# 基于UML的企业信息安全认证系统的设计

郝晓曦[1]，黄文军[2]

（1.五邑大学 机电系，广东 江门　529020；2.哈尔滨工业大学 自动化测试与控制研究所，黑龙江 哈尔滨　150001）

**摘　要**：针对安全级别较高的机要部门使用的网络传输系统，在分析其安全需求的基础上，发掘通用认证系统应用在此类传输系统中存在的安全漏洞。根据分析的结果对认证系统进行重新设计，制定合理的系统模型和安全策略。

**关键词**：企业信息安全；认证系统；机要部门；UML

**中图分类号**：TP393.09　　**文献标识码**：B　　**文章编号**：1671－749X(2007)03－0041－02

## 0　引言

由于企业电子商务、电子政务等网络传输系统经常需要在开放网络中不明身份的实体之间进行数据交换，因此需要传输系统能够保证数据安全和通信安全。数据安全通过加密算法解决被传输数据的机密性和完整性；通信安全主要解决为通信双方提供鉴别性证明和负责性证明。这些统称为认证系统，是传输系统中的核心技术。当前应用最广泛的是基于PKI（Public Key Infrastructure）技术[1]建立认证系统。

为了提高系统设计的完整性、正确性以及编写代码的效率，同时保证系统模型的可视化、准确性、易修改、可理解、可扩展等特性，现利用UML（Unified Modeling Language）所提供的建模机制和建模方法[2]分析和设计认证系统。

## 1　需求分析

企业机要部门的通信安全的基本要求包括：保密性、实时性、可用性及可控性。同时，还需要考虑到由于人们的疏忽造成安全隐患。通用认证系统模型主要包括：CA（Certification Authority），RA（Register Authority）、证书服务器（Certification Server，CS）以及用以查询证书状态的OCSP响应器（Online Certification Status Protocol Responder）。由于设计通用认证模型时淡化了具体的背景，因此将其直接应用在机要部门的安全传输系统时，将给攻击者破坏整个传输系统创造有利条件。具体安全漏洞有信任关系存在的安全隐患、证书持有者态度引起的安全隐患、证书撤销/状态查询时存在的安全隐患。

根据以上分析，机要部门的认证系统应该包括下列功能：①认证系统的基本功能。证书申请、身份验证、制作证书、发布证书、更新证书、查询证书、证书下载、作废证书、更新证书列表、数字签名等。②改进后新增加的功能：所有用户不允许直接访问CA和CS，系统对所有登录认证系统的客户端进行审核；证书使用权限设定，即通过限制证书的使用权限限制使用证书的用户；证书状态设定，CA根据证书的使用情况设定证书的状态；CS后端操作，CA可以直接控制CS；③对认证系统的结构和信任关系进行改进。所设计的认证系统在保证其功能完整的同时，尽量使其结构和信任关系简单[1,6]。

## 2　认证系统的设计

### 2.1　认证系统静态模型

认证系统的体系从物理结构图中可以看出，所设计的认证系统模型比通用认证系统模型缺少了OCSP响应器，简化了认证系统中的信任关系。在设计中，OCSP响应器的所有功能都由CA Server完成。用户与认证系统的所有信息交互都是通过RA完成的，RA与CA server上属于物理分离，它们之间

**收稿日期**：2007－01－31

**作者简介**：郝晓曦（1982－），女，陕西西安人，硕士，现广东五邑大学机电工程系工作，主要从事安全信息技术、机电产品设计等教学与科研工作。

信息交互通过安全网络完成,CA server 是所有 RA 和 CS 的信任锚。

按照 UML 模型组织结构的分组机制,认证系统按功能划分为如下几个包。

CA Package:该包实现 CA 相应的功能,包括审核证书申请,制作、发布、撤销证书,更新 CS,设定证书状态,生成根密钥、数字签名等。

RA Package:该包中的类实现 RA 的功能。RA 从功能上主要分为两个部分,即 RA-server 和 RA-client。RA-server 完成 RA 与 CA 之间的交互,其功能是,导入/导出证书、验证证书请求等;RA-client 完成 RA 与用户之间的交互,其功能是,用户身份验证、证书申请、证书状态查询、证书查询、证书权限设定等。

