复杂信息系统支撑平台研究

王 琨[①] 尹忠海[①] 周利华[①] 袁 峰[②]
[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)
[②](国家信息安全工程技术研究中心 北京 100093)

摘 要：保障复杂信息系统(CIS)的安全、互操作、可扩展和可管理非常关键。该文提出安全的 CIS 体系结构模型以指导 CIS 的建设或改造。模型把 CIS 划分为不同层次以降低系统复杂度，采用 Web Service 技术实现互操作和可扩展，使用密码支撑层、安全防护与可靠性支持层在不同层面保证安全性与可靠性。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、网络仿真证明模型不会影响业务系统性能。模型适用于政府、军队、银行等高安全级别的信息系统。适当简化模型中相应层次，模型也可用于相对简单的信息系统。

关键词：信息系统；安全；体系结构模型；电子政务
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2007)05-1215-05

Study on Complicated Information System Support Platform

Wang Kun[①] Yin Zhong-hai[①] Zhou Li-hua[①] Yuan Feng[②]
[①](*Ministry of Edu. Key Lab. of Computer Networks and Information Security*, *Xidian Univ.*, *Xi'an* 710071, *China*)
[②](*National Information Security Engineering and Technology Research Center*, *Beijing* 100093, *China*)

Abstract: It is crucial to make Complicated Information System (CIS) secure, interoperable, extensible and controllable. This paper presents a secure CIS architecture model to conduct the construction or reconstruction of CIS. It divides CIS into layers to reduce system complexity. Web service is adopted to fulfill interoperability and extensibility. It uses encryption support layer, security protection and reliability support layer to guarantee system security and stability. It uses system management layer to interact with other layers to make CIS administrable. A case study with performance statistic and network simulation show the model can satisfy the need of e-government without interfere with system performance. This model is apt to security-critical environment such as government, military and bank. Been properly simplified, it can be applied to relative simple information system too.

Key words: Information system; Security; Architecture model; E-government

1 引言

本文中复杂信息系统(CIS)指包含许多异构应用的信息系统，由于缺乏兼容性，这些应用之间无法充分共享信息。不同应用不得不构建各自的数据库用于存储甚至是相同的数据，这会导致数据不一致。应用系统还要求具有高安全性，并能够根据变化的需求方便扩展。这要求深入研究安全的 CIS 体系结构模型。

Shnitko[1]基于形式化自适应函数提出设计CIS的方法，它能够考虑到系统中动态元素对系统的影响。文献[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。这两篇论文都侧重于理论研究，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。它没有涉及加密、认证、授权、灾难恢复等重要的内容，安全性不高。并且这个模型相对简单，不适用于CIS。IAIMS architecture[4]和文献[5, 6]中的模型都适于指导工程实践，但是安全性不足，缺乏互操作性和可扩展性，也不适用于CIS。另一个医学信息系统模型[7]使用通用对象请求代理技术和商业逻辑提供可扩展的体系结构，但它不能满足CIS对高安全性、可靠性的要求，适用于规模较小的环境。此外，大多数模型着重解决软件层面的问题，然而对于CIS，还必须考虑诸如网络拓扑、机房选址、硬件建设、设备及人员管理等因素。总之，绝大多数信息系统模型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。这些模型安全强度不足以应对黑客，甚至是敌对国家的攻击。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)，有关CIS的研究成果

2005-12-26 收到，2006-07-24 改回
国家“十五”重点科技攻关计划(2002AA1Z67101)资助课题

往往并不公开。

由于历史原因，某政府部门应用系统由多家厂商分头建设，造成各异构应用缺乏安全性、互操作性、可扩展性。作为“十五”重点的某电子政务试点示范工程(EEDP)要求改造这一系统，在保障系统具有极高安全性的前提条件下，统一规划业务，实现业务的平滑移植，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 EEDP 的经验教训，制订国家电子政务相关规范以引导我国电子政务建设。在深入研究信息系统及其安全威胁的基础上，本文提出安全的复杂信息系统体系结构模型(SCISAM)。

