复杂信息系统模型研究*)

王 琨[1] 袁 峰[2] 周利华[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[1]
(国家信息安全工程技术研究中心 北京 100093)[2]

摘 要 为保障复杂信息系统(CIS)的安全性、互操作性、可扩展性和可管理性,论文提出一个安全的CIS体系结构模型。模型采用分层的方式,把CIS划分为不同的功能模块以降低系统的复杂度。在多层中采用Web Service技术,实现互操作和可扩展。模型采用密码支撑层、安全防护与可靠性支持层保证系统不同层面的安全性与可靠性。通过系统管理层与各层交互,实现系统的可管理性。某电子政务试点示范工程案例及其网络统计数据证明模型不会影响业务系统的性能要求,模型适用于政府、军队、银行等安全级别较高的信息系统。

关键词 网络安全,体系结构模型,电子政务,互操作性,可扩展性

Study on Complicated Information System Model

WANG Kun[1] YUAN Feng[2] ZHOU Li-Hua[1]
(Ministry of Edu. Key Lab. of Computer Networks and Information Security, Xidian Univ., Xi'an 710071)[1]
(National Information Security Engineering and Technology Research Center, Beijing 100093)[2]

Abstract In order to make complicated information system (CIS) possess the features of security, interoperability, extensibility and controllability, this paper presents a secure CIS architecture model. Using layered method, this model divides CIS into several modules and reduces system complexity. Web Service technology is widely adopted in layers to fulfill the interoperability and extensibility. This model uses Encryption Support Layer, Security Protection and Reliability Support Layer to guarantee the system security and stability in different aspects. The model uses System Management Layer to interact with all relative layers to make CIS administrable. A case study with performance analysis shows that the model can satisfy the need of e-government without interfere with the system performance. This model is apt to highly security-critical environment such as government, military and bank.

Keywords Network security, Architecture model, E-government, Interoperability, Extensibility

1 引言

论文中复杂信息系统(CIS, complicated information system)指包含许多异构应用的信息系统,这些应用可能运行在不同的操作系统之上,采用多种通信协议,使用多种程序语言开发而成,由多个互不兼容的应用组成。由于缺乏兼容性,多个应用之间无法共享信息从而导致信息浪费。不同应用不得不构建自己的数据库以存储甚至是相同的数据,除了重复建设之外,随着时间的推移,还会导致数据不一致。应用系统往往需要根据变化的需求不断进行修改,这要求应用系统必须能够方便扩展。保障CIS的安全性也是一个非常重要的问题。

在信息系统模型安全的研究方面,文[1]提出的设计CIS的方法能够考虑到系统中动态元素对系统的影响。文[2]把信息系统划分为单一域系统、简单系统和复杂系统,研究不同系统的特性以及它们之间的关系,并且提出了安全的信息系统模型。但是这两篇论文都更倾向于理论概念研究,不适于指导工程建设。Dual security model[3]是具有实践性的基于客户机/服务器的信息系统安全模型,它采用高层风险评估框架分析和评估系统环境。但是这个模型相对简单,并不适用于CIS。其它一些基于网络的信息系统模型[4~7]同样无法满足CIS对高安全性、高可靠性的要求,并且这些模型没有考虑到信息系统的互操作性和可扩展性。此外,这些模型都局限于软件层次,没有涉及在建设实际的CIS时还必须要考虑到许多其它重要问题,例如机房选址建设、硬件建设、系统管理等。

总之,绝大多数有关信息系统模型的研究都侧重于相对简单的系统,这些模型通常有特定适用的应用背景,侧重于解决某个应用环境中特定的问题,对互操作性、可扩展性考虑不足。这些模型在安全强度不足以应对黑客、甚至是敌对国家的攻击。与相对简单的信息系统不同,CIS需要有灵活的、可扩展的体系结构控制系统的设计、开发、使用和维护过程。然而由于众多原因(例如国家安全等),一些有关CIS的研究成果并不公开。

