基于容错和备份技术的网络信息安全策略研究

浦云明 林秀珍 廖江福 （集美大学计算机工程学院 厦门 361021）

摘要：本文分析网络信息安全的重要性极其产生的问题，网络信息安全的应对技术和方法，重点讨论了数据备份技术和容错技术对信息安全的作用以及企业界实施容错和备份的方案，保证和提高信息与数据安全性。

关键词：网络信息安全 备份 容错 策略研究

1 引言

计算机网络安全应确保网络正常运行、维护网上正常秩序、提高网络效率。计算机网络所面临的威胁主要有两种：一是对网络中信息的威胁，二是对网络设备的威胁。影响计算机网络信息安全的因素有些是有意的，有些是无意的。网络信息安全主要潜在威胁有：信息泄密、信息破坏、传输非法信息、网络资源的非法使用和计算机病毒等。网络信息安全的目标是保护信息的机密性、完整性、抗否认性和可用性。网络信息安全问题主要是信息被窃密和信息被破坏[1]。

2 网络信息安全的应对策略

计算机网络体系结构与信息安全的关系是全方位的、整体的。在 OSI 七层基础上，将安全体系划分为四个级别：网络级安全、系统级安全、应用级安全和企业级安全[2]。在物理层，可通过把传输线封装在含有氩气的封装管中来挫败偷听。任何钻管的尝试都会导致漏气、减压，并能触发警报装置。一些军用系统就采用了这样的技术。在数据链路层，实施了点到点链路加密，分组数据（称为帧）在离开一台机器时被编上密码，到达另一台时再解码。在网络层，可以安装防火墙来限制分组的进出。在传输层，整个连接执行端到端（也称为面向协议）的加密。在应用层，可采用数字签名等方法有效地解决身份认证和抗否认性问题。

根据网络信息安全问题的类型，网络信息安全技术可以从防止信息窃密和防止信息破坏两个方面来考虑。

2.1 防止信息窃密技术

防止信息窃密的技术有：通信反侦察、防电磁泄露、防火墙技术、密钥管理、报文鉴别、数字签名、加密技术等。

（1）通信反侦察。网络在传输信息过程中很容易被网络破坏者侦听，为了防止这种事件的出现，有线电通信常采用光缆和可防窃听的保密电缆线路等。无线电通信则通常采用扩频技术、猝发传输技术、毫米波和激光通信技术等，这几种通信手段都具有强的抗截获能力和抗干扰能力。

（2）防电磁泄露。计算机系统电磁辐射泄露也会使信息失密，因此，通常采用机房屏蔽和设备屏蔽技术来抑制和防护电磁辐射泄漏。机房屏蔽是用屏蔽室对计算机系统实施屏蔽。屏蔽性能最好的是采用实体的钢和钢板的双层屏蔽以及双层间绝缘的屏蔽室。设备屏蔽，比如为防止视频显示器电磁辐射，在其玻璃上喷涂一层导电薄膜，在玻璃周围用导电条将导电薄膜与机壳相连接地，达到屏蔽电磁场的效果。另外，还要从设备的研制和生产上考虑电子设备电磁辐射的防护和抑制问题，例如改善电路布局、搞好电源线路和信号线路滤波等。

（3）防火墙技术。防火墙是目前所有保护网络的方法中最能普遍接受的方法，防火墙的主要功能是控制对受保护网络的非法往返访问，防范方法可以是监视、限制、更改通过网络的数据流。从实际情况来看，防火墙是一个独立的进程或一组紧密联系的进程，运行在路由器或服务器上，控制经过它们的网络应用服务和数据传输。安全、管理、速度是防火墙的三大要素。防火墙作为内部网与外部网之间的一种访问控制设备，常常安装在内外网的交界点上。所有内部网络与外部网络之间的通信流量都必须经过这个唯一、狭窄的检查点，因此防火墙是阻塞点，可以实施集中的安全策略，不必针对每一台主机实施单独的安全策略。

（4）密钥管理。网络安全系统运行效率的高低与

密钥管理密切相关，若对于 DES 和 RSA 密码体制丢失了密钥，则整个网络安全系统变成为虚有。密钥管理由密钥的产生、分配和安装 3 个部分组成。

(5) 加密技术。加密技术可分为通信加密、存储加密、文件加密。在计算机网络中，通信保密分为链路加密、结点加密和端对端加密。在这 3 种方式中，端端加密从成本、灵活性和保密性方面看是优于其他两种方式的。端端加密指的是在发送结点加密数据，在中间结点传送加密数据(数据不以明文出现)，而在接收结点解密数据。网络信息在传输过程中需要加密，在存储时也要加密，防止非法拷贝和查询。存储加密能较彻底地防止信息窃密。依据存储方式，存储加密有文件加密和数据库加密两种形式。由于文件加密以文件为单位进行加密，只有文件的合法使用者用自己的密钥，才能看到文件的真实原文，数据库加密以数据库记录或字段为单位进行加密，所以文件加密比数据库加密容易实现。

