文章编号:1001 - 9081(2009)07 - 1793 - 03

VRML 文档的消隐数字签名安全模型

张亚玲,马春阳
(西安理工大学 计算机科学与工程学院,西安 710048)
(ylzhang@ xaut. edu. cn)

摘 要:针对网络化制造系统中产品设计文档流转的特殊安全需求,提出了基于 PKI 的文档安全解决方案。该方案采用对称加密技术保证设计图纸加解密的效率,通过数字信封技术实现对称密钥在多个用户之间的安全传输;将消隐数字签名技术应用于 VRML 格式文件中,实现了在不出示完整文档的情况下认证文档中的部分内容,解决了不可见性和完整性之间的矛盾。原型系统基于 B/S 模式和通用的 VRML 文件格式,具有良好的适应性和跨平台性。

关键词:消隐数字签名;虚拟现实建模语言;数字信封;数字证书
中图分类号: TP393. 08 **文献标志码**:A

Sanitizable digital signature secure scheme for VRML documents

ZHANG Ya-ling, MA Chun-yang
(*School of Computer Science and Engineering, Xi'an University of Technology, Xi'an Shaanxi* 710048, *China*)

Abstract: To meet the special security requirement for the transmission of product design documents in networked manufacturing systems, a secure scheme was proposed based on PKI. The scheme adopted symmetric encryption technology to assure the efficiency of the encryption and decryption of the design drawing, and realized safe transmission of the symmetric key among multiple users by digital-envelop technology; the sanitizable digital signature technology was used for documents in VRML format to realize the authentication of partial file without the whole file being demonstrated, by which the contradiction between invisibility and integrity was overcame. The system based on B/S mode and the general VRML format has good cross-platform adaptability.

Key words: sanitizable digital signature; Virtual Reality Modeling Language (VRML); data-envelop; digital certificate

0 引言

网络化制造系统是借助 Internet 和 Intranet 实现的制造企业的各种制造活动及其所涉及的制造技术和制造系统的总称[1]。在网络化制造系统中,不可避免地要在公共网络中传输大量的产品设计文档,这些信息极有可能在传输过程中被窃取、篡改或破坏,而核心机密数据的种种不安全可能给企业造成很大的经济损失。

众多的研究者对于网络化制造系统的文档安全问题进行研究和实践工作。文献[2]针对实际系统的应用,采用了基于角色的访问控制并使用数字证书中的属性证书来实现安全访问,用标准数字签名技术实现对文档的签名及验证。文献[3]阐述了从产品模型转换为虚拟现实建模语言(Virtual Reality Modeling Language,VRML)模型以及显示,描述了产品的层次和存储结构,文中对机械产品的数据模型和存储的处理方法值得借鉴。文献[4]研究了企业客户端的基于角色多重认证的权限控制策略,并提出一种适合应用服务提供商模式网络化制造的安全框架。文献[5]研究了 ASP 网络化制造平台的安全问题,在机械产品协同设计过程中,采取盟主统筹、盟主负责的总体方案,同时对设计过程进行基于角色的访问控制。

以上文献设计的安全方案大多采用标准的数字签名和加密技术,对于设计文档的数字签名没有考虑到内容的部分不可见性实际要求。考虑如下的应用场景:当设计人员将签名后的文档提交给资料员(签名拥有者),资料员将其下发给多个生产车间时,希望各个车间只能够看到与其生产任务相关的信息,而隐藏与其工作完全不相关的信息(比如是图纸中的某一个零件),同时生产车间还能够验证该设计文档确实来自于签名的设计人员。这一特殊的安全需求也就是要求保证文件的不可篡改性、身份的确定性以及不可否认性,同时要求部分文档内容不可见。

