基于三方通信技术的电子政务系统安全性研究

王斯刚[1],边根庆[2]
(1.第四军医大学,陕西 西安 710032;
2.西安建筑科技大学,陕西 西安 710055)

摘 要:随着网络应用越来越广泛,电子政务系统的敏感信息必须有效地安全保护,然而传统的加密方法不能满足系统的需求。针对当前电子政务系统中存在的安全性问题,文中提出了一种基于三方通信技术的新型电子政务应用系统平台构思,利用三方通信框架中元数据服务器的全局掌控功能,以及采用权能标识构建相应的安全系统,达到消除来自外界安全威胁的目的。同时论述了电子政务系统关于安全性实现方案和技术,以及DES加解密算法,旨在对系统的性能进行优化,以整体提高系统的安全性。

关键词:三方通信技术;电子政务;DES加解密算法;系统安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)12-0167-04

Research of Security System of Electronic Government Affairs Based on Third-party Transferring Technology

WANG Si-gang[1], BIAN Gen-qing[2]
(1. Fourth Military Medical University, Xi'an 710032, China;
2. Xi'an Univ. of Arch. & Tech, Xi'an 710055, China)

Abstract: With the widespread use of network, the sensitive information in electronic government affairs requires more effective secure protection. However, the traditional method of data encryption can't completely meet the requirements. In the light of the existing secure problems of electronic government affairs, it puts forward the conception about a new electronic government affairs application platform based on third-party transferring technology, adopts the overall control function of metadata server in the frame of third-party transferring, utilizes capability to build the security system, in order to eliminate from outside security threats. At the same time it also discusses the scheme and technique to fulfill the secure systems of electronic government affairs and the technology of DES encryption and decryption algorithm, aim at optimizing the electronic government affairs system performance to improve overall system security.

Key words: third-party transferring technology; electronic government affairs; DES encryption and decryption algorithm; system security

0 引 言

电子政务是政府信息化建设的首要问题,也是信息化社会的关键组成部分。加快推进电子政务发展,不仅是提高政府部门行政效率、降低行政成本的内在要求,也是全面提高政府管理和服务水平,建立起行为规范、运转协调、公正透明、廉洁高效的行政管理体制的重要保障。不过,在当今大部分的电子政务建设中,由于缺少有效的安全手段,导致应用系统在安全方面缺乏必要的保障,因此政府部门的重要数据将直接面临众多的安全隐患。

建设电子政务的首要条件是确保信息安全[1]。以密码学理论为基础[2]的传统信息安全技术在网络广泛应用的信息时代里,其弊端也随之暴露。随着网络应用的不断增多,越来越多的政务信息通过网络进行传输,以网络为基础的数据交换变得越来越重要。网络的应用一方面促进了电子政务的发展,另一方面社会各界越来越重视电子政务信息的安全性问题,所以传统单一的加密方式已经不能满足电子政务系统在安全性能上的要求,一旦密钥泄漏或加密算法被攻破,数据就再无任何保护,敏感数据[3]就会被非法使用、篡改,严重影响政府日常的运作,对国家安全造成无法估计

收稿日期:2012-02-27;**修回日期**:2012-05-29
基金项目:陕西省自然科学基础研究计划项目(2011JM8026);陕西省教育自然科学专项基金项目(11JK0982)
作者简介:王斯刚(1970-),男,江西吉安人,高级实验师,主要从事电子信息技术的教学和科研工作;边根庆,副教授,硕导,主要研究领域为海量信息处理、信息安全等。

的损失。因此,对于电子政务系统安全性的研究是十分必要的。

1 电子政务安全系统

电子政务系统[4]是一个庞大而复杂的系统,其安全需求应当从全方位、整体统筹考虑,自下而上可分为网络、系统层,信息资源管理层(数据访问层),应用服务支撑层,应用业务层四层基本结构,如图 1 所示。

