基于 PMI 的 ERP 系统安全基础设施研究

Researching the Information Security Infrastructure of PMI – based for ERP System

蒋泰 钟文龙 (重庆电子职业技术学院计算机工程系 重庆 400021)

摘 要:在网络平台上 ERP 系统的信息安全风险变日益的突出和严重。本文从安全体系结构的整体高度,针对 ERP 系统目前存在的安全风险,研究如何构建一个基于 PMI 的安全基础设施为 ERP 系统提供系统的、整体的安全解决方案。

关键词:ERP 系统 PMI PKI 安全风险 安全基础设施

1 前言

在现代信息技术的推动下,ERP 已经成为近年来企业管理界和信息产业界推广和应用的一个热点。与此同时在网络平台上的 ERP 系统信息安全问题正面临着巨大的挑战,安全隐患日益的突出和严重。而当前 ERP 系统的安全解决方案仅处于依靠各种单一的安全技术的简单叠加的层面上,没有从整体的安全体系高度上系统的考虑。

2 ERP 系统的安全需求

面对如此种种的安全威胁和隐患,作为一个安全的 ERP 系统,必须具有一个安全、可靠的网络基础平台,以保证信息安全、迅速地传递,保证数据库服务器绝对安全,防止黑客的恶意攻击;以及防止企业内鬼的有目的破坏和窃密,而且它自身的安全必须要求保证应用程序只能用于预定的目的以及只能被适当的用户使用。

2.1 ERP 系统的概念

ERP——Enterprise Resource Planning 企业资源计划,其实质是综合应用了 C/S(客户机/服务器)体系结构、关系数据库结构、面向对象技术、图形用户界面、第四代计算机语言(4GL)、网络通讯等信息技术成果,整合了企业管理理念、业务流程、基础数据、人力物力的一种高度信息集成的软件系统。它将企业整个营运过程的每一个环节和各个功能模块都集成在一起,管理和控制着一个完整的企业内部“供应链”,从而帮助企业获得在竞争中的整体优势。

2.2 ERP 系统的网络结构

ERP 系统通常都分布在企业的各个部门和各个分子机构,通过网络进行交互,所以构建高速、安全、有效的网络平台成为 ERP 系统成功实施的前提条件。

纵观目前的各种 ERP 系统软件产品,大多数的系统都采用 C/S 结构。顶层是运行后台数据库管理系统的数据库服务器,中间层是运行商业应用的一台或一组应用服务器,最底层的是运行具体应用的客户终端。随着 INTERNET 技术的发展和普及应用,一些 ERP 系统已采用了 B/S 结构,在中间层加入了 WEB 服务器,从而支持远程的业务交互。

2.3 ERP 系统的安全风险

由于 ERP 系统受企业网络平台的技术条件、网络产品、通信协议和人员素质等方面限制,就不可避免的可能存在安全风险,从而构成了对 ERP 系统的安全威胁和隐患。目前 ERP 系统的主要存在的安全风险来源于如下几方面:

