[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810117128.0

[43] 公开日 2010 年 1 月 27 日

[11] 公开号 CN 101635704A

[22] 申请日 2008.7.24
[21] 申请号 200810117128.0
[71] 申请人 北京盖特佳信息安全技术股份有限公司
地址 100086 北京市海淀区万泉河路 68 号紫金大厦 1201 室
[72] 发明人 张建荣 宋 辉
权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称

一种基于可信技术的应用安全交换平台

[57] 摘要

本发明涉及一种支持网络间可信应用进行安全信息交换的平台，属于信息安全领域。 本发明采用可信认证技术、安全隔离技术、协议分析和识别技术、访问控制技术、内容过滤和审查技术等最前沿的安全技术和信息处理技术，提供一个通用的安全交换平台，为可信应用之间提供安全数据交换通道，禁止未获得许可的应用数据在网络间交换，提高网络边界的安全。 本平台总体上由可信应用认证体系和安全应用交换平台两大部分组成，可信认证体系从各种不同的层面上保障应用交换的安全、可信，安全应用交换平台实现各种即时应用信息交换、数据库同步、文件交换功能，为各种数据交换提供跨越不同安全级别网络的安全交换机制。 根据行业应用特性，平台可以提供专业化的安全隔离与数据交换系统和工具。

1、一种基于可信技术的应用安全交换平台，其特征在于：系统在可信认证体系保障下，在安全隔离与信息交换系统的通道上建立安全应用交换平台，为不同网络间应用程序的各类信息交换模式提供安全传输工具，禁止未获得许可的应用数据在网络间进行交换，以提高网络边界的安全；

2、根据权利要求 1 所述的可信应用安全交换平台，其特征在于：平台总体上由可信应用认证体系（TACI，Trusted Application Certification Infrastructure）和安全应用交换平台（SAEP，Security Application Exchange Platform）两大部分组成，可信认证体系从各种不同的层面上保障应用交换的安全、可信；

3、根据权利要求 2 所述的平台构成，其特征在于：可信应用认证体系提供了三方面的保障：主/客体可信、行为可信和内容可信。应用认证不仅提供用户身份的认证，也提供应用系统的身份识别，防止未授权应用系统的数据在平台间进行交换；内容可信在使用基本的加、解密技术、完整性检查技术的基础上，进一步提供标准协议的专业内容审查工具、各种业务应用内容审查插件；行为可信则主要通过访问控制、访问授权等技术实现；

4、根据权利要求 2 所述的平台构成，其特征在于：安全应用交换平台实现各种即时应用信息交换、数据库同步、文件交换功能，为各种数据交换提供跨越不同安全级别网络的安全交换机制；

5、根据权利要求 4 所述的安全应用交换平台，其特征在于：平台采用层次化结构设计，按照功能从下至上依次划分为传输层、应用表示层和应用交换层，传输层重点解决基于标准网络协议的网路隔离和信息交换问题，多主机硬件平台、安全操作系统、专用通讯硬件、专用通讯协议从物理层到网络层彻底阻断了 TCP/IP 连接；应用表示层重点解决对主流标准应用协议和非标准定制协议数

据交换的协议封装和表示，实现传输协议无关的传输通道；而应用交换层则通过透明代理技术，提取出交换双方的应用数据，为业务数据安全交换提供开发接口。

一种基于可信技术的应用安全交换平台

技术领域

本发明涉及一种基于可信技术的应用安全交换平台，具体方法是在安全隔离与信息交换系统的传输通道基础上实现各种应用表示以及提供安全应用交换功能，平台在可信应用认证体系保障下，为各类应用之间提供安全数据交换工具，禁止未获得许可的应用数据在网络间交换，提高网络边界的安全。

本方法属于信息安全技术领域。

背景技术

二十世纪九十年代以来，随着计算机技术的高速发展，网络技术也得到了前所未有的发展，网络逐渐成为政府、企业和个人事物处理中不可或缺的一部分。

在网络技术的发展过程中，特别是互联网技术的发展，使得世界范围内的信息资源可以充分交流和共享，为人们的生活和工作带来了极大的便利。

随之而来的网络安全问题也逐渐成为人们关注的热点，特别是防范来自外部网络的攻击和内部网络的有意或者无意的泄密，已成政府、企业和个人适用网络资源过程中所关注的一大焦点。对于政府而言，这个问题尤为重要。在政府的信息网络中，许多信息都涉及到国家的机密信息，如果造成失窃或泄漏，将直接危及到整个国家的安全。为此，各国政府都制定了相应的政策和技术方案来确保网络信息的安全。