本文针对网络化制造系统产品设计文档流转中的上述特殊安全需求,提出了针对 VRML 文档的消隐数字签名解决方案。在深入研究各类 CAD 软件文档输出格式的基础上,本方案选择针对标准 VRML 文件进行安全方案设计,以保证系统具有良好的用户接口;将消隐数字签名技术应用于 VRML 格式文件中,实现在不出示完整文档的情况下认证文档中的部分内容,解决不可见性和完整性之间的矛盾。

1 产品设计文档安全解决方案

网络化制造系统中的产品设计文档一般都是由设计软件比如 PRO/E、CATIA、AUTOCAD、UG 等生成,各软件都有自己特定的图形文件格式,而在基于 Web 环境下的设计文档流转系统需要一种可通用的文档格式。VRML 具有文件容量小,便于在网络中传输,可以任意地插入到网页中,容易实现与其他协同工作的整合等特点;同时主流的三维 CAD 软件基本上

收稿日期:2008 - 12 - 18 ;**修回日期**:2009 - 03 - 09。
基金项目:教育部科学技术研究重点资助项目(208139);陕西省自然科学研究计划资助项目(2006F37)。
作者简介:张亚玲(1966 -),女,陕西西安人,副教授,博士,CCF 会员,主要研究方向:密码理论、网络安全; 马春阳(1981 -),男,陕西榆林人,硕士,主要研究方向:数据与网络信息安全。

都支持VRML格式的输出,采用VRML格式便于异构CAD系统间的交互协同,所以本方案选择针对VRML文件格式设计安全解决方案。由此涉及两个问题,即设计文档格式的预处理和针对VRML格式文件的安全方案。

1.1 设计文档的格式预处理

从CAD设计软件输出VRML文件后,需要对文件进行预处理操作。这里参考文献[6]的方法实现,以Pro/E为例说明CAD软件输出设计文档后需要的预处理工作。

首先在Pro/E中生成产品模型,然后导出为VRML格式,但Pro/E输出的VRML文件中包含一些Pro/E特有的元素,为了便于操作和控制,需要对输出的VRML模型文件做适当的转换,可以通过以下两点来实现:

1)把VRML模型中所有的Group节点都替换为Transform节点。

2)将Pro/E系统定义的几个命名视图(缺省视图、前视图、上视图、右视图、下视图、后视图、左视图)全部进行注释。

以上文件格式规范化工作通过Java编程来自动处理,并封装在一个JavaBean中(命名为TransformBean)。该类的核心是提供一个方法TransformFile(String fileName),实现逐行读取检查文件,分别进行替换和注释工作。同时TransformBean在图形服务器上新建一个临时文件,将被遍历和修改过的内容全部写到这里,然后将修改完后的临时文件内容写回到原文件中,这样VRML模型的转换就可以通过网络远程调用TransformBean来实现了。通过这一功能,产品设计人员不必对VRML有过多的了解就可以把产品文档发布给其他人员。

1.2 VRML消隐数字签名解决方案

针对VRML的消隐数字签名,本系统采用"PIATS"方案[7]。消隐数字签名方案中有签名者、消隐者和验证者三类角色,和我们实际工程项目中的设计组长、资料员和生产车间相对应,如图1所示。方案由设计组长执行的签名算法、资料员执行的消隐签名算法以及生产车间执行的验证算法组成。

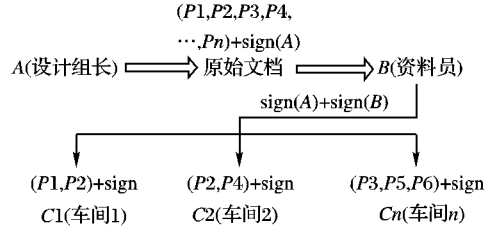


图1 消隐数字签名示意图

1.2.1 算法符号说明

$\{m_i\}_{1\leqslant i\leqslant n}$:代表原始文档被有效分为$n$块;

r:代表随机数;

Hash(·):代表一个哈希函数如SHA-1;

Sign(·):代表数字签名算法;