(1) 各种硬件设备。如路由器、交换机等广泛使用的网络设备可能存在的安全漏洞和“系统后门”。

(2) 操作系统平台。当前流行的操作系统都存在多种不同的系统级安全漏洞。

(3) 服务器配置。由于服务器的各种功能的配置纷繁复杂,特别是关于通信安全方面的配置,一旦配置有误就很容易遭到攻击导致整个系统的崩溃。

(4) 企业内鬼。企业内的员工作为授权合法用户

利用工作之便为了满足其好奇心或得到不当利益而进行的主动破坏和非法的访问。

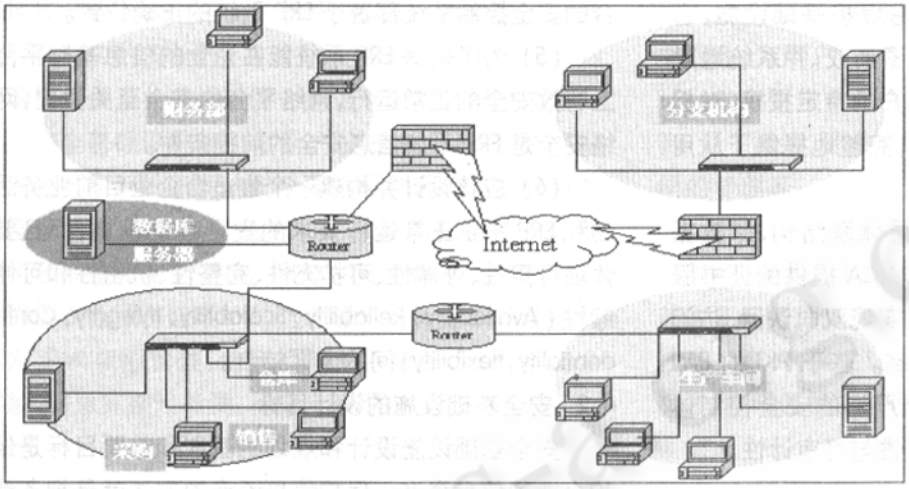

图 1　ERP 系统网络结构

(5) 人为过失。最多的错误来源于人为的无意失误,专家估计信息系统一半以上的经济和生产力损失是由人为的失误而不是有意或恶意的行为引起的。这些失误包括错误的安装和管理设备或软件、误删除文件、文件更新错误等能够造成信息损失和系统故障的行为。

(6) 系统设计缺陷。由于在系统设计阶段没有考虑或没有完全考虑各种可能的安全威胁和安全隐患,形成安全漏洞。

(7) 黑客和其他入侵者。来自黑客,职业罪犯,商业间谍,犯罪组织甚至国外情报机构等未经授权的非法入侵者数量在不断增长,他们有的为了金钱、商业秘密,有的为了挑战极限挑战自我而入侵,破坏系统窃取机密,造成极坏的影响存在极大的安全风险。

(8) 网络协议。网络协议普遍采用 TCP/IP 协议族,本身缺乏安全性。

(9) 安全产品。网络安全产品自身是否可靠,是否正确设置,以及缺乏有效的网监视手段都可能成为安全隐患。

(10) 病毒和其他恶意软件。病毒、蠕虫、特洛伊木马和其他恶意软件能够通过借来的磁盘、软件、电子邮件以及 Internet 连接进入企业网络从而影响 ERP 系统。

3　PMI 安全平台

目前大多数的 ERP 产品在安全控制方面仅采用了简单的身份认证“用户 ID + 用户口令”的单因素认证方式,和简单的二维表的权限管理方法,这是一种极易被攻破的安全控制措施,其安全级别是最低的。

3.1　PKI 信任体系

ERP 系统是一个纵向、横向跨越多个部门,连接多个业务子网的系统,如果没有一套强健完善的信任体系,那么系统运行过程中,重要文件、敏感信息的失密、伪造、篡改将泛滥成灾,从而严重影响系统的正常稳定运行,甚至造成难以估计的严重后果。因此,有必要采用基于密码学的 PKI 技术为 ERP 系统提供增强的用户身份认证方式,构建一套高可信度的信任体系。

PKI 被称为公共密钥基础设施,是通过数字证书的颁发和管理,为 ERP 系统提供用户身份识别和保证信息的机密性和完整性的安全服务。

数字证书是由其最主要的组件 CA 服务器来颁发的,作为验证用户身份的标识,其权威性与可信性可以有效解决网络中的信任问题,成为构建 ERP 系统信任体系的基础。

3.2　PMI 集中授权系统

采用基于 PKI 技术的 PMI 特权管理基础设施可以为 ERP 系统提供独立于应用的安全的授权管理模式,能切实地保障信息资源和业务处理的安全控制。

PMI(Privilege Management Infrastructure)是一种集中授权系统,采用基于属性证书(AC)的 RBAC 授权模式,向应用系统提供与应用相关的授权服务管理,提供用户身份到应用授权的映射功能。

PMI 可以有效实现用户的身份验证、身份的证实与访问控制,由于公钥证书是 ERP 系统主体(用户、主机、网络设备)的证实自己身份的唯一标识,因此用户或网络设备在访问相关密级的信息资源或连接资源服务器时,必须由系统验证用户所持有的公钥证书以及