(6) 报文鉴别。报文鉴别能提供对传输报文数据的有效性及完整性的验证，他是数据保密的一部分。他允许每一个通信者验证收报文的来源、内容、时间性和规定的目的地址。

(7) 数字签名。数字签名是以电子签名形式存储消息的方法，所签名的消息能够在通信网络中传输。数字签名可以采用 RSA 签名和 DSA 数字签名[1]。在 RSA 数字签名方法中，将要签名的消息作为一个散列函数的输入，产生一定长的安全散列码，使用签名者的私有密钥对这个散列码进行加密就形成签名，然后，将签名附在消息后。验证者根据消息产生一个散列码，同时使用签名者的公开密钥对签名进行解密，如果计算出的散列码与解密后的签名匹配，那么签名就是有效的。

2.2 防止信息破坏技术

防止信息破坏的技术主要有：通信反干扰、防止计算机病毒、阻止黑客侵袭、差错控制、冗余设计和备份技术。

在计算机网络信息传输过程中，有线电通信(如电缆和光缆通信)系统不会受到电子干扰的影响。无线电通信易受电子干扰，一般可采取扩频技术、自适应和调零天线技术等达到反干扰效果。

计算机病毒、特洛伊木马、" 黑客" 入侵、逻辑炸弹、协同攻击将造成信息破坏。所造成的后果有：数据丢失、数据被修改、增加无用数据及系统瘫痪等。

差错控制可发现和纠正传输信道等设备造成的错码。目前常用的基本的策略有两种。一种方法是在每一个要发送的数据块上附加足够的冗余信息，使接受方能够推导出已发出的字符应该是什么。另一种方法是只加入足够的冗余位，使接受方知道有差错发生，但不知道是什么样的差错。前者的策略是纠错码，而后者则使用检错码。冗余设计是采用 2 个以上功能完全相同且完全独立的并行系统或设备，来完成给定的任务。当工作网络出现故障，备用网络会接替原先的工作，保障系统不间断地运行，从而保证信息的正常流通。

采用了防止网络信息破坏的相应技术，一旦发现问题，即可报警并实施隔离工作。但是，世界上没有万无一失的信息安全防护措施。信息世界的" 攻击和反攻击" 进程也永无止境，信息的攻击和防护是在螺旋式地向前发展进程中。从防护技术来看，容错设计、数据备份和恢复是保护数据的最后手段，也是防止" 主动型信息攻击" 的最后一道防线。

3 容错设计在网络信息安全中的应用

可靠、安全的设计必须考虑容错技术(fault tolerance)，实现容错的主要手段是冗余，一般的容错技术有结构、信息、时间的冗余，如 3 模冗余、多模冗余、RAID 技术、双机容错技术等。目前在企业界普遍采用的技术是双机容错技术，外加磁盘阵列。不同的系统结构，在可靠性上的得益是不同的，高可靠性的获得取决于系统结构的选择，并达到工程要求和具有较好的成本 - 效益比。

(1) 静态冗余。静态冗余[4]常用 3 模冗余 TMR (triple module redundancy) 和多模冗余。静态冗余使用表决和比较来屏蔽系统中出现的错误，图 1 中的 M1、M2、M3 是并行独立工作的模块。

U = (u1 and u2) or (u2 and u3) or (u1 and u3)

(2) 动态冗余。动态冗余[4]主要是多重设备待机储备，相继运行，以维持系统的正常运转。当某个工作模块出现错误时，使用另一备用模块来顶替并重新运行，这包括一系列的检测、切换、恢复过程，图 2 中的 M1、M2、M3 是具有相同功能的不同模块，M1 是主模

块，M2、M3 是备用模块，当 M1 出错，M2 接替 M1 的工作，M3 又成为 M2 的备用，当所有模块出现故障，系统才会失败。当一个故障模块被备用模块替换后，冗余

