电子商务安全解决方案

文 王凌云

电子商务对网络安全的挑战

随着网络技术不断成熟，电子商务正作为一种高效率的商务运做方式向传统的商务发起着冲击。然而，由于网络信息安全传输、资源访问控制和网上身份鉴定等安全技术的缺乏，电子商务中在线支付、重要单据和数据的传输以及身份鉴定等重要的电子商务操作程序都无以保证其安全可靠性。所以，网络信息安全问题已成为电子商务发展的瓶颈，广大电子商务企业迫切需要完善的电子商务安全解决方案。

关于电子商务安全，我们必须从两方面来考虑——消费者与企业。

消费者的个人资料必须保密，还必须确认与之交易的实体不是冒牌货。要赢得消费者的信赖，安全解决方案必须确保消费者的个人资料严格保密，无论是在存贮、发送和使用时。此外，安全解决方案还必须保证与消费者进行交易的完整性。

对于企业方面，主要存在两个问题。第一，确认用户的身份，界定用户的权限，确保用户只能执行权限内的行为；第二，保护企业资产免受恶意攻击，如病毒、拒绝服务攻击，以及资料被盗窃和损坏。

安全检查清单

传统的安全检查清单还继续是机构内保护企业资源的有效安全基础，伴随着电子商务时代的来临，还应在其上添加其它措施，包括可视化、智能化、连续操作、细化拒绝和许可优先权。因而清单应包括以下组件:

◆明确的政策和步骤——保护资产需要程序性的和技术性的对抗措施，需保护的资产范围明确，在机构内有所有权

◆系统访问控制——根据公司政策在机构的服务器和应用软件上实施有效用户认证和资源授权

◆可审计性——受保护的审计可以跟踪用户的操作，有跨服务器和应用软件的全貌视图

◆管理功能的分离——预防对敏感数据的非授权访问

◆网络误用检测——监视和自动阻止违反安全政策的电子邮件、web及其它网络访问

◆网络保护——检测／防止网络入侵和拒绝服务

◆安全远程访问——强大的认证功能允许有预定访问权限和控制权的授权用户从外部访问网络

◆防止有害内容侵入——检测／防止病毒和有毒的ActiveX控件或Java小应用程序进入

◆数据单元保护——为信件和官方业务文档提供完整性、保密性和无拒绝服务

◆预防网络安全威胁——使用加密技术，避免口令、数据和流量以清晰文本的形式，通过网络在移动用户和办公室和／或办公室之间和／或内部交流

◆脆弱性评估——经常确保系统可以防止已知因素的袭击，并与机构定义的基本安全水平准则相一致

◆合并管理——对用户帐户、权限和资源进行单点管理

◆安全事件管理——监视、警告和自动响应来自系统、内部网或外部网的潜在入侵／违规问题

◆安全性报告——说明哪些人可以访问什么内容、哪些内容可由什么人访问、安全政策违规情况、趋势等

◆应用体系结构——将涉及许多内部开发小组，在用一致方法构筑电子商务应用软件方面好处颇多。能保证用一致的方法满足通用要求（如web规模安全基础设施，包括目录、PKI、授权、审计服务等）

◆审计——根据业务或资产变化、攻击和误用形式、新的脆弱性和利用情况等定期评估安全政策

电子商务安全解决方案

eTrust是一套完整的电子商务安全解决方案，它提供包括风险资产、攻击检测、避免损失在内的完善的安全解决方案，并且拥有强大的关键组件管理功能，而这是成功的电子商务所必须的。

eTrust所包括的一整套工具可独立使用，也可与Unicenter TNG一起使用。eTrust的基础是一套通用服务，这些服务支持客户的企业应用软件，能实现与第三方工具和物理安全性的互操作。eTrust技术可作为独立产品，也可作为集成安全套件或特定解决方案的一部分。