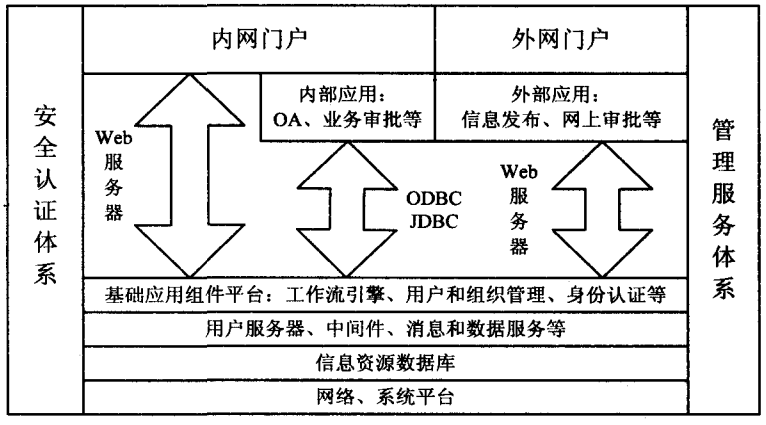

图 1 电子政务系统架构

电子政务应用服务整合平台和数据交换中心是电子政务应用体系的中枢环节,在统一的数据交换标准基础上,通过电子政务数据交换中心把不同的数据资源有效地连接起来,实现应用系统之间业务和数据的交换、信息资源共享,实现不同的部门与业务之间无缝的连接,如图 2 所示。

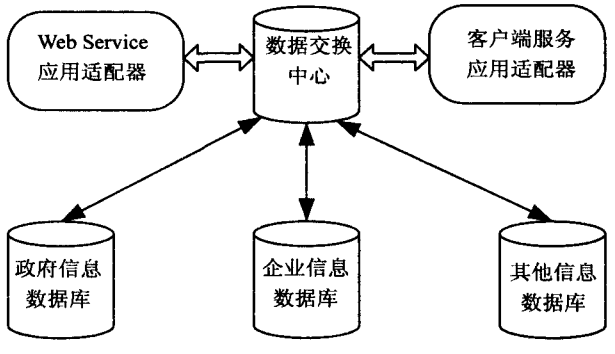

图 2 数据中心与数据交换中心

系统安全和数据安全[5]是电子政务系统首先要考虑的问题,大部分的电子政务系统主要由五部分构成:

· IT 基础设施平台提供电子政务系统网络通信和系统服务。

· 信息资源服务层主要整合政府内部或外部的数据,包括来自不同系统的结构化或非结构化数据,它们都是信息资源层需要整合的对象。

· 应用服务支持层为政府信息集成平台实现资源整合提供底层构件库,包括本地和远程应用集成构件,为实现不同类型的信息集成提供底层支持。同时提供对所有信息资源的统一管理、统一授权,实现对信息的统一访问。

· 业务应用层包括电子政务各个应用系统。

· 表现层主要是通过信息交互完成政府沟通,展现政府信息等职能。

电子政务系统逻辑结构如图 3 所示。

2 电子政务安全系统特性

根据系统网络的体系结构[6],电子政务安全系统具有以下特性[7,8]:

(1)安全性。

在电子政务中,安全性是必须考虑的核心问题。欺骗、窃听、病毒和非法入侵都在威胁着电子政务,因此要求网络能提供一种端到端的安全解决方案,包括:加密机制、签名机制、分布式安全管理、存取控制、防火墙、安全服务器等。

(2)集成性。

电子政务系统的集成性,在于事务处理的整体性和统一性,它能规范事务处理的工作流程,将人工操作和电子信息处理集成为一个不可分割的整体。不仅能提高人力和物力的利用,也提高了系统运行的严密性。

(3)可扩展性。

对于电子政务系统来说,可扩展的系统才是稳定的系统。如果出现高峰状态时能及时扩展,就可使得系统阻塞的可能性大为下降。

3 三方通信模式的安全系统

在三方通信模式下,元数据服务器(MDS)是存在于该框架中一组比较特殊的服务器。在三方通信工作中,数据信息以及控制信息通过在不同的通道上传输,而且通过独立设置服务器对控制信息[9]进行专门管理。在三方通信框架下,利用 MDS 的全局掌控功能,能够保证顺利构建存储系统,而且利用权能机制[10],通过权能标识构建相对应的安全存储系统。

4 三方通信的电子政务流程

电子政务系统在三方通信构架下的具体流程如下(如图 4 所示):

