文章编号: 1007- 2985(2009) 05- 0049- 04

基于 PKI 的校园网络化办公模型设计*

张晓丹, 李 海
(吉首大学 数学与计算机科学学院, 湖南 吉首 416000)

摘 要: 安全对于校园网络化办公系统的建设是至关重要的. PKI 技术作为一种公钥基础设施提供了一个框架, 在这个框架下可以实施基于加密的校园网络化办公的安全服务. 分析了吉首大学网络化办公系统的使用现状和安全需求, 设计了一种基于混合信任模型的吉首大学网络化办公的 PKI 框架.

关键词: 校园网络化办公系统; 层次信任模型; 交叉信任模型; PKI
中图分类号: T P393. 08 文献标识码: A

高等教育和科研机构是互联网诞生的摇篮, 也是最早的应用环境. 各国的高等教育都是最早建设和应用互联网技术的行业之一, 中国的高校校园网一般都最先应用最先进的网络技术, 网络应用普及, 用户群密集而且活跃. 借助校园网来进行网络化办公成为高校校园办公的一种趋势, 一方面催生了一种新的工作方式, 极大地提高了工作效率; 另一方面由于校园网是安全问题比较突出的地方, 安全管理也更为复杂、困难. 校园网络化办公系统面临诸多的安全风险, 如拒绝服务、信息泄密、信息篡改、资源盗用、声誉损害等, 这些安全风险的存在严重阻碍了校园网络化办公的应用与发展[1]. 以吉首大学网络化办公系统为例, 首先分析了吉首大学网络化办公系统存在的问题和安全需求, 并分析了目前系统所采用的层次信任模型的缺陷, 设计了结合层次模型和交叉认证模型特点的一种信任模型, 最后设计了吉首大学网络化办公系统的 PKI 框架.

1 吉首大学网络化办公的安全需求

吉首大学网络化办公系统目前存在的安全问题主要有以下几个方面:

(1) 网上信息发布安全缺乏保障, 办公网络系统依赖于校园网, 由于教学和科研的特点决定了校园网络环境应该是开放的, 管理也是较为宽松的. 高等学校的学生通常是最活跃的网络用户, 对网络新技术充满好奇, 勇于尝试. 如果没有意识到后果的严重性, 有些学生就会尝试使用网上学到的、甚至自己研究的各种攻击技术, 可能对网络造成一定的影响和破坏.

(2) 院系级的网络办公系统没有实现交互式办公. 在网上实现交互式办公, 实现全天的电子校园办公方式, 可以实现信息传递的完整性、数据的保密性和收发信息双方的不可低耐性.

(3) 校园网内部用户对网络资源的滥用, 有的校园网用户利用免费的校园网资源提供商业的或者免费的视频、软件资源下载, 占用了大量的网络带宽, 影响了校园网的应用, 造成网上办公系统的办公效率低下.

吉首大学现行的网络化办公系统安全涉及到物理安全、网络安全、信息安全和管理安全多个方面. 笔

* 收稿日期: 2009- 07- 05
作者简介: 张晓丹(1981-), 男, 湖南常德人, 吉首大学数学与计算机科学学院讲师, 国防科技大学硕士, 主要从事计算机应用技术研究.

者仅从信息安全的角度探讨 PKI 技术在网络化办公应用系统的安全解决方案. 吉首大学网络化办公系统以电子公文处理为主, 电子公文以电子文档的形式在网上传输, 必须满足以下安全需求[1]:

(1) 有效性. 确保公文在确定的时间, 确定的地点是有效的.

(2) 机密性. 预防信息的非法保存及信息的泄露

(3) 完整性. 公文在传输的过程中是完整的不被丢失.

(4) 可靠性. 电子公文无法提供手工签名和印章, 需要在信息传输过程中提供参与通信的组织和个人提供可靠的标识.

2 一种基于 PKI 的吉首大学网络化办公模型设计

设计的网络化办公系统模型需建立有效的 PKI 平台, PKI 是一种基于公钥加密技术提供网络安全的基础设施. 一个典型的 PKI 系统如图 1 所示, 包括 PKI 策略、软硬件系统、证书机构 CA、注册机构 RA(Register Authority, 即证书注册机构)、证书发布系统和 PKI 应用等[2].

