DOI:10.13657/j.cnki.gxkxyxb.2013.01.020

广西科学院学报
Journal of Guangxi Academy of Sciences

2013,29(1):62～65
Vol. 29,No. 1 February 2013

电子招标投标系统的安全防护设计方案
Electronic Tendering and Bidding System Safety Design

刘 菁
LIU Jing

(广西有色金属集团有限公司,广西南宁 530028)
(Guangxi Non-ferrous Metal Group Co.,Ltd.,Nanning,Guangxi,530028,China)

摘要:针对电子招标投标系统遇到的安全问题,提出一个电子招标投标系统的安全防护设计方案。该方案从系统备份、网络安全防护、应用软件安全防护、安全制度等方面,通过部署高性能的安全设备、使用数字签名、数据加密等技术以及完善的管理制度来规范网上招标投标的全过程,为招标方及投标方提供了一个安全的数据交换平台,为电子招标投标系统的运行提供有效的安全保障。

关键词:系统安全 电子招标投标 设计方案
中图法分类号:TP311.522 **文献标识码**:A **文章编号**:1002-7378(2013)01-0062-04

Abstract:We provided a design scheme of safety protection for electronic bidding and tendering system,in order to solve the related safety problems. This plan included the system backup,network security maintenance,software security maintenance and security system. The whole process of bidding and tendering was regulated by adopting high-quality security equipment,digital signature,data encryption technique and other techniques, and management system, which offered a safe platform for data interchange between tenderer and bidder,and guaranteed security protection to electronic bidding and tendering system.

Key words:system safety,electronic tendering and bidding,design scheme

随着电子商务和项目管理信息化的迅速发展,招标投标行业和社会各界已经广泛和迫切地意识到,运用电子信息技术改造和提升传统纸质招标投标形式,推行电子招标投标,是进一步有效规范招标投标公开、公平、公正和诚信秩序,转变招标投标行业发展方式,促进行业健康、科学发展的必然趋势。

然而,电子招标投标在带来便利的同时也带来了不安全因素,由于电子招标投标系统是构建在开放的、虚拟的互联网中,而且系统中传输和存储着大量机密和敏感的数据,系统安全建设就成为了一项非常重要的工作。另一方面,招标投标系统设计的招标投标流程是否合法有效、招标投标运用电子信息而产生的一系列特定问题的操作处理等都需要相关配套的直接依据和制度保障。作者参与了一项省级电子招标系统的建设工作,本文就该电子招标投标系统的安全防护设计做简要介绍。

1 电子招标投标系统遇到的安全问题

电子招标投标系统与互联网通常采用逻辑隔离,用户既有通过 Internet 进入访问的合法用户,也有来自内部及接入单位的用户,电子招标投标系统网络面临着两个方面的安全威胁:一是外部威胁,即来自 Internet 黑客的各种恶意攻击,以及依靠网络传播渗透的各种病毒、木马。二是内部威胁,内部威胁主要来自内部人员的移动存储设备携带的各种病毒、代码、木马,以及内部人员的误操作或恶意攻击。网络系统的这些威胁如果不能有效消除,首先会危害网络数据的传输,由于现在很多网络协议基于明文传输,客观上存在被窃听和篡改的可能,任何一个对通信进行监测的人都可以对通信数据进行截取。其次,如无安全的数据库及个人终端安全保护措施,不能抵御来自网络上的各种对数据库及个人终端的

收稿日期:2012-10-05
修回日期:2013-01-08
作者简介:刘 菁(1986-),女,助理工程师,主要从事网络和计算机设备管理工作。

攻击,数据在传输和存储的过程中遭到人为的恶意篡改,将导致难以想象的后果。

2 电子招标投标系统的安全防护设计方案

为解决电子招标投标系统遇到的安全问题,电子招标投标系统的安全防护应从系统备份、网络安全防护、招标投标应用软件安全防护、安全防护制度等方面进行综合设计。

2.1 系统备份

电子招标投标系统主要用于内部办公、网络招标投标、电子监察等,连接了包括监察部门、行业监察单位以及国际互联网,涉及行政管理、行政业务访问等大量业务。另外,无论是相关的硬件问题、配置改变、应用程序故障、病毒攻击,还是恶意黑客攻击都可能造成系统的服务器瘫痪。在网络设计上要从应用服务器集群、数据库服务器、核心交换层、汇聚层、存储系统、异地容灾备份等方面,充分考虑硬件备份、应用级备份和数据级备份,保证电子招标投标系统网络是一个实用的、高可靠、高效率、高扩展性、高安全性的信息化系统。