1、用户通过阈值与初始验证码的比较,得到的比较结果使用户权限在阈值间的区域进行加密,否则跳到步骤 5;

2、对数据进行加密,把密文传送到 MDS;

3、数据通过 MDS 进行解密认证;

4、MDS 根据客户端的可信任程度,返回元数据信

息;

5、客户端取得元数据服务器返回信息之后,就能够向数据存储器发送数据请求;

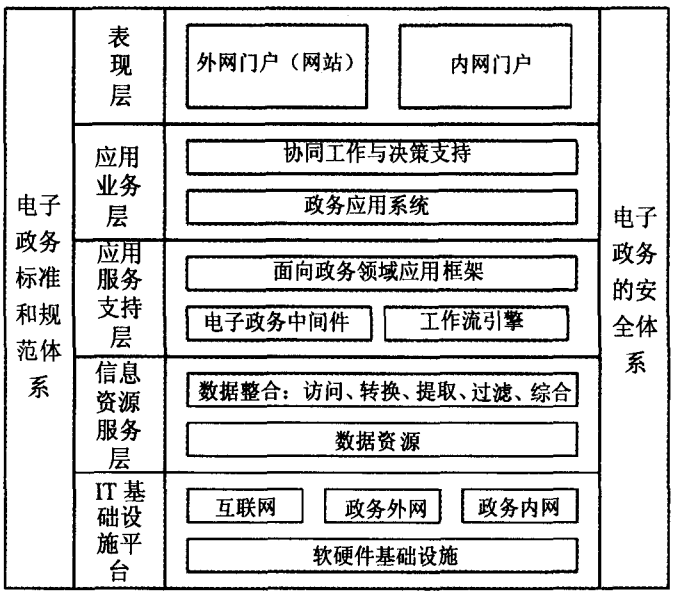

图 3　电子政务系统逻辑结构图

6、数据存储器根据客户端发送过来的请求权值进行响应,用户能够根据不同的权限对数据库内容进行读取操作;

7、客户端在执行撤销操作之前,必须先向 MDS 发送一个撤销命令的请求;

8、MDS 给数据存储器转发撤销命令的请求,数据存储器通过标示符执行撤销命令;

9、MDS 和数据存储器之间能不间断地执行元数据的更新服务。

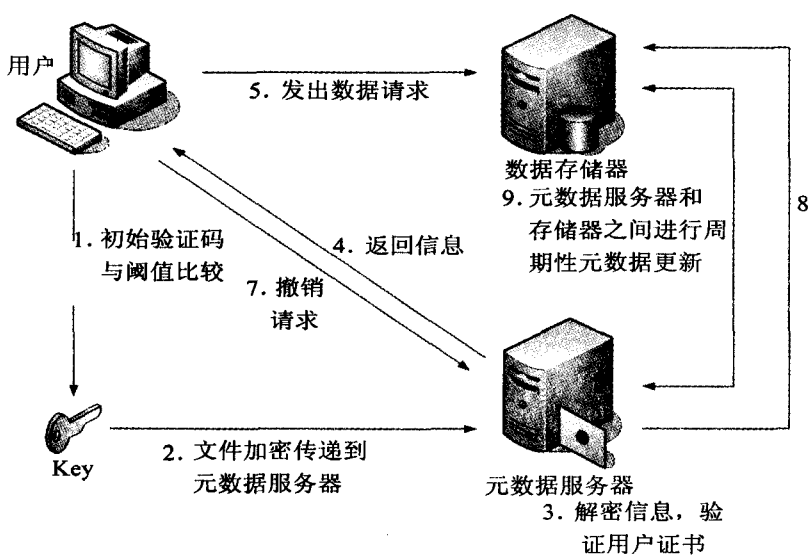

图 4　三方架构电子政务系统流程

根据基于三方通信构架下的电子政务系统的流程可知,最关键的两点分别是用户初始验证码与阈值的比较以及元数据的加密、解密过程。因此针对这两个关键点,作出了以下的解决方法。