SCISAM 在以下方面区别与其它模型：(1) 它是一个实践性模型，设计 SCISAM 的目的是为了指导 CIS 的建设，因此它包括许多在工程建设中需要关心的问题。(2) SCISAM 适用于高安全性的 CIS。它的密码支撑层能够提供多安全级别的密码服务，安全防护与可靠性支撑层提供 IDS、防病毒、安全审计等服务。持续服务能力对于电子政务、军队、银行等至关重要，SCISAM 具备本地故障恢复与灾难恢复能力。(3) SCISAM 的灵活平台能够对业务应用提供互操作和可扩展性支持。(4) 绝大多数模型是过程驱动的，而 SCISAM 是分层的模型。在过程驱动的模型中，设计人员需要紧密结合特定应用系统，不易于灵活适应应用的变化。而分层模型则更加灵活，可以加速系统设计、开发、部署过程。分层模型还能够在不同组件之间提供更加清晰的接口，方便系统调试和错误的定位。在 SCISAM 的指导下，EEDP 已经成功完成建设。对系统网络通信采样的统计以及网络仿真都证明系统能够满足应用性能需求。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。

2 复杂信息系统分析

CIS 涵盖范围宽、涉及技术复杂，以下主要从业务应用和安全威胁方面研究 CIS。

CIS包含许多业务应用系统(BAS)，互连互通、信息共享是业务应用的核心。然而由于多方面原因，这些异构应用各自独立，缺乏互操作性。另一方面，还必须考虑系统将来可能的扩充。为实现互操作和可扩展，必须对CIS和BAS制订规范，重点是接口标准、通讯协议、数据交换标准[8]、安全协议等。

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等攻击，还要防止工作人员失误、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。下面从微观上分析 CIS 可能存在安全威胁。

(1) 物理层安全威胁　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，它们面临地震、火灾等灾害，以及电磁辐射泄漏、人为操作失误、计算机犯罪的破坏。物理安全是 CIS 安全的前提。

(2) 网络层安全威胁　网络层是网络入侵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　主要包括由于应用层协议缺陷引起的安全威胁，以及应用系统设计缺陷和对系统的误操作和恶意破坏。CIS 中用户技术水平参差不齐，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，对系统的配置不当会造成安全隐患，从而影响到 CIS 中应用系统的安全性。

(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。

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 4 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。

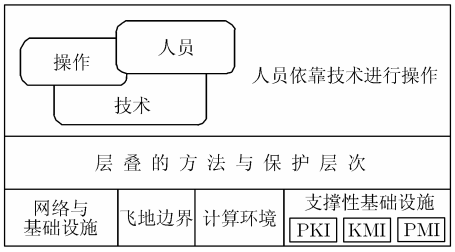

图 1 全面深度防御战略

3 安全的复杂信息系统体系结构模型

经过对 CIS 的深入分析，本文提出如图 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)，密码支撑层(ESL)，应用支撑层(ASL)，业务应用层(AL)，服务接口层(SAL)，安全防护与可靠性支持层(SPRSL)，系统管理层(SML)。

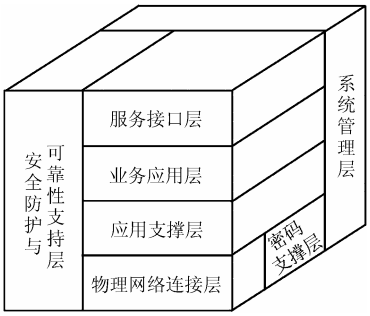

图 2 安全的复杂信息系统体系结构模型

3.1 物理网络连接层

PNCL为CIS提供信息传输和交换的硬件平台。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[9–12]。PNCL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，它与可信网络之间采用防火墙、认证网关进行逻辑隔离，国家涉密网络与可信网络之间物理隔离。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。

国家《计算机信息系统国际联网保密管理规定》第六条规定，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中国家涉密网络必须与其它网络物理隔离。为同时满足它与外界信息交换的需要，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中必须对密级精确定位，定密过宽会降低网络安全性；定密过严会增加网络安全保密经费负担，并且影响互连互通和互操作[13]。

3.2 密码支撑层

仅通过防火墙、入侵检测、防病毒等技术保障 CIS 安全是不够的，EEDP 的安全需求十分显著，还需要确保信息的机密性、完整性、操作的授权和不可抵赖性等，这些都需要大量的密码运算。ESL 提供必要的密码服务支撑，它的技术核心是 PKI 技术。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；时间戳服务提供从权威部门获取的精确可信的时间戳服务，为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；授权管理提供授权及访问控制服务。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 的服务。

3.3 应用支撑层

ASL 在 ESL 之上，它承载 BAS 中共性化的公共业务应用模块和安全应用模块，体现不同 CIS 的服务特色，对上层 AL 中的具体业务提供服务。它基于 ESL、信息交换规范和 Web Service 为 CIS 的互操作和可扩展提供支持。EEDP 中 ASL 主要包括安全消息服务系统、GIS 支持系统、安全文件传输、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。

