计算机安全加密技术应用研究

何玉芳
（浙江省诸暨市职教中心，浙江诸暨 311800）

摘 要：本文就计算机信息数据整体安全重要性展开探讨，并制定了加密技术实践应用策略。对提升计算机系统可靠安全性能水平，确保信息数据真实、全面、准确，优化加密技术应用效果，有重要的实践意义。

关键词：计算机；安全加密；应用
中图分类号：TP309 文献标识码：A 文章编号：1003-9767（2013）01-0004-02

1. 计算机系统数据信息安全重要性

计算机系统具有强大的处理、存储数据信息功能，计算机用户则会将较多重要资料保存至计算机之中，通过网络平台实现优质数据共享与高效信息传输。先进的计算机网络技术大大提升了各行业工作效率，令人们实现了跨时空地域的交流。然而计算机系统在处理存储数据信息过程中，则面临着较多威胁入侵影响。例如病毒入侵、黑客程序、网络邮件炸弹、利用漏洞实现远程监督操控等。严重时会造成重要信息的丢失，系统的中断、崩溃以及网络瘫痪。为此做好计算机系统数据信息的安全性保护尤为重要，我们可通过应用安全加密技术确保信息数据不容易遭到破解，提升价值化资料信息的完整性以及安全传输应用水平，进而营造良好、有序、健康的计算机应用服务环境。

2. 计算机系统数据安全加密方式

计算机系统安全加密应用方式包括对称加密以及非对称加密两类。前者方式在加密与解密过程中应用相同密钥，因而令具体加密应用算法相对较为简便，应用密钥简短，同时破译起来具有一定难度。该加密技术需要通信双方保证交换过程中不存在泄露现象，倘若密钥被其他人以非法方式获取，则会令数据失去加密效果。其中DES 便为典型的加密应用算法实例，可对二元数据安全加密，通过划分信息为六十四位，应用长度为五十六位密钥，剩下八位则进行奇偶的校验。该加密应用方式令各个分组应用复杂变位替换以及组合，而后实施异或计算，进而形成加密数据。该加密阶段中各个分组需要经过十九步的处理，各个步骤输出为后步骤的输入。首步针对六十四位数据以及密钥实施变位，到了第二步开始直至十七步在应用不同密钥基础上，各个步骤运算均同样，且涵盖较多操作，在第十八步中则令前后三十二位做变换，最终则进行首部逆向过程变位。该应用方式解密阶段同加密过程大致一致，只是密钥的具体顺序恰恰相反。另一类加密应用方式为非对称法，其应用加密以及解密密钥互不相同，通常为两个，即公钥与私钥，两者应配对应用，不然将无法将加密信息文件打开。应用该加密技术实施通信阶段中，加密算法自身可公开，同时密钥也可公开。而用于解密的密钥则由数据接收方进行保管，进而可提升安全保密性。各个用户均存储公开与私密的一对密钥，该密钥虽成对出现，然而我们无法依据公钥将私钥计算出来。实施密钥管理阶段中，应确保一个对话的密钥应用在一条信息或对话之中，还可构建一类定时变化的密钥应用模式，进而降低密钥被窃取与暴露的不安全因素。为优化多密钥的综合管理效果，我们可创建安全密钥的相关分发中心，这样各个用户只需知晓一个与中心展开会话的对应密钥便可。

3. 计算机安全加密技术应用

3.1 电子商务领域 SSL3.0 技术应用

随着网络交易的兴起，电子商务迅速崛起，计算机安全加密技术在电子商务领域的应用近年来快速发展，其可满足客户借助网络系统从事多种商务活动的需求。长久以来，一些用户为预防信用卡信息帐号被盗造成财务损失，通常利用电话订货进行商务活动。伴随计算机安全加密技术的逐步应用，人们认识到了应用 RSA 技术进行加密的优势，可有效提升应用信用卡从事交易阶段中的可靠安全性，确保电子商务各类交易活动的顺畅有序，为人们经济活动提供了便利。SSL3.0 技术的应用通过电子证书进行身份确认，而后双方可在安全的环境下进行会话。而各类客户同电子商务相关服务器实施沟通的阶段中会形成 Session Key，客户则可利用公钥对其实施加密，并传输至服务器一端，当双方均明确了密钥后，各类传输信息数据均以该密钥做加密与解密处理，而服务器一端发送至用户的各个公钥则应首先面向相关发证方进行申请，方能实现公证。就该加密应用技术的安全优质保障作用，广大用户便可从事自由的电子商务活动，订购自己心仪的商品并利用信用卡进行付款。还可借助网络平台同合作方进行各类商业信息的传递交流，可令供应方将订单以及收货的凭证通过网络进行发送，极大的为电子商务活动的开展提供了便利，足以见得安全加密技术的应用价值。

3.2 虚拟专用网应用

计算机安全加密技术在虚拟专用网络中也得到了越来越广泛的应用。伴随市场经济的持续发展，较多公司逐步迈向国际化，一些大型集团在较多区域国家均设立了办事处与销售分公司，并架设了局域网络系统。然而其设置却往往形成总公司控制管理层面的一定障碍，令管理控制效率较低，还有可能引发公司的不良经济损失。为此，企业集团优质经营管理需要利用 LAN 构建连接形成广域网络，进而实现高效的统一管理，便于集团总公司查阅汇总信息，进而创建优质的发展经营策略。当前一些企业逐步应用专用虚拟网络解决这一问题，在数据传送阶段中，位于用户端先连入互联网络路由器实施硬盘安全加密，通过加密方式实现传送。在抵达目标路由器，则由其负责对数据做解密处理，进而广域网中的用户便可应用查阅该类安全信息。通过利用安全加密技术，可令广域网系统用户更便捷、安全的查询、传递、交流信息，提升工作效率，进而创设显著效益。