4.1　选取阈值

在满足安全性的前提下,就要考虑两种情况,第一,指定的用户对数据库的快速访问也必须要保证。第二,针对完全性非常高的网络环境,可以不用对数据进行加解密等操作,所以必须要准确地进行阈值选取。由于出现上述的两种情况并不是太多,因此绝大部分的用户就会出现在需要加解密区域。终上所述,选择 $\chi^2(n-1)$ 分布,如图 5 所示:

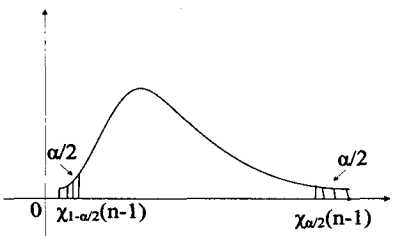

图 5　$\chi^2(n-1)$ 分布图

其中需要对阈值进行选取的区域在 α/2 这个区域之间。由图 5 可知,右侧 α/2 的区域可以不需要加解密,能够加快其访问数据库的速度,而左侧 α/2 的区域由于可信度太低,对该区域可以不考虑,直接对其进行禁止访问操作。所以用户是随机获取验证码的,验证码应该满足公式(1):

$$\chi^2 = \frac{(n-1)S^2}{\sigma^2} \sim \chi^2(n-1) \qquad (1)$$

同时,验证边界必须服从独立同分布,且 $X_1 \sim N(\mu,\sigma^2)$, $\bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i$, $S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \bar{X})$ 分别是验证码均值和方差,则:

(1) $\bar{X}$ 与 S^2 相互独立;

(2) $\frac{(n-1)S^2}{\sigma^2} \sim \chi^2(n-1)$。

确定验证边界之后,在其区域内选取验证码,由于 χ^2 分布存在不对称性,通过对所给定的置信度取 1-α,常取下侧分位数 $\chi^2_{1-\frac{\alpha}{2}}(n-1)$,上侧分位数 $\chi^2_{\frac{\alpha}{2}}(n-1)$ 使:

$$P\{\chi^2_{1-\frac{\alpha}{2}}(n-1) < \chi^2 < \chi^2_{\frac{\alpha}{2}}(n-1)\} = 1-\alpha \qquad (2)$$

阈值的选取可以按照上述步骤进行,大部分用户

根据阈值选取的结果进行加密操作，然而上图的阴影部分可以根据实际情况进行适当的调整。

4.2 DES 算法分析

按技术体征对算法可以分为对称算法、非对称算法、HASH 函数[11]这三类。

文中并非特定针对加解密算法[12]进行优化，现有的算法在安全性、速度快速性等性能都能满足要求，所以此处选用 DES 加解密算法。DES 算法是一个分组加密算法，以 64 位分组对数据加密。

DES 首先利用初始置换对 8 字节的明文进行分组，分成左、右两部分，各 4 个字节。然后进行完全相同的运算，一共 16 次。上述的运算通常被命名为函数 f，同时，每一次运算过程中密钥与数据进行结合。经过 16 次相同的运算之后，左、右两部分相互结合，最后经过一次末置换之后算法就完成。

每一次的算法如下：

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{3}$$

在经过全部的代替、置换、异或和循环移动等一系列操作之后，DES 算法解密过程使用相同的算法，只是在 16 次迭代中使用的子密钥的次序恰恰与加密相反。解密的过程，第一次迭代使用子密钥 K_{16}，第二次使用子密匙的次序正好和加密相反。解密时，第一次迭代使用子密匙 K_{16}，以此类推。解密时的 16 次迭代可以形式化地表示为：

$$R_{i-1} = L_i,\ L_{i-1} = R_i \oplus f(R_{i-1}, K_i),\ i = 16, 15, \cdots, 2, 1 \tag{4}$$

不难验证，对任意的明文 x，有：

$$DES_{k-1}(DES_k(x)) = y \tag{5}$$
$$DES_k(DES_{k-1}(y)) = x \tag{6}$$

其中 $DES_k(x)$ 表示当密匙为 k 时利用 DES 对明文 x 进行加密得到的密文，$DES_{k-1}(y)$ 表示当密匙为 $k-1$ 时利用 DES 对 y 进行解密得到的明文。

