电子商务 安全 Internet 环境 (18)

计算机科学 2000Vol. 27№. 12

安全电子商务应用环境

Secure Environment for E-business Applications

王 茜 朱庆生 吴中福
(重庆大学计算机学院 重庆 400044)

Abstract E-busnisse has become a hot issue for Internet application, in which security is a key factor. This paper introduces the importance of security to e-busmess, some main techniques of security and their implementation on AS/400.

Keywords E-business, Security, Internet

1 引言

Internet 的发展和广泛普及,使得越来越多的公司、企业和机构在 Internet 上进行商务活动,将传统商务转变为电子商务,包括在网上进行信息发布,交易处理以及实现网上支付。然而,Internet 诞生主要是为了方便资源共享,其协议并无安全方面的考虑,这与当今网络计算所要求的保密性和安全性产生了矛盾。在各种电子商务活动中,安全威胁着参与活动的每一方,可以说安全性是电子商务顺利实施最重要的因素。

Internet 的安全性主要体现在通过 Internet 或 Intranet 进行加密的和可鉴别的通信。与封闭系统主要依靠物理上的安全措施及对资源的良好管理来达到安全要求不同,电子商务不再处于一个封闭、孤立的环境中,不再能单独通过物理的屏障保证安全。分布于世界各地的供应商、消费者、合作伙伴、政府及银行需进行交互,由此带来的一个问题是:如何保护所有保密的数据和交易?

与传统商务不同,在电子商务过程中,你不能面对顾客,确定你正在与谁交谈与交易本身一样重要。在电子商务世界里,需要一种新的方式来保证信任和可靠。伴随 Internet 的使用,物理上的保护已远远不够,任何信息都可能在任何时间被截获。因此,通过加密的方式来保护资源(数据)是主要的手段。

由于服务器遭到攻击引起的损失最大,服务器所受的安全威胁也最大。一旦一个服务器被放到 Internet 上,就立即成为黑客攻击的目标。这种威胁在 Internet 环境下不可能被彻底消除,但可被降低到一个易于管理的级别上,以使商务活动能够顺利进行。

AS/400 具有很高的安全性,满足了进行电子商务的要求,并提供了对系统有效的安全管理。

2 安全系统构建模块

Internet 的安全系统通常建立在如下三个安全构建模块上。

①服务器安全 保护服务器上的数据是保证实施商务处理最重要的方面。服务器安全主要使用认证与授权(访问控制)技术。

②交易安全 对用户处理进行了认证和授权,还需保证交易是合法的。为此,使用防抵赖技术(nonrepudiation)。

③传输安全 一旦用户通过了认证并被授权,接下来的两个安全方面的问题是数据的完整性和保密性。

3 电子商务安全技术

3.1 认证

认证是保证连接另一端的人(或系统)与其声称的一致。在 AS/400 上使用了两个主要的机制以提供基于 Web 的认证:用户号与口令认证、数字证书认证。

使用用户号与口令认证的一个常见例子是由 Web 服务器所使用的 HTTP 基本认证。HTTP 基本认证要求客户端(通常是一个浏览器用户)通过用户号与口令来对一个受保护的服务器标识自己。在该方式下,AS/400 支持两种类型的用户:第一种是具有有效的 AS/400 的用户描述(user profiles)的标准系统用户;第二种是在有效表(validation list)中的用户。第二种用户只能访问授权给 Web 服务器或在 Web 服务器上运行的应用的资源。

另一种认证方法称为数字证书或数字 ID。数字证书依赖于第三方——认证中心(CA)的支持。客户端通过提供其签名的数字证书来证明其身份。当用户与服务器进行连接时,其将证书传给服务器,由其检查证书

并确认证书由一个可信的权威机构颁发。数字证书可用于建立用户的在线身份，并定义其在一定商务处理、小组或团体中的权限。数字证书也允许用户在开放或私有的网络上加密传送信息，由此确保未经授权的用户不能打开数据，并且可检测出任何对数据传输安全的危害。

由于口令在网上未经加密传送容易被破译，用户号与口令认证被认为是弱认证；而数字证书由认证中心鉴发并受数字签名保护，数字 ID 被认为是强认证。

3.2 授权(或访问控制)

授权是赋予用户对一个对象、资源、功能全部或部分的访问权限，基于 Web 的授权通常都与认证紧密相关并由 HTTP 服务器完成。服务器建立管理员希望保护的保护域或保护范围，这些范围在 HTTP 服务器的配置文件中定义。当访问一个受保护的范围时，由 HTTP 基本认证或数字 ID 认证对其进行认证，通过在用户或组文件中查找用户并确定该用户已注册，才可对其授权，允许用户进行访问。

