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）.

（1）机房环境宽大、安全，应有防火灾、防地震、防雷击的措施，并要针对防盗、碰撞等情况做好相应的准备。

（2）保证机房的供电安全。随着设备的不断增加，机房能耗问题日趋严重。由于电网供电质量不稳定，有时会出现电源故障，包括电压浪涌、电压过压、欠压、瞬时电流冲击和故障停电等各种情况，而硬件故障往往由这些问题引起。良好的供电设计可以为机房安全提供保障，并维持计算机系统持续稳定的运行。

3.2.2 计算机或服务器的管理

计算机及服务器是数据和系统的直接载体，上面保存着业务系统和各种数据。要保障其安全性，在管理上必须做到以下几点：

（1）根据其安全需求安装对应的操作系统，并应对系统进行定期维护，保证它的稳定性。如服务器必须安装特定的服务器版操作系统。

（2）在系统中安装杀毒软件以及防火墙，可以有效避免黑客的攻击以及病毒木马的入侵。

（3）提高计算机或服务器操作系统的安全策略等级，避免未获得授权的人通过各种手段远程连接计算机获取数据。

3.2.3 保障计算机网络稳定安全地运行

网络安全是系统安全的核心。计算机网络作为信息的主要收集、存储、分配、传输和应用的载体，其安全对信息安全起着至关重要甚至是决定性的作用。不稳定的网络会引成数据完整性破坏、拒绝服务等种种的问题，让用户不能完整快速地获取数据；存在网络漏洞则常常会因为别人故意利用或误操作，造成信息泄露、窃听等种种危害。保障计算机网络稳定安全，应从以下几点出发：

（1）保护网络关键设备，制定严格的网络安全规章制度，安装不间断电源（UPS），避免网络意外中断。

（2）在用户访问网络资源时对其权限进行严格的认证和控制。可以采取用户身份认证，口令加密，设置用户访问目录和文件的权限，控制网络设备权限等种种手段。访问控制是系统安全防范和保护的主要核心策略，它的主要任务是保护系统资源不被非法使用和访问。访问控制规定了主体对客体访问的限制，并在身份识别的基础上，根据身份对提出资源访问的请求加以控制。

（3）使用网闸和防火墙等设备，在不同网域之间设置屏障，阻止对信息资源的非法访问，也可以阻止重要信息从内部网络中非法输出。必要时还可以使用虚拟专用网（VPN）等技术，在公共网络上创建安全的私有连接，提高网络中通信的安全性。

（4）采用信息过滤等手段来保护网络上信息传播安全，防止和控制由非法、有害的信息进行传播所产生的后果，避免信息失控。

3.2.4 在业务系统中采取良好的设计

许多业务是通过网上业务系统来进行的，用户通过业务系统存储以及查看数据，所以业务系统的设计也与系统中的数据安全息息相关。在业务系统的设计实现中应该主要注意以下方面，以提高系统和数据的安全性：

（1）数据传输的保密性。在业务系统中应该采取比较安全的数据传输方式。为了避免保密数据泄露，在传输这类数据时可以通过一定的技术手段进行处理，而不是明文传输，从而避免保密信息泄露。比如密码传输时采用 md5 等散列函数进行处理，可以有效避免密码泄露。

（2）应为系统设计良好的权限管理功能。权限管理，一般指根据系统设置的安全规则或者安全策略，用户可以访问而且只能访问自己被授权的资源。“ 用户认证 ”让系统知道用户“ 能不能用 ”，而“ 权限管理 ”则通知系统用户“ 能用什么 ”。良好的权限管理设计能够避免用户使用不被授权的功能和数据，从而降低了信息泄露、非法使用、授权侵犯的风险。

3.2.5 数据加密技术

加密技术对于互联网上信息安全来说有着举足轻重的地位。在互联网上进行文件传输、电子邮件商务往来存在许多不安全因素，而且这种不安全性是不可避免的，由互联网存在的基础——TCP/IP 协议所引起。为了尽量降低信息泄露的风险，采用技术手段对数据进行加密是一种通用的做法。现在一般采用非对称加密对数据进行处理（如 RSA 算法），该方法的特点是存在两个密钥，公共密钥由于加密，面向外部公开；私人密钥用于解密，内部保存。只要私人密钥不泄露，就可以极大地保证数据的安全性。所以在实际工作中传输保密数据，应该先对数据进行加密，这样就算数据被别人恶意获取，在没有私人密钥的情况下，数据也不能使用，进而避免因为数据泄露而造成的损失。

3.2.6 管理人员泄密风险

造成数据泄露还存在一种非技术的原因。由于管理员的松懈或者其它种种原因，造成数据外流。我们在实际工作中也应该通过一些手段尽量减少风险：

定期对管理人员进行培训，提高他们的安全保密意识。制定严格的安全管理制度，从规章制度上避免这种情况的发生。

3.2.7 数据恢复

上面所说种种措施都是用于预防风险，而数据恢复技术主要用于减少损失。数据恢复是指通过技术手段，将保存在各种介质上丢失的电子数据进行抢救和恢复的技术。一般造成数据损坏的原因有硬件故障和人为破坏两种。硬件故障是指由于硬件损坏造成数据全部或部分丢失，如硬盘出现坏道等，应注意在故障后尽快找专业公司进行修复，不应勉强继续使用，以免发生更大的损失。人为破坏是指由于误操作或者恶意操作，对数据的完整性造成了破坏，甚至数据遭到删除。这种情况可以通过数据恢复软件对数据进行恢复，但应注意在恢复之前尽量避免对数据所在硬盘进行写入操作，以免删除数据在硬盘中的残余信息遭到破坏。

4. 结语

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏。为了达到这一目标，我们在日常工作中应该抱着严谨负责的态度，并熟练掌握各种防范手段和技术，这样才能最大限度地保障计算机及网络信息的安全。

参考文献：

[1] 鲁立，龚涛 .《计算机网络安全》，ISBN：9787111335054，机械工业出版社，2011 年 4 月

[2] 蔡立军，《网络安全技术》，ISBN：9787810828758，北方交通大学出版社，2006 年 9 月

[3] 刘安定，浅谈计算机网络安全与防范 [J]，佳木斯教育学院学报，2011 年 6 月

[4] 龚奕，计算机网络安全问题和对策研究 [J]，软件导刊，2009 年 2 月