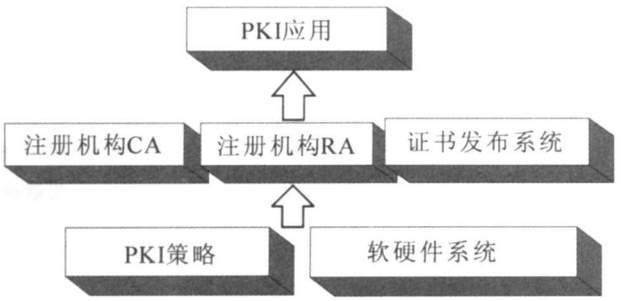

图 1 典型的 PKI 系统

2.1 信任模型的选择

吉首大学是一所综合性大学, 网络化办公系统用户由校、学院、系部、办公用户 4 级构成, 目前该系统采用的 PKI 信任模型是层次信任模型. 信任模型是建立 PKI 的理论基础, 设计合适的 PKI 信任模型关系到整个基于 PKI 的网络化办公系统的工作效能. 层次模型具有结构简单、易于实现、安全性高的特点[3]. 但是这种模型的信任关系的确立都取决于根节点, 这种过分依赖根 CA 的模式大大增加了根 CA 的负担, 一旦学校一级的 CA 出现故障, 一级 CA 和二级 CA 的信任关系就无法确立, 整个系统就会处于瘫痪的状态, 在实际运行过程中会出现 有网无用 的情况, 致使整个系统的效率低下, 不能保证信息传输的时效性, 严重制约了吉首大学网络化办公系统建设的发展. 为了最大限度地保证吉首大学校内公文传输的时效性, 必须设计新的信任模型. 笔者设计的信任模型如图 2 所示, 该信任模型将层次模型和交叉模型结合在一起, 将根 CA 的主导性削弱, 选择一级 CA 和二级 CA 在遵循 PKI 规范的前提下, 当根 CA 出现故障时履行部分根 CA 的职能[4].

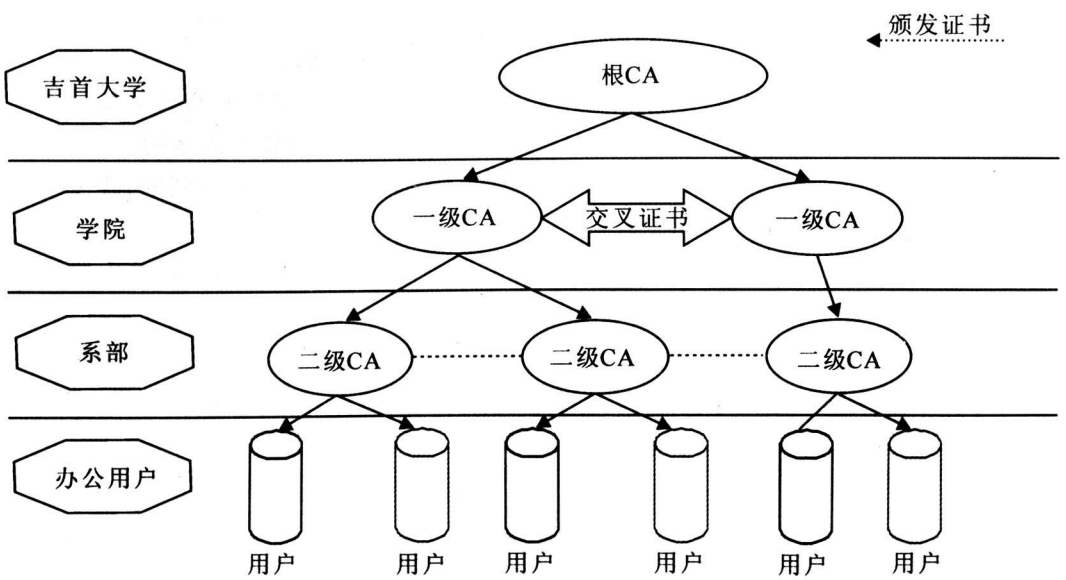

图 2 吉首大学校园网络化办公系统 PKI 信任模型

该信任模型在学校一级采用层次信任模型, 可以增加信息传输的安全性. 由于学院处于校级根 CA 的信任域内, 新加入的学院的 PKI 只需要与校级的根 CA 建立信任关系, 不必与下属的系部设立的 CA 重新进行信任关系的确立, 既避免了 CA 的重建, 又使得每个学院内部的用户都处于根 CA 的信任域内. 而此信任模型在学院一级实现了交叉认证, 当校级的根 CA 出现故障的时候, 学院一级 CA 可以履行根 CA 的部分功能, 实现学院之间和各个学院内部公文的安全传输. 综上所述, 采用混合模型的优点一是减少了学校一级根 CA 的负载, 二是在院系一级实现大交叉, 可以提高系统的运行效率和系统的稳定性.

