基于PKI和SSL技术的高职院校网络安全通信研究与应用

代锐锋

（内蒙古电子信息职业技术学院）

摘要：近年来，随着社会和商业的快速发展，以及专业院校对交流的推动和兴趣。高校之间的交流给高校的网络营销业务带来了巨大的好处，同时，其安全问题也备受关注。对网络通信进行数据加密和监控，提高高校网络通信的安全性，是现阶段高校网络通信发展必须解决的重要问题。PKI 和 SSL 技术的融合，融合了高等院校的通信网络专业，对根据 PK 和 SSL 的高职院校网络通信的探索与完成进行全方位的讨论。

关键词：PKI；SSL；高职院校网络通信；

Research and application of network security communication in higher vocational colleges based on PKI and SSL technology

Dai Ruifeng

（Inner Mongolia Electronic Information Vocational Technical College）

Abstract: In recent years, with the rapid development of society and business, as well as the promotion and interest of professional colleges in communication. The exchange between colleges and universities has brought great benefits to the network marketing business of colleges and universities. At the same time, its security issues have also attracted much attention. Data encryption and monitoring of network communication and improving the security of university network communication are important issues that must be solved in the development of university network communication at this stage. The integration of PKI and SSL technology integrates the communication network specialty of colleges and universities, and carries out a comprehensive discussion on the exploration and completion of network communication in higher vocational colleges based on PK and SSL.

Key words: PKI; SSL; Network communication in higher vocational colleges;

引言

近些年，在我国在面对现代信息技术高速发展的环境趋势下，教学工作在持续进行改革创新，绝大多数高职院校都设立了自己的高职院校网。是现阶段高职院校基础建设十分重要的一部分，高职院校网为提升高职院校课堂教学管理能力及改善教学水平也起到了十分重要的功效。高职院校网络的安全性情况直接影响院校正常课堂教学活动，但现在网络安全难题愈来愈多，黑客攻击严重影响了了高职院校网络通信安全性。完善的 PKI 技术性能够用于校园安全应用系统当中，通过打造属于自己的高等院校互联网数字证书认证系统软件，再次保障了高等院校网络架构的安全。PKI 可以利用公钥理论为高校建立安全的网络通信，集成 SSL 协议，建立连接客户端和服务器的安全私密通道。

一、高职院校网络通信面临的安全问题

伴随着当代信息技术发展与推广普及化，高职院校网络的基本建设为高职院校的知识信息传送和互动增添了里程碑式的改变，这类改变让高职院校的教学活动、学生学习活动，都能够摆脱时间与空间限制，完成信息知识的无缝衔接。可以说，高职院校网络传播的产生和发展，改变了专业院校的信息交流知识。但除此之外，互联网的交互性和复杂性也影响着高校网络通信的安全性。如何保障专业院校网络通信中的网络通信安全，成为双方都非常重视的问题。，而目前，高职院校互联网中出现的网络通信安全隐患主要体现在以下几个方面。

（一）信息泄露

在目前的高职院校网络信息系统内，许多网络专业知识信息全是独创具备信息保密市场需求的，但因为高职院校网络信息全面的安全漏洞，造成这种信息在传送和贮存的过程当中被第三方盗取，或是通讯活动中一方给予给另一方的信息文档被第三方违法应用。

（二）信息篡改

在高职院校网络信息系统内，知识信息一般都具备全面性和系统性，换句话说存放高职院校网络信息系统中知识信息仅有确保自己的完好性和系统性，才存有应用其价值，但因为高职院校网络信息全面的网络安全问题，系统软件内部知识信息非常容易受到破坏，导致很多知识信息损失。

（三）身份被窃取

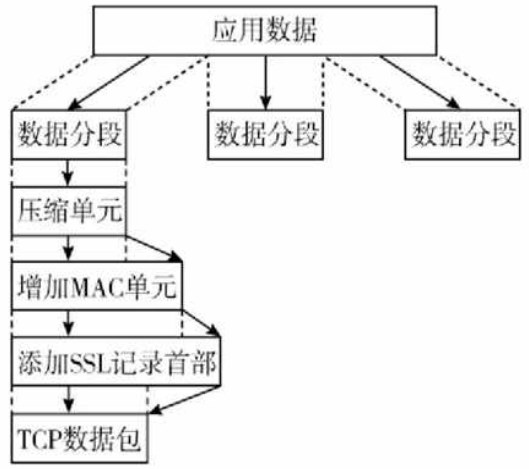
在高职院校的高职院校网络信息系统中，为了确保对高职院校全校师生服务水平，因此很多系统软件都是有身份核查设置，进而对高职院校网络系统中应用主体开展区别的看待及管理，因为高职院校网络信息系统自己的安全漏洞，容易出现使用人真实身份被窃取的情况，会让高职院校网络信息系统与被窃取者产生极大的不良影响。