绑定的属性证书，并检查证书持有者的身份和权限属性等信息。

3.3 构建基于 PMI 的安全平台

PMI 实际提出了一个新的信息保护基础设施，它是以 PKI 为基础的，和目录服务紧密集成，并系统地建立起对用户的身份认证，对认可用户的特定授权，对权限管理进行了系统的定义和描述，完整地提供了从用户认证到授权服务的所需过程。

ERP 系统一般采用严格的三层体系结构，即数据库服务器、应用服务器、客户机。以 CA 提供的证书服务为基础，应用服务器可以很容易实现双向认证、访问控制、访问过滤等应用级安全机制。基于 PKI 的 PMI 安全平台为 ERP 系统构建了一个严密的安全控制体系，充分保证敏感资源访问的可控性与可审计性。

4 基于 PMI 的安全基础设施的研究

将若干单一的安全技术（产品）有机的结合在一起形成一个系统的整体的安全解决方案，为 ERP 系统提供一个统一的安全基础设施，从而发挥各个单一组件结合后的“1+1>2”的整体效能，这样才能从根本上解决安全问题。

构建一个基于 PMI 的安全基础平台，结合企业的安全策略与安全管理为企业的 ERP 系统提供统一的、系统的、整体的、全方位的安全解决方案。

4.1 安全基础设施的设计原则

安全基础设施的设计通常是科学技术、技巧艺术和实施过程三者的有机结合。不仅必须清楚安全基础设施所要保护的企业信息资产的价值和重要性，而且还要对安全威胁与隐患的多种形式和它的延伸形式有清晰的认识和预先的判断。因此在设计和规划企业信息与网络安全基础设施时应该遵循如下的原则：

（1）在设计和规划安全基础设施之前，对企业当前的安全威胁与隐患的发展趋势和最新的黑客工具和攻击技巧要有充分的理解和意识。

（2）为了保护企业的信息资产，必须清楚它的信息资产在哪里，它们支持什么样的商业过程和应用，应使用多种技术评估的方法来确定企业的信息资产，并记录它们所支持的商业。

（3）安全基础设施应该能够确保其体系结构中的大量安全组件协同作用，以全面提高安全保障力度，使之超越任何单一组件的方式进行组织。

（4）要让所构建的安全基础设施能有效的发挥作用，其中关键的一点就是有将有各种安全组件有机组合的安全控制系统部署于 ERP 系统的正确位置。

（5）为了确保 ERP 系统能在企业的信息基础平台上有效安全的正常运行，网络平台的安全至关重要，网络安全是 ERP 系统信息安全的前提条件。

（6）应该设计并构建一个最适合企业目前业务活动和 ERP 系统正常运行要求的安全基础设施，而且要体现可用性、可靠性、可扩充性、完整性、机密性和可伸缩性（Availability, Reliability, Scalability, Integrity, Confidentiality, flexibility）间的全面结合。

4.2 安全基础设施的设计目标

安全基础设施设计和规划的基本和首要目标是保护企业的信息资产。保护信息资产的方法就是把各种安全组件有组织的、有效的、系统的集成到基于 PKI/PMI 的安全基础设施中。应用在信息资产上的安全控制措施应该符合企业的安全目标和企业的安全策略文档中的要求。尽管只提到了信息资产的保护，但在保护信息资产以及确保其可用性的过程中，企业的 ERP 系统和网络基础平台也同时得到了安全保护。图 2 描述了安全基础设施的设计目标。

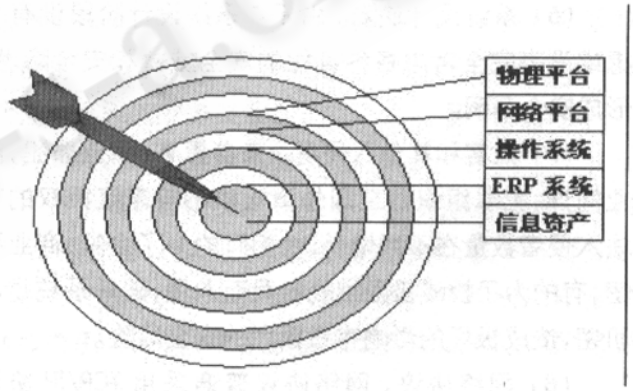

图 2　安全基础设施设计的靶心

4.3 安全基础设施的体系结构

通过对 ERP 系统的安全风险的分析，按照安全基础设施设计的原则和实现安全基础设施的基本与首要目标，需要以 PMI 技术为基础构建一个全方位的，完善的安全基础设施。

