基于可信计算的CSCW系统访问控制

张志勇[1,3] 杨 林[2] 马建峰[1] 普杰信[2]
(1 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,陕西 西安 710071;
2 河南科技大学 电子信息工程学院,河南 洛阳 471003;
3 中国电子设备系统工程公司,北京 100039)

摘要:针对现有的CSCW系统不能有效地保障终端平台的可信性以及安全策略和上层应用实施的完整性等问题,提出了基于可信计算技术的CSCW访问控制架构和协作站点间的基于角色的委托授权策略,分别描述了安全策略与共享对象密钥的分发协议、角色委托协议及策略完整性实施协议等.应用实例表明:该框架基于完整的协作实体-平台-应用信任链的构建,提供了可信的协作实体身份与访问控制平台,依赖平台远程证明和策略分发实现了在本地站点上的完整性实施;同时角色委托提高了协同工作能力,也减轻了服务器端集中式策略执行的负担.

关 键 词:计算机支持协同工作(CSCW);访问控制;可信计算;策略实施;角色委托
中图分类号:TP393 **文献标识码**:A **文章编号**:1671-4512(2008)01-0059-04

CSCW system access control based on trusted computing

Zhang Zhiyong[1,2] *Yang Lin*[3] *Ma Jianfeng*[1] *Pu Jiexin*[2]
(1 Key Laboratory of Computer Network and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China; 2 Electronic Information Engineering College, Henan University of Science and Technology, Luoyang 471003, Henan China; 3 The Research Institute of the China Electronic Equipment and Systems Engineering Corporation, Beijing 100039, China)

Abstract: The trustworthiness of terminal platforms was not ensured effectively and the integrity of security policies and upper application was not implemented in existing CSCW systems. Therefore, trusted computing-based access control architecture for CSCW and roles-based delegation policy between collaboration workstations were presented. The security policies and sharing object key dissemination protocol, role delegation one and policy integrity enforcement one were respectively described. An example shows that owing to constructing a general entity-platform-application trust chain, the trusted cooperative entity identity and the access control platform were provided in the architecture, and the integrity of policies was implemented on the platform in a local workstation through platform remote attestation and policy distribution. Moreover, the capability of cooperative work was improved and the burden of the centralized policies that was executed on server side is lessened.

Key words: computer supported cooperative work (CSCW); access control; trusted computing; policy enforcement; role delegation

计算机支持协同工作(computer supported cooperative work, CSCW)研究旨在基于开放式计算机网络和分布式协作环境实现多实体成员间的协同工作和资源共享[1].目前CSCW访问控制

收稿日期:2006-11-10.
作者简介:张志勇(1975-),男,博士研究生;西安,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(710071).
E-mail:xidianzzy@126.com
基金项目:国家自然科学基金资助项目(60633020);国家自然科学基金资助项目(60573036);河南科技大学青年研究基金资助项目(2005QN019).

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,但存在如何保障软硬件平台的可信性,安全策略的分发、实施及CSCW上层应用执行的完整性等问题.文献[2,3]较集中地提出了基于角色的协同工作中需要解决的问题及基本解决方案,主要涉及角色分配、迁移与冲突解决等;文献[4,5]面向基于角色的CSCW环境对基本组件、普通授权规则和委托授权分别进行了形式化描述;文献[6]也结合RBAC策略和协同策略提出了CSCW安全模型,并给出了基于活动树的实现.近年来可信计算技术的产生能够有效地保障终端平台及其上层应用的可信与完整性[7],Sandhu提出了支持可信计算实现资源共享的解决方案[8],该方案适用于不同的安全策略如RBAC、UCON等,因此具有一定的普遍意义.为解决上述问题,本文提出面向CSCW基于可信计算的访问控制架构TCBAC(trusted computing based access control)及其相关协议等,从而实现可信的协作平台,以及共享对象密钥、策略的安全分发和完整性实施.

TCBAC架构(图1)采用CSCW群件系统中的混合模式,由集中式服务器负责安全策略的管理,共享对象和策略使用服务器端"推"模式(server-push)被分发到地理上分布的各协作站点,然后在本地站点保障策略的完整性实施.这里所采用的资源服务器和协同工作站都是基于可信计算的软硬件环境,包括可信芯片TPM(CRTM)、提供TSS基本服务的enforced security kernel(ESK)和关键部件AC-TCB(access control-trusted computing base).其中AC-TCB是实现访问控制的可信计算基,不可被旁路,可信性由ESK证明和保障,而ESK的可信则由TPM验证,从而形成完整的平台信任链.AC-TCB_s负责定义和管理系统安全策略和管理协作者,为它们进行共享数据资源的访问授权,同时当协作站点访问对象时,由AC-TCB_s将本次访问相关的安全策略发送到协作站点AC-TCB_{w1},并安全地存储在本地,此后在本地便可以执行系统安全策略.此外,依据委托策略协作实体之间可以委托权利(职责),实现更为广泛的资源共享,提高平台的协作能力[5].本文所采用的委托策略是基于角色粒度的单步委托和撤销,即AC-TCB_{w1}借助于远程证明技术验证AC-TCB_{w2}的可信性,并向其委托角色(集),然后由AC-TCB_{w2}负责委托策略的本地实施.在保障平台可信的同时,协作实体的身份证书从CICA(cooperative identity CA)获取,在站点登陆和访问资源时将被用于身份鉴别.