二、基于 SSL 协议的高职院校网络通信模型构建

（一）SSL 协议原理及组成

SSL 协议是介于传输层协议和表单请求协议层之间的重要协议，用于支持 Internet 上安全的点对点数据通信。SSL 协议的基础协议位于传输协议之上。分析模型如下图 1 所示。

SSL 协议将处理接收到的数据。数据经过加密压缩后，会被送到下一层互联网传输协议进行处理。但是，对于接收到的数据内容，会完成解密、解压和认证，以及完成数据发送给上级用户。根据 SSL 数据处理的数据处理流程，分割、压缩模块、数据加密模块和 SSL 数据的第一部分等。具体实现过程如下图 2 所示。



SSL 协议含有 2 个十分重要的定义，各是 SSL 联接和 SSL 会话。sSL 联接是指点到点之间的关系，一般这种联接是一时的特殊类服务项目传送，每一个联接都对应的是一个会话。挥手协议建立的会话包括了加密技术、原始空间向量等，能是好几个连接的分享，从而减少了单独连接安全性主要参数商议所浪费时长[16]。手机客户端和服务器中间需要由好几个安全性 SSL 连接在一起，他们通常分享同一个会话，一旦会话设立了，就会有实际操作情况开展数据的接受和推送。SSL 协议常用的加密技术包括了密钥互换、数据库加密及其散列算法这 3 种。

SSL 协议引入了许多安全策略来提高网络数据通信的安全性，采用数据库加密、身份验证等方式提供警示安全功能，这种安全保护要求软件能够携带重要信息。Master_secret 生成的数据加密密钥可以控制数据和信息的质量，是所有法规安全的关键。如果 Internet 攻击者可以成功访问 Master_secret，会话就会被破坏。生成主键通常是通过多次哈希计算来实现的。攻击者必须进行 Master_secres 攻击才能获得云服务器的公钥或移动客户端与恶意服务器生成的随机数。在众多的反对中，流量转化为对立的认可，是必须满足的，同时有很多必要，一般来说，只需要阻止通信服务的重要信息被发布为尽可能在使用过程中。SSL 协议中有很多加密技术可以防止攻击者获取与保密相关的密文，但他可以利用“中间人”的个性和方式提取数据，并可以编辑删除等，选择 SSL 协议 它可以防止针对[18]的“中介”或“监视”。尽管 SSL 协议对于大多数安全任务都运行良好，然而，SSL 协议的大部分任务都不是必需的，例如，数据复制是不可能的。

（二）基于 PKI 技术的高职院校数字证书认证系统

将 PKI 运用到高职院校网络通讯安全性中，实施精益和可靠学校的整个过程包括许多计划和集成产品，如图 3 所示。任何基于 PKI 技术的高校数字证书认证系统都必须结合不同高校的具体情况，仔细考虑不同学校的所在地、应用需求和经济性。

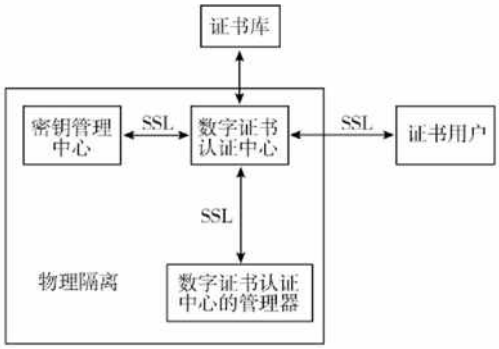


图 3　基于 PKI 技术的高职院校数字证书认证系统功能结构图

为了能可以满足高职院校网络的各类功能性需求，与此同时降低成本，高职院校网络的可信任地区界限是确立的，在开展高职院校网数字证书验证模式创新时，应该将高职院校网看作是单独的主体。在此系统当中，用户和组身份授权由中央权威进程决定，因此很容易解决信任问题。数字证书的维护实际上包括数字证书的申请、颁发、修改、注销和可视化，这是一切的关键。数字证书申请分为在线申请和离线申请两种。在线申请通常使用计算机浏览器或其他在线申请软件来申请相应的证书。离线应用程序是一种离线支持形式，支持员工直接从专业组织接收内容。批准后索取证书。本文证书申请表选择线下申请方式，因为报名网站都在学校，因此有利于教职工与学生去申请和注册网站审批。数字证书拥有比较复杂的签发全过程，当验证中心管理者接受有关申请后，若签证办理验证成功则表明客户申请资格证书要求获得允许[201。给消费者签发加密证书时，必须双因素认证中心得到加密密钥对，数字证书验证中心对证件开展签字，全部回到客户资料都要通过验证中心签字以确保消息完好性，其主要步骤如下图 4 所显示。加密证书签发结束后，双因素认证中心及其数字证书验证中心中间都有着和认可彼此之间的资格证书，二者都是基于数字证书完成 SSL 的安全性网络通讯。