由于历史原因,某政府部门现有应用系统由多家厂商分头建设,造成各异构应用系统缺乏安全性、互操作性、可扩展性。作为"十五"重点电子政务试点示范工程(EEDP, E-government Experimental and Demonstration Project)需要改造这一系统。要求在保障系统具有极高安全性的前提条件下,统一规划业务系统,实现原有业务的平滑移植,使它们和新业务

*)基金项目:国家"十五"重点科技攻关计划(2002AA1Z67101)。王 琨 博士研究生,研究方向:网络与信息安全。袁 峰 高级工程师,研究方向:网络与信息安全。周利华 教授,博士生导师,研究方向:网络与信息安全,网络多媒体。

架构在统一的支撑平台上，保障业务系统具有良好的互操作性和可扩展性。同时，通过吸取试点示范工程中的经验教训，制订国家电子政务相关规范，对我国电子政务的建设起到示范和引导作用。在深入研究信息系统及其安全威胁的基础上，论文提出安全的复杂信息系统体系结构模型(SCISAM, Secure Complicated Information System Architecture Model)。工程实践及其网络统计数据证明模型不会影响业务系统的性能要求，成功指导了 EEDP 的建设。在模型的基础上，已经制订并通过了国家电子政务应用支撑平台和安全保密支撑平台规范，以指导我国电子政务的建设。

2 复杂信息系统分析

在建设 CIS 前，有必要首先深入分析 CIS。以下主要从业务应用和安全威胁方面研究 CIS。

2.1 业务应用分析

CIS 通常包含许多业务应用系统(BAS, Business Application System)，这些应用广泛集成多种信息。互连互通、信息共享是业务应用的核心，然而由于多方面的原因，这些异构应用系统各自独立，各自形成了信息孤岛，缺乏互操作性，不能充分发挥信息的价值。另一方面，随着人们对 BAS 的不断充实、丰富和完善，必须考虑系统将来可能的扩充。为实现 CIS 的互操作性和可扩展性，需要建设一个强大的支撑平台，这包括许多标准，例如：接口标准、通信协议、数据交换标准[8]，安全协议等。

2.2 安全威胁分析

不断出现的安全事件会给 CIS 造成巨大损失，像 EEDP 这样的 CIS 往往含有大量敏感信息，必须能够抵御来自外部或内部的包括黑客、邪教组织或敌对国家的攻击等各种攻击，还要防止工作人员失误、系统内部设施互相干扰、电磁泄漏等造成的安全受损。

要保证 CIS 的安全与可靠，宏观上要从分析内外环境存在的不安全因素及攻击方式入手。攻击行为一般包括侦听、截获、窃取、破译等被动攻击和修改、伪造、破坏、冒充、病毒扩散等主动攻击。微观上要从系统各个层面可能存在的安全威胁入手。下面主要从微观上分析 CIS 可能存在安全隐患。

1)物理层安全威胁。这里的物理层包括信息系统网络中所有机房、通信线路、网络设备等，物理层安全对 BAS 有着严重的影响，保证设备的物理安全是保障整个 CIS 安全的前提。物理设备面临着地震、水灾、火灾等环境事故，以及人为操作失误、计算机犯罪行为的破坏。要防止设备被盗、恶意破坏、电磁信息辐射泄漏、线路截获监听、电磁干扰、电源掉电、物理设备损坏等。

2)网络层安全威胁。网络层是网络入侵者攻击信息系统的渠道和通路，许多安全问题都集中体现在网络层。

3)应用层安全威胁。它主要涉及两个方面，一是由于应用层协议缺陷和漏洞而引起的安全威胁；二是应用系统设计缺陷和对系统的误操作、用户恶意或非恶意破坏。CIS 中用户众多，技术水平参差不齐，应用层安全隐患多种多样，非常难以防范。

4)系统层安全威胁。主要指操作系统安全威胁，由于现代操作系统和应用系统代码庞大，不同程度上都存在安全漏洞，对系统的配置不当也会造成安全隐患。操作系统的脆弱性将直接影响到其上应用系统的安全性。

