PKI研究以及在数字化校园中的应用

唐 洁,张月琳
(东南大学 网络与信息中心,江苏 南京 210096)

摘 要:要保证网络应用的数据真实性、保密性、完整性和不可否认性,PKI是一种行之有效的方法。在对数字化校园发展现状分析的基础上,研究了PKI在数字化校园建设中的作用,并利用OpenCA以及OpenSSL等工具,构建一个适合校园网的PKI,为相关网络应用提供加密和数字证书等服务,不但解决了网络传输的安全问题,还能将其应用到电子邮件、电子公章及校园网络交易平台中,对目前大学数字化校园建设具有一定的参考价值。

关键词:数字化校园;PKI;数字证书;OpenCA
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)08-0159-04

Research of PKI and Its Applications in Digital Campus

TANG Jie, ZHANG Yue-lin
(Network and Information Centre, Southeast University, Nanjing 210096, China)

Abstract: PKI is a practical and effective method to guarantee the authentication, confidentiality, integrity and non-repudiation of the network applications. Analyses the status quo of the evolution of digital campus, analyses PKI and its applications in digital campus and then constructs a PKI suitable for campus that made use of OpenCA and OpenSSL. It serves the concerned network applications encryption and digital certificate, and it also resolves the secure problems of the network transfers. Also applies PKI to email, electronic-seal and business platform in campus network that valuable for the construction of digital campus.

Key words: digital campus; PKI; digital certificate; OpenCA

0 引 言

数字化校园是我国教育信息化的主题之一,也是国内高校提升自身管理水平及综合竞争实力的重要手段,很多高校都将实施建设数字化校园作为今后相当一段时间的工作重点。然而,数字化校园的实施建设是一项系统工程,涉及到高校的各个方面,最基本的一步就是网络安全体系的建设。PKI(Public Key Infrastructure)是解决信任和加密问题的基本解决方案,它提供了一个框架,使得可以在这个框架下实施基于加密的安全服务,是国际上目前较为成熟的解决开放式互联网络信息安全需求的一套体系,而且还在发展之中。要保证数字化校园网络应用的数据真实性、保密性、完整性和不可否认性,PKI是种行之有效的方法。

1 数字化校园

1.1 数字化校园概念

数字化校园是指采用先进的管理理念,应用先进的计算机及网络技术把学校现有的教学、科研、管理、生活、服务等有关的数据资源进行整合和集成,以实现统一的用户管理、资源管理和权限控制;实现资源的有效配置和充分利用,实现校务管理和服务过程的优化。

数字化校园建设内容大体包括以下主要部分:

(1) 网络安全体系建设;

(2) 校园门户网站建设;

(3) 数据标准以及数据中心建设;

(4) 建立统一身份认证系统;

(5) 校园一卡通等各种应用系统的建设以及与系统平台的集成。

另外,建设数字图书馆、校园无线网、构建远程教育平台、教育资源建设等也是数字化校园软硬件建设的重要内容。

1.2 数字化校园应用需求

在数字化校园建设中,网络安全体系建设是最基础也是最重要的一步。然而,校园网拥有几万的教师和学生用户,而且应用繁多,主要有DNS、Email、VPN、电话拨号服务、WWW、FTP、办公自动化系统、图书、教务、财务等各种基础服务和应用系统。校园网环境

收稿日期:2007-10-13
作者简介:唐 洁(1983-),女,江苏泰州人,硕士研究生,研究方向为计算机系统结构;张月琳,教授,研究方向为计算机系统结构。

开放,用户活跃,数据资源相对集中,不同的应用又有不同的安全需求。

因此,在数字化校园网络安全体系建设中,对身份识别和安全加密有很高的需求。校园网上大量传统的C/S应用是基于帐号/口令进行身份认证和访问授权的。这种方式中每个应用一般独立维护自己的口令数据库,这不但增加了系统管理维护的成本,而且增加了用户的记忆和输入负担,降低了工作效率。更为严重的是,由于用户通常在不同信息价值级别的系统中设置相同的口令,这样当低价值级别的系统口令泄漏时,会影响到高价值级别的系统安全性[1]。虽然统一身份认证系统可以解决这一问题,但是随之而来的数据安全和信任问题又需要更好的系统来解决,这就需要引入PKI技术。

2 PKI技术

2.1 PKI基础

公钥基础设施——PKI是以公钥密码学和数字签名为基础,以数字证书为核心的实现网络信息安全的一套硬件、软件、策略和过程的集合[2]。PKI使用成熟的公开密钥机制,综合了密码技术、数字摘要技术、数字签名等多项安全技术以及一套成熟的安全管理机制来提供有效的信息安全服务,通过建设CA(Certification Authority,证书认证中心)为用户签发数字证书,用户在业务系统中使用证书,完成用户的身份认证、访问控制以及信息传输的机密性、完整性和抗抵赖性[3]。