2.2 PKI 框架的设计

根据吉首大学的安全需求, 结合 PKI 技术的特点, 设计的吉首大学的网络化办公的 PKI 框架如图 3 所示. 在此模型中, 选择建设独立的 CA 和 RA, 二者相互配合, 负责 PKI 系统中的数字证书的申请、审核、签发和管理. 密钥管理中心与 IT 系统中的用户管理中心协同工作, 负责 PKI 中的密钥对的生成、备份和恢复[5]. IT 系统中的应用系统通过安全中间件使用 PKI 系统提供的各种安全服务. PKI 中的加密服务组件负责驱动系统底层的加密软件和硬件. 安全中间件为应用系统隔离了 PKI 系统中的复杂技术细节, 而加密服务组件实现了 PKI 系统与来自第 3 方的加密软件和硬件集成的能力[6]. PKI 系统中可以配置多套加密服务组件, 以驱动不同的加软件和硬件. 安全中间件与加密服务组件的组合方式通过安全策略管理中心配置, 而不由应用系统控制, 因此保证了该 PKI 方案的可扩展能力和可定制能力.

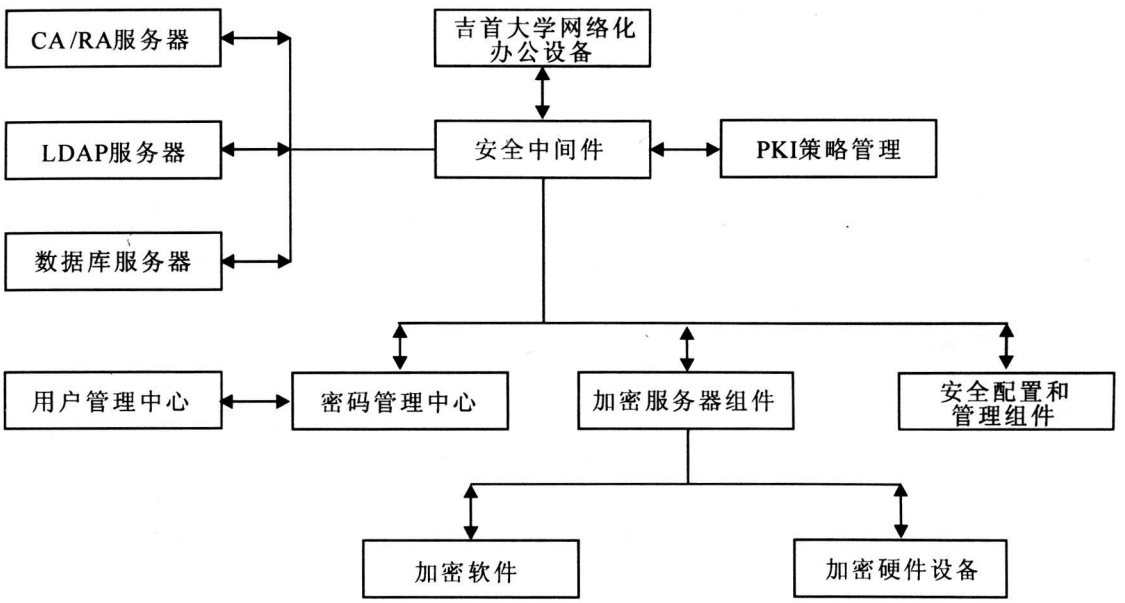

图 3　基于 PKI 的吉首大学网络化办公系统结构

该方案的优势有如下几个方面:

(1) 独立的 CA 和 RA. 认证机构 CA 是 PKI 的信任基础, 它管理公钥的整个生命周期, 其作用包括签发证书、规定证书的有效期、通过发布证书废除列表(CRL) 来确保必要时可以废除证书. 注册审核机构 RA 提供用户和 CA 之间的接口, 主要完成收集用户信息和确认用户身份的功能. 通常对规模较小的 PKI 应用系统来说, 可把注册管理的职能由认证中心 CA 来完成, 而不设立独立运行的 RA[7]. 但这并不是取消了 PKI 的注册功能, 而只是将其作为 CA 的一项功能而已. 吉首大学网络化办公的 PKI 框架, 采用独立的 RA 来完成注册功能, 保证 CA 和 IT 其余部分物理隔绝, 增强网络化办公系统的安全.