已经发布的CA eTrust解决方案如下:

eTrust Access Control

分布式企业网（OS/390、UNIX、NT）上基于政策的授权和访问控制。

eTrust Admin

混合企业系统（OS/390、UNIX、NT、email、RDBMS、ERP、Directories）上基于政策的用户和资源管理。

eTrust Anti-virus

企业网上完整的病毒保护，从Internet网关到本地桌面，带集中政策管理。

eTrust Audit

整个安全套件的集中企业网审计。

eTrust Active Content Inspection

基于政策的智能保护，对抗的对象是网关和桌面的Java和ActiveX敌意码。

eTrust Certificate

为银行间的信用授权电子信件提供在线认证支持协议（OCSP）。

eTrust Desktop Security

智能防护恶意代码，包括Java与ActiveX。

eTrust Directory

针对企业骨干网结构的X500标准兼容型容错目录服务器。

eTrust Encryption

简化的端到端安全通信。

eTrust Firewall

快速、高效、便于管理地确保网络在采用现代技术时免受低级协议攻击，管理多重管道，与eTrust入侵检测一道，禁止滥用。

eTrust Intrusion Protection

智能实时网络入侵检测和预防，带主动损害预定保护。

eTrust PKI

基于策略安全的公用关键基础结构。

eTrust Policy Compliance

企业范围内安全政策评估，包括自动纠正措施。

eTrust Single Sign-on

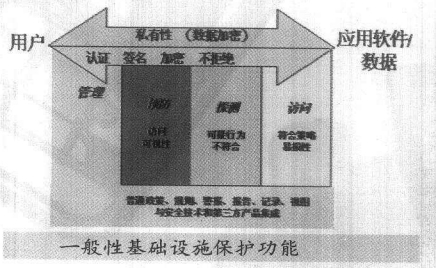
一次登录到分布式企业网上的应用软件、数据库和系统，包括Web登录。

eTrust VPN

能够授权与鉴定的可信的虚拟个人网络。可使个人通过Internet、外部网或内部网进行通讯，并可确保未经授权的人无法访问或窃取他们的通讯内容。

eTrust的保护模型

CA定义了安全模型以便帮助确定保护电子商务基础设施所需的全套功能。该模型如下图所示。



一般性基础设施保护功能

该过程的一个目标是通过向用户授予应用软件和资源的访问权使之能简单、安全地进行访问（对于最普通的电子商务处理），另一个目标是确定支持此过程的以下基础设施保护功能:

①对用户、权限和资源访问控制的管理;

②主动、实时地防止违犯政策、入侵、恶意内容、黑客袭击、用户的非授权意外／恶意访问等发生;

③实时检测入侵和可疑行为;

④定期评估与政策的符合程度。

应用需求与方案组合

下面列举一些典型需求和相应的eTrust解决方案:

●防止恶意内容

问题：防止可从web下载或从电子邮件进入的病毒、ActiveX控制、Java小应用程序。

解决方案：eTrust Anti-Virus + eTrust Active Content Inspection(网络／台式机)。

●防止网络入侵

问题：防止外部黑客或拒绝服务袭击

解决方案：eTrust Firewall + eTrust Intrusion Protection + eTrust Firewall/web/邮件访问控制 + eTrust保护分析服务。

●用户控制

问题：多个用户帐户和随之而来的口令管理、管理成本。

解决方案：eTrust Admin + eTrust Single Sign-on。

●台式机安全

问题：影响台式机上用户／业务数据的完整性。

解决方案：eTrust Active Content Inspection(台式机) + eTrust Anti-Virus(台式机)。

●内部网服务器／应用软件保护

问题：为内部／网络用户保护防火墙后的资源。

解决方案：eTrust Access Control + eTrust Policy Compliance + eTrust Audit + eTrust Single Sign-on + eTrust PKI。

●电子商务应用软件安全基础设施

问题：为新应用软件提供一致的安全基础设施。

解决方案：eTrust Directory + eTrust Access Control + eTrust Audit + eTrust PKI。

整体方案综合应用

通过eTrust Directory为电子交易双方提供与X.500标准相容的目录服务，并为目录资料库引擎提供高扩充、高容错性的企业讯息骨干架构，提供LDAP界面并可与其他目录服务整合。同时，有授权与鉴定功能的虚拟个人网络——eTrust VPN不仅可使用户通过Internet、外部网或内部网进行安全的通讯，还提供对多种标准加密算法的支持，可构造网络数据传输的低层安全保护。另外，eTrust PKI提供的公开的密钥构架解决方案将使企业在电子商务中信息传输更为安全。而eTrust Certificate为银行间的信用授权电子信件提供的在线认证支持协议（OCSP）也正是众多企业解决电子商务在线支付问题的必需。再配以可定义系统资源权限的eTrust Access Control和可为企业完全提供系统安全状况报告的eTrust Audit，eTrust电子商务企业解决方案可使企业用户在授权后，安全方便地使用企业电子商务应用系统和资料，从而保障电子商务各个环节的实现。（方案提供：CA公司）

本版责任编辑 王凌云
本版美术编辑 纬 圆