5)管理层安全威胁。管理层包括对设备、网络、应用系统的管理，还包括人员、机房等管理。仅从技术上无法解决 CIS 的管理安全，还必须建立完善的管理制度和操作章程防止对系统的滥用[9,10]。

3 研究思路

CIS 涵盖内容多、应用范围宽、涉及技术复杂，应该在研究它涉及的不同层面问题的同时建立合理的体系结构模型。

为实现互操作性和可扩展性，必须对 CIS 和 BAS 制订规范，重点是接口标准、通讯协议、安全协议等，实现不同应用系统间的安全连接。

安全方面，CIS 涉及人员、技术和操作，应该采用全面深度防御战略保护这三者的安全。如图 1 所示，信息系统的安全需求可分为保护网络与基础设施、保护飞地安全、保护计算环境、建立支撑性基础设施这四个方面：保护计算环境指保护信息系统的内部系统应用和服务器。CIS 中频繁的跨网络数据交换和业务应用，使得飞地边界的安全显得十分重要。保护网络与基础设施的重要性是不言而喻的。支撑性基础设施为 CIS 实现深度防御战略提供公钥基础设施(PKI)、密钥管理基础设施(KMI)和授权管理基础设施(PMI)支持。

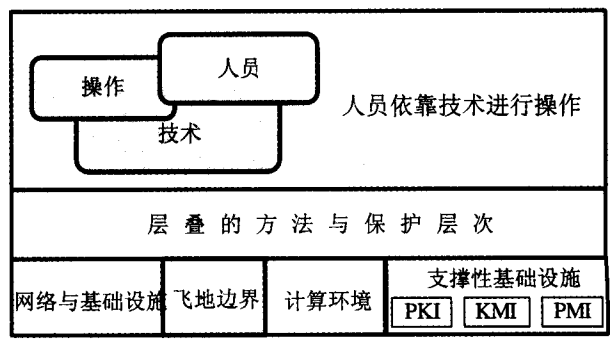

图 1 全面深度防御战略

4 安全的复杂信息系统体系结构模型

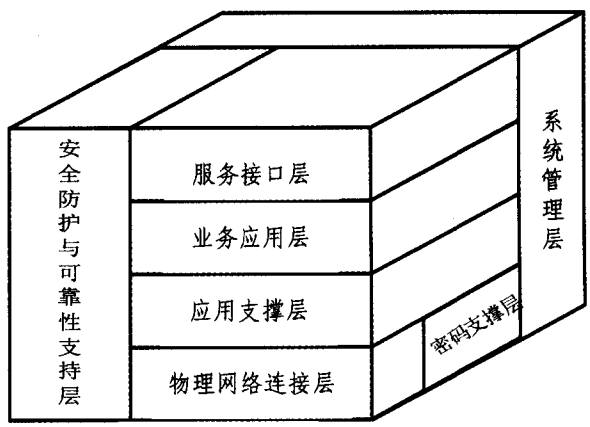

图 2 安全的复杂信息系统体系结构模型

经过对 CIS 的深入分析，我们提出如图 2 所示的安全的复杂信息系统体系结构模型。模型包括：物理网络连接层(PNCL, Physical Network Connection Layer)、密码支撑层(ESL, Encryption Support Layer)、应用支撑层(ASL, Application Support Layer)、业务应用层(AL, Application Layer)、服务接口层(SAL, Service Access Layer)、安全防护与可靠性支持层(SPRSL, Security Protection and Reliability Support

Layer)、系统管理层(SML, System Management Layer)。通过这种分层的逻辑结构,不仅能够保障系统的安全,实现业务的互操作性和可扩展性,而且便于对具体CIS进行分解,有助于系统建设的统筹规划和分步实施。

