多层次动态权限策略的 CAD 模型安全保护①

贾文质 陈志杨 (浙江工业大学 软件学院 浙江 杭州 310023)

摘 要: 着眼于 CAD 安全模型的创新，针对 CAD 文档保护系统的现状，分析并提出了目前 CAD 文档保护系统存在的问题，提出了一个以多层次动态权限策略为基础的 CAD 模型/文档保护算法。该算法通过对产品设计生命周期中不同角色在不同阶段的权限/行为分析，结合访问控制、权限管理、加解密技术等，实现了对 CAD 产品模型在整个产品设计周期内的安全控制。

关键词: 多层次动态权限；CAD 模型保护；产品生命周期；CAD 模型访问控制；权限状态迁移

Multi-Level and Dynamic Permission Strategy for CAD Model Security Protection

JIA Wen-Zhi, CHEN Zhi-Yang

(College of Software, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract: Based on the present situation of CAD document protection system, the paper focuses on the innovation of CAD security model. It analyses current problems and puts forward a CAD model protection algorithm whose basis is a multi-level and dynamic permission strategy. This algorithm allows different access permissions or operations to the CAD models while in different phases of the product life cycle. Combined with the technologies of Access Control, Permission Manage, Encryption and Decryption, the paper successfully makes the security control of the CAD model more reliable in its product life cycle.

Keywords: dynamic permission; CAD model protection; product life cycle; CAD model access control; permission state migration

1 引言

1.1 CAD 模型安全保护应用现状

信息技术高速发展及人才频繁流动为我们如何保护我们的系统及企业信息安全提出了更高的要求。病毒防护、外部控制等手段阻止不了企业内部人员的非法行为，产品模型的安全保护日益成为各个企业关心的重点。目前我们看到的 CAD 文件/文档保护的产品很多，而且都各有其特点，如：大恒文档加密系统、华途文档加密软件、思智企业权限管理系统等。

但事实上，CAD 模型是有层次的，一个部件可以由一个或多个零件体组成，一个零件体又可以由多个特征体组成，如图 1 所示。所以，CAD 文件的安全需求应该不同于 Word、PDF 等常规文件。虽然目前的 CAD 模型保护产品在一定程度上可以实现对 CAD 模型的保护，但是其只是在文件级上的防护，并不能针对模型的某一层次或者一个模块。一旦文件被解密，那么对模型的操作完全是开放的、不受限制的。在实际产品设计过程中，我们经常遇到既要客户看到或使用 CAD 模型，又不想让客户可以随意改变模型的情况。在这种情况下，目前的 CAD 文档保护产品是无能为力的。更进一步的应用是，在产品设计开发过程中，不同设计人员参与不同部件设计，相互之间可能存在不允许互相查看模型的情况。目前传统 CAD 文档保护工具由于仅仅是一个 CAD 软件的普通插件或独立的文件加密模块，无法考虑根据用户角色动态分配权限。

① 基金项目:国家高技术研究发展计划(863)(2007AA04Z1A5)
收稿时间:2009-05-25

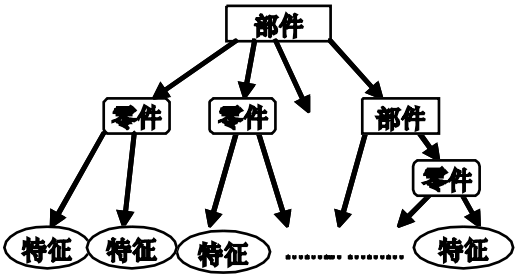


图 1　CAD 模型的层次结构

1.2 相关研究工作

访问控制技术已经成为最重要的安全控制手段之一。20 世纪 70 年代，Lampson 提出了访问矩阵的概念，并将其成功地应用在操作系统中。Conway 等人在对数据的访问控制中也使用了安全矩阵[1]，并将矩阵标准化，从而形成了自主访问控制(DAC)的思想。1996 年，Sandhu 等人总结了前人的经验，创新地提出了基于角色的访问控制模型(RBAC 模型)[2]。