基于 PMI 的的安全基础设施，其安全控制系统的

体系架构基础必须是公钥证书 PKC 提供的唯一性身份识别加上属性证书 AC 提供的独立的权限控制。并在此基础上通过数字签名加强系统操作的可靠性，结合 VPN 技术保障数据传输的私密性，确保敏感数据在传输和存储中的安全性，通过防火墙技术和 IDS 技术防止网络入侵来共同构建统一的信息与网络安全体系。

安全基础设施提供了全方位的安全服务，并根据不同业务子网的不同的安全要求分别采用不同等级的安全保护措施，从而实现对 ERP 系统的信息资产和网络平台的整体安全保护。具体的安全体系结构由七个方面的安全服务组成：安全策略与信息分级，PKI 身份识别，PMI 权限管理，访问控制与入侵检测，信息安全传输，信息完整性检测，和安全管理。

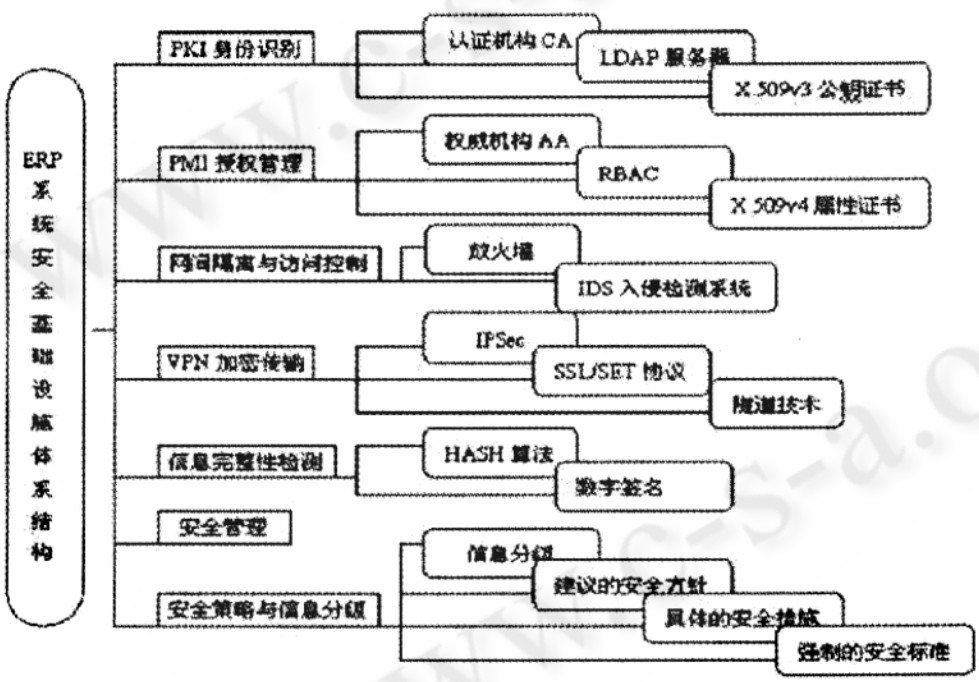

图 3　安全基础设施的体系结构

4.4 安全基础设施组件

根据安全基础设施的体系结构的需要，安全基础设施组件主要包括：数字证书系统、权限管理系统、安全服务器、VPN 网关、防火墙、入侵检测系统、智能卡或 USB Key、安全策略和安全管理说明文档等安全组件。各个组件的部署和构成关系见图 4。

在这样的安全基础设施中，PMI 安全平台是核心和基础，通过数字证书系统颁发的公钥证书来提供信任服务以及通过权限管理系统颁发的属性证书提供权限控制，结合其他安全组件协同工作构成了一个立体的全方位的安全体系。