4.1 物理网络连接层

物理网络连接层为信息系统提供信息传输和交换的硬件平台,是CIS的基础。根据物理层和网络层安全威胁分析,必须严格执行国家相关安全标准,保证系统环境安全和设备安全,还要保证网络设计安全[11~14]。如图3,把网络划分为不可信网络、可信网络和国家涉密网络。不可信网络指Internet或其它公众信息网络,它与可信网络两者之间采用防火墙、认证网关进行逻辑隔离。根据安全需要,还可以对可信网络中的多个网段进行逻辑隔离。使用PKI、KMI和PMI技术,对系统中的所有或关键设备分配证书构建网络信任域,为CIS提供统一的可信网络基础环境、可信网络接入、安全通信及可信管理等服务。网络信任域可跨多种密级的局域网和广域网,在提高信息交换便捷的基础上,又能够很好地保护网络和基础设施,保护网络边界安全。

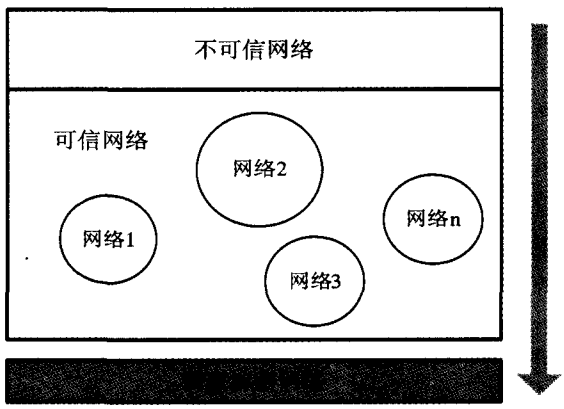

图3 网络隔离

国家《计算机信息系统国际联网保密管理规定》第六条明确规定,凡涉及国家秘密的计算机信息系统,不得直接或间接地与国际互联网或者其它公众信息网络相连接,必须实行物理隔离。因此,CIS中国家涉密的网络必须与其它网络物理隔离,在其中也可划分信任域,进行信任域管理。为同时满足它与外界信息交换的需要,可以使用网络安全隔离卡、物理隔离交换机等在可信网络与国家涉密网络之间交换信息。必须强调的是,在CIS中一定要对密级进行精准的定位,定密过宽会降低网络的安全性;定密过严,会增加网络安全保密经费负担,还会影响互连互通和互操作性[15,16]。

4.2 密码支撑层

仅通过防火墙、入侵检测、病毒防治等技术保障信息系统安全是不够的,EEDP的安全需求十分显著,除传统的安全技术外,还需要高强度的身份认证与授权,确保信息的机密性、完整性、不可抵赖性等。必须对接入政务网的硬件设备进行认证,以保证接入设备的合法性,这些都需要大量的密码运算。密码支撑层提供必要的密码服务支撑,它的技术核心是PKI技术,实现核心是数字证书认证中心CA。采用公钥技术提供身份认证、数据机密性、完整性、不可抵赖性等安全服务,并在其上实现授权管理。

ESL包括密码服务、目录服务、密钥管理、时间戳服务、证书认证、授权管理。密码服务提供系统所需要的密码服务,包括不同安全等级的对称密码、非对称密码,随机数生成和数据摘要;目录服务提供分布式环境中快速信息查询;密钥管理能够管理对称密钥和非对称密钥;时间戳服务提供精确可信的时间戳服务,时间戳从权威部门获取,保证处理数据在某一时间的存在性及该操作的相对时间顺序,为业务处理的抗抵赖性提供有效支持;证书认证是对证书进行全过程管理的安全系统;授权管理在身份认证的基础上,为应用提供资源的授权管理及访问控制服务,根据应用的实际需要,可以采用集中式授权管理模式或分布式授权管理模式。

ESL是保障CIS安全的核心,模型中各层都可以直接调用ESL提供的服务,也可以通过ASL、AL间接调用ESL进行密码运算。

4.3 应用支撑层

应用支撑层在ESL之上,是承载业务应用通用组件的综合平台。它基于目录服务系统和标准规范的信息交换格式构建可信Web Service平台和安全的信息交换系统,同时集成了BAS中共性化的公共业务应用模块和安全应用模块,能够集中体现不同CIS的服务特色,对上层AL中的具体业务提供服务,为CIS的互操作性和可扩展性提供支持。通过有机集成PKI技术和各类安全密码运算,为各类应用系统提供统一、标准和规范化的安全功能支持。例如:EEDP中ASL主要包括Web服务系统、信息交换系统、安全电子邮件系统、安全消息服务系统、GIS支持系统、安全文件传输、安全责任认定系统、安全数据库访问等。ASL能够有效加速业务应用的设计、开发与部署,有助于节省投资,提高应用系统的专业化水平。