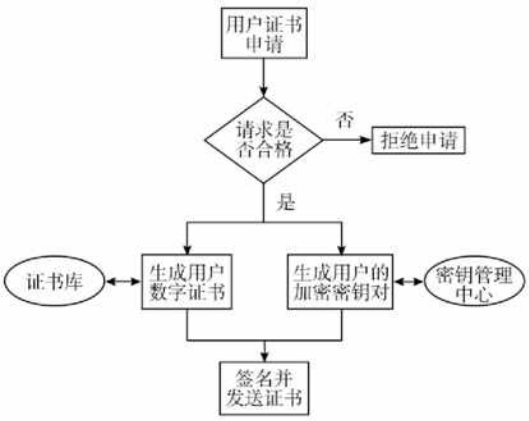


图 4　数字证书签发流程图

密钥管理方法中心获得国家有关机构受权后，可以在特定通讯环节中开展保密破解，其本身是没有进行数据加密的密钥，只不过是提供一个可以进行密钥修复的方法。运用密钥管理方法中心能够实现密钥原材料的备案、消毁、验证、销户等，适当的时候，在征求用户或法律法规下才可以解开并取下代管密钥。

PKI 运用中的关键问题之一就是密钥管理方法，现阶段针对同

一个 PKI 实体线并且拥有好几个密钥对已经十分普遍，文中所提出的高等职业院校安全通信应用系统中数字证书认证管理系统使用的是不同类型的密钥安全保密性及不能否性 2 种服务项目分离出来开体制。签名证书中的私钥由客户自行创建，禁止其他用户知晓私钥的相关信息，保证了信息的完整性和不可否认性。加密证书中的私钥由密钥管理中心代用户生成，备份到用户对象的文件系统中，用于解密密钥。一般来说，证书的有效期为 2–3 年，用户必须及时更新密钥。每次用户创建当前证书和以前使用过的几个“旧”证书时，都会创建用户私钥的历史记录。.由于密钥有过期日期，因此应采取适当的预防措施来存储过期的密钥，以避免数据恢复的风险。

（三）基于 PKI 技术和 SSL 协议的高职院校网络安全通信模型构建

高校网络通信的建立基于 SSL 协议数据加密，保护数据不受监控。移动客户端和服务器创建一个可信身份存储库，以确保彼此的身份有效。，合法且不可信任。在高性能大学通信网络模型中，服务器是院系或学校的数据中心，移动用户是数据用户。该标准的核心是 SSL 协议，它位于应用层和 TCP 协议之间，数据的采集和处理依赖于应用层控制模块。如下图 6 所示。

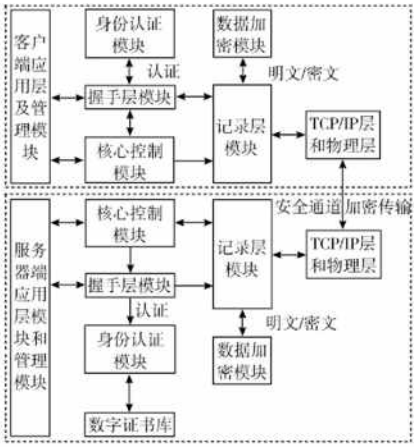


图 6　密钥管理中心系统结构模块逻辑图

全部模型顶层是网络层模块，其他软件模块都是围绕运用模块相连的。网络层模块在接受到数据后，会让数据予以处理并获得适宜的数据文件格式，数据经过握手层模块推送传送到纪录层模块当中，所有网络层模块文件都是密文文件。所有模型控制设置均由控制模块控制，用户数据传输通过本网站完成。用户可以使用模板来设置私人聊天、公钥和监控私人凭证。整个结构的中控部分是中控模块，它利用数据层模块和握手层模块完成交互，为服务器及其移动用户提供身份证明。

