

企业电子商务系统的安全性分析

曾 孜

(广东工业大学 计算机学院, 广东 广州 510090)

摘要: 在企业电子商务的概念、特点和功能的基础上, 分析了企业电子商务的安全性问题, 并就网络访问、系统、交易过程及数据传输的安全性等几个关键问题作了研究与探讨。

关键词: 电子商务; 互联网; 安全性

中图分类号: TP399

文献标识码: A

文章编号: 1007-7162(2001)03-0022-04

随着 Internet 的普及和万维网(www)的兴起, 电子商务(e-business)应运而生。所谓电子商务是指商品在采购、生产、仓储、销售、运输的过程中, 利用计算机网络与电子技术, 促使交易的顺畅与高效。对于商家而言, 电子商务展现的是更多的商机、效率的提高、成本的下降以及顾客满意程度的增加; 对个人而言, 可以通过电子商务方便快捷地获得所需商品信息, 原有的地域界限将不复存在, 人们购物的模式将彻底改变; 而对企业而言, 电子商务有助于降低企业的成本, 提高企业的竞争力, 尤其能使中、小型企业以更低的成本进入国际市场参与竞争。作为一种商务活动过程, 电子商务将带来一场史无前例的革命。而其影响将远远超出商务本身, 它将会对社会的生产和管理、人们的生活和就业、政府职能、法律制度以及教育文化带来巨大的影响。电子商务在全球刚刚起步, 在中国由于环境还不成熟, 电子商务仍起步艰难, 但却普遍相信将是必然的趋势, 也是企业在激烈的市场竞争中寻求生存和发展的必然选择。

网络正逐步改变着人们的生活方式和工作方式, 网络的开放性、互连性、共享性给人们带来巨大利益的同时, 也带来了严重的安全隐患。同样, 电子商务将使每个人越来越依靠我们的“用户名”和“密码”, 我们的数码身份一旦被盗后果不堪设想, 因此企业在建造自己的电子商务系统时, 系统的安全性是首要考虑的问题之一。电子商务系统架构在 Internet 之上, 而 Internet 与世界各地数以百万计的计算机相连, 如何使用 Internet 的快速与便捷, 又能保障商务活动的安全, 保守自身的商业机密是系统最重要的技术问题。

1 企业电子商务的主要功能

1.1 电子信息发布

利用 Internet 的 Web 技术, 企业可以在自己的网页上刊登广告, 开展多种宣传, 把信息发布到企业以外, 传给供应商、批发商、客户、投资者和其它合作伙伴。

1.2 销售管理

Internet 商务的销售是商务活动的核心内容。企业的所有分支机构、销售网点通过 Internet

收稿日期: 2000 12-18

作者简介: 曾孜(1967), 女, 工程师, 主要研究方向为计算机网络与数据库技术。

相连. 通过网络, 分布于各地的部门可把每天的经营情况及时、准确地传送到总分司, 实现企业内部数据汇总的自动化, 企业领导可以把有关指示和工作安排迅速下放到各部门. 各分公司也可以随时查询总分司的相应数据库, 提高信息处理效率.

1.3 企业外部通信与合作

企业与原材料供应商、生产制造商、批发商、零售商以及消费者之间的信息传递频繁, 企业电子商务为这一系统的管理提供了及时、准确的服务.

1.4 电子购物

电子商务能让客户自己帮助自己获得购买前后所需的信息, 并通过访问企业的主页, 输入自己的购买意向, 通过 Internet 电子货币结算业务, 企业和客户之间可立即实行电子贸易结算, 实现在线消费.

2 安全性是企业电子商务建设的首要问题

企业电子商务建设方案主要的技术问题来自于网络的安全性. 首先, 企业站点涉及企业的形象, 必须保证安全, 防止黑客的攻击和篡改; 其次, 企业内部包含有大量的商业机密, 必须严加保护, 防止来自于 Internet 上的攻击; 第三, 企业内部各部门需要有严格的权限控制, 防止未经授权的用户访问到机密信息; 第四, 确保交易过程的高度隐密, 确认交易双方的身份, 同时, 保证网络中传输的数据不被人监听, 或者即使被人监听也可以保证传输的数据不会被人解密而泄密.

3 企业电子商务的安全层次结构

企业电子商务的安全性层次结构如图 1 所示.

3.1 网络的安全性

网络访问安全性的核心是网络是否得到控制, 即是不是任何一个 IP 地址来源的用户都能进入一个网络. 它主要依赖于网点的系统平台、WEB 服务器软件以及应用系统对操作用户的管理. 用于解决网络访问安全性问题的产品主要有防火墙和 VPN(虚拟专用网). 防火墙的主要目的在于判断来源 IP, 将危害或未经授权的 IP 数据拒之于系统之外, 只让安全的 IP 数据通过^[1]. 企业电子商务防火墙应采用被屏蔽主机体系结构, 这种双层式的防火墙体系由一个堡垒主机和分组过滤路由器组成, 它可以屏蔽内部服务器的网址与名字, 把 WWW、Email、FTP、日志系统、加密系统、身份认证系统放在堡垒主机中, 堡垒主机位于外部网和内部网之间, 以防止公司内部数据外泄^[2].

数据传输	加 密			
交易过程	安全电子交易标准		鉴权	
网络访问	防火墙	系统安全	用户管理	备份

图 1 安全性层次结构图

VPN 是客户端 PC 用特殊软件通过专用设备或服务器上的特殊软件连接到企业内部网或 Internet. VPN 的实质是在不安全的 Internet 环境中建立一条可以信赖的安全连接. 加密、密钥管理、认证、访问控制是保证安全 VPN 的四大要素. Ipsec 协议集是维系这些要素的纽带. 它是基于网络层的安全协议, 灵活地将这四个要素结合在一起, 在 Internet 环境下提供一个安全的网络. VPN 主要解决数据传输的安全问题. 如果企业在地域上跨度较大, 使用专网、专线过于昂贵, 则可以考虑使用 VPN, 其主要目的在于保证公司内部的关键数据能安全地借助公共网络进行频繁的交流.

