

构建市级电子政务安全平台

冉 艳,胡学钢

(合肥工业大学 计算机学院,安徽 合肥 230009)

摘 要:随着信息化建设的逐步推进,电子政务系统对其安全运行的依赖性越来越强。为了给市级电子政务系统的运行提供必要的安全保障,文中在基于 PKI 技术的安全平台建设的基础上,又增加了为系统防范网络内部的行为滥用和网络外部的恶意攻击而提供的安全辅助支撑平台,从而构建了市级电子政务系统全方位的安全平台。

关键词:安全平台;安全支撑平台;电子政务;PKI

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2007)08-0144-04

Setting up Safe Terrace of City Class Electronics Governmental Affairs System

RAN Yan, HU Xue-gang

(School of Computer & Information, Hefei University of Technology, Hefei 230009, China)

Abstract: Push forward gradually along with the information-based construction, the electronics governmental affairs system as to its dependence of the safe movement is more and more stronger, for providing the safety guarantee of the necessity for the movement of the city class electronics governmental affairs system, in the text at according to the PKI foundation of the technical and safe terrace construction up, and then increase for the system guards against the network inner part of behavior abuse and the malice attack of the network exterior but the safety that provide the assistance prop up the terrace, thus setting up the all-directions safe terrace of the city class electronics governmental affairs system.

Key words: safe terrace; security supports platform; electronics governmental affairs; PKI

0 引 言

电子政务是近几年才在我国开始的政府服务方式,并快速普及到各级政府职能部门。电子政务的实施可转变政府部门的工作模式,提高办公效率,加强监督功能,反腐倡廉,它在实现各级政府间的信息传递,改变政府在公众心目中的形象。搞好电子政务,是我国各级政府和企业参与国际竞争最基本、快捷的手段。

所谓电子政务(e-Government Affairs),就是政府机构应用现代信息和通信技术,将管理和服务通过网络技术进行集成,彻底转变传统工作模式,实现公务、政务、商务、事务的一体化管理与运行,在互联网上实现政府组织结构和 workflows 的优化重组,超越时间和空间及部门之间的分隔限制,向社会提供优质和全方位的、规范而透明的、符合国际水准的管理和服务^[1]。

电子政务的功能定位为以数据获取和整合为核心、以信息安全为基础,面向决策支持、面向公众服务。

其中“信息安全”既要求电子政务系统能够提供统一的身份认证机制,又能进一步提供授权、加密、完整性、抗抵赖等安全服务接口的平台,遵循科学、先进、安全、实用和经济的原则,文中针对市级电子政务系统实际情况和要求,建议不完全照搬现成的商用 PKI 系统,而是选择能够支持集中管理、扩展性好、维护成本低、使用起来方便灵活的密钥管理系统作为安全平台基础,同时选择国内自主产权的密码产品和密码技术构建市级电子政务系统。

1 构建安全平台

1.1 安全平台的结构

安全平台为各用户终端发放公开密钥和数字证书,统一标识用户在市政府电子政务系统中的数字化身份,这样,在安全平台的各种安全机制的支持下,一个具备合法数字化身份的工作人员和合法用户,可以在任何时间和任何地点访问被授权的信息和资源;同时,也可以有效保证业务处理过程中信息的机密性、完整性,有效防止来自内部和外部的对信息的恶意攻击;

收稿日期:2006-10-26

作者简介:冉 艳(1974-),女,贵州贵阳人,工程师,研究方向为计算机技术应用;胡学钢,教授,研究方向为人工智能、数据挖掘。

再者,安全平台支持的审计管理功能为安全应用系统提供了审计服务的底层支持,应用系统可根据不同的用户需求编制完善的审计服务和审计管理软件,不仅对非法访问和操作做出记录,并且对内部用户的系统使用情况做出记录,从而便于管理者对行为滥用者的行为做出管理策略^[2],其体系结构如图 1 所示。