DES 算法加密、解密过程如图 6 所示。

DES 算法的参数主要分为 Data、Key、Mode。其中 Data 为 8 个字节，是要被加密或被解密的数据；Key 也为 8 个字节，属于 DES 算法的工作密钥；Mode 可以划分为加密或解密，是 DES 其中一种工作模式。如果 Mode 选择加密模式，那么 Key 自动对 Data 加密，DES 的输出结果就是生成之后的密码形式；倘若 Mode 选择解密模式，则 Key 自动对密码形式的 Data 进行解密，最后 DES 的输出结果为 Data 的明码还原形式。

5 结束语

电子政务安全，是信息安全在电子政务中的一种具体的应用，是电子政务运作中必不可少的重要角色，是一个政府部门能够有效地完成法律所赋予的政府职能必需的。文中通过在电子政务系统平台上应用三方通信技术，能有效解决电子政务系统中数据泄露、恶意修改等问题，为政务信息能够进行安全发送以及信息安全处理提供强有力保障，及时保证各级政府部门可以很好掌握和处理之后的信息，提高政府各部门的办事效率，而且工作透明化大大增加。而对于 DES 算法的改进以及进一步深入研究电子政务的信息安全技术将是下一步的主要工作。

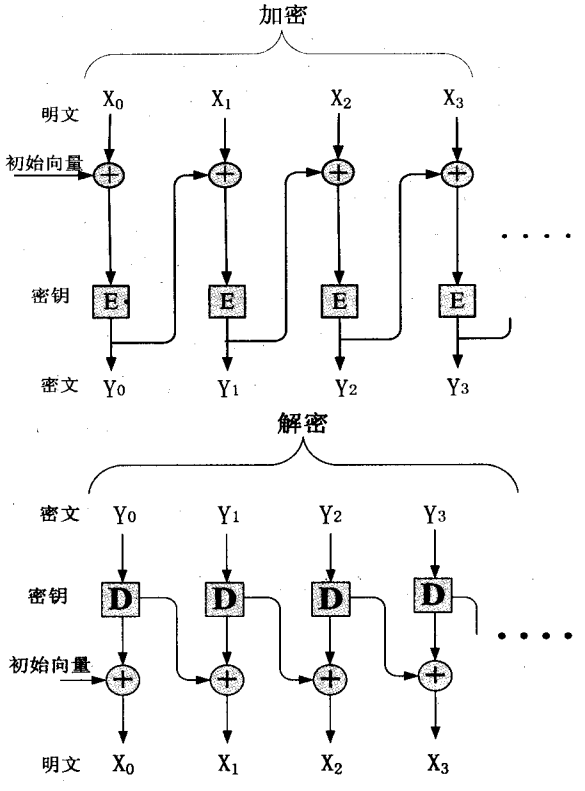

图 6 DES 算法加密、解密示意图

参考文献：

[1] 付中华，赵荣椿. 用窗口法在小存储器中实现 DTW 算法[J]. 西北工业大学学报，2002，20(4)：540-543.

[2] Keogh E，Ratanamahatana A C. Exact Indexing of Dynamic Time Warping[J]. Knowledge and Information Systems，2005(7)：358-386.

[3] 陈 征，张成芬. 陕西省电子政务安全保障体系的研究[J]. 西安邮电学院学报，2010，15(4)：32-35.

[4] 冀 峰. 基于 PKI 体系的电子政务应用层安全的研究[J]. 计算机技术与发展，2006，16(10)：149-152.

[5] 刘邦凡. 电子政务建设与管理[M]. 北京：北京大学出版社，2005.

[6] 蒋建春，扬 凡，文伟平. 计算机网络信息安全理论与实践教程[M]. 西安：西安电子科技大学出版社，2005.