我国政府最早在1999年由国家保密局发布了《计算机信息系统国际联网保密管理规定》，其中规定了涉密信息系统的联网要求：“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其它公共信息网络相联接，必须

实行物理隔离”（第二章第六条）。

2002 年，随着我国电子政务如火如荼的发展，《国家信息化领导小组关于我国电子政务建设指导意见》[中办发〔2002〕17 号]由中共中央办公厅和国务院办公厅联合发布。本意见中，对于电子政务中的网络隔离问题做了明确的规定：“电子政务网络由政务内网和政务外网构成，两网之间物理隔离，政务外网与互联网之间逻辑隔离。”

2007 年，国家保密局、国务院信息化工作办公室联合颁布了《电子政务保密管理指南》[国保发〔2007〕5 号]文件，文件重点规定了电子政务网络的互联问题，规范了隔离产品的使用方式和技术要求。

安全隔离与信息交换系统正是在这样的产业背景之下，发展起来的新一代信息安全产品，其主要在保证不同安全级别的网络安全隔离的前提下提供安全可控的适度信息交换。

在电子政务和各种业务领域中，不同安全级别的网络，涉及的应用信息安全级别不同，网络之间必须进行必要的边界控制或安全隔离，来控制应用数据的非授权交换；另一方面，由于关联网络之间存在业务关系，必须进行必要的应用数据交换，才能保证业务的正常、高效地开展。实现网络之间的安全隔离与信息交换，不管是在我国的电子政务建设中，还是在电子商务或其他行业的应用中，已成为一种关键的边界防护技术要求。

目前国内已有大量的网络隔离产品，但是为网络边界提供可信的应用交换的产品和解决方案还比较欠缺。本平台正是在这样的要求下，采用可信认证技术、安全隔离技术、协议分析和识别技术、访问控制技术、内容过滤和审查技术等最前沿的安全技术和信息处理技术，在安全隔离与信息交换系统上提供一个通用的安全应用交换平台，为可信应用之间提供安全数据交换方式；同时可

根据应用特性，为电子政务、银行、海关等行业提供专业化的安全隔离与数据交换系统。

发明内容

本发明的目的是为了解决在不同安全级别和安全需求的网络间应用数据交换的安全问题。本发明采用可信认证技术、安全隔离技术、协议分析和识别技术、访问控制技术、内容过滤和审查技术等最前沿的安全技术和信息处理技术，提供一个通用的安全交换平台，为可信应用之间提供安全数据交换通道，避免非法数据在网络间传输；同时可根据行业应用特性，提供专业化的安全隔离与数据交换系统和工具。

本平台实现的主要方法包括：

本平台总体上由可信应用认证体系（TACI，Trusted Application Certification Infrastructure）和安全应用交换平台（SAEP，Security Application Exchange Platform）两大部分组成，可信认证体系从各种不同的层面上保障应用交换的安全、可信。

可信应用认证体系提供了三方面的保障：主/客体可信、行为可信和内容可信。应用认证不仅提供用户身份的认证，也提供应用系统的身份识别，防止未授权应用系统的数据在平台间进行交换；内容可信在使用基本的加、解密技术、完整性检查技术的基础上，进一步提供标准协议的专业内容审查工具、各种业务应用内容审查插件；行为可信则主要通过访问控制、访问授权等技术实现。

安全应用交换平台实现各种即时应用信息交换、数据库同步、文件交换功能，为各种数据交换提供跨越不同安全级别网络的安全交换机制。平台采用层次化结构设计，按照功能从下至上依次划分为传输层、应用表示层和应用交换层，传输层重点解决基于标准网络协议的网路隔离和信息交换问题；应用表示