2.1.1 公钥密码学

公钥体制是目前应用最广泛的一种加密体制,在这一体制中,加密密钥与解密密钥各不相同,发送信息的人利用接收者的公钥发送加密信息,接收者再利用自己专有的私钥进行解密。这种方式既能保证信息的机密性,又能保证信息具有不可抵赖性。

2.1.2 数字摘要

采用单向Hash函数将需加密的明文摘要成一串(如128bit)密文,它有固定的长度,且不同的明文摘要成密文,其结果总是不同的,而同样的明文其摘要必定一致。

2.1.3 数字签名

数字签名是利用一套规则和一个参数对数据计算所得的结果,用此结果能够确认签名者的身份和数据的完整性。采用数字签名,可以确认以下两点:信息是由签名者发送的;信息自签发后到收到为止未曾作过任何修改。

2.1.4 数字证书

数字证书是用电子手段来证实一个用户的身份和对网络资源的访问的权限,它包含了用户身份的部分信息及用户所持有的公钥。认证中心利用自己的私钥为每一个数字证书加上数字签名,从而保证每个数字证书的权威性。每个用户通过证书及唯一拥有的私钥,就可以在互联网络中实现身份识别、数据加密等操作[4]。数字证书一般采用X.509标准。

2.2 PKI在数字化校园中的作用

通过PKI可以在校园网中构建一个可管、可控的安全互联网络,使校园网内的每个用户均可被识别,从而有效地解决了网络上"你是谁"的问题。通过PKI,可以在校园网中构建一个完整的授权服务体系,从而解决了在网络应用中"你能干什么"的授权问题。通过PKI还可以在校园网中建设一个普遍适用性好、安全性高的统一平台,方便地建立一站式服务的软件中间平台,十分有利于多种应用系统的整合。

3 PKI在数字化校园中的部署及应用

3.1 PKI部署方法

3.1.1 OpenCA部署

构建校园网PKI的工具很多,其中OpenCA是OpenCA Labs开源组织一直致力于开发的一套完善的PKI免费软件。OpenCA的树状层次结构如图1所示。

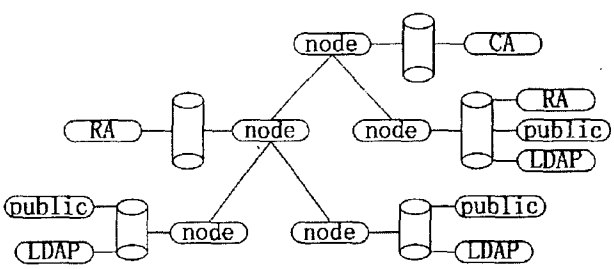

图1 OpenCA体系结构

(1) Node:这个接口管理本地节点的数据库,以及处理数据交换(与上级或下级节点交换数据)功能。

(2) CA:创建证书和CRL(Custody Receipt Listing,证书吊销列表)。

(3) RA:处理各种请求,比如编辑请求、批准请求,产生密钥对,删除错误请求等。

(4) LDAP:管理LDAP数据库,查看有效或无效的证书。

(5) Public:面向用户,为不同的浏览器生成证书请求,生成证书撤销请求,查询证书等。

3.1.2 OpenSSL部署

为了实现PKI的基本功能,必须选择一个实现了基本的对称加密、非对称加密、信息摘要等算法的软件包来搭建这样的模型,而开放源码的OpenSSL软件包可以充分满足需求。OpenSSL分为三层:底层为各种

密码算法的实现,中间层是密码算法的抽象接口,上层是围绕加密算法的 PKCS(Public - Key Cryptography Standards,公钥密码标准)的实现,以及 ASN. 1 的 DER、BER 编码接口,让这些抽象数据结构最终成为能够在网上传输、在硬盘上存储的数据[5]。OpenSSL 体系结构如表 1 所示。

表 1　OpenSSL 体系结构

PKCS 实现	编解码实现	X.509 实现
密码抽象接口		
对称加密算法	非对称加密算法	信息摘要算法

3.1.3　轻量级目录访问协议

X.500 目录访问协议是网络目录服务的标准,为了更实用,可以将 X.500 协议进行简化,取消很多限制,改变为轻量级目录访问协议 LDAP(Light Directory Access Protocol)。LDAP 使用树形结构来组织目录中的信息。支持 LDAP 协议的目录系统能够支持大量的用户同时访问,对检索请求有较好的响应能力,并且能够被分布在整个网络上,以满足大规模和分布式组织的要求。