3.4 业务应用层

AL 调用 ASL 的服务运行着系统中的 BAS，通过 SAL 为用户提供业务服务。不同 CIS 在 AL 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。

3.5 服务接口层

SAL 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。

3.6 安全防护与可靠性支持层

ESL为CIS提供密码服务，SPRSL的安全防护则侧重于基本安全防护，包括防火墙、病毒防治、入侵检测、漏洞扫描、安全审计、Web信息防篡改、黑客诱捕等。它可以很大程度上屏蔽网络层、应用层和系统层安全威胁。SPRSL还提供故障恢复和容灾备份功能。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，在灾难时快速切换本地和异地备份中心，确保系统在任何情况下都能正常运行[14]。

SPRSL 贯穿于模型中涉及到的所有层。对安全和可靠性要求相对不高的信息系统，可以根据具体情况在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。

3.7 系统管理层

SML不仅包括对设备、网络、应用的管理，还包括人员的管理，以最大程度降低管理层安全威胁。它贯穿于模型中所有层。为保障系统安全，在技术因素之外，还必须制订相应的人员管理制度[15]。由于需要集成SPRSL的组件到SML中，SPRSL同样需要可管理性。因此，SML和SPRSL之间应该有良好的接口。

4　模型分析

4.1 复杂性

模型采用分层方式把 CIS 和业务系统划分成较小的功能模块，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。模型可以节省系统开发和维护的投入，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，模型能够有效降低系统复杂度。

4.2 安全性

SCISAM 为建设 CIS 提供总体框架，它以 PKI 为安全基础，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。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 必须严格遵守国家的相关法规，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、病毒防治系统、入侵检测系统、漏洞扫描系统、故障恢复与容灾备份等配置科学的安全策略。在 SML 中应制订合理的系统管理策略和人员管理制度。

4.3 互操作与可扩展性

Web Service 包括简单对象访问协议、Web 服务描述语言以及通用描述、发现和集成等协议。通过在相关层中使用 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分布式模块化组件，使系统以不依赖语言的方法相互兼容，实现 BAS 之间的互操作和可扩展。

5 应用实例

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，它们分布于 20 多座楼宇中，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3 是简化的EEDP网络连接示意图，该网络大部分区域都与Internet物理隔离。EEDP使用ESL为系统提供通用密码服务。不同部门使用认证网关把整个网络划分成多个信任域。按照SPRSL的要求，在适当位置部署IDS、防病毒等系统，在关键位置采用多机冗余技术，在异地建设灾难恢复中心实现灾难恢复能力。EEDP抽取并封装系统中众多应用的通用功能以提供通用的服务，例如：GIS服务、消息服务等。EEDP的业务应用位于AL层。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、安全的运行。

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

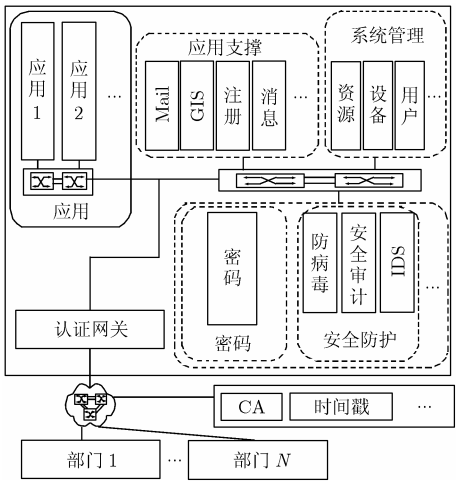

图 3 简化的 EEDP 网络连接示意图

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。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。

信息技术的应用发展迅速，虽然该电子政务系统当前能够满足应用需求，但是未来几年情况如何呢？为更好保护投资，有必要确信该系统在未来几年仍然能够满足要求。因此，我们使用OPNET对整个网络系统建模，仿真未来四年中网络的通信情况。中国电子政务 2001 和 2002 年的应用增长率都大约为 20%[16]，因此本文在仿真中设置系统在今后几年的网络通信年增长率为 30%，以考察系统在较高网络通信增长率时的性能。这意味着在未来的四年中，网络通信增长率将为当前的 130%，169%，219.7%，285.61%，仿真结果如图 4 所示。随着网络通信的增长，数据库查询响应时间从 0.000255s增至 0.000259s，接收和发送电子邮件的响应时间依然为 0.0024s和 0.0016s，HTTP页面响应时间从 0.00266s 增至 0.00267s，FTP下载和上传响应时间从 0.00181s增至 0.00182s。可以看出，各种应用响应时间的变化都不会严重影响应用的性能。