层重点解决对主流标准应用协议和非标准定制协议数据交换的协议表示；而应用交换层则通过透明代理技术，提取出交换双方的应用数据，为业务数据安全交换提供开发接口。

本发明总体实现采用模块化技术，将安全应用交换平台的不同层次与所需的可信认证模块相结合。在实际应用中组合实现多种形态的产品，如可信隔离交换网关型设备、可信应用交换和内容审计工具、可信数据库交换与同步软件、可信邮件网关、可信文件交换与同步网关和行业数据交换网关等。

附图说明

附图 1　可信应用安全交换平台的系统框架图

附图 2　可信应用安全交换平台部署示意图

具体实施方式

可信应用交换平台的主要技术原理是在可信应用认证体系保障下，通过彻底阻断网络间的直接 TCP/IP 连接，并结合不同的安全技术和策略来实现各种应用安全交换的总体目标。

本平台总体上由可信应用认证体系和安全应用交换平台两大部分组成。安全交换平台由传输层，应用表示层和应用交换层组成（如附图 1 所示），分别实现彻底隔断 TCP/IP 协议的信息传输、应用数据的统一表示和传输、各种应用交换软件和开发接口。可信应用认证体系是整个系统的基础，贯穿于系统的传输层、应用表示层和应用交换层，通过 PKI/PMI、数据加密、内容审查、访问控制等技术，提供主、客体可信，内容可信和行为可信三方面的安全保障。

可信应用认证是是整个系统的安全基础，贯穿于系统的传输层、应用表示层和应用交换层，其主要包括主、客体可信，内容可信，行为可信。

1）主、客体可信主要提供安全证书管理、业务应用认证和身份认证功能；业务应用认证通过业务管理功能来实现，它负责对使用交换平台的业务进行注册，发放应用证书，所有应用传输数据必须携带应用证书，方能通过平台进行数据交换。

2）内容可信，实现通用的内容加、解密，内容完整性检查功能，以及内容审计功能。内容审计按照标准协议提供 HTTP、FTP、MAIL 的内容审计，同时还可以根据平台交换的业务应用提供行业数据的专项内容审计模块，如金融行业、公安行业，或为第三方定制的数据内容等；

3）行为可信，则主要实现访问控制功能和授权访问功能。

主、客体可信主要通过身份认证技术（PKI）技术来实现，它不仅能够对服务器和客户端的使用者进行认证，同时还要能够对应用本身的身份进行认证，而不仅仅基于应用的协议进行策略限定，以保证平台交换的应用程序的合法性。内容可信使用加、解密技术，完整性技术保证应用数据交换的可靠性，在此基础上，进一步提供基于标准网络应用协议的内容审计工具，如 Web 网页过滤、邮件过滤等工具，以及针对各种业务应用系统的专项内容审计工具。行为可信则主要通过访问控制技术和访问授权技术（PMI）来实现，保证应用的数据交换行为都是得到允许的。

安全应用交换平台，实现各种数据库同步、文件同步、即时应用信息交换功能，为各种数据交换提供跨越不同安全级别网络的安全交换机制。平台分为三层实现：传输层、应用表示层和应用交换层：

1）传输层实现与数据、应用无关的网络隔离和信息交换网关。在设计上，以隔离为手段，交换为目的，安全保护和防止泄密为基本出发点，能够在“防外保内”的前提下，在不同安全级别的网络之间，保证网络隔离的情况下完成

安全可控的技术信息安全交换。

传输层通过专用隔离硬件、私有交换协议结合安全的加密签名、通用内容检查等模块，实现了在不同安全级别的网络之间完成风险可控的信息交换，不仅彻底阻断了网络间的直接 TCP/IP 连接，而且对信息交换的双方、内容、过程施以严格的身份认证、安全过滤、审计监控等多种安全机制，从而保证了信息交换的安全可控，杜绝了由于操作系统和网络协议自身的弱点和漏洞带来的安全风险，能够有效地防范已知和未知的攻击行为。在此平台基础上可实现病毒扫描、入侵检测、安全审计等多种专业安全检测和防护机制，能最大限度地保护网络免受外部攻击入侵并防止内部重要信息外泄。