3.1.4　PKI 部署

校园网 PKI 框架结构如图 2 所示。

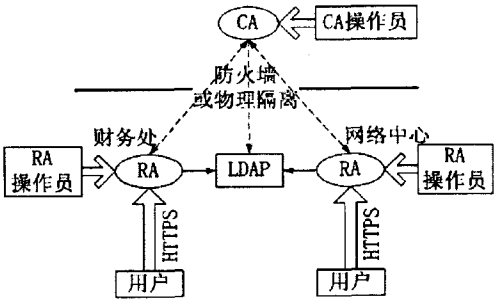

图 2　校园网 PKI 框架结构

图中:

1) CA:CA 服务器是系统核心,为保证安全,CA 服务器需通过安全信道或移动介质与 RA 服务器通信。CA 操作员可通过 Web 页面的管理工具来管理 CA 服务器。

2) RA:RA 服务器面向 RA 操作员和用户。由于学校部门较多,可能需要搭建多个 RA 服务器。数字证书从创建到销毁要经历五个阶段,其操作流程如下:

(1) 证书申请:用户通过 HTTPS(Secure Hypertext Transfer Protocol,安全超文本传输协议)方式向 RA 服务器提交证书申请请求,服务器端使用数据库方式保存用户申请信息,申请信息主要分为用户身份信息和证书相关信息两个部分。RA 操作员对该申请进行审核,若批准,则用 CA 颁发给自己的 RA 操作员证书进行签名。

(2) 证书生成:CA 服务器通过安全信道从 RA 服务器获取已审核通过的证书申请信息,该过程中为确保安全,RA 操作员也可通过带外方式将申请交给 CA 操作员。CA 操作员查看请求的签名证书,确认后在服务器端生成密钥对,私钥写入私钥库存档,以便备份及恢复,然后使用签名私钥为该请求生成证书。

(3) 证书存储:CA 操作员通过带外方式或安全信道将证书交给 RA 操作员。用户从 RA 服务器获得证书,用户可将证书保存在硬盘、智能卡等介质上。

(4) 证书发布:CA 服务器将生成的证书保存到证书库的证书表中,同时将证书的一个副本发布到 LDAP 目录服务器,用户可由此获得所需的其他用户的证书及公钥。

(5) 证书废止:用户通过 HTTPS 方式向 RA 服务器提交证书撤销申请,RA 操作员验证证书撤销申请中的数字签名,确认后对撤销申请进行签名。CA 操作员获取撤销请求后查看 RA 操作员的数字签名,确认后同意撤销并更新 CRL 列表,通知 RA 服务器证书撤销成功,然后将更新后的 CRL 发送给 RA 服务器和 LDAP 目录服务器。

要验证一份证书的真伪(即验证 CA 中心对该证书信息的签名是否有效),需要用 CA 中心的公钥验证。数字证书的验证过程:

①发送者提供一份数字证书,该证书已被认证中心签名,即用认证中心私钥加密后的证书摘要。

②接收者验证证书,接收者计算该证书的摘要并将其和证书当中的摘要(用认证中心的公钥解密获得)进行比较,如果匹配,则证书没有被修改。接收者从证书中取得发送者的公钥,验证通过发送者的数字签名后则可加密自己的会话,与发送者建立信任关系。

3.2　PKI 的应用

PKI 作为安全基础设施,能为不同的用户按不同安全需求提供多种安全服务。这些服务主要包括认证、数据完整性、数据保密性、不可否认性、公正及时间戳服务。这些安全服务为 PKI 在校园网中各项应用提供了安全保障。

3.2.1　HTTPS

涉及网络计费、本科生教务学籍与成绩管理、研究生信息管理等的应用系统与学生个人的切身利益密切相关,有些还涉及到个人"钱包"问题,其安全性应受到格外重视。为了提高 Web 服务的安全性,很多 Web 服务器软件都加入了 SSL 协议的支持。HTTPS 是一个安全通信通道,它基于 HTTP 开发,用于在客户计算机和服务器之间交换信息。利用 PKI 技术,SSL 协议允许在浏览器和服务器之间进行加密通信。然而 SSL 协议本身并不能提供对不可否认性的支持,因此再利

用数字证书保证通信安全,服务器端和浏览器端分别由可信的第三方颁发数字证书,这样在交易时,双方可以通过数字证书确认对方的身份。简单来说,HTTPS是HTTP的安全版,配置上SSL后再结合CA证书,就可以使得Web服务器的身份得到保证。