4.4 业务应用层

业务应用层调用ASL的服务,AL中运行着系统中BAS,通过SAL为用户提供业务功能,最终实现信息系统的价值。不同信息系统在业务应用层差异非常大。EEDP的业务应用层主要运行值班与会议管理类系统、公文处理类系统、辅助决策类系统等。信息系统面临的一个重要风险就是当系统建设完成后,用户是否愿意使用这一系统[17]。因此,在设计开发应用系统时,应尽可能使应用系统具备友好的界面,符合用户的操作习惯。

4.5 服务接口层

服务接口层在AL之上,是外界与CIS进行信息交换的唯一接口,它对进出CIS的用户进行最上层的身份认证,授权管理,外界通过服务接口层调用业务应用层,访问CIS中的不同BAS。

4.6 安全防护与可靠性支持层

ESL为系统提供密码服务,安全防护与可靠性支持层也具有安全防护功能,但主要涉及基本安全防护系统,包括防火墙、入侵检测系统、漏洞扫描系统、安全审计系统、病毒防治系统、Web信息防篡改、黑客诱捕等组成,它可以很大程度上屏蔽网络层、应用层和系统层安全威胁。

CIS往往要求具备高稳定性和可靠性,这要求提供故障恢复和容灾备份。通过对关键设备多机热备份实现故障恢复。建设本地和异地备份中心,在发生重大故障或灾难时,快速切换本地和异地备份中心,可以确保系统在任何情况下都能正常运行。

SPRSL贯穿于模型中涉及到的所有层。对于对安全和可靠性要求相对较低的信息系统,也可以根据具体情况在模型中适当层面降低安全防护与可靠性支持的投入,从而简化

系统，降低投资。

4.7 系统管理层

系统管理层不仅包括对机房、设备、网络、应用系统的管理，还包括人员的管理，以最大程度降低管理层安全威胁。和SPRSL一样，它贯穿于模型中涉及到的所有层，也可以进行适当简化。SML保障系统正常运行、计费、查错和安全管理，它包括网络配置管理、故障管理、网络性能管理、网络安全管理、网络计费管理等。要真正保障信息系统的安全，除技术因素之外，还必须制订相应的人员管理规章制度[18]。

5 模型分析

SCISAM为建设CIS提供总体框架，它以PKI技术为核心构筑信息安全保障体系，在信息的采集、处理、交换、传输、存储等环节中采用安全认证和授权技术。采用不同等级的密码技术、密钥管理技术、网络信任域技术和安全防护与可靠性支持，可切实提高信息系统的安全防护强度。在具体实现中还需要在模型基础上制订各层的安全策略，尤其是在密码的使用上，必须严格遵守国家的相关法规。

在PNCL必须合理规划网络拓扑结构，冗余关键网络设备和网络连接，正确选择物理隔离和逻辑隔离的边界。ESL应选择恰当的密码算法、密码设备、密码协议，为不同密级的应用提供不同等级的密码保护。ASL应调用ESL所提供的服务提供安全的信息化应用环境。SAL和AL应利用ASL提供的服务，实现互操作性、可扩展性。应对SPRSL中的防火墙、入侵检测系统、漏洞扫描系统、安全审计系统、病毒防治系统、Web信息防篡改、故障恢复与容灾备份配置科学的安全策略。在SML中，应制订恰当的系统管理策略和人员管理规章制度。