所有信息在传输前都必须经过处理，然后进入数据传输阶段。当移动客户端和服务器端就协议版本达成一致后，将使用加密和认证算法生成共享密钥，完成数据加密和处理，实现安全通信。交流的主要目的是为了方便文字的交流。在通信过程中，双方必须进行交互，在双方完成对话并生成加密密钥后进行握手。. 网络安全设备运行时，SSL 握手模块接收并上传大量报文，需要解码的报文来自不同方、不同语言，取决于下一步的工作和接收方的连接.当时，“形势新闻→姿势”系统区分了语言类型。收到消息后，不仅需要通过语言来判断，而且语言的差异会延伸到服务端和客户端使用手机的方式上。

录音系统采用并行加密算法对数据进行加密，分为流加密算法和块加密算法。因为流加密算法生成的每个文件不超过一个字节，所以每次分层都要完成一次。

三、SSL 协议及其相关技术研究

SSL 是安全性套接字层的英文缩写，作为一种专业化的互联网信息安全协议书，它在运行中关键的作用是为通讯的两方给予安全信息传送安全通道，具体而言具有下列三个基本特征。

（一）传输通道是安全的

数据通道基于 SSL 协议，采用数据加密算法。数据文件的这种数据加密是随机事件。数据发送给第三方后，从通信网络侧接收会话密钥。.为了加快数据文件的响应速度，通常采用对称加密算法。

（二）安全通道是通过认证的

在数据通信活动中，安全的数据通道是非常必要的标准，因此有必要证明通信服务器在通信活动中的安全性。也就是说，在数据通信活动中，如果一端是服务器，另一端是用户，则用户必须对服务器上的数据文本进行认证。服务器对客户端的认证可以根据系统优化的需要和对策来确定。通信使用身份证书和可信第三方认证来帮助客户端和服务器确认数据中对方的身份。

（三）安全通道是可靠的

特别地在信息的传输中，信息的完整性得到保证，在合约中，信息的完整性通过消息公平校验来保证。在现有的数据完整性校验技术中，流行 MAC 理论。

结论

高职院校安全性网络体系结构的构建是现阶段高职院校基础建设及其基础教育改革的主要方位，高职院校网络通信实体模型可以为院校提供一个行政工作、教学交流、消息传输的方便服务平台。文中根据 PKI 技术性融合 SSL 协议书构建了高职院校网络信息安全通信模型，根据该实体模型能够实现手机客户端及服务端的网络信息安全传送。此系统的关键所在核心内容是构建根据 PKI 科技的数字证书系统软件。为了能融入高职院校的生活环境和安全操作要求，文中实际制定了双因素认证中心具体实施方案。为了能认证本次定制的高职院校网络通信管理体系实效性和应用性，在 Stunnel 软件上构建了网络通信实体模型，并通过 2 台电子计算机各自做为网络服务器和手机客户端开展仿真实验。模拟仿真数据显示，高职院校网络通信系统软件可以正常运转，运行中可以确保系统安全性。可是文中所提出的系统软件仅展开了仿真分析，后面拟向其用于高职院校中，打造出根据 PKI 及 SS L 合同的高职院校网络信息安全通讯系统。

参考文献：

[1]VPN 网络中的通信安全隐患论述[].陈春平。信息通信.2019（05）

[2]RFCcertDT：SSL/TLS 中证书验证的测试工具[J].陈。西安电子科技大学学报.2019（03）

[3]基于 SSL 安全协议实现工业控制通讯协议加密及认证的研究[J].高锐强，朱虹，贾立东，孙超.化工设计通讯.2019（01）

[4]HTTPS/TLS 协议设计和实现中的安全缺陷综述[J].韦俊琳，段海新，万涛.信息安全学报.2018（02）

[5]一种基于混合加密的数据安全传输方案的设计与实现[J].未利民，未晓锐，信息网络安全.2017（12）

[6]大型移动网络信息传输安全性评估方案设计[J].叶卫，盛红雷，黄宇腾，韦金良.电子设计工程.2017（23）

[7]云存储环境中基于离线密钥传递的加密重复数据删除方法研究[J].张曙光，咸鹤群，刘红燕，侯瑞涛.信息网络安全.2017（07）

[8]基于 PKI 技术的应用及密钥的管理探讨[J].何历怀。网络安全技术与应用.2016（07）

[9]基于 ECC 算法的 SSL 协议改进[J].杨文军，孙希杰，王春东，莫秀良.南开大学学报（自然科学版）.2016（02）

[10]高速无线局域网大数据传输内存安全监测仿真[J].王晓雯，柴大鹏.计算机仿真。2016（04）

课题号：NJZY21299，项目名称：基于 PKI 和 SSL 技术的高职院校网络安全通信研究与应用