AS/400 使用保护域，并使用操作系统中的授权机制。未被授权的用户以及被确认为是"Internet 用户"的用户只能以一个缺省的用户身份或在 Web 服务器配置文件中指定的 ID 身份进行操作。真正的 AS/400 用户(通过基本的或数字 ID 认证)，在其自己的用户 ID 下运行。来自客户端的认证信息(用户号与口令或数字 ID)被映射成一个有效的 AS/400 用户描述，AS/400 可在对象级上提供细粒度的授权。

在服务器外部，防火墙被用来提供访问控制。

3.3 防抵赖

防抵赖是为了防止发送方在事后否认曾发送过数据，其可由数字签名来实现(数字签名是数字证书的一部分)，数字签名使用私钥加密，公钥解密。防抵赖还使用数字邮戳等其它信息。

3.4 数据完整性

数据完整性是指到达接收端的信息与发送出的信息一致，并能检测出信息的改变。数据完整性的实现，是通过对原始信息执行哈希算法产生一信息摘要，将其加密后与原始信息一起发送，接收端执行相同的哈希算法产生摘要，并与接收到解密后的摘要进行比较，以确定收到的信息是否与发出的信息一致。AS/400 具有该功能。

3.5 数据保密性

数据保密性是防止系统间数据交换时被截取而造成信息泄露，加密技术用于实现数据保密。AS/400 采用不同技术，使用多种加密算法。加密可以在几个不同级别上实现：应用加密、应用 API 加密、网络加密。

3.5.1 *应用加密* 在 AS/400 上，一个应用可使用特定的加密服务，例如公共加密服务 CCA。通过使用这些服务，实现由应用控制的加密。多数金融和银行应用需要控制加密，并使用这些接口。另一个应用加密的例子是电子邮件，AS/400 上的加密邮件是由 Domino 的 S/MIME 支持的，S/MIME 使用 RSA 公钥加密技术实现电子邮件的加密传输。

3.5.2 *应用 API 加密* 一些应用并不想控制加密，但仍希望其发送和接收的数据被加密保护。在 AS/400 上，主要的服务器(如 HTTP、Telnet、OPVav、Management Central、LDAP、Java Servers、Client Access、DDM and DRDA)支持 SSL 协议。应用接口使用 SSL 来实现对应用数据加密。

AS/400 支持软件加密服务和硬件加密服务。软件加密服务使用由 RSA 公司开发的 BSAFE 工具集，在 AS/400 上，加密服务由 SSL 和虚拟专用网 VPN (Virtual Private Network)使用，硬件加密服务基于 IBM4758—001 卡，4758 卡插入 AS/400 系统作为一个输入/输出适配器 IOA(Input/Output Adapter)，并作为一个协处理器运行，传送到卡上的数据被加密，然后被返回至应用。

3.5.3 *网络加密* Internet 的使用和增长是无限的，除客户访问外，为了便于对商务应用和数据的访问，许多公司也通过 Internet 实现全球访问。现在，通过 VPN，公司可安全、经济地延伸其应用和数据至世界各地。

VPN 是网络安全的一个副产品。今天，网络安全主要由防火墙来实现，防火墙在内部网络与 Internet 之间建立起一个软件屏障，许多防火墙产品通过包过滤来实现安全保护，VPN 则将过滤和加密技术进行延伸。第一个阶段的加密只对发往 Internet 的每个 IP 包的数据信息进行加密，而源和目的的地址则未加密，网络安全的第二阶段则集中于 VPN 服务，VPN 的特点是具有封装(或隧道)整个 IP 包的能力，包括从源站到目的主机的地址信息。

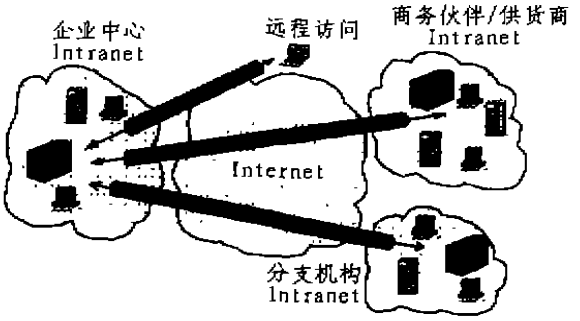

图 1 VPN 方案

VPN 是一个企业私有的 Intranet 通过一个公共

网络(如 Internet)进行的扩展，其通过一个私有隧道建立了一个安全的私有连接。VPN 在 Internet 上将远程用户、分支机构、商业伙伴连接在一个扩展的网络中，并在其上安全地传送信息。