Web Service为系统的互操作和可扩展问题提供解决方案，它包括Simple Object Access Protocol(SOAP)、Web Services Description Language(WSDL)、Universal Description、Discovery and Integration(UDDI)等协议。SOAP定义了数据传送的消息格式，WSDL定义了描述Web Service的方法，UDDI实现对Web Service发现、描述和集成。通过在相关层中广泛使用Web Service技术，开发人员可以选择适当的语言，在适合的平台上开发部署基于网络的、分布式模块化组件，并且使系统通过平台及不依赖语言的方法确保相互兼容，实现BAS之间的互操作，并且方便系统的扩展。此外，Web Service还包括在安全性、协调和事务处理方面的一些扩展规范。

通过分层的方式，模型把CIS和业务系统划分成小的功能模块，更易于系统分析员研究系统需求。开发人员能够高效地开发和共享通用的服务组件，加速系统开发和部署。由于共享服务组件，还可以节省系统开发和维护方面的投入。模型还有利于限制错误发生的范围，有助于差错定位和故障排查。

总之，模型能够满足EEDP对高安全性、互操作性、可扩展性的要求。对于相对简单的信息系统，可以适当简化模型中的某些层次以适应不同的需要。例如通过简化安全防护与可靠性支持层、简化或去除密码支持层，可以很大程度简化系统，降低投资。

6 实例分析

EEDP中主要包含五类应用系统：值班与会议管理类系统、公文处理类系统、政务信息管理类系统、决策支持类系统、公众服务类系统。每类应用系统又包含多个应用，EEDP中共有超过40种应用，这些应用分布于20多座建筑物中，由超过1500台计算机通过1000Mbps以太网相连组成了EEDP的网络环境。

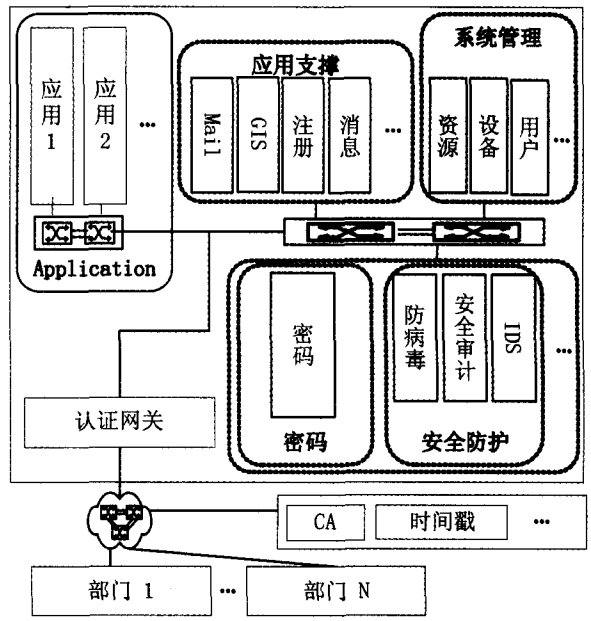

图4 简化的EEDP网络连接示意图

图4是简化的EEDP网络连接示意图。EEDP根据国家信息系统法规要求强化物理层安全，该网络的大部分区域都与Internet物理隔离。EEDP使用ESL为其它各层提供通用的密码服务。网络中不同部门使用认证网关把整个网络划分成多个子网。按照SPRSL的要求，在适当位置部署IDS、防病毒、安全审计等系统，在关键位置(例如关键数据库)采用多机冗余技术防止由于本地局部失效而导致系统不可用，同时，在异地建设灾难恢复中心保证系统在发生重大灾难时依然能够持续提供服务。虽然系统中有众多应用，由于这些应用中包含大量通用的功能，因此，EEDP抽取系统中通用的功能，并把它们封装起来以提供通用的服务，例如：GIS服务、安全邮件服务、消息服务等。EEDP的业务应用位于AL层，它采用密码技术保护重要的应用。与技术措施相配套，EEDP还制订了相应的管理措施保障系统可靠、安全地运行。