Verify(·):代表签名验证算法。

1.2.2 方案算法描述

设计组长执行的签名算法:

1)设原始文档为$\{m_i\}_{1\leqslant i\leqslant n}$,对每个VRML部件信息用随机数$r_i$填充。

2)填充后的VRML文档定义为$M=\{(m_i,r_i)\}_{1\leqslant i\leqslant n}$,对$M$的每个节点用SHA-1哈希函数产生相应的hash值,生成hash集合,定义为$H=\{h_i=\mathrm{Hash}(m_i,r_i)\}_{1\leqslant i\leqslant n}$。

3)对H签名,生成签名$s=\mathrm{Sign}_{\mathrm{signer}}(H)$。

4)设置$S=H\|s$,$\|$代表连接。

5)输出(M,S)作为原始文档和签名。

资料员执行的消隐签名算法:

1)针对每个生产车间产生一个索引集$D\subset\{1,\cdots,n\}$,其中$(m_i,r_i)(i\in D)$对该车间而言是可见的内容。

2)将文档M转换成一个新的文档$\widetilde{M}=\{\widetilde{m}_i\}_{1\leqslant i\leqslant n}$,定义如下:

$$\widetilde{m}_i=\begin{cases}(m_i,r_i), & i\in D\\(m_i',r_i'), & i\notin D\end{cases}$$

其中m_i'是特征串(比如"XXXXXXXX"),r_i'是用来填充的新随机数。

3)重新生成一个哈希集合定义为$H'=\{h_i'=\mathrm{Hash}(m_i')\}_{1\leqslant i\leqslant n}$。然后消隐者对其签名,生成一个新的签名$s'=\mathrm{Sign}_{\mathrm{sanitizer}}(H')$,置$S'=H'\|s'$。

4)输出消隐后的文档和签名$(\widetilde{M},S')$以及索引集D。

生产车间执行的验证算法:

1)接收到原始文档的签名s,消隐后的文档和签名$S'=H'\|s'$,获得H,s,H',s'。

2)计算$\mathrm{Verify}_{\mathrm{signer}}(H,s)$,验证签名者签名,确定原始文档完整性。

3)计算$\mathrm{Verify}_{\mathrm{sanitizer}}(H',s')$,验证消隐者签名,确定消隐文档的完整性以及确定消隐者身份。

该方案中被消隐的节点可以通过比较H和H'这两个哈希集合来确定。根据显示的文档和索引集D,生产车间可以验证消隐的正确性,也可以验证显示文档的完整性,同时确定被消隐的部分和资料员。

2 系统设计与实现

2.1 系统结构

系统的设计严格遵守PKI规范,综合应用加密和数字信封技术保证设计文档加解密效率及密钥在多个用户之间的安全传输,使用消隐数字签名技术实现对VRML模型的部分内容盲化。通过java.security包中的KeyStore类提供的load()、setKeyEntry()等方法生成RSA非对称密钥和X.509v3证书来构建系统CA,用getCertificate()、getPublicKey()方法从密钥库读取证书和获取证书公钥,并用Applet和Servlet技术实现了客户端与服务器之间的相互认证。本系统主要由客户端、CA认证服务器、Web服务器和数据库服务器组成,系统结构如图2所示。

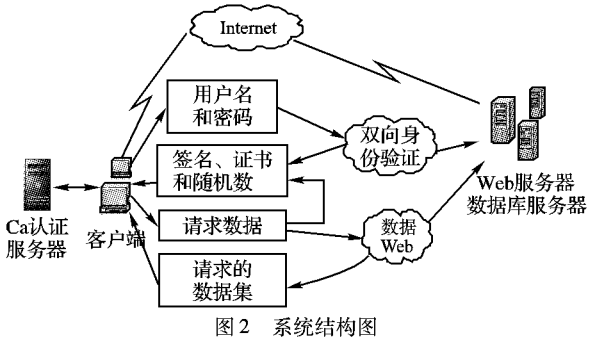


图2 系统结构图

2.2 安全模型设计

为了保证重要设计文档的机密性,本系统采用的解决方法是:首先发送方使用对称加密算法AES-256(密钥长度是256 bit)生成一个会话密钥,保存在本地并加密要传输的产品文档,生成密文;然后通过RSA密钥交换协议用于密钥共享,