韦科，范磊，李建华[3]等提出了主体角色及客体角色的概念，并探讨了一种可行的文件保护模型。但是，该模型不是针对 CAD 文档的，不适合 CAD 文档的特性。

方萃浩[4]提出了一个协同环境下 CAD 模型的多层次动态的安全访问控制(multi-level and dynamic security access control，简称 MLDAC)模型。它根据 CAD 模型的层次性，提出了角色分层和权限分层管理的概念，构造了一个多层次的权限模型，以简化权限定义及其分配过程。MLDAC 的分层访问权限模型中，访问权限被分为零件层权限和特征层权限两个层次，丰富了权限表达能力，较好地实现了产品模型的多粒度访问控制。但是，在大型的装配体设计中，一个 CAD 模型的特征可能是非常之多的，所以为每个特征分配权限显然是非常繁琐，甚至是不切实际的。

1.3 存在的问题

当今主流的文档保护系统结合 RBAC、加解密、水印等主要安全技术，较好的保证了文档的安全。但其针对 CAD 模型保护方面仍然存在着以下问题：

1) RBAC 没有对某些特殊操作进行控制。要保证文件的安全，除了安全的访问控制机制以外，也要考虑到有恶意企图的用户盗取宝贵的模型。对于文件资源，对其进行复制、剪切、拷屏、FTP、邮件发送、另存、打印到文件等操作是非常容易的。

2) RBAC 模型中通过分类主体角色来简化权限分配，但是在客体数目庞大的时候，文件访问权限将非常复杂。

3) RBAC 保护的数据模型相对简单，而 CAD 模型所要求的层次化、特征化访问权限等特点使得它不适用于复杂 CAD 产品模型的访问控制[4,5]。CAD 文档保护系统在对文件进行加密的时候大多是文件级的加密。用户或者看不到文件的任何内容，或者能看到文件所有的内容，不能满足查看部分模型的要求。

4) 当今大多数 CAD 文档保护系统都是基于局域网的企业级的应用，只能在一个公司内部或者小范围内起作用，模型的保护受地域的限制。

因此，我们迫切需要一个创新的、行之有效的 CAD 模型安全保护策略，它应该具备的一个重要特点：即使用户有权限解密一个模型，系统仍然可以通过限制用户对模型的修改、编辑、输出等功能来保护模型安全。

2　多层次动态权限策略的CAD安全模型

本文从产品设计生命周期考虑，提出了多层次动态权限策略的 CAD 安全模型。它主要体现在针对 CAD 模型的多层次的动态权限访问控制策略上，并结合加解密、系统钩子等技术，限制用户对 CAD 文档的操作，保护模型的安全。该安全模型的主要框架如图 2 所示。

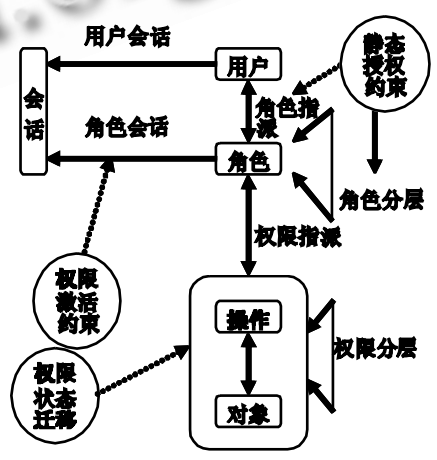


图 2　多层次动态访问控制模型

2.1 多层次动态的 CAD 模型访问控制

针对 CAD 安全保护策略所存在的问题，本文结合

MLDAC 和主客体角色概念，提出了一个改进的多层次动态的安全访问控制(Improved multi-level and dynamic security access control,简称IMLDAC)模型。