3.2 系统安全性

在系统的安全性问题中, 主要考虑的问题有两个: 一是病毒对于系统的威胁; 二是黑客对系统的侵入和破坏.

病毒的传播途径已由过去的软、光盘等存储介质变成了网络. 电子邮件、文件传输以及网络页面中的 ASP、Java 插件件和 Active X 控件等都能携带病毒. 因此, 网络防病毒工具必须能够针对网络中可能的病毒入口进行防护.

对于黑客而言, 他们的主要目的在于窃取数据和非法修改系统. 其手段之一是窃取合法用户的口令, 在合法身份的掩护下进行非法操作; 其手段之二是利用网络操作系统的某些合法但不为系统员和合法用户所知的操作指令. 例如, 在 UNIX 系统的缺省安装过程中, 会自动安装大量系统指令. 据统计, 其中大约有 300 个指令是大多数合法用户根本不会使用的, 但这些指令往往被黑客所利用. 要弥补这些漏洞, 我们需要专门的系统风险评估工具, 帮助系统管理员找出哪些指令是不应该安装的, 哪些用户是应该缩小用户使用权限的, 以保障系统的安全性. 对重要的文件和数据可定期进行备份, 备份的方式可采取全盘备份和增量备份两种. 另外, 系统备份用来在遭受攻击之后恢复系统. 也可以用在网络主机的安全检查方面. 例如, 定期检查现存的文件系统和备份系统的差异, 判断系统是否被篡改, 以便及时恢复.

3.3 交易过程的安全性

电子商务的国际安全标准已建立, 安全超文本传输协议(S-HTTP)、安全套接层协议(SSL)、安全交易技术协议(STT)和安全电子交易协议(SET)等一系列电子交易协议提供了安全的方式来建立与用户的加密通信连接. 在网上交易过程中, 可以使用客户证书确认电子商务各方的身份以保证交易的合法性. 利用 Certificate Server 进行证书管理, 利用 Active X 服务器组件技术, 对访问用户进行管理, 在 Web 页面上进行访问授权, 利用现有的几种用户目录协议(DAP)实施用户控制. 对用户进行分组管理, 并且这种分组管理是针对安全性问题而考虑的分组. 根据不同的安全级别将用户分成若干等级. 每一等级的用户只能访问到与其等级相对应的系统资源和数据.

3.4 数据传输的安全性

在数据传输的过程中, 机密的数据即使处于安全的空间也应对其进行加密处理, 以确保失窃时, 偷窃者也读不懂其中的数据内容. 它可以通过加密/解密技术来保证, 这一技术保障体系包括密码技术(公用密钥 Public key、私用密钥 Private key 和数字摘要 digital digest)、数字签名 digital signature、数字时间戳 digital time-stamp、数字凭证 digital Certificate 和认证中心 Certification Authority. 密码技术是将数据变成不可读的形式, 防止数据在传输过程中被篡改、删除、替换、重发等. 同时, 采用数字签名技术防止通信双方的任一方对自己行为的否认. 数字签名技术是建立在公开密钥加密体制的基础上. 它保持了常规书写签名的本质特点, 利用一种单向函数对信息产生摘要, 发送方用私钥 SK 和摘要进行 DSA 算法计算, 产生数字签名. 数字签名的功能是能够保证数据的完整性和不可抵赖性. 如果数据在传送过程中被修改过或者根本就是伪造的, 则无法通过接受方的数字签名验证. 发送方无法抵赖他曾发送过的信息, 因为别人无法伪造他的数字签名, 除非他的私人密钥被窃取. 数字证书是建立网络信任关系的关键. 数字证书将用户基本信息与用户公钥有机的绑定在一起, 绑定功能通过发布证书的权威机构的数字签名来完成. 用户之间通过交换数字证书来建立信任关系. 由一个可靠的 CA 机构来发放数字证书. CA 在派发公钥时, 将为每个公钥产生一个证书, 并附上数字签名以证明用户的身份.

4 结束语

电子商务是一种全新的经营方式,有着远大的发展前景,发展电子商务是跨世纪的战略选择,是企业竞争力的来源.电子商务的实施和发展是一项系统工程,不仅仅包含技术问题,同时还必须解决许多法规、制度问题.例如:电子商务法律的制定、财务政策、风险对策、税收问题、保险问题、管理制度、知识产权和网络基础设施建设.同样,对于电子商务中的安全问题,除了技术上的保障以外,还需要有相应的法律来约束交易双方的行为和保证交易双方的权利.尽管如此,我们必须明确一个实事,那就是:没有绝对的安全,只有使它更安全的管理办法.但这并不能阻碍电子商务的发展,随着中国 Internet 用户的不断增加,电子商务安全性、保密性、可靠性、可测性技术的不断成熟,法律制度的日益完善,相信 21 世纪将是中国电子商务的快速增长期,电子商务将把人类带入一个信息化的新时代.

参考文献:

- [1] Andrews, Tanenbaum. Computer networks[M]. 北京: 清华大学出版社, 1999. 447- 480.
- [2] 沈华峰. 实用型企业电子商务系统 I—solution 的设计和实现[J]. 计算机工程, 1999, 25(9) : 90- 92.

Security Analysis on Electronic Business System

ZENG Zi

(Faculty of Computer, GDUT, Guangzhou, 510090, China)

Abstract: Based on the concepts and features of electronic business, this paper analyses the security of electronic business, discusses several key questions.

Key words: electronic business; Internet; security