(2) 统一集中的密钥管理, 并结合加密软件和硬件设备保障密钥对的安全. 密钥管理是 PKI (主要指 CA) 中的一个核心问题, 主要是指密钥对的安全管理, 包括密钥产生、密钥备份和密钥恢复等. 对于吉首大学的网络化办公系统来说, 维护密钥对的备份至关重要. 如果没有这种措施, 当密钥丢失后, 将意味着加密数据的完全丢失, 对于一些重要数据, 这将是灾难性的. 因此, 吉首大学网络化办公的 PKI 框架设计时应该支持用于加密的安全密钥的存储、备份和恢复.

(3) 采用安全中间件. 安全中间件是以公钥基础设施(PKI) 为核心, 建立在一系列相关国际安全标准

之上的一个开放式应用开发平台,并对 PKI 基本功能如对称加密与解密、非对称加密与解密、信息摘要、单向散列、数字签名、签名验证、证书从证,以及密钥生成、存储、销毁等进一步扩充,进而形成系统安全服务器接口和通信安全服务接口. 安全中间件可以跨平台操作,为不同操作系统上的应用软件集成提供方便,满足用户对系统伸缩性和可扩展性的要求. 网络化办公系统通过安全中间件与底层的 PKI 服务组件相互作用,协同工作,从而保证整个 IT 系统的安全性. 该 PKI 方案通过构造安全中间件实现与来自第 3 方的 CA 服务器产品、加密软件、加密硬件的集成的途径. 该 PKI 方案具有集成来自不同厂商的 CA 服务器产品、加密软件和加密硬件的能力,这种能力是通过部署不同的加密服务组件来实现的. 加密服务组件向安全中间件提供支持,在加密服务组件之上的安全中间件为网络化系统屏蔽了底层的复杂的 PKI 组件.

3 结语

校园网络化办公安全在技术上要求有一种完整的安全体制来实现用户身份标识. 目前具有一定知名度的 CA 软件都是国外开发掌握的,要从他们那里获得合法认证的证书,一是需要缴纳高昂的认证费用,二是没有掌握核心技术,一些高加密应用不便实施.[7] 而国内研发的 CA 较少,对于重要的政府机关、企业、科研教育部门最好的方式就是构建自已的认证中心. 结合吉首大学自身的特点,提出了将 PKI 技术移植到吉首大学校园网络化办公系统中实施应用的方案,为吉首大学校园网络化办公的建设提供了一种参考模型,也为建立安全可信的吉首大学校园网络化办公环境奠定了基础.

参考文献:

[1] 刘钦创. 高校校园网的安全现状与对策 [J]. 现代计算机,2006(3):103-106.
[2] ANDREW NASH, WILLIAM DUANE, CELIA JOSEPH, et al. PKI: Implementing and Managing E-Security [M]. McGraw-Hill, 2002.
[3] 史伟奇. 基于 PKI 信任模型的研究 [J]. 电脑开发与应用,2005(3):36-38.
[4] 冯运波,任金强,杨义先. 传统 PKI 与桥 CA 认证体系 [J]. 计算机与数字工程,2003(6):37-42.
[5] 张文凯,曹元大. 基于 PKI/PMI 的应用安全平台模型的研究 [J]. 计算机工程,2004(9):58-61.
[6] 李明柱. PKI 技术及应用开发指南 [M]. 北京:机械出版社,2000.
[7] 关振胜. 公匙基础设施 PKI 与认证机构 GA [M]. 北京:电子工业出版社,2002.

Design of Campus Network Work Model Based on PKI

ZHANG Xiao-dan, LI Hai
(College of Math and Computer Science, Jishou University, Jishou 416000, Hunan China)

Abstract: Safety is very important for construction of the campus network work. PKI technology, as one kind of public key infrastructure, has provided a frame, under which the encrypted campus network work safety service can be implemented. In this paper, the security problems and requirements of the Jishou university network work system are firstly analysed; and then a kind network work model of Jishou university based on the mixed trust model and PKI is designed.

Key words: campus network work system; level trust model; overlapping trust model; PKI

(责任编辑 向阳洁)