(1) 数字证书系统。提供基于 X.509v3 的数字证书服务，为用户、网络设备或主机提供唯一的身份认证。其主要任务是受理证书申请，签发证书，证书查询，证书撤消，证书有效期，管理 CRL 证书撤消列表，密钥的管理等。

(2) 权限管理系统。提供基于 X.509v4 的属性证书服务，为 ERP 系统提供独立的和灵活的权限管理。其主要任务是受理属性证书的申请，签发属性证书，属性证书查询，属性证书撤消，管理 ACRL 属性证书撤消列表，权限属性的管理等。

(3) 安全服务器。对其他的安全组件提供集中的控制服务，协调和统一指挥安全组件的协同工作。其主要任务是根据企业的最新安全策略初始化和集中配置 VPN 网关、防火墙和入侵检测系统等安全组件，记录它们的每一次改动和原始配置信息，保存 IDS 入侵检测系统的审计日志，管理 VPN 网关的证书、私钥和隧道配置信息等。

(4) VPN 网关。提供系统在开放的不安全的公用网络上建立专用的安全的数据加密传输通道，从而实现对企业内部网络的安全扩展。这将极大的方便企业分支机构和在外出差工作人员的远程访问企业数据中心，实现无缝业务处理。

(5) 防火墙。提供各个业务子网之间和内外网之间的安全隔离。通过各种隔离技术相结合使用包括数据包过滤、状态检测、以及应用代理等限制和控制网络间的流量来保护系统中重要的信息资源，防止未经受

权的访问。防火墙是整体安全防护体系的一个重要组成部分，而不是全部，必须将防火墙的安全保护融合到系统的整体安全策略中。

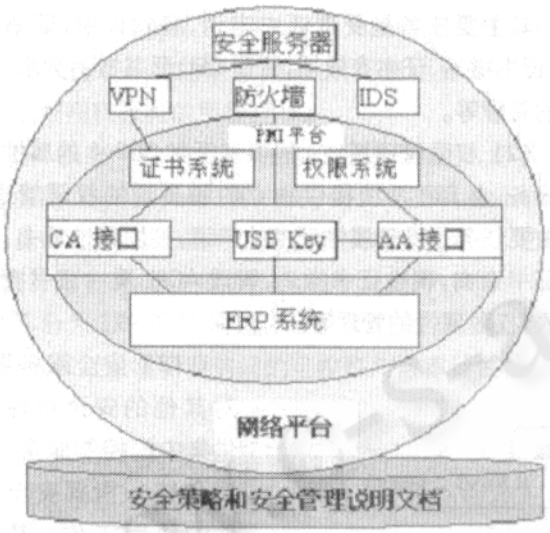

图 4　安全基础设施组件

(6) 入侵检测系统。入侵监测系统处于防火墙之后对网络活动进行实时检测和及时反应。它是防火墙的延续，可以和防火墙、路由器协同工作。

(7) 智能卡或 USB Key。智能卡或 USB Key 具有生成和存储用户密钥对以及保存数字证书的功能，以硬件的形式来保护用户的私钥。这样就使得 ERP 系统可以用用户知道的东西加上拥有的东西来进行双因素认证。

(8) 安全策略和安全管理说明文档。这是一个基本的安全基础设施组件，是安全基础设施有机组成部分。它定义了企业信息资产的保护范围以及提出或要求对这些信息资源采取何等的特定安全保护机制。

5　结束语

从安全体系结构的整体高度开展对安全基础设施的研究工作，能够为解决信息与网络安全提供一个整体的理论指导和基础构件的支撑，并为信息与网络安全的工程奠定坚实的基础，推动信息安全产业的发展。全方位的可集成的安全基础设施，为 ERP 系统的综合应用以及企业组织内部业务运作中信息安全的统一发展提供了整体框架。

参考文献

1 关振胜，公钥基础设施 PKI 与认证机构 CA[M]，北京：电子工业出版社，2002.

2 张大江、钱华林，RBAC 的数字证书方案[J]，系统工程与理论，2002.4.

3 ERP 系统技术白皮书[J]，用友软件股份有限公司，2002.9.5.

4 William Stallings, Network Security Essentials: Applications and Standards, Published by Prentice - Hall, Inc. 2002.