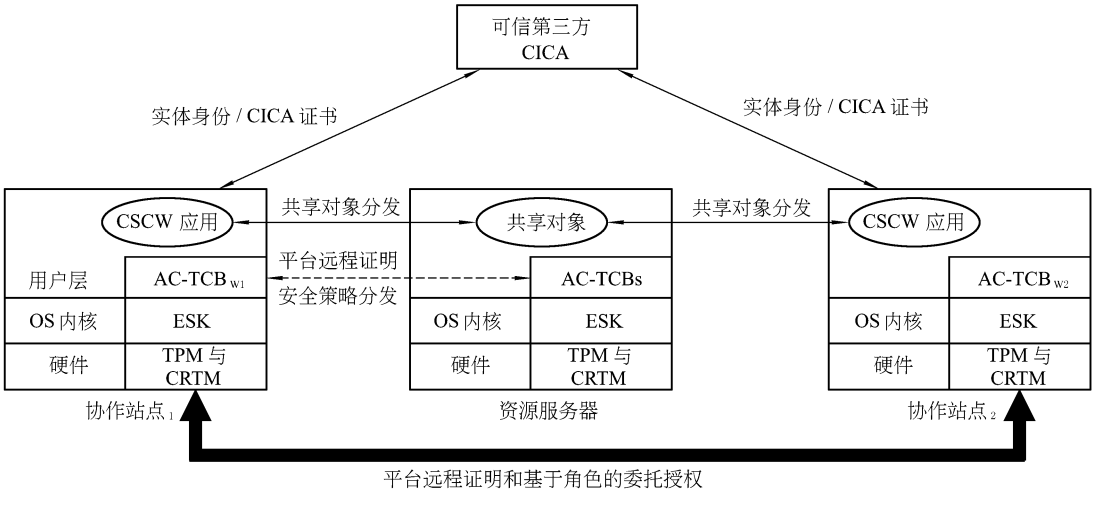

图1 基于可信计算的CSCW访问控制架构

协议1(协作实体认证与角色指派) 参与协作的实体身份需要经过可信第三方CICA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[7];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,决定是否指派角色(集),然后绑定到CICA证书上,发往AC-TCB_w.

协议2(角色安全策略与对象密钥的分发) 在协议1的基础上,协作实体ce使用所获得角色请求访问server中的共享对象,进行协同工作;AC-TCB_s需要远程验证AC-TCB_w的可信性和完整性,然后将与该角色访问请求相关的安全策略role-related policies和对象加解密密钥发往AC-TCB_w,此后在协作站点本地实施安全策略.这里假定平台OS内核已安全加载,并且是可信和完整性保持的,即仅需验证AC-TCB和app的

可信性. 该协议双方交互过程如图 2 所示(图中: (a) 访问请求{obj_i, $role_j$, app, {PKce}$_{SK(CICA)}$}; (b) 获取及验证实体身份; (c) 平台远程证明质询; (d) 质询应答{{SHA(app)}$_{SK(W.ESK)}$, {SHA(W. AC-TCB)}$_{SK(W.ESK)}$, cert(PK_{app}), cert($PK_{W.AC-TCB}$), {$PK_{W.ESK}$}$_{SK(TPM-W.AIK)}$}; (e) 实施远程证明与分发角色相关安全策略,产生对象加密密钥 K_{obj}, {role-related policy | K_{obj}}$_{PK(W.AC-TCB)}$; (f) 获取 policy 和 K_{obj}.