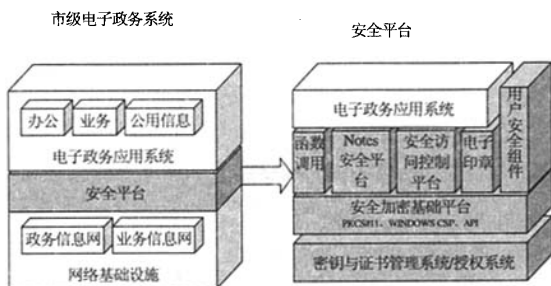


图 1 安全平台的结构

1.2 安全平台的安全机制

安全平台应提供身份认证、授权与访问控制、保密性、完整性、抗抵赖等安全机制,各种安全机制之间相互依赖。安全机制的层次结构及与电子政务系统的关系如图 2 所示。

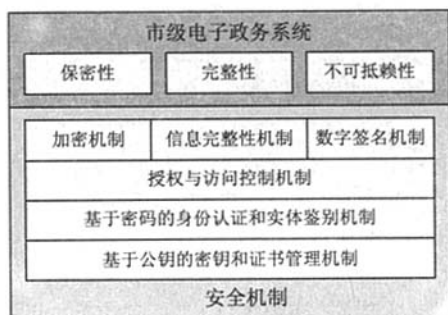


图 2 安全平台为市政府电子政务系统提供安全服务

安全基础平台应以基于公钥的密钥和证书管理系统为基础,建立统一的身份认证机制对用户进行管理。它对信息的防护可分为两层结构:第一层防护为授权和访问控制,通过灵活的授权与访问控制机制,控制对信息的访问者范围;第二层利用密码手段进一步保证信息的保密性、完整性和不可抵赖性。

(1) 身份认证机制。

安全平台提供统一的身份认证机制。用户的身份证书是用户在电子政务系统中的唯一身份标识。基于证书的身份认证方式代替了原有基于口令的认证,不仅提高了安全性,也为多个应用业务系统实现单点登录奠定了基础。

平台支持的身份认证分为两个阶段:本地认证、基于网络的双向认证。首先,个人终端通过 IC 卡认证用户的合法身份。然后个人终端将用户身份传到服务

器,进行基于公钥的双向认证^[3],认证过程如图 3 所示。严格的身份认证机制为下一步的访问控制和授权奠定基础。

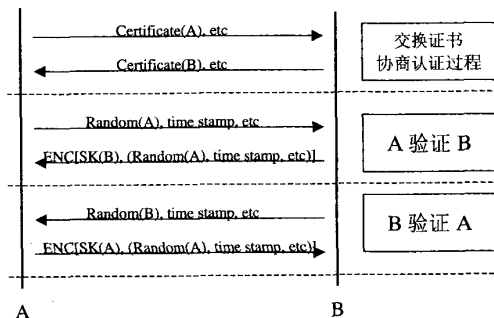


图 3 安全平台中的双向身份认证

(2) 授权与访问控制机制。

为了适应电子政务系统的集中管理要求,安全平台采用集中授权访问控制的模式。授权中心具有两大功能:一是集中管理用户的授权属性信息;二是为用户发放授权证书。用户的授权属性信息由负责的业务人员管理,应用系统通过验证用户的身份证书和授权证书来判定用户权限,实现访问控制。由于授权证书中可以提供各种访问控制所需要的用户属性信息,应用系统可以方便地实现多种访问控制机制,如基于用户标识(名称)的访问控制、基于用户角色的访问控制、基于用户和资源级别的访问控制等等。访问控制的粒度可灵活变化,从基于 IP 和端口的控制到基于 URL 的控制直至对数据库字段的控制,粒度从粗到细,根据不同应用进行选择。

(3) 数据机密性。

安全平台中的数据机密性体现在两个方面^[4]:

①对信息源的加密保护:办公系统中的信息源主要指以文件方式或数据方式存在的文字、数字、声音、图像信息。安全平台提供文件加密、加密 API 的方式保证信息存储的机密性。

②信息传输的加密通道:安全平台中各个基于网络的安全子系统均提供信息传输加密的功能,根据应用的具体需求,选择是否需要加密传输或在哪一层进行加密传输,或在应用系统中调用加密 API 来建立加密传输通道。

安全平台既支持公钥加密体制,也支持对称密钥加密体制。在不同的应用场合选择不同的加密手段,不仅能保证系统的安全性,而且可以极大地提高系统效率。

(4) 数字签名机制。

办公系统中,公文交流中的完整性和不可抵赖性是一个重要的需求。安全平台的数字签名机制也主要

体现在与公文交流密切相关的安全子系统中,如用户安全组件中的文件和邮件加密系统、电子印章系统等,应用系统则调用 NOTES 安全平台功能、安全平台安全 API 等实现数字签名。

2 构建安全支撑平台

随着信息化建设的逐步推进,电子政务系统对其安全运行的依赖性越来越强,为了给市级电子政务系统的运行提供必要的安全保障,在对系统进行基于 PKI 技术的安全平台建设的基础上,还需要为系统防范网络内部的行为滥用和网络外部的恶意攻击提供必不可少的安全辅助支撑平台,因此,市级电子政务系统应通过对网络进行合理的配置和部署必要的网络安全设备和软件,系统才能够在最大程度上抵御外来的入侵,防止病毒的侵害和杜绝不良信息在网上的传播和信息的安全保密。安全辅助支撑平台实施方案主要包括防病毒系统、防火墙系统、入侵检测系统、漏洞扫描系统、安全审计系统、NOTES 安全插件和备份系统等,电子政务系统安全辅助支撑平台建设实施方案结构示意如图 4 所示,这样的设计将为网络用户构建全方位的整体解决方案提出可操作依据。