传输层功能上具有高度的自身安全性、严谨的安全访问机制、广泛的网络应用支持和强大的应用防护能力。平台采用多处理单元、安全操作系统和专用隔离硬件保证了自身的高安全性；支持 MAC 地址、IP 地址、端口、协议、用户等多种网络对象，支持基于会话的数字证书身份认证并具备详细的日志审计功能；支持 Web 浏览、文件交换、邮件交换、数据库、流媒体等多种网络应用的信息交换；专业防护 IIS 和 Apache 网站服务器、Exchange 和 Domino 邮件服务器、Sql Server 和 Oracle 数据库服务器等应用系统，有效防范 DDoS 拒绝服务、Unicode 恶意编码、Sql Injection 注入攻击等非法行为。

传输层在管理上，可以提供独立的采用基于 GUI 界面的集中式分权管理。通过设置既相互独立又相互制约的超级管理员、策略管理员和安全审计员，有效保证管理的可靠性；管理策略支持脚本语言，能够对系统进行远程集中管理；管理认证方式采用基于 PKI 的身份鉴别和认证技术，支持标准 X.509 数字证书，密钥存储支持磁盘文件和 USB Key，能够有效的保证管理员身份鉴别的可靠性；提供详细的安全审计功能，能够对所有信息交换活动和管理行为进行监控和审

计。

传输层作为网关型设备，即可以单独使用，也可以和应用表示层和应用交换层配合使用，实现真正的可信应用的安全数据交换。

2）应用表示层，整个项目平台中起承上启下的作用。在技术上，表示层通过对应用层数据，进行统一标识和协议封装，通过统一的数据传输通道再交由传输层进行基于标准网络协议的安全信息交换。在实现上，表示层定义了一套应用数据会话表示范式，可以正确的标识数据交换的状态和数据，为业务层可信的应用数据交换提供表示基础。

通过对各种应用协议应用的分析，对于应用的表示，定义了三种基本的应用数据会话表示范式。

第一种基本范式：基于标准请求响应模式的会话范式。在这种范式下，所有的应用会话都是基于一应一答的模式，即客户端（请求发起者）向服务器（响应提供者）发送一次请求，服务器提供一次服务响应，如此反复，提供交互式会话服务。常见的标准网络服务都是基于这种范式工作的，如 Http、Smtp、Pop3、Imap 等。

第二种基本范式：基于层次化的文件目录范式。在这种范式下，所有的应用会话都是基于指定的目录或指定的文件，这些文件或者是格式化的数据，或者是非格式化的数据。在会话过程中，可以指定将网络一端的数据同步传输到对端的指定位置，传输方式可以是单向，也可以是双向。一些标准网络服务采用这种范式，如 Ftp 协议的数据传输通道就是采用这种范式工作的，还有像一些大的行业用户，其网络之间数据的传输也多采用这种方式，如海关系统、电力系统、银行等。

第三种基本范式：基于结构化的数据组织范式，即数据库方式。在这种方

式下，所有的应用会话都是基于数据库的数据交换。在会话过程中，可以指定将网络一段的数据库的指定数据变化实时或定时同步到对端的数据中，传输方式可以是单向，也可以是双向。在一些大的应用系统中，常采用这种范式，如电子政务的内外网数据库、电子商务的内外网数据库等。

基于以上三种范式，提供了对应用业务的表示方式。除此而外，还要解决表示后的数据如何传输的问题，在这里，采用中间件技术，以消息队列为基本的数据传输模型，实现基于统一的传输通道进行可靠传输。中间件是先进技术和技术标准的载体，采用中间件可使平台的先进性、可靠性得到保证。

3）应用交换层，即系统的业务层，是整个平台的业务实现层。在技术上，其通过透明代理和数据挖掘技术，将网络之间所有要交换的应用数据通过数据挖掘，提取出交换双方的应用数据，然后由应用表示层进行统一表示，再利用传输层的统一交换功能实现可信交换。

正是从应用交换层就对数据进行控制，因而可以根据不同的应用协议，实现更加精细的安全访问控制：

针对第一种范式的应用业务，不但可以对请求的指令进行指令控制，还可以对响应的数据进行内容控制。例如，对于最常见的 Http 协议，可以对所有的请求指令进行控制，包括 OPTION、GET、HEAD、POST、PUT、DELETE、TRACE、CONNECT 等，也可以进行 URL 过滤和内容审查，内容审查支持 ActiveX、Java Applet、cookies、Java script、VB Script 和关键字等的检查和过滤。