[7] 楮 峻，苏 震. 电子政务安全技术保障[M]. 北京：中国

(下转第 174 页)

伪造的 SYN 报文,半连接数量超过了 TcpMaxHalfOpen 键值的设置,此时系统为了保证 TCP/IP 堆栈不会溢出,将会丢弃接下来所有的 SYN 报文,包括正常用户的请求。

这种通过设置注册表防御 SYN Flood 攻击,是一种被动的防御策略。下面来看看另外一种比较有效的方法[10]。

介绍这种方法前,首先来了解一下 SYN Flood 的攻击方法:SYN Flood 只在攻击开始前一次性解析出要攻击服务器的 IP 地址。这种一次解析目标 IP 地址的攻击方式暴露它最大的弱点:当攻击目标在检测到自己受到了 SYN Flood 攻击后迅速更换自己的 IP 地址,那么由于攻击者没有对被攻击系统的 IP 地址重新解析,接下来的 SYN 攻击包被发给了一个并不存在的主机,攻击的效果就无法达到了。为了不影响正常用户的访问,管理员只需将域名的 DNS 解析更改到新的 IP 地址,在本地 DNS 的刷新之前用户的正常访问会受到影响。

如今要完全杜绝 DDOS 攻击是不可能的,但可通过适当的方法增加 DDOS 攻击者的成本,那么很多攻击者不能承受这样的成本开销而放弃攻击,也算是成功抵御了 DDOS 攻击。由于 DDOS 不可能完全杜绝,只能通过采取一定的措施将攻击带来的危害降到最低。互联网的专家们一直在努力寻找更好的方法,让我们拭目以待新技术和新产品的诞生[11]。

4 结束语

当今计算机网络飞速发展同样也带来了很大的隐患,不怀好意的黑客攻击和病毒的肆虐给计算机安全带来巨大压力,计算机安全方面的专家们也在为维护网络安全作不懈的努力。但是各种攻击手段在不停地更新,一方面要加强系统自身的安全性,不给人以可乘之机,另一方面,要对现存的攻击手段做详细分析,以便更新对攻击的防范手段[11]。

文中通过叙述威胁计算机网络安全的因素有哪些,然后通过一个具体的实例(SYN Flood 攻击)分析其具体的防范技术,对其他的网络安全问题也起到一定的启发作用,让人们在生活和工作时能够放心地畅游计算机网络世界。

参考文献:

[1] 赵 敬,孙洪峰. 信息与网络安全防范技术[J]. 现代电子技术,2003(8):5-9.

[2] 宋渊明,杨 明. 信息与计算机通信网络安全技术研究[J]. 信息技术,2003(4):202-251.

[3] 戴启艳. 影响信息系统安全的主要因素及主要防范技术[J]. 中国科技信息,2010(6):34-58.

[4] 李晓明,付丹丹. 计算机网络攻击分析及防范技术[J]. 电脑学习,2010(6):24-26.

[5] 韩 卫,薛 健,白 灵. 一种基于安全隧道技术的 SSL VPN 及其性能分析[J]. 科学技术与工程,2005(12):791-796.

[6] 张大成,韩 坤. 信息加密技术分析[J]. 科技信息(学术版),2007(5):53-53.

[7] 刘 伟. 访问控制技术研究[J]. 农业网络信息,2007(7):96-97.

[8] 万 琳,张 鹰,李 理. 浅谈基于角色的访问控制技术[J]. 计算机与数字工程,2007,35(10):145-148.

[9] Microsoft Windows Server 2003 TCP/IP Implementation Details[M]. Microsoft Corporation,2010:12-24.

[10] Jurjens J. Code security analysis of a biometric authentication system using automated theorem provers[C]//21st Annual Computer Security Applications Conference (ACSAC 2005). [s.l.]:IEEE Computer Society,2005:54-58.

[11] Rubin A D,Geer D E. A Survey of Web Security[J]. Computer,1998,31(9):34-41.

(上接第 170 页)

人民大学出版社,2004.

[8] Milanovic N, Malek M. Current Solutions for Web Service Composition[J]. IEEE Internet Computing,2004,8(6):51-59.

[9] 黄建忠,谢长生,曹 强,等. 基于三方通信构架的可信任网络存储安全系统的研究[J]. 华中科技大学学报(自然科学版),2005,33(S1):158-160.

[10] 黄建忠,谢长生,罗东健,等. 一种基于权能标识的三方安全协议的设计和分析[J]. 计算机科学,2007,34(3):50-53.

[11] 欧洲银行标准委员会. 加密算法使用与密钥管理指南[S]. TR406V2-CN,2001.

[12] 王全民,周 清,刘宇明,等. 文件透明加密技术研究[J]. 计算机技术与发展,2010,20(3):147-150.