Database Package:提供证书数据库。

Protocol Package:主要包括各种安全传输协议,这些协议是客户端与认证系统安全通信的保证。

UI Package:描述整个用户界面所使用的类,这些类提供的操作允许用户和认证系统进行数据交换。

### 2.2 认证系统动态模型

认证系统的动态模型用于详细描述静态模型中各个类的交互关系,通过类之间的传递消息实现系统具体功能。

证书申请:用户在本地生成密钥对,并将公钥提交以申请证书。用户申请证书时,RA-client 会提示用户是否需要设置证书的使用权限,若用户选择设定使用权限,则 RA - client 将用户所提交的使用权限列表与其证书绑定,只有权限列表上的用户才能使用该证书,此时证书的结构中将增加出现 CertificationPromission 属性。

证书状态设置:根据证书的使用情况将其状态分为 5 种:可用、锁定、撤销、过期、使用。可用状态是指该证书能够正常使用;锁定状态是指证书在一段时间内没有使用,但尚未过期或被撤销。若证书用户需要继续使用该证书时,需要证书持有者激活该证书;证书撤销状态是指证书已经被该证书持有者撤销,此时证书不能被使用;证书过期状态是指证书超过有效期,此时证书不能被使用;证书使用状态是指证书持有者正对其进行操作(如修改、撤销证书等)。证书各状态间可以实现转换。

证书状态查询/证书下载:当证书被设置使用权限,查询/下载证书时,RA - client 验证用户身份确定其是否是权限列表中的用户,如果该用户的名字在权限列表中,该用户可以访问证书,否则,不能访问证书。

证书撤销:当要求证书的有效性在证书有效期之前终止,或者要求用户身份与私钥分离时,证书持有者可以提出撤销证书。

## 3 认证系统实现与安全性分析

### 3.1 实现

实现认证系统的过程就是进行类的程序编写工作。UML 所提供的建模机制中,可以方便的将模型与实际代码一一对应。编写代码时,只需从所设计的模型中获取各种规格说明。这样有效地提高了编码地效率,而且在编码时发现设计模型中存在的缺陷,并做出相应地改进,从而实现了设计模型和程序代码地同步。

本设计的认证系统是构建于 Windows 平台之上,采用 VC + +作为系统的开发环境,并利用 OpenSSL 开放源代码的工具包实现系统的功能。在本设计中利用 OpenSSL 所提供的安全套接层协议和传输层安全协议实现用户与认证中心的安全通信。

### 3.2 安全性分析

通过对认证系统模型进行安全分析可知:①用户必须通过 RA-client 完成与认证系统的交互(包括申请、查询、撤销证书等操作),不能直接访问证书,这样有效减少基于用户登录时的攻击;②认证系统通过设定证书的使用权限限制证书使用者的范围,从而避免了基于证书发布时攻击者对认证系统的攻击;③通过设定证书的状态可以有效避免和减少攻击者通过认证系统更新 CRL 的时间差或是利用证书持有者的疏忽对其的攻击;④在设计中将 OCSP 响应器的功能设置在 CA-server 中,不单独设置证书状态查询服务器,简化了认证系统的结构,避免攻击者通过信任关系攻击系统,同时提高了系统证书查询的效率。

综上所述,所设计的认证系统模型比通用认证系统模型具有更高的安全性,能够有效的抵御攻击者对认证系统的攻击,而且能够在一定程度上消除人为因素造成的安全隐患。因此能够满足机要部门安全传输系统对认证系统的安全需要。

## 4 结论

PKI 技术现已越来越广泛地应用于电子商务、电子政务以及政府机要部门,针对机要部门的安全需求,设计了一个认证系统模型,它通过对证书状态设定、证书使用权限设置、 (下转第 44 页)