由于 VPN 在网络端到端提供加密，能阻止网络内部和外部黑客攻击，因此比防火墙或网关加密具有更高的安全性。AS/400 分别在其 TCP/IP 协议及防火墙中提供 VPN 功能。

3.6 防火墙

对 Internet 的访问变得越来越重要，Internet 提供了大量的信息资源，放弃这些资源将使公司处于不利地位；而通过 Internet 交换电子邮件也成为必需。问题是如何保护内部网络？一旦建立了一条能使公司员工访问 Internet 的连接，也就同时建立了一条外部人员进入内部网络的通道。防火墙提供了保护内部网络不受来自未授权的 Internet 访问的手段，内部网络与 Internet 之间的所有通信均通过防火墙。

防火墙被用于实现网络互联的安全策略。通过访问控制，其提供了一个在安全的内部网络与不可信赖网络(如 Internet)之间的屏障。AS/400 防火墙提供了许多可用来保护内部网络的技术，包括：①IP 包过滤；②代理服务器；③SOCKS 服务器；④域名服务(DNS)；⑤网络地址转换(NAT)服务；⑥虚拟专用网(VPN)服务；⑦记录；⑧实时监控。

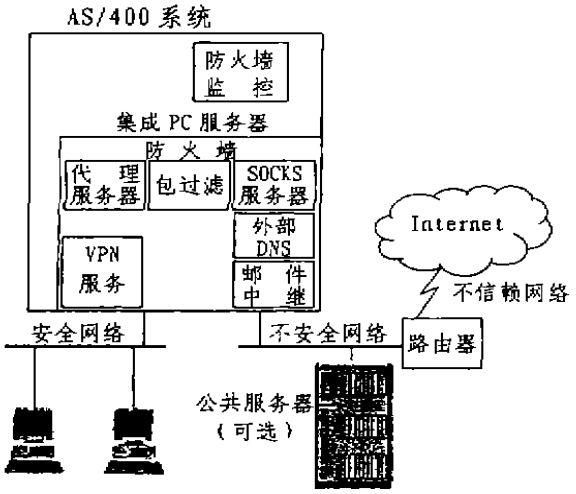

图 2 AS/400 防火墙实现

AS/400 防火墙巩固安全管理以强化安全策略，防止外部人员通过 Internet 访问内部网络信息，从而提供保密性；通过记录与 Internet 之间的通信量，以监控网络使用。AS/400 防火墙配置很灵活，可支持多种安全策略，图 2 是 AS/400 防火墙通常的实现形式。

3.7 安全审计

有时判断安全机制是否起作用与安全机制能做什么一样重要。AS/400 提供了很宽范围的审计以完成该任务。正如提供安全功能一样，审计也是集成在操作系统中的，当系统运行在安全级别 40 或 50 上时，要绕过审计是极其困难的。

AS/400 的审计能力相当全面，可以审计整个系统的安全行为，也可审计一个特定用户的安全行为；可审计系统范围的对某一对象的访问，也可审计一指定用户对一特定对象的访问。AS/400 的审记还是一个方便的 debugging 工具。

除审计工具之外，AS/400 还提供了一组工具来帮助管理用户和组，以及它们对系统中的对象所具有的权限。

结束语 电子商务意味着信息技术、销售、市场、制造、金融和业务运作等各方面之间史无前例的协作，甚至是集中；它还意味着同供应商、业务伙伴和客户一起共享重要数据。随着壁垒的消失，安全性成为电子商务领域中越来越关键的部分。AS/400 提供的多种安全机制，使电子商务能在一个安全的环境运作，也使 AS/400 在电子商务应用中显示出具有优良的性能。AS/400 的安全性来自于：第一，AS/400 安全机制不是附加的一个软件包，而是集成在整个系统中——从硬件到操作系统的每个部件；第二，AS/400 提供了许多工具来控制和监测系统安全；第三，在增加新功能(如 TCP/IP)时，首先分析其对系统安全性的影响，在安全性得到保证后再将其加入到系统。

参 考 文 献

1 AS/400 Security Advisor. Available at: http: // www. AS400. ibm com/tstudio/securel/secdex. htm

2 AS/400 Firewall. Available. at: http: // www. AS400. ibm. com/firewall

3 AS/400 Redbooks

4 AS/400 TCP/IP V4 Internet Access

5 Mark McKelvey. Secure Internet Applications on the AS/400 system, 1999

6 Bill Rapp , Brad Brech. Creating Web Applications, 1999