应用服务器集群按照网站服务器、会员服务器、业务服务器、开/评标服务器 4 个类别分别配置 4 组应用服务器,采用每 2 台服务器组成一组应用服务器均衡负载群集,应用负载均衡技术,当某台服务器出现故障时,负载均衡服务器会自动进行检测并停止将服务请求分发至该服务器,而由其他工作正常的服务器继续提供服务,保证服务的可靠性。数据库服务器采用 2 台高性能 PC 服务器,实现双机热备份,当一台主机因为某种原因出现故障,如死机、主机断电、病毒发作、硬盘损坏等,不能继续提供服务时,备用机能够在规定的时间内接替主机的服务,继续提供服务,从而将系统风险降低到最低限度。核心交换层是电子招标投标系统的核心交换平台,主要负责完成各汇聚层的流量聚合、提供高速的信息传输和数据交换、提供路由快速收敛功能、隔离故障域。网络核心层是整个网络平台的神经中枢,采用 2 台高性能多业务核心路由交换机组建高性能的双核心网络平台,双核心之间采用双链路捆绑(port-channel),增加核心设备之间的带宽,同时做冗余链路保障。2 台核心交换机通过安全网关,以 2 条运营商 100M 链路接入国际互联网。汇聚层是网络的信息汇聚点,是连接接入层和核心层的网络设备,为接入层提供数据的汇聚\传输\管理\分发处理;汇聚层为接入层提供基于策略的连接,控制和限制接入层对核心层的访问,保证核心层的安全和稳定。电子招标投标系统的汇聚网络包含 2 个部分:服务器区域汇聚和共用服务器区(交易中心开、评标和办公区域)汇聚。服务器区域配置 2 台路由交换机,2 台汇聚交换机分别与 2 台核心交换机连接,实现链路冗余和负载均衡。共用服务器区的应用服务器集群、数据库服务器、防毒服务器、备份服务器、AD 服务器、安全接入网关,以及漏洞扫描、WEB 安全防护、日志审计等设备分别以 FE 链路连接至 2 台汇聚交换机。存储备份系统主要包括磁盘阵列、交换机和存储管理软件等。磁盘阵列采取关键部分冗余、支持多种 RAID 方式等技术,最大程度地保证减少因为硬件故障造成数据丢失。存储系统配置 2 台磁盘阵列,一台为主用磁盘阵列,另一台为备份磁盘阵列。存储控制器采用多核处理器,支持冗余备份、镜像等功能。此外,采用双链路冗余连接,服务器上配置双 HBA 卡,配置双交换机。当一条线路出现 HBA 卡、连接线路、交换机或连接端口故障时,另一条冗余线路可提供可靠性的数据正常访问。异地容灾备份即建立容灾系统。建立容灾系统是提高重要信息系统健壮性的重要手段。当本地生产中心由于故障或其它不可预知的事件而出现非计划性的宕机时,异地容灾中心可以及时地接管各项业务,继续提供应用服务,保证业务的连续性。实现业务系统健壮、可靠的运行。

2.2 网络安全防护

电子招标投标网络系统是电子招标业务正常运转的高速通道,必须做好安全防护工作,确保各种网络服务安全、稳定、快捷,满足各应用系统间数据畅通传送的需求。首先,建设一个安全信息平台,即安全网管,包括对安全产品事件的收集、分析和管理;这里的安全网管不仅包括对安全设备的管理,而且也包括基础网络设备如防火墙、交换机等设备安全特性的管理与维护,还应该包括安全知识库,病毒知识及防病毒软件升级库等。其次要进防火墙部署、入侵防御部署、VPN 部署、安全网闸部署和防病毒部署。

防火墙重点考虑支持外部攻击防范、内部安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能,能够有效的保证网络的安全,同时还要对防火墙做硬件上的升级和配置上的评估,避免网络结构上存在旁路,对其软件存在的漏洞进行修补或及时升级。入侵防御部署是在电子招标投标系统专网核心层入口以及内部重要网段的数据流实施监控,对攻击实

