture Using Trusted Computing Technology. In: Proc of SACMAT05, Stockholm, Sweden, June 2005
3 龚能，李玉顺，史美林. 协作环境中的关键技术研究[J]. 计算机科学，2005，32(9)：230～233
4 Zhu H. Some issues of Role-based Collaboration. In: Proceedings of IEEE CCECE2003- CCGEI2003, Montreal, May 2003
5 Zhu H. Conflict Resolution with Roles in a Collaborative System. International Journal of Intelligent Control and Systems, 2005, 10(1)：11～20
6 Lang Bo, Lu You, Zhang Xin, et al. A flexible access control mechanism supporting large scale distributed collaboration. In: Proceedings of the 8th International Conferenceon Computer Supported Cooperative Work in Design. Vol 1. May 2004. 500～504
7 Tripathi A R, Ahmed T, Kumar R. Specification of Secure Distributed Collaboration System[C]. In: IEEE Proceedings of the sixth International Symposium on Autonomous Decentralized Systems, 2003
8 李成锴，詹永照，茅兵，等. 基于角色的 CSCW 系统访问控制模型[J]. 软件学报，2000，11(7)：931～937
9 Sandhu R, Zhang X, Ranganatham K, et al. Client-side access control enforcement using trusted computing and PEI models. Journal of High Speed Network, 2006, 15：229～245
10 Sandhu R. Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way. In: the Proc. of ACM Workshop on Role Based Access Control, Berlin, Germany, 2000
11 Balacheff B, Chen L, Pearson S, et al. Trusted Computing Platforms: TCPA Technology in Context[M]. Prentice Hall Press, Jul, 2002
12 TCG Specification Architecture Overview Revision 1.2. Trusted Computing Group, Apr, 2004. http://www.trustedcomputinggroup.org
13 Bishop M. Computer Security: Art and Science(English version)[M]. 北京：清华大学出版社，2004，5.47，103