2.1.1 IMLDAC 模型的基本组成元素

该模型应用在具体 CAD 模型产品生命周期中，其各个基本元素对应如下：

* 用户集 U——全体用户。

* 主体角色集 R——组、项目经理、设计人员、普通用户等。其中组表示一个特殊的角色，它的权限包括了一个组里面所有成员权限的共有部分。

* 客体角色集 ORD——模型中的零件(Part)；零件中的特征类型(FT)，如圆角、倒角、孔洞等。

* 访问类型 AT——读取、编辑等访问类型。

* 零件层权限 PP——由主体角色及客体角色 Part、访问类型组成的一张访问权限表，由三元组(R, Part, AT)表示。

* 特征层权限 FP——由主体角色及客体角色 Feature、访问类型组成的一张访问权限表，由三元组(R, FT, AT)表示。

* 主体角色分配 UA——用户与主体角色的对应关系表。

* 客体角色分配 ORA——客体角色与零件、特征类型等的对应关系表。

IMLDAC 模型继承了 MLDAC 多层次的特点，将访问权限划分为零件和零件类型两个层次，通过把 MLDAC 中标识每个特征权限转变为标识每个特征类型的权限，极大的简化了权限的赋值过程，同时可以使得权限分配更加清晰。下例说明了如何表示一个模型的权限集过程。

假如我们有一个零件 P，包含了圆角、倒角、孔洞、圆柱等特征类型，分别记各类型为 FT1、FT2、FT3、FT4。若某个用户 R 的权限对零件可编辑，则该用户的权限集对应为 PS={PP(R, P, EDIT)}，可以编辑整个零件；若 R 对于 P 只读，则该用户的权限集为 PS={PP{R, P, READ}}；若 R 只能读取倒角和圆角，则可以定义该用户的权限集为 PS={PP(R, P, READ), FP(R, T1, READ), FP(R, T2, READ)}。

2.1.2 权限状态动态迁移

在产品设计生命周期的不同阶段，不同角色的权限/行为是不同的，所以我们有必要参照工作流的基本理念，引入权限的依赖关系及权限状态迁移，来实现权限的动态授权管理，如图 3 所示。当用户通过登录且验证后，用户权限即为就绪状态。若此时权限可用，则迁移为运行状态。用户使用期间还可能因为某些资源分配不到或者与当前已登录用户的权限之间有冲突等问题，而导致权限暂时挂起，待一切正常后恢复为运行状态。若执行中出现异常，则终止权限执行，并还原权限为初始化状态。

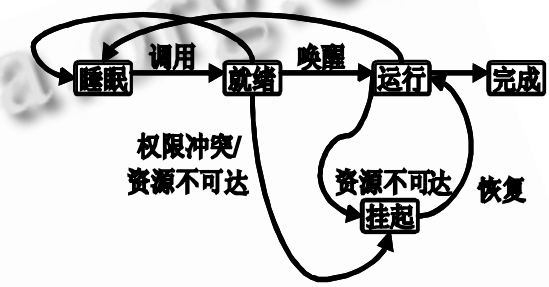


图 3 权限状态迁移图

3 实例系统

为了验证本文提出的安全模型的设想，我们开发了一个基于 SolidWorks 的 CAD 文档保护原型系统来验证其可行性。

首先，基于 SolidWorks 的 CAD 文档保护系统用 C/S 架构来控制用户的认证、权限的动态分配等过程，该过程主要由系统管理员来管理。

要特别说明的是，用户的权限分为两类：一类决定用户可以对应用程序进行哪些操作，简称操作权限；另一类权限依据 IMLDAC 模型，决定 CAD 模型中哪些特征可以对用户显示，简称显示权限。IMLDAC 模型适应 CAD 模型所要求的层次化、特征化访问权限等特点，简化了权限定义及其分配过程。系统根据不同角色、不同权限相应屏蔽应用程序的相关操作和 CAD 模型的特征显示。所以，即使同一个 CAD 模型和 SolidWorks 版本，不同权限的用户看到的界面和 CAD 模型将是不一样的。

其次，我们采用新型高级加密标准 AES[6](The Advanced Encryption Standard)来进行文档的加密。AES 强大的加密算法进一步保护了文档内容的安全性。