现实时防护，尤其对服务器群进行虚拟补丁管理，保证对“拒绝服务攻击 DoS”的防范。VPN 部署是在电子招标投标系统专网核心层建立 VPN 接入和认证中心，保证全网都能够从外网安全接入，另外设 IPSEC VPN 线路为主线路做备份，以便于在主线路不可用时备用。安全网闸部署是为了保证内部网络的绝对安全，电子招标投标系统专网采取安全分区的方法，从物理链路上分为内网、外网两部分，同时采用安全隔离网闸实现内、外网之间的信息交互和摆渡，保证内、外网络在隔断的状态下数据的交流。防病毒部署是增加网络版企业防病毒软件部署，通过管理员控制台对网络内的计算机进行安装、设置、管理、维护和升级，从而实现全局网络防病毒的目的。最后还要进行周期性风险评估与系统加固。组建专业的安全服务团队承担风险评估与系统加固服务，可以对网络结构、网络服务、主机系统、数据、应用系统、安全系统、安全相关人员、处理流程、安全管理制度、安全策略等进行风险评估，根据评估结果制定设备加固手册，系统风险修正措施以及系统安全指导性架构。加固以评估结果为依据，实现对漏洞的修补，加强系统安全。

2.3 招标投标应用系统安全防护

自 2012 年 2 月 1 日起，全国各地推行《招标投标法实施条例》，为电子招标采购扫清了法律上的障碍。电子招标投标应该与传统的纸制招标投标一样，其采购过程必须符合招标投标法的要求。因此电子招标投标应用系统设计面临许多要解决的技术问题。第一，招标投标的参与方很多，各个招标投标主体的数量非常庞大，系统如何确认参与方的身份；第二，投标文件如何封标、如何传送，如何拆封以及开标如何进行。第三，招标投标过程产生的电子文档如何保密、如何防篡改、签署过的电子文档如何防抵赖等等。由于我国电子招标投标法尚未颁布，国内电子招标投标面临法规不足和标准缺失的问题。各电子招标投标软件开发商运用现有的技术积极进行这方面的探索，目前普遍采用的行之有效的安全防护技术包括数字证书、数字信封、数字签名和时间戳等，这些技术为电子招标投标提供了可靠的安全保障。

数字证书解决投标主体身份认证问题。招标投标的各参与方使用浏览器访问电子招标投标系统，进行系统安全登录，系统对用户完成身份认证和访问控制流程。在用户浏览器和系统服务器之间，用户出示自己的数字证书供服务器验证（用户证书存放在 USBKey 中，登录的时候通过 pin 码来认证，现有技术下，不存在伪造现象），服务器出示其证书供用户确认。如果互相认证通过，用户则能登录应用系统。用户登录后还要进行身份识别（如是投标人、招标人还是评委等），确定访问者能够访问的系统模块。这种基于身份证书的访问控制安全功能需要使用证书解析 API 来完成对证书内容的解析，然后将解析结果传给访问控制模块，由访问控制模块来实现基于证书的访问控制。这样就解决了电子招标投标庞大客户群的身份认证问题。

数字信封技术解决标书的保密性问题。所谓信息加密就是通过密码算术对数据进行转化，使之成为没有正确密钥任何人都无法读懂的报文。为了读懂报文，必须重新转变为它的最初形式——明文。而含有用来以数学方式转换报文的双重密码就是密钥。通常的加密算法分为两种：一种叫私钥加密算法或对称加密算法，另外一种是公钥加密算法或非对称加密算法。两种加密算法各有优缺点，数字信封是将对称密钥通过非对称加密（即：有公钥和私钥两个）的结果分发对称密钥的方法，是一种综合利用了对称加密技术和非对称加密技术两者的优点进行信息安全传输的一种技术。数字信封既发挥了对称加密算法速度快、安全性好的优点，又发挥了非对称加密算法密钥管理方便的优点。在电子招标投标中利用稍作改动的数字信封技术能够很好地解决投标文件密封和解封以及电子开标问题。首先，投标方采用随机得来的对称密钥加密投标书，将此对称密钥用招标代理的公钥来加密一次，再用投标人的公钥进行再次加密，之后将再次加密的密钥和加密的投标文件一起发送给招标代理。按招标投标法的规定投标文件必须在截标之日前传送到招标代理处，投标文件由于经过了招标代理公钥和投标人公钥的两层加密，单方面的私钥是无法打开投标文件的，因此开标前投标文件存放在系统中是安全的。其次，在开标的时候，各投标人提前用私钥依次解开各自投标文件第一层数字信封。当开标时间到来时，招标代理用私钥一次打开所有投标人的第二层数字信封，得到对称密钥，然后使用得到的对称密钥逐一解开所有投标人的加密投标文件。这种技术的安全性相当高，很好地保护了招标文件传送、存放和开标的安全。