即发送方通过程序获取接收方证书中相应的公钥来加密该会话密钥之后,将密钥密文和文档密文一起发送给接收方。接收方先用对应的私钥解封数字信封,得到对称密钥,再用对称密钥解开加密信息,获得设计文档原文。

为了保证文档在流转过程中的完整性、不可否认性和部分不可见性,本系统采用消隐数字签名实现在不出示完整文档的情况下认证文档的发送者通过两次数字签名(包括签名者 A 和消隐者 B 分别签名),有效地保证原始文档和消隐文档的完整性。系统的安全模型如图 3 所示。

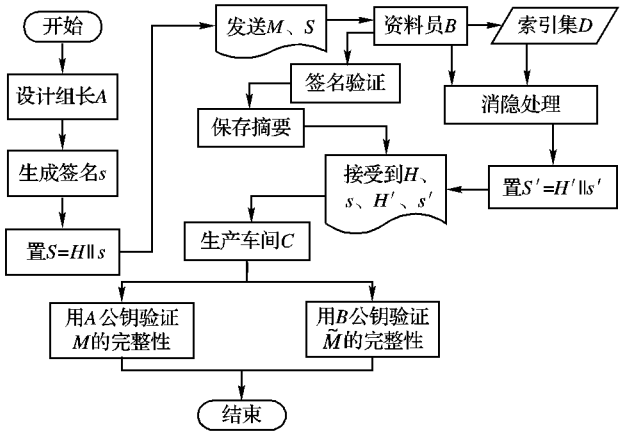


图 3　系统的安全模型

2.3　安全模型实现

在安全方案的具体实现中,针对 VRML 模型的消隐算法封装在一个 JavaBean 中(命名为 SanitizeBean)。它提供两个函数:通过函数 Partition(String strSrc,String Nodename)(参数含义:strSrc 代表源文件, Nodename 代表零件节点名称,即分割点)实现零件的摘取和分割;通过函数 Combination 实现将要消隐的节点用特征串和新的随机数来替换,特征串用 Java 中 8 字节 salt 来生成;最后组装合并,形成消隐文档。程序可以通过 VRML 模型名称和节点名称这两个参数来实现对指定模型某个节点的消隐。

具体实现:

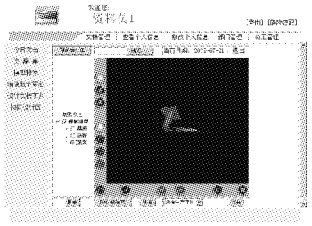
1)首先设计组长 A 对原始文档 M 的各个节点分别填充随机数,该随机数用 Java 中的 Random 类提供的 nextBytes( ) 方法实现,方法参数为 salt,是一个 8 字节的数组;然后用 SHA-1 哈希函数对填充后的每个节点哈希,分别生成长度为 160 bit 的消息摘要,具体地可以通过 java. security 包中的 MessageDigest 类提供的 digest( ) 方法,生成一个哈希集合;再用哈希函数对 H 生成消息摘要,然后使用 A 的私钥对 H 的消息摘要签名生成 $s = \mathrm{Sign}_{\mathrm{signer}}(H)$,可通过 javax. security 包中的 Signature 类提供的 sign( ) 方法实现,置 $S = H \| s$,输出 (M,S);