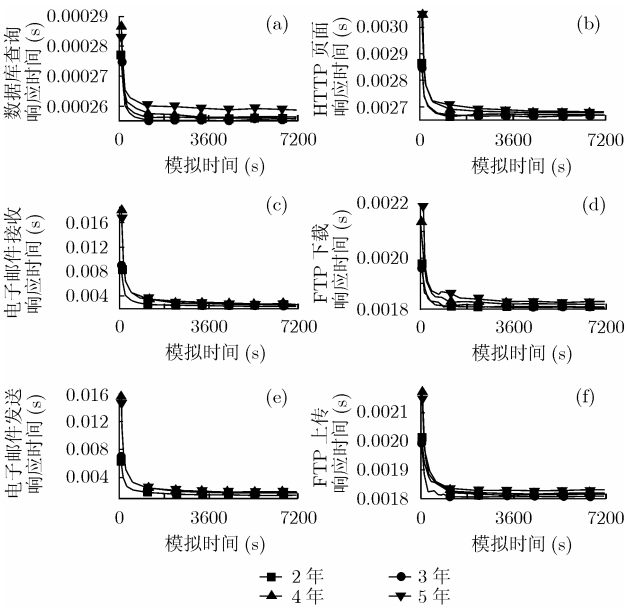

图 4 应用响应时间预测

6　结束语

根据 “十五”某电子政务试点示范工程的要求，本文提出安全的复杂信息系统体系结构模型，为新建或改造复杂信息系统提供框架指导。EEDP 已经在模型的指导下建设完成，实践、统计数据和网络仿真证明模型能够满足 EEDP 的要求。模型支持业务应用之间的安全性、互操作性、可扩展性，适用于对安全要求非常高的 CIS。对模型中相应层次适当简化，模型也可用于相对简单的信息系统。在模型的基础上，国家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，以引导我国电子政务的建设。

参 考 文 献

[1] Shnitko A. Adaptive security in complex information systems[C]. Proceedings of the 7th Korea-Russia International Symposium on Science and Technology, Ulsan, South Korea, 2003: 206–210.

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

[3] Zhou B Y. Security analysis and the DSM model[C]. Proceedings of 13th International Workshop on Database and Expert Systems Applications, Aix-en-Provence, France, 2002: 17–21.

[4] Hripcsak G. IAIMS Architecture[J]. *Journal of the American Medical Informatics Association*, 1997, 4(2): S20–S30.

[5] Lee S Y and Koh J S. WWW-based reliability information system[J]. *Computers & Industrial Engineering*, 1998, 35(3 4): 599–602.

[6] Chou S C T. Migrating to the web: A web financial information system server[J]. *Decision Support Systems*, 1998, 23(1): 29-40.

[7] Van R and de Velde. Framework for a clinical information system[J]. *International Journal of Medical Informatics*, 2000, 57(1): 57–72.

[8] XML 在电子政务中的应用指南[S]. 2005, GB/Z 19669–2005.

[9] 信息技术设备的安全[S]. 2001, GB 4943–2001.

[10] 路由器安全技术要求[S]. 1999, GB/T 18018–1999.

[11] 信息技术包过滤防火墙安全技术要求[S]. 1999, GB/T 18019–1999.

[12] 信息技术应用级防火墙安全技术要求[S]. 1999, GB/T 18020–1999.

[13] 朱鲁华, 施军, 沈昌祥. 涉密网的物理隔离问题[J]. 电子计算机, 2002, 154: 16–19.

[14] Wang K, Su R D, and Li Z X, *et al*.. Robust disaster recovery system model[J]. *Wuhan University Journal of Natural Sciences*, 2006, 11(1): 170–174.

[15] Grimaila M R. Maximizing business information security's educational value[J]. *IEEE Security & Privacy Magazine*, 2004, 2(1): 56–60.

[16] 刘权. 我国电子政务发展现状与趋势[J]. 中国信息导报, 2004, 12: 21–23.

王　琨： 男，1973 年生，博士生，研究方向为网络与信息安全.

尹忠海： 男，1964 年生，博士生，副教授，研究方向为网络与信息安全.

周利华： 男，1942 年生，教授，博士生导师，研究方向为网络与信息安全、网络多媒体.

袁　峰： 男，1976 年生，高级工程师，研究方向为网络与信息安全.