这样，该系统即保证了恶意用户的操作安全性，又防止了 CAD 模型内容被窃取。原型系统的文档保护流程如图 4 所示。

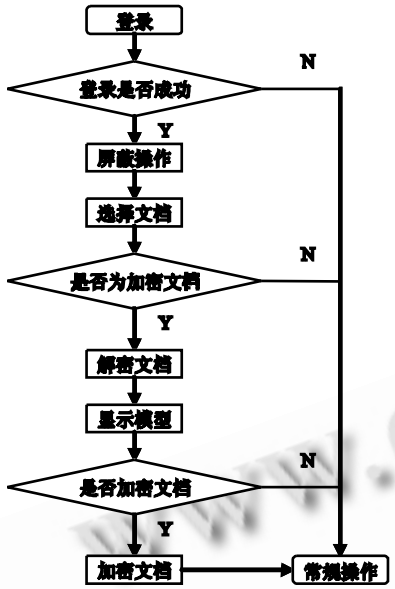
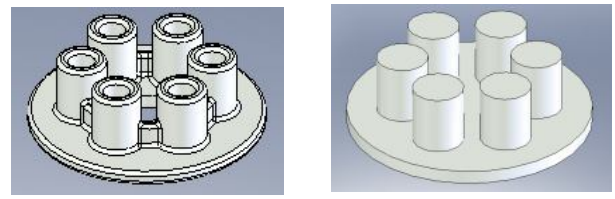


图 4　多层次动态权限策略的 CAD 文档保护流程

1) 首先，用户请求登陆，服务器验证用户名和密码。若存在该用户，则返回该用户所在的组、权限等相关信息。若不存在，则返回错误信息，但用户可以继续使用 SolidWorks 的常规功能。

2) 登录成功后，该用户的操作权限决定 SolidWorks 的界面。比如用户 U 的操作权限为只读，那么系统将禁止他所有试图“保存”、“另存为”、“出工程图”甚至拷屏等可以泄露文档信息的操作。

3) 若用户试图打开一个经过系统加密的 CAD 文档，系统将读取该文档的相关信息。如果该用户有相应的权限，则解密并按显示权限显示模型。否则，不允解密，但用户可以继续使用 SolidWorks 的常规功能。如用户 U 的显示权限为圆角、孔洞特征不可见，则系统将抑制所有圆角和孔洞特征为用户 U 不可见。图 5(a)为原始模型，(b)为用户 U 所能看到的模型。



(a)　原始模型　　(b)　简化后模型

图 5　应用多层次动态权限策略实例

4) 若某用户有权限进行“保存”或“另存为”操作，本系统可以在用户进行保存操作的时候自动对文档内容进行 AES 的文档加密。

4　总结和展望

本文提出了一个专门针对 CAD 模型的多层次动态权限 CAD 安全保护模型，并且完成了实例系统的开发，验证了该安全模型的可行性。从 CAD 模型本身保护技术分析，我们的策略与 CAD 软件绑定，在文件级加密的基础上对 CAD 软件功能进行了限制，也对模型特征的显示进行了有效的控制，既保证了模型本身的不可更改性，又保证了用户对模型的正常使用。从产品设计周期中的模型安全性分析，在不同设计阶段，不同的设计者给予不同的模型查看/修改权限，保证了整个产品设计过程中资料的安全性。

参考文献

1 Conway R, Maxwell W, Morgan H. On the Implementation of Security Measures in Information Systems. Communications of the ACM, 1972,15(4): 211－220.
2 Sandhu R, Coyne E, Feinstein H. Role-based Access Control Models. IEEE Computer, 1996, 29(2):38－47.
3 韦科,范磊,李建华.基于角色的文件保护模型及其实现.信息安全与通信保密, 2008,(5):53－56.
4 方翠浩,叶修梓,张引.协同环境下 CAD 模型的多层次动态安全访问控制.软件学报, 2007,18(9):2295－2305.
5 严巍,黄志球,刘毅,王凯.协同设计中层次访问控制模型的研究.计算机工程, 2008,34(13):40－42.
6 小刀人.加密它:用新的高级加密标准(AES)保持你的数据安全. 2004. http://www.vckbase.com