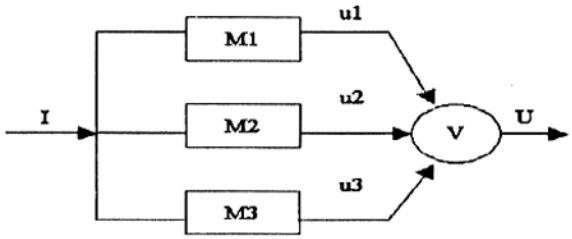

图 1　静态冗余结构

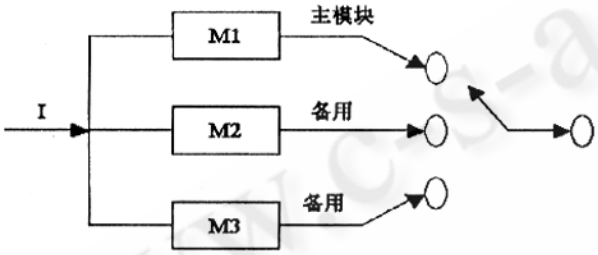

图 2　动态冗余结构

Channel 存储子系统，外置磁盘阵列柜，内有 10 个 18G 的热插拔 SCSI 硬盘，采用 RAID 0 +1 技术，象屿码头双机容错方案如图 3 所示。CTMS (Container Terminal Management System) 集装箱管理系统使用 Oracle 数据库储存了历年的数据，系统和数据的安全性就成为 CTMS 系统的第一考量，一旦系统故障或数据丢失将带来不可估量的损失，系统采用了磁盘阵列的双机容错技术，通过一条不占用网络带宽的专用高速链路和一套使用独立 I/O 请求的驱动级别的镜像设计，不但确保 NT 服务器的数据获得传统意义上的双服务器热备份，更能确保应用程序、文件系统和打印机等网络资源获得同等程度的高可靠性。这样双服务器可实现"active to active"的同等级别并互为备份的容错方式，在双方互相而持续地监控镜像资源的过程中，如果其中一台服务器由于硬件或软件原因发生故障失效，另一台可在保证提供自己原有服务的同时，启动失效服务器的应用程序，文件系统、IP 地址和打印机等网络资源服务，从而取代原服务功能，以上切换可由用户根据环境要求和硬件设备能力自行定义，切换时间仅以秒为单位。

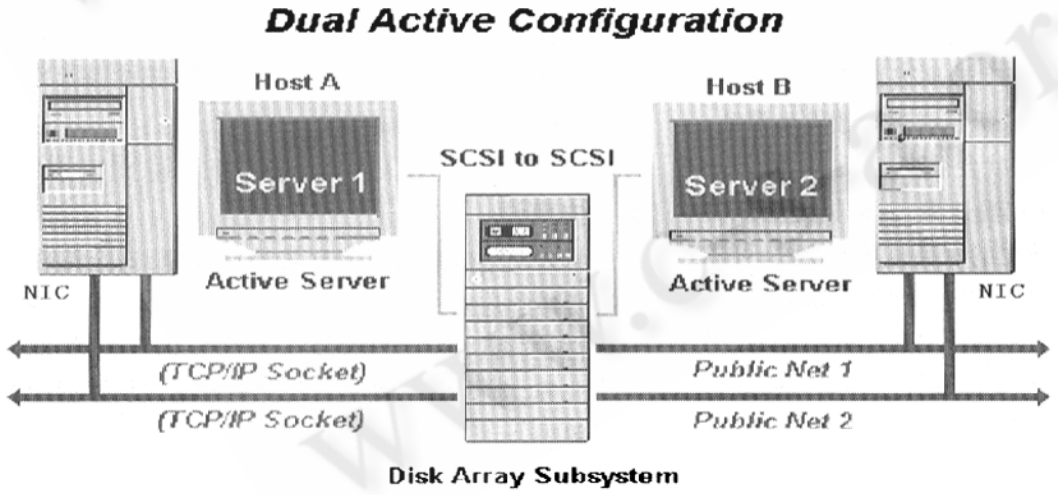

图 3　厦门象屿集装箱码头 CTMS 双机容错系统

4　备份技术在网络信息安全中的应用

系统备份主要保护操作系统，应用软件及其配置和备份重要的文件和数据库的数据文件及日志文件、控制文件和参数文件。在发生文件和数据丢失时，我们能够及时恢复所需要的文件和数据；在系统崩溃或发生地震等自然灾害时，我们能够及时恢复操作系统，应用软件及其配置。

4.1　数据管理系统

计算机网络系统包含了多台服务器，服务器上的数据库包含了越来越多的业务数据，这需要对整个网络的数据有统一的管理策略，建立对计算机系统安全

系统进行了一次重构，各备用模块在待机时，可以不工作(称为冷备份系统)，也可与主模块一样工作(称为热备份)，其结果不影响系统输出，而且热备份系统各模块在待机过程中的失效率可视为 0。