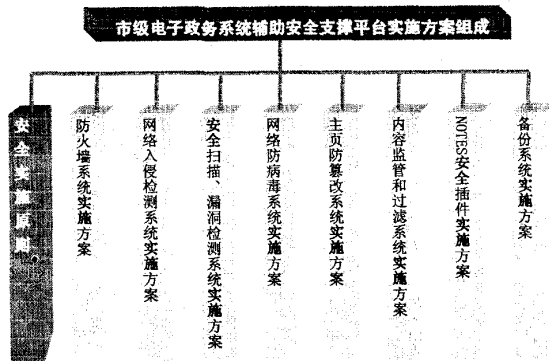


图 4 安全辅助支撑平台建设实施方案结构示意图

下面只对安全支撑平台的部分方案进行阐述。

(1) 基于防火墙实现的访问控制实施方案。

防火墙作为不同网络或网络安全域之间信息的出入口,能根据网络系统的安全策略控制出入网络的信息流,且本身具有较强的抗攻击能力。它是提供信息安全服务,实现网络和信息安全的基础设施。在逻辑上,防火墙是一个分离器、一个限制器,也是一个分析器,有效地监控了内部网和公众网之间的任何活动,保证了内部网络的安全。

针对防火墙的分级访问控制介绍相关的配置方案如下:

① 业务专网的访问控制配置方案。

方案主要针对业务专网的公共信息发布区的访问

控制进行配置。公共信息网站是市级电子政务系统对社会进行信息发布的平台,是市级的信息窗口,它既要求具有较强的开放性,又要求安全系统保护网站免受来自 Internet 的网络攻击,还要防止黑客通过公共信息网站攻击业务专网和内部/控制区,因此在设置公共信息网站的访问控制规则和安全策略时应遵循以下原则:

- * 允许 Internet 用户通过防火墙透明的应用代理、包过滤安全机制访问公共信息网站;

- * 允许公共信息网站通过防火墙透明的应用代理、包过滤安全机制从业务专网获取网站更新信息;

- * 拒绝公共信息网站与内部/控制区的互相访问;

- * 拒绝公共信息网站对业务专网上传信息;

- * 拒绝业务专网访问公共信息网站。

② 业务专网 OA 网的访问控制配置方案。

业务专网的 OA 网是对网络系统内部信息发布的平台,涉及网络系统部分敏感信息,它对安全强度的要求比政务专网低比业务专网的公共信息区高,在设置业务专网的访问控制规则和安全策略时应遵循以下原则:

- * 允许电子政务网络系统内部用户通过 VPN 资料加密和防火墙的应用代理、包过滤安全机制访问业务专网;

- * 拒绝来自 Internet 其它用户的访问。

③ 政务专网的访问控制配置方案。

政务专网涉及大量敏感度较高的信息,是对安全强度要求最高的一个区域,这就要求在设置规则和安全策略时应遵循以下原则:

- * 防止其他专网用户对市级政务专网的非法访问;

- * 隔离政务专网 CA 系统的 DMZ 区、控制区和安全区;

- * 只允许安全管理服务器访问控制安全设备。

(2) 入侵检测系统实施建议方案。

入侵检测功能是防火墙的合理补充,帮助系统对付网络攻击,扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息,并分析这些信息,看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门,在不影响网络性能的情况下能对网络进行监测,从而提供对整个网络系统的实时保护^[5]。