3.2.2 Email

由于Internet的开放性和SMTP(Simple Mail Transfer Protocol)协议本身的弱点,用户在收到一封邮件时,并不能肯定该邮件就是由信件中的发件人发出的,另外他也无法知道该邮件在转发过程中是否被篡改。校园网的Email系统虽然可以加入发信认证机制,但是并不能从根本上解决发信人身份确认以及发信途中被篡改等问题。将CA证书引入后,这一情况将发生根本的改变,利用数字证书和私钥,用户可以对他所发的邮件进行数字签名,这样就可以获得认证、完整性和不可否认性,如果证书是某一可信第三方颁发的,收到邮件的人就可以信任该邮件的来源,无论他是否认识发邮件的人;另一方面,在政策和法律允许的情况下,用加密的方法就可以保障信息的保密性。

目前常用的有以下两种机制[6]。

(1) PGP(Pretty Good Privacy):PGP的用户拥有一张公钥列表,列出了他所需要通信的用户及其公钥,为防止一些恶意攻击,这些公钥列表都被每个用户自己的私钥加密。在PGP中,每个用户都是他自己本人的CA,每个用户之间的信任关系都是通过网络传播的。

(2) PEM(Privacy Enhanced Mail):PEM是基于X.509v1而提出的一个专用于加密Email通信的正式因特网标准,它使用由顶至底的层次结构,建立了基于证书中心的安全机制。

3.2.3 电子公章

2005年4月1日,《中华人民共和国电子签名法》正式实施,对于在电子文件中识别交易人身份,保证交易安全起到与手写签字或者盖章同等作用等方面提供了法律保证。因此,通过CA认证方式传送的电子数据是具有法律效力的。如果把个人使用的数字签名比成"私章",那么单位的数字签名就是"公章",它能验证发件人的身份和签名以及文件的原文在传输过程中有无变动。将电子公章应用到校园网中,可以使得开放的网络更加安全,简化办公过程,提高办公效率。

高校学生离校前通常要到学校很多部门签字盖章,即所谓的"离校单",这不仅对学生本人是个麻烦的事情,也给学校各部门工作带来很大压力。PKI签名的核心元素是由CA签发的数字证书,学校各个部门都由可信的第三方颁发了数字证书,利用证书公钥和与之对应的私钥进行加/解密,并产生对数字电文的签名及验证签名,其验证的准确度是在物理世界中对手工签名和图章的验证是无法比拟的。应用电子公章后,很多工作都可以在网上完成,盖上各部门电子公章的"电子离校单"既可保证权威性和可靠性,又能有效节约资源。

3.2.4 校园网络交易平台

校园一卡通系统以学校校园网或者物理专网为载体进行建设,是集身份识别、校内消费、校务管理、金融服务为一体的新型数字化校园核心应用项目。而电子钱包是电子商务活动中购物顾客常用的一种电子支付工具,是在小额购物或购买小商品时常用的新式钱包。随着数字化校园建设的发展成熟,与"校园一卡通"相关联的电子钱包技术因其灵活、方便、快捷的优点将有很大的发展前景。电子钱包的应用需要有完善的安全系统,确保在网络上的信息的安全传输。在通信中,利用数字证书可消除匿名带来的风险,利用加密技术可消除开放网络带来的风险,这样,商业交易就可以安全可靠地在网上进行。

4 结束语

通过对高校校园网的分析和对PKI技术的研究,运用OpenCA、OpenSSL等工具将PKI应用到数字化校园建设中,很好地解决了校园网中数据传输的安全问题,并进一步利用PKI技术的优势,提出数字化校园中更多可能的应用。然而PKI作为一种还在发展中的技术,仍然有其局限性,主要体现在技术缺陷、法规制度缺乏和人为影响等因素上。因此必须不断地探索研究,解决现有的问题,才能让PKI在数字化校园建设中真正地获得更好的应用空间。

参考文献:

[1] 杨 波,王常吉,段海新,等.基于PKI/PMI的校园网安全单一登录方案[J].计算机工程与应用,2004(36):118-121.

[2] 龙银香.应用PKI构建校园网的安全环境[J].微计算机应用,2005,26(4):402-406.

[3] Andrew N,William D,Celia J. 公钥基础设施(PKI)实现和管理电子安全[M].张玉清,陈建奇,杨 波,等译.北京:清华大学出版社,2002.

[4] 孔 宁,毛 伟.用OpenCA构建自己的PKI[J].微电子学与计算机,2005,22(8):71-75.

[5] 杜广荣.PKI证书管理策略的研究与实现[D].南京:东南大学,2005.

[6] 黄 茹,张世永,周志荣,等.利用PKI加密的Email[J].计算机工程,2000,26(5):9-11.