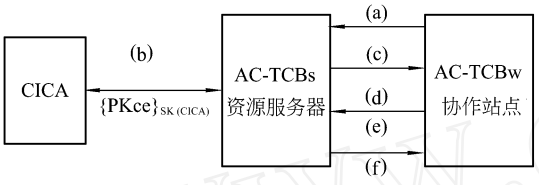

图 2　安全策略与对象密钥的分发协议

a. 协作站点发送一个包含访问对象 obj_i, 访问角色 $role_j$ 和应用 app 的访问请求串,以及被 CICA 签名的 ce 公钥证书等发送给 AC-TCBs.

b. AC-TCBs 获取实体身份和相应请求角色,进行合法性鉴别;同时也可将 ce 公钥证书发往 CICA,配合鉴别身份的有效性.

c. 在实体身份与角色通过一致性验证后,则向实体所在协作站点发出远程证明质询(remote attestation challenge).

d. 实体平台接到验证质询后,准备被签名的平台完整性信息作为应答,其中包括终端平台中 ESK 和 AC-TCB 的证书,以及 AC-TCB 和 app 的完整性度量值(哈希值)等,重新发给服务器端,接受平台可信性和完整性验证.

e. 服务器将 AC-TCBw 和 app 的哈希值和各自公钥证书中提供的标准校验值对比,以及验证被 AIK 签名的{$PK_{W.ESK}$}的有效性,从而判定该协作站点是否被攻击和篡改过;此外生成一个 obj 的加解密密钥 K_{obj},然后将需要在协作站点实施的角色相关 policy 和 K_{obj} 利用 AC-TCBw 的公钥再次加密后,发给 AC-TCBw.

f. 协作站点 AC-TCBw 使用自身的私钥解密,便可获得 K_{obj} 和 policy,并将其安全地存储在本地,从而完成了安全策略和对象密钥的分发.

协议 3 (角色委托)　这里约定协作实体 ce_1 和 ce_2 所在的站点分别为 W_1 和 W_2, AC-TCB$_{W1}$ 和 AC-TCB$_{W2}$ 是两站点的访问控制可信计算基. 委托者(delegator)所在的协作站点需要验证受托者站点的完整性,然后将写有委托角色集及时限的委托证书(delegation certificate)绑定到受托者身份证书 IC 上(假设受托者已从 CICA 获得 IC). 若本次委托符合来自于服务器端的委托策略,则由委托者签名 DC 后发给受托者(delegatee),从而完成角色委托过程,协议交互如图 3 所示,图中:(b) 发送(或接收)委托请求,并发出远程证明质询; (c) 质询应答{{SHA(W2. app)}$_{SK(W2,ESK)}$, {SHA(W2. AC-TCB)}$_{SK(W2,ESK)}$, cert(PK_{app}), cert($PK_{W2.AC-TCB}$), {$PK_{W2.ESK}$}$_{SK(TPM-W2.AIK)}$, {PK_{dlgtee}}$_{SK(CICA)}$}; (d) 实施平台证明,根据委托策略,使用 DC 委托角色(集)并与受托者的 IC 绑定; (e) {{PK_{dlgtee}}$_{SK(CICA)}$ | DC}$_{SK(W1.AC-TCB)}$ | K_{obj}}$_{PK(W2.AC-TCB)}$.

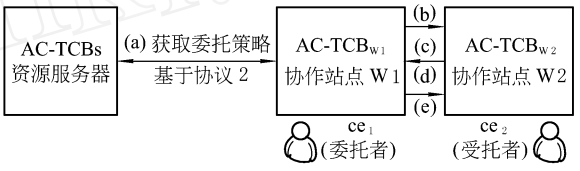

图 3　协作实体间的角色委托协议

a. 利用协议 2, AC-TCBs 向 AC-TCB$_{W1}$ 分发角色相关安全策略(包含角色委托策略)和共享对象密钥 K_{obj}. 委托者 ce_1 可以根据协作需要,委托其中的某个角色或全部角色集.

b. ce_1 所在的 AC-TCB$_{W1}$ 向 AC-TCB$_{W2}$ 发送委托请求,或者接收来自协作站点 W_2 的请求,随后发出平台远程证明质询.

c. AC-TCB$_{W2}$ 收到验证质询后,则将签名后的平台完整性哈希值、相关公钥证书以及 ce_2 的公钥证书{PK_{dlgtee}}$_{SK(CICA)}$ 发送给 AC-TCB$_{W1}$,作为质询应答.

d. AC-TCB$_{W1}$ 收到受托者平台完整性信息后,判定 W2 是否可信,其过程类似于协议 2(e),并使用{PK_{dlgtee}}$_{SK(CICA)}$ 判断 ce_2 的身份;若实体和平台是可信的,则根据(a)中获取的委托策略,将委托角色(集)与委托时限写入 DC 后和 ce_2 身份证书绑定.

e. AC-TCB$_{W1}$ 将绑定后的证书签名后,使用 AC-TCB$_{W1}$ 的公钥将其和 K_{obj} 加密,并发给受托者,此后委托者可依据证书上的委托角色行使协作能力.