入侵检测系统方案结构图如图 5 所示。

现在国内入侵检测厂家和产品都很多,且比较成熟,可以根据具体需要进行选配。

为市政府电子政务建立安全、可靠的基础和环境。其中,安全平台以密码技术为核心,为电子政务应用系统

提供统一的安全、可靠和可信的服务;安全支撑平台以 PDR(保护、监测、响应)为模型,为网络环境提供入侵检测、病毒防范、防火墙和信息过滤等安全功能。

市政府电子政务系统安全平台和安全支撑平台安全功能如图 6 所示。

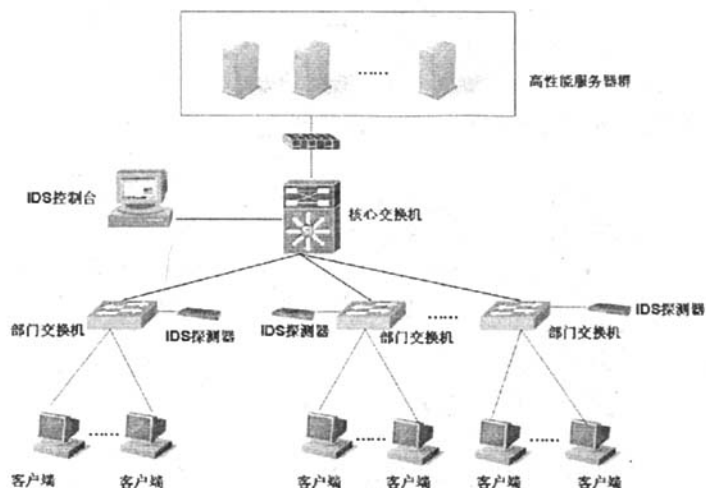


图 5 入侵检测系统方案结构图

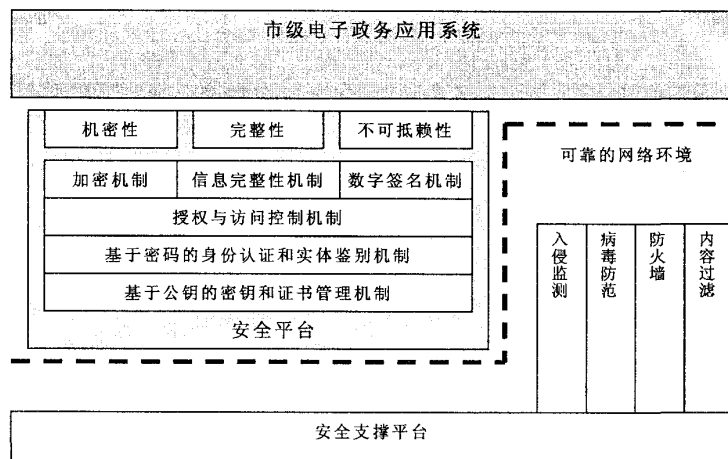


图 6 安全平台和安全支撑平台关系

3 系统总体安全性

市级电子政务系统安全平台和安全支撑平台共同

4 结束语

市级电子政务安全平台,为市政府电子政务应用系统构建了以密码技术为基础的统一的的安全平台,提供了统一的身份认证、授权与访问控制、保密性、完整性、抗抵赖等安全服务和安全机制。为政府构筑政务信息平台,实现政府网上信息交换、信息发布和信息服务提供安全保障。

参考文献:

- [1] 李广乾. 电子政务及其国外发展[EB/OL]. 2006-06. www.chinainfo.gov.cn.
- [2] 秦天保. 电子政务安全体系结构研究[J]. 计算机系统应用, 2006(1): 8-11.
- [3] 濮小金. 电子政务[M]. 北京: 机械工业出版社, 2005: 117-181.
- [4] Lloyd S. Understanding the Public - Key Infrastructure: Concepts, Standards, and Deployment Considerations[M]. Carlisle: Macmillan Technical Publishing, 2004: 40-42.
- [5] Edir A. Economics of Information Security[J]. IEEE Security & Privacy, 2005(2): 1233-1238.

(上接第 143 页)

- able MASs[C]//In Eighteenth International Joint Conference on Artificial Intelligence (IJCAI'03). Acapulco, Mexico: [s. n.], 2003: 789-795.
- [6] Guerraoui R, Garbinato B, Mazouni K. Lessons from designing and implementing GARF[C]//In Object - Based Parallel and Distributed Computation, number 791 in LNCS. London, UK: Springer - Verlag, 1995: 238-256.
- [7] Castelfranchi C. Decentralized AI, chapter Dependence relations in multi - agent systems[M]. Amsterdam, The Netherlands: Elsevier, 1992.

- [8] Sichman J S, Conte R. Multi - agent dependence by dependence graphs[C]//In AAMAS2002. Bologna, Italy: ACM, 2002: 483-490.
- [9] Sichman J S, Conte R, Demazeau Y. Reasoning about others using dependence networks[C]//In Actes de Incontro del gruppo AI * IA di interesse speciale sul intelligenza artificiale distribuita. Roma, Italy: IP/CNR & ENEA, 1993.
- [10] Sichman J S, Conte R, Demazeau Y. A social reasoning mechanism based on dependence networks[C]//In Proceedings of ECAI'94 - European Conference on Artificial Intelligence. Amsterdam, The Netherlands: John Wiley and Sons, 1994.