31.73 MJ/kg(见表3)。

表3 纯煤发热量的均值

| $M_t$/% | $A_d$/% | 实测发热量 | 纯煤发热量 | 平均值 |
|---|---|---|---|---|
| 6.4 | 17.31 | 25.38 | 31.92 | |
| 6.6 | 9.68 | 27.67 | 31.96 | |
| 8.0 | 27.42 | 21.18 | 31.09 | |
| 6.1 | 17.67 | 25.14 | 31.72 | |
| 7.8 | 16.78 | 24.68 | 31.40 | |
| 6.0 | 38.53 | 17.94 | 30.76 | |
| 7.4 | 9.03 | 28.43 | 32.68 | 31.73 |
| 8.6 | 9.62 | 27.59 | 32.28 | |
| 7.0 | 11.38 | 27.10 | 31.98 | |
| 8.0 | 12.24 | 26.43 | 31.78 | |
| 6.7 | 19.48 | 24.31 | 31.55 | |
| 8.0 | 10.42 | 27.40 | 32.20 | |
| 7.3 | 11.46 | 26.74 | 31.71 | |
| 5.7 | 28.97 | 21.14 | 31.02 | |

将31.73 MJ/kg作为彬长矿区煤炭的纯煤发热量,得出收到基低位发热量经验公式:$Q_{net,ar} = 31.73 - 0.21M_t - 0.30\ A_d$。

## 2 经验公式的准确度和应用

由表4可看出,实测值与经验公式计算值之差的绝对值,最大为0.96 MJ/kg,最小为0.01 MJ/kg平均为0.38 MJ/kg,完全可以满足精度需要。

基低位发热量的精确测出的确较复杂,需要测定全水、水分、全硫、氢、发热量、灰分等项目,要想快速了解煤样的发热量数据就可以只测定全水、灰分,通过经验公式计算出其热值,在销售工作中作到心中有数,在日常化验工作中偶然误差和系统误差是难免的,有了全水和灰分的数据,根据经验公式计算出其热值可以控制质量,减少人为的偶然误差和系统误差,尤其是对校正后热值偏差较大的样品,可以进行复查,保证了分析质量。

表4 实测值与经验公式计算值的比对

| 实测值 | 计算值 | 实测值减计算值 |
|---|---|---|
| 25.14 | 25.15 | -0.01 |
| 24.68 | 25.04 | -0.37 |
| 17.94 | 18.91 | -0.97 |
| 28.43 | 27.47 | 0.96 |
| 27.10 | 26.85 | 0.25 |
| 26.43 | 26.38 | 0.05 |
| 24.31 | 24.49 | -0.18 |
| 27.40 | 26.92 | 0.48 |
| 26.74 | 26.77 | -0.03 |
| 21.14 | 21.85 | -0.71 |
| 25.38 | 25.20 | 0.18 |
| 27.67 | 27.44 | 0.23 |
| 21.18 | 21.82 | -0.64 |

## 3 结语

煤的发热量是煤中十分重要的指标,应该引起足够的重视,为了管理工作的方便,可以用经验公式检查分析结果的正确性,以免在出现偶然误差的情况下,而无从发现,让错误数据在眼皮下溜过。另外,彬长矿区的煤炭绝大部分在咸阳火车站上车运往外地,装车前许多销售人员想了解煤质情况,特别是发热量的数据,有了此经验公式,可以方便、迅速了解其热值情况,避免出现大的偏差和失误,保证了销售工作正常进行。

(上接第42页)

认证系统结构和信任关系的设计,有效地避免攻击者基于证书持有者消极态度、CRL更新以及证书发布时的攻击,在一定程度上满足了机要部门网络传输系统的特殊要求。

**参考文献:**


[1] 谢冬青,冷 健. PKI原理与技术[M]. 北京:清华大学出版社, 2004.

[2] Hans-Erik Eriksson, Magnus Penker. UML Toolkit. Publishing House of Electronics Industry.

[3] Foss JA. Multi-protocol Attacks and the Public-Key Infrastructure. In Proc. 21st National Information Systems Security Conference, Arlington, Va., 1998 -10, 566 -576.

[4] Housley R, Ford W, Polk W, et al, RFC 2459. Internet X509 Public key Infrastructure Certificate and CRL Profile. 1999.

[5] 李 新,任传伦,杨文宪. 在线证书状态查询协议的改进与应用[J]. 计算机工程与应用, 2002,(10):21 -23.

[6] El Bakkali, H.; Kaitouni, B. I., A predicate calculus logic for the PKI trust model analysis. Network Computing and Applications, 2001. NCA 2001. IEEE International Symposium on 8 -10 Oct. 2001, 368 -371.

[7] Eric Rescorla, An Introduction to OpenSSL Programming, Version 1.0, January, 2002.