协议 4 (策略完整性实施)　假设 ce_2 通过 $role_j$ 调用 CSCW 应用 app 访问 obj_i,进行协同工作, AC-TCB$_{W2}$ 首先判定 $role_j$ 是普通角色或委托角色. 若 $role_j$ 是委托角色(集)时,本地 AC-TCB$_{W2}$ 根据获得的角色委托策略 $policy_d$,判定委托角色是否有效,若已超出委托时限,则不再提交给 app 执行,并返回访问请求失败. 若 $role_j$ 是普

通角色,则判定本次访问是否符合普通角色策略 $policy_g$,然后由 AC-TCB_{W2} 开始验证 app,保证它目前运行在一个可信的状态. 这里 AC-TCB_{W2} 需要验证被 ESK 私钥签名的 app 完整性度量值,并生成一次性会话密钥 K_S,然后使用该会话密钥加密 obj_i,后发给 app,由 app 执行该角色有关的权限. 该协议中本地应用的完整性保护类似于面向终端的可信计算中的远程证明过程,这里将不再赘述.

依据上述架构与协议,这里给出一个协同处理(签发)包含有敏感数据文件 F 的访问控制过程. 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,四个角色之间的协作也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 和 R_3 之后执行,R_1 和 R_2 存在角色指派冲突等. 下面以 Alice 拥有 R_2 和 R_4 为例,描述一次完整的协同工作访问控制过程:

a. 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 RBAC 安全策略 Policies(其中包括角色委托策略).

b. 利用协议 1,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;角色指派时若存在冲突约束,则由 AC-TCB_S 完成.

c. 利用协议 2,Alice 在协作站点 AC-TCB_{W1} 上须首先激活 R_2(由于时序约束),以 R_2 身份请求 F, AC-TCB_{W1} 将平台完整性信息发给 AC-TCB_S 接受远程证明;待验证通过后,AC-TCB_S 将分发与 R_2 相关的安全策略 P_{R_2}、文件 F 及其加解密密钥 K_F,此后由 Alice 所在的站点在本地进行安全存储.

d. Alice 使用普通角色 R_2,在本地启用协作程序 CSCW-app 访问 F,利用协议 4 由 AC-TCB_{W1} 首先判定本次访问是否满足 P_{R_2}. 若满足,则验证 CSCW-app 的完整性,然后由 CSCW-app 执行本次会话,这样便保障了策略 P_{R_2} 的实施. 基于 CSCW 平台完整的信任链和实体认证协议 1,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. 此后,Alice 如果需要发布 F,可以再激活 R_4 行使职责.

e. 如果 Alice 由于缺席暂时不能行使角色职责,那么她可以把自身拥有的角色(集)委托给 Eve,委托策略从 AC-TCB_S 获得,由委托者 Alice 的平台 AC-TCB_{W1} 执行委托授权给 AC-TCB_{W2}. 这里假设他只把角色 R_4 通过协议 3 委托给 Eve,且 R_4 委托时限为 3 d. 那么 Eve 可以代替 Alice 使用委托角色 R_4,利用协议 4 访问文件 F. 委托角色超过 3 d 时限之后将自动失效,当 Eve 再次访问 F 时,将被所在站点的 AC-TCB_{W2} 禁止.

面向 CSCW 的 TCBAC 架构基于可信计算平台和远程证明技术,通过分发机制实现了策略在本地站点上的完整性实施,角色委托策略的引入则提高了平台的协作能力,降低了服务器端集中式访问控制的负担,同时协作实体的认证与鉴别也提高了共享对象的安全性. TCBAC 架构中如何解决角色传播控制和委托撤销等问题,将作为进一步的研究目标.

参 考 文 献

[1] 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.

[2] Zhu Haibin. Some issues of role-based collaboration [C] // Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering. Montreal: Institute of Electrical and Electronics Engineers Inc, 2003: 687-690.

[3] Zhu Haibin. Conflict resolution with roles in a collaborative system[J]. International Journal of Intelligent Control and Systems, 2005, 10(1): 11-20.

[4] 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.

[5] 张志勇,普杰信. 异构分布式 CSCW 委托授权模型及其访问控制[J]. 计算机工程, 2006, 32(12): 71-73.

[6] 肖道举,刘 超,陈晓苏. 基于角色的 CSCW 系统安全模型[J]. 华中科技大学学报:自然科学版, 2004, 32(5): 56-58.

[7] Smith S W. Trusted computing platforms: design and applications. Boston: Springer, 2005.

[8] Sandhu R, Zhang Xinwen, Ranganatham Kumar, et al. Client-side access control enforcement using trusted computing and PEI models[J]. Journal of High Speed Network, 2006(15): 229-245.