针对第二种范式的应用业务，不但可以对交换文件的类型和格式进行匹配，还可以对文件的内容进行关键字检查。

针对第三种方式的应用业务，不但可以实现远程数据库的访问，还可以实现同构或异构数据库的同步功能。无论是数据库的访问，还是数据库的同步，

都可以实现基于指令和数据的双重控制。

基于上述三种范式的分析，在可信应用业务数据交换平台上，重点关注业务应用数据的可信问题，而不再关注交换主体和交换过程的可信，这是由核心层和表示层所重点关注的问题。

可信应用安全交换平台基于可信认证体系、完整的私有网络协议，建立安全的应用交换平台。系统为用户提供应用交换客户端，通过配置客户端程序，实现可信应用之间的文件数据交换、数据库数据交换以及其它允许的应用程序之间的实时数据交换，彻底隔绝标准的网络数据传输模式和非法的数据交换。经过平台交换的数据均可以通过内容审查保证数据的有效性和准确性。

本平台的实际应用场景如附图 2 所示，平台由以安全隔离网关和应用软件两部分组成。安全隔离网关部署在网络边界处，是内、外网的唯一出入口。平台管理工具直接部署在安全管理网关上。应用安全交换工具则分别部署在内、外网的应用交换前置机上。

可信应用安全交换平台硬件系统运行于经过安全加固的 Linux 操作系统上，将支持网络协议的核心系统软件采用 C/C++开发，内部通讯使用自主开发的私有网络协议，专用隔离硬件。客户端系统支持 Linux 和 Windows 操作系统。

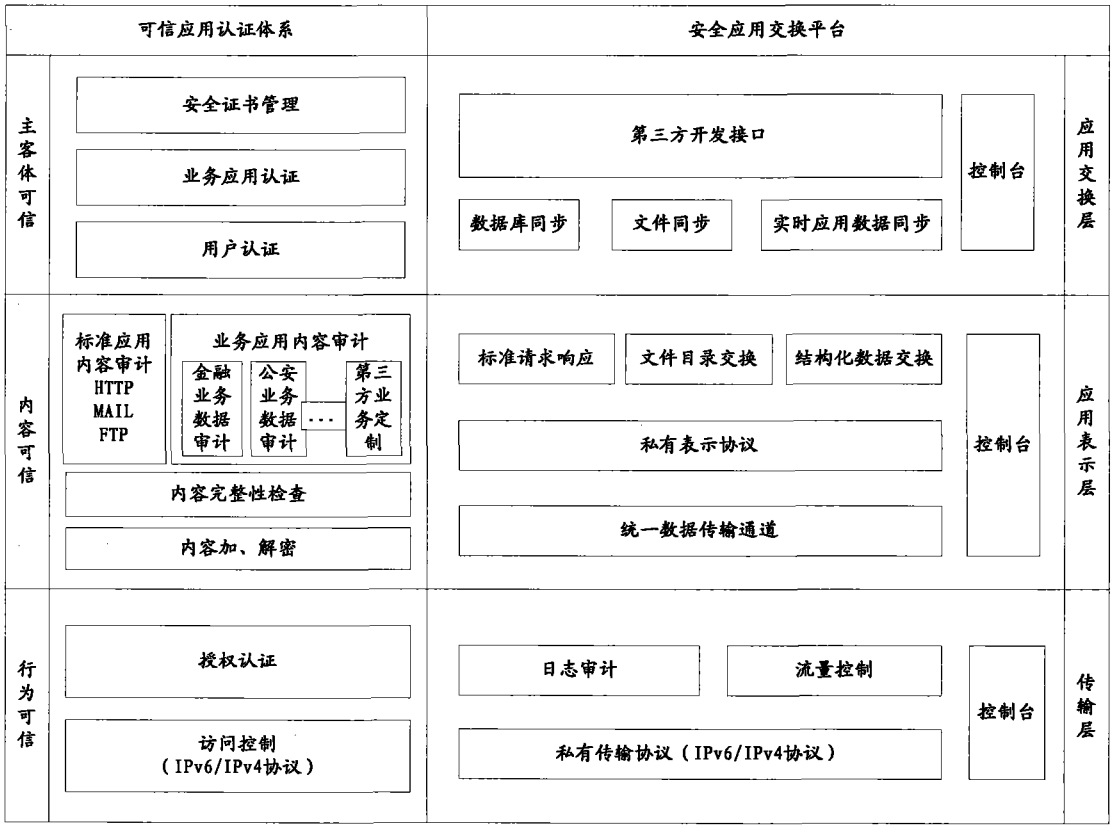
可信应用认证体系
安全应用交换平台
主客体可信
安全证书管理
业务应用认证
用户认证
第三方开发接口
控制台
数据库同步
文件同步
实时应用数据同步
应用交换层
内容可信
标准应用内容审计
HTTP
MAIL
FTP
业务应用内容审计
金融业务数据审计
公安业务数据审计
...
第三方业务定制
内容完整性检查
内容加、解密
标准请求响应
文件目录交换
结构化数据交换
私有表示协议
统一数据传输通道
控制台
应用表示层
行为可信
授权认证
访问控制
（IPv6/IPv4协议）
日志审计
流量控制
私有传输协议（IPv6/IPv4协议）
控制台
传输层