由于该电子政务系统的特殊性，安全性是该需要考虑的首要因素，因此系统中采用了大量的安全措施。另一方面，我们希望应用的性能不会由于这些安全措施而产生较大的负面影响，这需要对系统性能进行深入的研究。由于系统中几乎所有的电子政务应用都需要数据库支持，而且这些应用绝大多数都基于Web浏览器，这意味着绝大多数应用在底层都使用HTTP协议。电子邮件同样是系统中非常重要的应用，此外还有不少应用系统使用FTP协议进行文件传输。通过分析知道，EEDP的网络通信流量主要被数据库应用、HTTP、Email和FTP所占用。

因此，我们在系统中许多网络连接的源点和目的点放置探头，收集分析上午9:00至10:00(系统最繁忙时间)的网络通信数据。图5所示的统计数据显示：系统的平均数据库查询响应时间约为0.0003s，接收和发送电子邮件的平均响应时间分别约为0.0024s和0.0016s，平均HTTP页面响应时

间约为 0.0027s，平均 FTP 下载和上传响应时间都大约为 0.0018s。由此可以认为，EEDP 应用系统的性能完全能够满足要求。

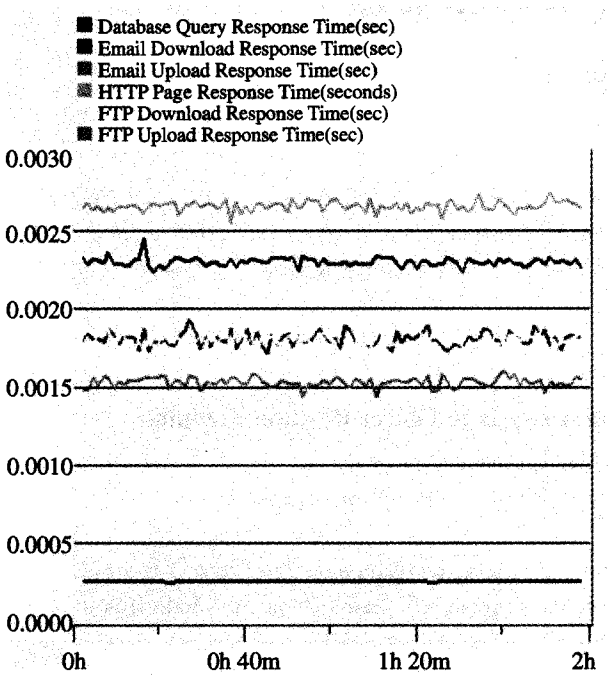

图 5　应用响应时间

结论　论文提出了安全的复杂信息系统体系结构模型，支持业务应用之间的安全性、互操作性、可扩展性，为新建或改造复杂信息系统提供框架指导。模型适用于对安全要求非常高的复杂信息系统，对模型中相应层次适当简化，模型也可适用于相对简单的信息系统。EEDP 已经在模型的指导下建设完成并成功运行了 1 年，实践和统计数据证明模型能够满足 EEDP 的要求。在模型的基础上，已经制订并通过了国家电子政务应用支撑平台和安全保密支撑平台规范。

参 考 文 献

1　Shnitko A. Adaptive Security in Complex Information Systems, In: Proc. of the 7th Korea-Russia Int. Symposium on Science and Technology, Ulsan, South Korea, June 2003. 206～210

2　李守鹏，孙红波. 信息系统安全模型研究. 电子学报，2003，31(10)：1491～1495

3　Zhou B Y. Security Analysis and the DSM Model. In: Proc. of 13th Intrnational Workshop on Database and Expert Systems Applications, Aix-en-Provence, France, September 2002. 17～21

4　Lee S Y, Koh J S. WWW-Based Reliability Information System. Computers & Industrial Engineering, 1998, 35(3-4): 599～602

5　Chou S C T. Migrating to the Web: a Web Financial Information System Server. Decision Support Systems, 1998, 23(1): 29～40

6　Van de Velde R. Framework for a Clinical Information System. International Journal of Medical Informatics, 2000, 57(1): 57～72