3.3 数字签名加密技术应用

由于公开密钥加密算法操作起来相对复杂，加密与解密过程的实践速度有限，因而对于大量文件信息的传输并不适用。在处理该类计

计算机网络信息安全与信息管理

陈瑞平
（广东省国土资源技术中心，广东广州 510075）

摘 要：本文结合作者多年信息化的工作经验，重点讨论了如何在数据及业务信息化的过程中，保证其安全性。文中先是陈述了影响信息安全的各种因素，接着基于这些因素提出了增强信息安全的各种技术及策略。

关键词：信息安全；网络安全
中图分类号：TP309 文献标识码：A 文章编号：1003-9767（2013）01-0005-02

1. 引言

随着信息化进程的深入和互联网的快速发展，人们越来越习惯把日益繁多的事情托付给计算机来完成。网络化已经成为单位企业信息化的发展大趋势，信息资源也得到最大程度的共享。但是，紧随信息化及互联网发展而来的网络安全问题日益突出，已成为影响信息化进一步发展的重大问题。目前，危害计算机信息安全的事件频繁发生，对很多人造成了损失。如何保护数据不受破坏修改泄露，维持各种业务系统连续可靠的运行，已经成为全世界很多专家学者的研究课题。

2. 信息安全简介

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

在公司单位具体的事务中，信息安全主要是指要保证业务系统能够稳定持续的运行，以及各种业务数据的保密性、真实性、完整性和防止未授权拷贝。

3. 详细说明

3.1 信息安全的目标

真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

完整性：保证数据的一致性，防止数据被非法用户篡改。

可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

可控制性：对信息的传播及内容具有控制能力。

可审查性：对出现的网络安全问题提供调查的依据和手段

3.2 信息安全主要措施

信息安全的威胁来自方方面面，不可一一罗列。但这些威胁根据其性质常被归纳为信息泄露、破坏信息的完整性、拒绝服务、非法使用（非授权访问）、窃听、业务流分析、假冒、旁路控制、授权侵犯、抵赖、病毒以及法律法规等几个方面，下面将结合工作实际简要讲述一下预防这些风险的技术手段：

3.2.1 保障机房的物理安全与电气安全。

服务器或计算机是系统运行和数据存储的物理基础，而机房作为放置这些设备的场所，保证其安全性是保障信息安全的重中之重。一旦机房环境设备出现故障，就会影响到计算机系统的运行，对数据传输、存储以及整个系统运行的可靠性构成威胁，若没有及时处理，就可能损坏硬件设备，造成严重后果。在所有造成数据丢失的原因中，硬件损害对于数据恢复来说难度是最大的，恢复的结果也经常不很理想。所以，保障机房安全是信息安全的基础，应该做到以下两点：

算机系统文件信息的加密过程中，可应用数字摘要进行数字签名。利用 Hash 函数进行计算，令原文信息通过加密处理压缩成为数字摘要。而后可应用自有私钥实施数字摘要加密，令结果同原文同步传送。接下来通过公开密钥解密数字摘要，利用 Hash 算法实施原文信息的加密压缩令其成为数字摘要，同获取数字摘要展开对比。该类方式可形成数字签名，还可确保数据信息的安全整体性，对大量数据文件信息的安全传输体现了优质应用价值。

3.4 信息隐藏加密技术应用

将计算机信息数据嵌入至隐蔽载体内形成加密的信息技术为数字水印技术。其体现了良好的保真性、操作的稳定性、可靠安全性与便利性。保真性即嵌入水印各类数据信息、媒体不会形成视觉与听觉的显著差异。可靠稳定性则是数字水印加密技术可应对抵御各类信号处理以及影响攻击。可靠安全性为数字水印较难被人为复制以及非法伪造，同时提取操作算法相对较为容易。该隐藏信息加密技术主体将保护数据信息有效的隐藏到多媒体工具载体之内，令非法用户无法意识到隐藏数据信息存在性，或无法将其检测出来。该加密技术应用不仅可预防非法用户将水印信息不良提取，同时可有效的避开攻击影响。一般来讲传统的计算机密码护理技术可进行数字作品的安全保护。然而媒体倘若被解密，便可任意自由的进行信息复制与交流传输。同时，解密算法具有一定的复杂性，因而较难符合实时性应用需求，利用数字水印隐藏信息加密技术则可有效的弥补缺陷，达到良好的加密效果。

4. 结语

总之，计算机安全加密应用技术可确保系统之中各类数据信息的综合安全性，营造规范有序的计算机、网络技术应用环境，发挥各类软硬件的优质、高效应用价值。因此，我们只有明晰加密技术应用重要性，探索科学应用途径，方能优化计算机安全加密技术应用效果，创设显著的应用服务效益。

参考文献：

[1] 徐秦 . 详解加密技术概念及加密方法 [J]. 科技信息，2010，（11）.

[2] 唐松生 . 康金兵 . 计算机安全技术之加密技术 [J]. 中国教育技术装备，2010，（27）.