

ERP 系统中 IAM 功能的应用设计

朱诗生^{1,2}, 汪 涛^{1,2}

(1. 汕头大学计算机系, 汕头 515063; 2. 汕头大学智能制造技术教育部重点实验室, 汕头 515063)

摘 要: 针对安全领域存在的身份识别与访问管理(IAM)问题, 提出在企业资源计划(ERP)应用系统中正确鉴别用户身份的设计方法。采用多因子认证技术, 为 ERP 系统定制防火墙, 使用 AES 和 MD5 算法对保存或传输的数据进行加密, 通过进程间的通信将 IAM 系统与 ERP 系统平滑连接, 从而避免来自系统内外的攻击, 为系统资源的安全管理提供可靠保证。

关键词: 身份识别与访问管理; ERP 系统; 系统设计

Application Design of IAM Function in ERP System

ZHU Shi-sheng^{1,2}, WANG Tao^{1,2}

(1. Department of Computer, Shantou University, Shantou 515063;

2. Key Laboratory of Intelligent Manufacturing Technology, Ministry of Education, Shantou University, Shantou 515063)

【Abstract】 Aiming at Identification and Accessing Management(IAM) in security area, the design scheme is put forward for the correctness of identifying consumers' identities in Enterprise Resource Planning(ERP) system. It uses technique of multiple factors certification. Moreover, a firewall is designed for ERP system specially. It encrypts the saving or transmission data by AES/MD5 algorithms. Process communication technique is applied in connecting IAM system and ERP system smoothly. In these ways, ERP system avoids attacks from outside and inside, so that ensures its own system resources' security management.

【Key words】 Identification and Accessing Management(IAM); Enterprise Resource Planning(ERP) system; design of system

IAM(身份识别与访问管理)是近年来比较热的一个信息安全产品, 包括 2 个方面: 身份识别与访问管理^[1]。身份识别是指计算机及网络系统确认操作者数字身份的过程, 访问管理是指权限的分配。IAM 是由连续 5 年被 IDC 评为 IAM 市场领军企业的 CA 公司最新推出的产品, 其良好的特性(即全面性、集成性、开放性^[2]), 使客户得以将 CA 的安全策略引擎成功地延伸到所开发的应用程序中。本文在开发实施 ERP 应用系统的过程中, 针对 IAM 系统所做的应用设计进行了介绍。

1 IAM系统功能

IAM 系统独立于 ERP 系统, 其功能是负责 ERP 系统的用户身份认证与访问管理。该系统在使用传统用户/密码技术的基础上增加了指纹验证、USB Key、智能卡等识别技术, 是一个多因子可选择认证系统。该系统采用 C/S 架构, 与 ERP 系统之间采用共享内存与加密文件的方式进行交互。针对 ERP 系统的访问, 使用了防火墙技术。

IAM 系统的功能模块包括注册子模块、销户子模块、身份认证子模块、访问管理子模块、IAM 与 ERP 系统的接口子模块、针对 ERP 系统的防火墙子模块、加密传输子模块等。

(1)注册子模块

用户注册时需提交用户的基本信息。如果采用指纹验证, 还需要提供指纹图像。IAM 系统客户端先记录用户的基本信息, 接着对提交的指纹图像进行预处理后提取其特征。

用户在填写基本信息时, 需重复输入密码。一旦 2 次密码匹配且采集到指纹, 系统则将用户的基本信息加密后传输给服务器, 以验证用户的合法性。如果合法, 则用户的注册资料将存入相关数据库, 并返回注册成功信息; 否则, 返回

注册失败的信息。

(2)销户子模块

用户退出 ERP 系统时需进行用户注销操作。用户注销由 IAM 客户端发起请求, 由 IAM 服务器端进行处理。销户时也要进行用户信息的核对, 并将操作记录存进日志中。

(3)身份认证子模块

身份认证是 IAM 系统的灵魂和基础, 该模块提供了多种识别方式供 ERP 实施人员在实施的过程中自由选择组合。

1)指纹认证

指纹是一种比较稳定的生物特征, 不会因年龄或健康情况的变化而变化, 2 枚指纹即使具有相同的总体特征, 但局部特征(即特征点)却不可能完全相同。指纹识别技术通常使用指纹的总体特征, 即纹形、三角点等来进行分类后, 再用局部特征, 即位置、方向等来识别用户身份。识别过程包括: 指纹的获取, 指纹图像预处理, 指纹特征提取, 以及指纹特征匹配。

指纹特征匹配采用指纹几何特征技术^[3]。考虑到指纹可能存在茧、刀伤或者采集干扰等问题, 同一用户可以新增 2 个~3 个指纹, 目的是使数据库里尽可能存有用户的最新指纹。

2)智能卡认证

用户可以使用智能卡来登录系统。智能卡是一种用于存

基金项目: 广东省高教厅基金资助项目“中小企业的 ERP 系统的研究与开发”(0139)