数字签名解决招标投标文件的完整性和不可串改。招标投标的参与方在进行招标投标文件传输和招标投标信息确认时，需要留下类似于传统纸质招

标投标文件签章的“痕迹”。即在相应的电子文档中应用相应的技术手段确认操作确实由发起人完成,招标投标文件等电子文档没有被修改,且不可抵赖。电子招标投标系统普遍采用数字签名技术来实现交易的抗抵赖性。招标投标的各方在进行重要操作时,必须对于招标投标文件的确认信息进行数字签名,签名后的结果被保存下来。当出现纠纷时,CA认证中心作为公信的第三方,对于数字签名进行验证。任何对于数字签名原文的微小的篡改都能够被检验出来,因此,通过数字签名的校验判断招标投标文件的原文是否被篡改是十分有效的。

时间戳能够为电子文件提供日期和时间信息的安全保护。在整个招标投标过程中时间是十分重要的信息。招标投标文件签署的日期和签名一样均是十分重要的防止文件被伪造和篡改的关键性内容。在签署各种招标投标文件的时候,要求参与各方不能否认其行为。这其中需要在经过数字签名上打上一个可信赖的时间戳,从而解决一系列的实际和法律问题。时间戳产生的过程为:用户首先将需要加时间戳的招标投标文件用 Hash 编码加密形成摘要,然后将该摘要发送到 DTS(时间戳服务商),DTS 在加入了收到文件摘要的日期和时间信息后再对该文件加密(数字签名),然后送回用户。时间戳是一个经加密后形成的凭证文档,它包括 3 个部分:(1)需加时间戳的文件的摘要(digest);(2)DTS 收到文件的日期和时间;(3)DTS 的数字签名。可信时间戳是由国家法定时间源来负责保障时间的授时和守时监测,任何机构包括 DTS 不能对时间进行修改以保障时间的权威性和具备法律效力。

2.4 安全防护制度

信息系统发生的大部分安全事故往往都是由于安全管理制度的漏洞所引发。因此仅仅依靠电子招标投标系统各个层面的安全保障技术手段并不能完全保证电子招标投标系统的安全运行。安全管理制度不落实和安全防范意识薄弱将是造成电子招标投标系统安全问题的主要原因。为了保证各个层面的安全保障技术手段能够真正发挥作用,切实保证电子招标投标系统的安全,需要做好以下三方面的工作。(1)系统化管理。安全管理制度体系是自上而下、自下而上,基于过程、基于状况、基于资源、基于活动的文件化管理。所有的制度都不是单独设立的,而是制度体系的一部分,电子招标投标系统所属各个组成部分的岗位责任制、各项管理制度、报告制度、内部审计制度,以及应急预案制度等组成一整套完整的安全管理制度体系。(2)工作制度。安全管理制度是规范和指导电子招标投标系统全部安全工作的程序和方法,通过管理制度确保人人各司其职,各尽其责,忠于职守,勤奋工作,各项信息安全活动做到规范化、高效率化,并在各职能部门和环节之间分工、协调地展开。(3)保障机制。信息安全管理制度的建立使电子招标投标系统信息安全管理具有自稳、自组功能。电子招标投标系统内部和外部各种动态信息根据信息内容迅速按规定的流程进入责任系统,由相应的责任人启动相关程序采取对应措施,动用各种资源(包括应急资源)及时处理和解决问题,并根据问题调整信息安全管理制度。

3 结束语

本文从实际业务需求出发,从系统备份、网络安全防护、应用软件安全防护、安全制度等方面阐述电子招标投标系统的安全防护设计方案,通过部署高性能的安全设备、使用数字签名、数据加密等技术以及完善的管理制度来规范网上招标投标的全过程,为招标方及投标方提供了一个安全的数据交换平台,为电子招标投标系统的运行提供了有效的安全保障。该设计方案已经在某省级公共资源招标中心成功实施并安全运行,取得了较好的效果,能够满足相关的电子招标投标的安全性需求。

参考文献:

[1] 陈相琳. 数字签名技术及算法的研究[D]. 哈尔滨理工大学,2007(1):10-12.

[2] 花奎. 安全中间件架构的设计与实现[D]. 南京理工大学,2007,15(3):38-46.

[3] 李冬冬. 网络防火墙关键技术的研究与实现[D]. 燕山大学,2001,35(13):67-69.

[4] 徐立新,郭祖华,陈震,等. 在线招投标 Web 系统安全结构及关键技术的研究[J]. 计算机工程与设计,2006,27(17):3142-3144.

[5] 张璐,张景,井浩等. 网络采购系统中安全机制的研究与实现[J]. 计算机应用,2007,27(2):318-323.

(责任编辑:邓大玉)