7　Hripcsak G. IAIMS Architecture. Journal of the American Medical Informatics Association, 1997, 4(2): S20～S30

8　XML 在电子政务中的应用指南. 国家标准：GB/Z 19669-2005, 2005

9　Grimaila M R. Maximizing Business Information Security's Educational Value. IEEE Security & Privacy Magazine, 2004, 2(1): 56～60

10　国家信息安全工程技术研究中心. 国家信息安全基础设施研究中心. 电子政务总体设计与技术实现. 北京：电子工业出版社，2003

11　信息技术设备的安全. 国家标准：GB 4943-2001, 2001

12　路由器安全技术要求. 国家标准：GB/T 18018-1999, 1999

13　信息技术. 包过滤防火墙安全技术要求，国家标准：GB/T 18019-1999, 1999

14　信息技术. 应用级防火墙安全技术要求. 国家标准：GB/T 18020-1999, 1999

15　朱鲁华，施军，沈昌祥. 涉密网的物理隔离问题. 电子计算机，2002, 154: 16～19

16　计算机信息系统. 安全保护等级划分准则. 国家标准：GB 17859-1999, 1999

17　Bajaj A, Nidumolu S R. A Feedback Model to Understand Information System Usage. Information & Management, 1998, 33(4): 213～224

18　Al-Salihy W, Ann J, Sures R. Effectiveness of Information Systems Security in IT Organizations in Malaysia. In: Proc. of 9th Asia-Pacific Conference on Communications. Penang, Malaysia, September, 2003. 716～720

(上接第 47 页)

下 ODMRP 的平均传输延时最大，ADMR 和 DRMR 相差不大，但在组播组规模较大时 DRMR 的平均传输延时最大。

由此看出，ODMRP 适合要求高分组递交率、网络规模不大的非实时业务，ADMR 适合分组递交率要求不高、网络规模中等的实时业务，而 DRMR 由于协议平衡性比较好，适合网络规模比较大且节点移动速度较快、对分组递交率要求较高的实时/非实时业务。

参 考 文 献

1　Obraczka K, Tsudik G. Multicast Routing Issues in Ad Hoc Networks. In: International Conference on Universal Personal Communications, 1998. ICUPC'98. IEEE 1998, 1998, 1: 751～756

2　Jetcheva J G, Johnson D B. Adaptive Demand-Driven Multicast Routing in Multi Hop Wireless Ad Hoc Networks. In: Proceedings of Mobihoc 2001 [C]. Long Beach, CA, October 2001. 33～44

3　Xie J. Route A M: Ad hoc multicast routing protocol [J]. Mobile Networks and Applications, 2002, 7(6): 429～439

4　Wu C W, Tay Y C. AMRIS: a multicast protocol for ad hoc wireless networks [C]. In: Proc. of IEEE Military Communications Conference, Atlantic City, USA, V1, 1999. 25～29

5　Lee S J, Gerla M, Chiang C C. On- demand multicast routing protocol in multi hop wireless mobile networks [J]. Mobile Networks and Applications, 2002, 7(6): 441～453

6　Garcia-Luna-Aceves J J, Madruga E L. Core-assisted mesh protocol [J]. IEEE Journal on Selected Areas in Communications, 1999, 17(8): 1380～1394

7　Zhou Y, Li GL, Zhan Y Z, et al. DRMR: Dynamic-Ring-Based Multicast Routing Protocol for Ad Hoc Networks. Journal of Computer Science & Technology [J], 2004, 19(6): 909～919

8　Lee S, Su W, Hsu J, et al. A performance comparison study of ad hoc wireless multicast protocols [C]. In: Proc. of 19th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM), Tel Aviv, Israel, v 2, 2000. 565～574

9　Corson S, Macker J. Mobile Ad hoc networking: routing protocol performance Issues and evaluation considerations. EB/OL. http://www.ietf.org/rfc/rfc2501.txt, Jan. 1999

10　Fall K, Varadhan K. ns notes and documentation. The VINT Project, UC Berkeley, LBL, USC/ISI and Xerox PARC, Available at http://www.isi.edu/nsnam/ns/, 1997-11