作者简介: 朱诗生(1963—), 男, 副教授、硕士, 主研方向: 企业建模, 应用集成; 汪 涛, 硕士研究生

收稿日期: 2009-09-23 **E-mail:** sszhu@stu.edu.cn

放用户身份信息的、内置的、不可复制的集成电路。智能卡认证通过使用不可复制的硬件来保证用户身份的唯一性。

用户将自己的信息存储到智能卡上,当 IAM 系统检测到有智能卡插入时,就读取智能卡上的数据,并将其发送到 IAM 系统的服务器端,进行验证。

3)USB Key 认证

USB Key认证使用了具有USB接口的USB Key硬件。每个USB Key 硬件都有用户PIN码,且内置单向散列算法(MD5)。USB Key认证首先要在USB Key和服务器中各存储一个能证明用户身份的密钥。当需要验证用户身份时,先由客户端向服务器发出一个验证请求。服务器接到此请求后生成一个随机数并传给客户端(此为冲击)。客户端将收到的随机数提供给插在客户端上的USB Key,由USB Key使用该随机数与存储在USB Key中的密钥进行带密钥的单向散列运算(HMAC-MD5),并将得到的结果作为认证证据传送给服务器(此为响应)。与此同时,服务器也使用该随机数与存储在服务器数据库中的该客户密钥进行HMAC-MD5 运算。如果服务器的运算结果与客户端传回的响应结果相同,则认为客户端是一个合法用户。

(4)访问管理子模块

在 ERP 系统中,每一种用户能够访问的资源是不同的,因此要由系统管理员来对各用户进行划分权限。系统管理员甚至可以设置系统中各个用户的用户名和密码,这对系统的安全造成了隐患。本系统在为用户重设密码时,采用了系统产生随机数后发送到用户邮箱的方式,在数据库中的密码也要经过 MD5 加密后再进行存放。

(5)IAM 系统与 ERP 系统的接口子模块

开放性是一个 IAM 系统的重要特性。开放就是必须要有通用的开放接口,能通过简单、灵活的开发,与各种应用系统紧密连接^[2]。

(6)ERP 系统的防火墙子模块

系统在用户登录时, IAM 对其 IP 地址和端口进行登记,

另外再获取正在与 ERP 系统通信的 IP 和端口^[4],通过对比,当正在发生通信的源 IP 和端口与已经登记的不同时,就对其进行拦截。

(7)加密传输子模块

在往网络发送信息之前,协议层需调用安全层中的加密模块加密后发送信息,以达到安全通信的目的。本系统采用以随机数作为 AES(Advanced Encryption Standard)加密算法的 Key 加密机制^[5],并配合 MD5 散列算法,较好地解决了网络传输的安全性问题。

2 IAM系统设计

下面介绍系统的设计:

(1)软件平台和开发工具

操作系统:带有 Service Pack 2.0 的 Microsoft Windows XP Professional。

数据库平台: MySQL-4.0.13 for Windows。

开发工具: Microsoft Visual Studio, ADO.NET(连接数据库)。

(2)服务器端设计

IAM 系统 Server 端负责管理用户身份以及完成与客户端的交互,并管理用户的智能卡信息、USB Key 信息、指纹信息等数据库。

IAM 系统结构关系如图 1 所示。图 2 是以指纹认证为例的服务器端的运行界面。

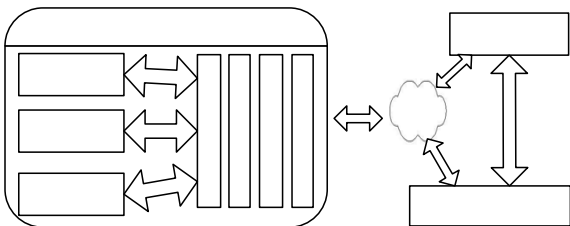


图 1 IAM 系统结构关系

身份认证服务器端								
文件(F) 数据库编辑(E) 数据库查看(V) 指纹数据库维护(T) 系统设置(S) 管理(M) 帮助(H)								
身份认证管理								
iam								
fingerprint								
user_priv								
userinfo								
NO	ID	pwd	FPID	IP	state	countstate	UserType	
1	111	8fae1645fdb13...	1	0.0.0.0	0	0	1	
2	222	8fae1645fdb13...	2	0.0.0.0	0	0	2	
3	hgy	8fae1645fdb13...	3	127.0.0.1	1	0	5	
4	333	8fae1645fdb13...	4	0.0.0.0	0	0	3	

图 2 指纹认证服务端界面

(3)客户端设计

以指纹认证为例,注册子模块完成对授权新用户信息的注册,主要工作包括指纹特征信息获取、用户认证信息加密、用户认证信息传输、用户认证信息解密和指纹特征信息匹配。认证子模块用于验证请求登录的用户是否是合法的用户,用户在登录过程中,需要输入正确的用户名/密码及相匹配的指纹才能通过认证。注册及认证模块会调用图像的预处理模块、特征值提取以及网络传输等模块。在网络传输子模块中使用了 AES 加密技术。用户登录时,如果成功登录,则会获得通过验证用户特有的权限。一旦通过验证,对应的菜单栏将加亮,用户便通过了进入 ERP 系统的认证,获得了访问管理的资格。

3 设计过程中遇到的问题以及解决方法

与现有的 ERP 系统的平滑连接是 IAM 系统设计追求的

目标。下面介绍在本系统设计中提出并实现的 IAM 与 ERP 系统的 3 种对接机制。

(1)机制 1——加密文件作中间桥梁

用户登录 IAM 系统通过验证后, IAM 系统会在其服务器端生成一个加密文件。当用户调用 ERP 系统时, ERP 系统会连接到 IAM 服务器端去读加密文件,获得该用户成功登录的资料后,系统直接进入 ERP 系统的功能界面。

此机制的特点是:使用加密文件作为中间桥梁,以实现 2 个不同系统的对接。

(2)机制 2——标识变量交互

登录 IAM 系统通过验证后, IAM 服务器会给 IAM 客户端返回一个标识变量。当该用户在本次登录中使用 ERP 系统时,由 IAM 客户端直接将此标记变量传递给 ERP 系统。

(下转第 188 页)