(3) 双机容错系统。厦门象屿码头是一个集装箱专用码头[3]，厦门象屿码头建设了支持集群的 SCSI

和备份的管理制度，将迅速增大的日常数据安全管理与灾难恢复系统的建设结合起来，使用数据管理系统实现自动备份和无忧化管理。数据管理系统能解决如下问题：

(1) 由于系统数据量大，如果由人工来进行数据的备份工作将给系统管理带来很大的工作量。工作人员的情绪化，每天备份日程的变化，误操作等都可能造成可靠性得不到保障，难以形成制度化。一旦备份人员外出、生病等则可能导致备份工作中断。而使用数据管理系统，结合大容量存储设备，可以实现自动化的数据备份管理。

(2) 数据分散在不同的机器、不同的应用上，管理分散，安全性得不到保障。若各种数据分布在不同的服务器或不同应用软件上，加上操作人员技术掌握的差异性，数据备份工作的可靠性得不到保障。

(3) 运行着的系统使得维护人员寸步难离，一旦发生数据的丢失，损坏等，就不得不由系统维护人员来帮助，使得系统维护人员忙于应付这些日常工作，变得寸步难离。当发生数据损坏时，如果系统维护人员不在现场，就会使业务停顿下来。

(4) 存储媒体管理困难，随着应用系统的运行，用来存储数据的介质越来越多，各种不同系统下存储产生的软盘、磁带、光盘将给管理带来很大的麻烦，如果介质没有电子标签，一旦人工标签脱落导致发生混乱，要想知道介质上数据的内容就会很难。

(5) 历史数据的保存和快速查询，数据是企业发展的重要基础材料，历史数据的保存有其安全性，可靠性方面的特殊要求，这就需要数据管理系统来完成。

(6) 数据库在线备份，针对打开状态的数据库，如何提供接口实现在线备份，实现系统连续运行以提供 24 小时不间断服务。

4.2 备份应用方案

(1) 需求。嵩屿电厂的计算机网络系统主机以 Windows NT 为平台，OA 系统包含了以 Lotus Notes 为基础的邮件系统，采用了 SQL Server 和 Oracle 数据库服务器，考虑重要的业务数据和信息，我们需要对整个网络的数据有统一的管理策略；同时我们需要有一简单有效的手段，将操作系统中的如用户和安全权限等系统配置备份下来，使我们在系统崩溃或文件丢失时，能够快速有效的恢复数据和整个系统。在嵩屿电厂的方案中选择了美国 Legato 公司的 Networker 数据存储管理系统来解决系统管理及数据备份问题。之所以选择 NetWorker 数据管理系统，主要基于该数据管理系统的全自动的备份、集中式管理、归档管理和有效的媒体管理等特点。

(2) 备份的实施。备份系统采用客户机/服务器方式，备份服务器采用 PC 服务器连结 Quantum DLT 磁带机. 由于嵩屿电厂的整体环境大多是以 Windows NT 的平台为主，因此，将磁带库挂在一个 NT 主机上，并安装一套 Legato Networker 网络版的网络备份软件。购买 Oracle Agent、Notes Agent、SQL Server Agent 模块分别安装在各个数据库服务器上，便可以备份以上三种数据库了。另外，在启动 Legato 备份软件时，已开启或正在使用或是被锁定的文件通常会被跳过，万一硬盘损坏或系统宕机造成数据毁损时，文件即会遗失，为避免在备份时段上遇到这类状况，建议在每一台服务器上各安装一套 Backup Agent for Open Files 选项，即可做 100% 的数据备份。

(3) 灾难防治与重建。Disaster Recovery(灾难防治与重建)是一独立软件，一般与 Networker 结合使用，为 Windows NT 网络提供非平行式的数据保护，它可以让使用者无须手动重新安装操作系统，宕掉的服务器就可完全恢复，简化了重建的程序，并可显著地降低服务器宕机的时间。

5 结束语

针对网络信息被窃密和被破坏问题，安全策略应设计相应的应对技术和方法，保证网络信息的机密性、完整性、抗否认性和可用性。从防护技术来看，特别是在企业界，容错设计、数据备份和恢复是保护数据的最后手段。

参考文献

1 信息安全概论，段云所著，高等教育出版社，2003.9.
2 网络与信息安全技术，清华万博网络技术有限公司，2002.
3 中小企业存储技术初探，浦云明，计算机系统应用，2001.8.
4 软件工程，郑人杰主编，清华大学出版社，1999.8.