图 1

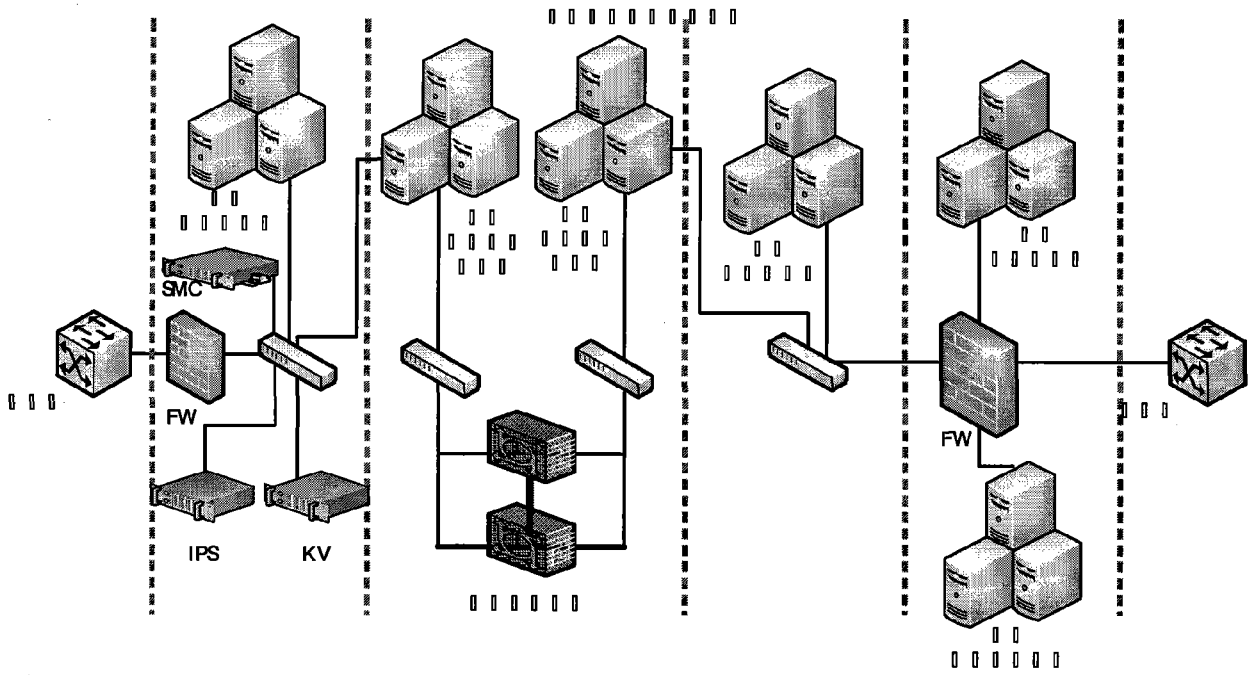

图 2