2)资料员 B 从 A 的证书中通过程序获取其公钥并验证原始文档 M 的完整性,并产生一个索引集 $D \subset \{1,\cdots,n\}$,根据 D 的描述,把需要消隐的节点用一个特征串(比如"XXXXXXXX")代替,特征串用 salt 来生成,同时给相应节点填充新的随机数,随机数产生方法同上,这样便将原始文档 M 转换为一个新文档 $\tilde{M}$。对 $\tilde{M}$ 的每个节点通过哈希函数生成消息摘要,产生新的哈希集合 $H' = \{h'_i = \mathrm{Hash}(m'_i)\}_{1 \leqslant i \leqslant n}$,对 H' 生成消息摘要,然后消隐者用其私钥对其签名,生成一个新的签名 $s' = \mathrm{Sign}_{\mathrm{sanitizer}}(H')$,并置 $S' = H' \| s'$,输出消隐后的文档和签名以及索引集 D。

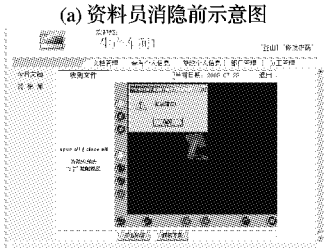
3)生产车间 C 接受到原始文档的签名 s,消隐后的文档和签名 $S' = H' \| s'$,获得 H,s,H',s',使用设计组长公钥验证原始文档完整性,使用资料员公钥验证消隐文档完整性并确定消隐者身份。

2.4　系统实现效果

系统的实现基于 B/S 模式和通用的 VRML 文件格式,经过测试使用,达到了对于设计文档进行消隐数字签名目的,使得生产车间既可以验证收到文档的有效性,又保证了部分与其无关的生产零件的不可见性。运行效果如图 4 所示。由于篇幅所限,这里仅展现了消隐数字签名及验证部分的实现效果。资料员针对生产车间 1 进行了消隐数字签名,并指定了消隐"拔叉"部分。生产车间 1 收到该文件后,可以验证该文件确实来自于资料员,同时与其生产无关的"拔叉"部分不可见。



(a) 资料员消隐前示意图



(b) 生产车间收到消隐文件示意图

图 4　运行效果

3　结语

本文从网络化制造系统设计文档流转的实际安全问题出发,经过分析、研究,提出一套有效和实用的安全解决方案。首次将"PIATS"使用在 VRML 模型中,基于 B/S 模式和结合 Spring 开源框架实现了系统,取得了良好的效果。本系统可以使得协同设计工程人员在网络环境下安全地进行文档流转,保证了其中的机密性、完整性、不可否认性、部分不可见性和身份认证等安全性,更进一步使系统完善还需要解决访问控制、密钥管理等问题。

参考文献:

[1] 刘飞,雷琦,宋豫川. 网络化制造的内涵及研究发展趋势[J]. 机械工程学报,2003,39(8):1-6.

[2] 付勇. J2EE 环境下协同设计系统信息安全解决方案的研究[D]. 成都:西南交通大学,2005.

[3] LIANG J S. A Web-based 3D virtual technologies for developing product information framework[J]. The International Journal of Advanced Manufacturing Technology,2007,34(5): 617-630.

[4] 徐立云,李爱平. 基于应用服务提供商模式网络化制造的安全技术研究[J]. 计算机集成制造系统,2006,12(11):1-6.

[5] 付翠玉,李爱平,徐立云. ASP 网络化制造协同设计安全研究[J]. 制造业自动化,2006,28(12):1-6.

[6] 陈亮,罗志伟,高诚辉. 网络化协同设计中图形协同的研究及系统开发[J]. 工程图学学报,2006,27(3):18-24.

[7] TETSUYA I, NOBUYUKI K, MASAHIKO T, *et al*. PIATS: A partially sanitizable signature scheme[EB/OL]. [2008-10-22]. http://www.cs. cityu. edu. hk/~ ispec2007/ppt/Tetsuya% 20Izu% 20-% 20Sanitizable%20Signatre%20Schemes%20with%20Aggregation. pdf.