

网络环境中的数据完整性和数据安全问题研究

[作者] 周瑛, 潘紫薇

[单位] 安徽中医学院图书馆

[摘要] 详细阐述网络环境中的数据完整性和数据安全问题的定义和主要种类,在此基础上提出这两个问题的解决办法,并分析它们在未来对某些领域的影响。

[关键词] 网络环境,数据完整性,数据安全

1 数据完整性和数据安全的定义

在当今的信息化社会中,计算机和网络已经广泛应用于社会的各个领域,基于这些先进技术建立起来的信息系统正改变着人们的生活和工作方式。然而,在我们享受着众多信息系统带来的方便的同时,也时常受到来自各方面对其安全的威胁。据美国 FBI 统计,每年因信息和网络安全问题所造成的损失高达 75 亿美元,而且还有上升的趋势。而数据作为信息的表示形式,它的完整性与安全性问题,则成了系统安全的重要内容。

数据完整性是指与损坏和丢失相对的数据的状态,是“一种未受损的状态”,即存储器中的数据必须和它被输入时或最后一次修改时一样,通常表明数据在可靠性与准确性上是可信赖的,若丧失了数据的完整性,则意味着数据可能被改变或丢失,成为无效的数据。这些危险常常来自一些简单的计算不周、人为的错误判断或设备出错等行为。数据完整性的目的就是保证计算机系统上的数据和信息处于一种完整和未受损害的状态。

数据安全是指计算机系统上的数据未被窃取和损坏。网络是一个开放式系统,如果不保护数据的安全,那么与网络系统连接的任何用户,都可以进入和访问网络中的资源,修改网络中的数据,最终使整个网络陷于瘫痪。数据安全的目的是保证计算机系统上的数据能被合法有效地使用。

2 数据完整性问题的种类

对数据完整性最常见的威胁主要来自 4 个方面。

2.1 人类

分布式系统中最薄弱的环节是使用它的人,人易犯错误的天性是许多难以解释的错误得以发生的根源。

意外事故。这类错误是由于人(包括系统管理员)的误操作所致,如按 Cancel 按钮时误按了 OK 按钮等。

通讯不畅。由于网络用户剧增,它的反应速度与我们的耐心相比已显得太慢。当人们将信息从一台服务器上转移到作为临时存储器的另一台服务器上,并为所有的服务器做每日备份时,由于一些硬件故障,有些服务器不能及时进行备份;或当人们从临时服务器拷贝文件时,往往由于误操作而丢失数据,这意味着我们并不能完全信赖通讯系统在传递信息时确保该信息能被收件人阅读。

2.2 硬件故障

任何高性能的机器包括计算机部件都不可能长久地运行。一些电子和机械故障时常发生，主要有以下几种：

磁盘故障。这是计算机运行过程中最常见的问题。硬盘是一种十分重要的设备，一般在平均无故障时间之前就应更换，否则当硬盘损坏时，其中的所有数据都将丢失。

存储器故障。由于射线、电磁场这些不可见的射线会导致芯片内部数据的改变，随机存储器常出现故障错误，这类故障很难检测。目前，只有装有奇偶检验存储器的服务器系统可识别出被损坏的代码段并防止其在系统运行。

介质、设备和其他备份故障。数据存储可在可移动介质上用来备份，而恢复工作需对数据进行拷贝。若服务器、存储设备或其使用的介质中的任何一个出现问题都会导致数据丢失。在这种情况下，虽然做了备份，但备份盘上却不是完整的有效数据。

2.3 网络故障

在网络中，电信号在计算机中产生并被输送到网络上，数据在机器之间高速传输。用来连接机器的线缆会受到干扰和物理损伤，从而导致数据的损毁或丢失。这些故障主要包括：

网络接口卡和驱动程序问题。网络接口卡的故障并不损害数据，仅仅表现在使用户无法访问数据；而当服务器上的网络接口卡出现故障时，服务器一般会停止运行，这就很难知道哪些打开的文件被损坏了。

网络连接问题。在网络连接中，路由器和网桥中的缓冲区不够大就会被备份操作阻塞，而导致数据包的丢失。反之，若路由器和网桥中有大量的缓冲容量，那么高强度的信息流量造成的延时极有可能会造成会话超时。

辐射问题。辐射能使电子移动，所以它会损坏计算机中的数据，由于辐射很难控制，所以最好的办法是避开它。

2.4 逻辑问题

继用户、硬件和网络之后，最有可能威胁数据安全的就是软件，这些威胁包括：

软件错误。软件错误通常与应用程序的逻辑有关。没有任何一家软件开发机构有能力测试软件使用中的缺陷，所以用户应慎重使用软件。

文件损坏。文件可能由于系统控制或应用逻辑中的一些缺陷而导致损坏。若被损坏的文件自己又被用来创建数据，则生成的新数据就会出错。

数据交换错误。当文件在转换过程中生成的新文件不具有正确的格式时，就会产生错误，影响数据的完整性。

3 数据安全问题种类

数据的安全问题主要来自 3 个方面。

3.1 线缆连接

计算机网络的使用对数据造成了新的安全威胁，主要包括：

窃听的。在网络中，每台计算机通过一些媒介相互通讯，窃听者可通过检测从连线上发射出来的电磁辐射来收集所要的信号，以达到窃听的目的。对于这种威胁，可用加密手段来防止信息轻易地被解密。

拨号进入。对任何拥有调制解调器和电话号码的人来说，若他了解某个机构的帐户时，就可通过远程拨号访问该机构的网络，从而威胁到该机构的数据安全。

3.2 身份鉴别

指计算机在决定用户是否有权在服务器上要求提供某些服务时，对用户进行身份鉴别。常见的威胁身份鉴别的方式有：

口令圈套。指设计圈套者先写出一个代码模块（运行后和登录屏幕一样），使用户看到的是两个登录屏幕，第一次登录显示失败后，用户被要求输入用户名和口令。而实际上第一次登录并未失败，设计圈套者只是将登录的数据（如用户名和口令）写入了一个数据文件以便今后使用，从而非法进入该系统。

口令破解。指专业人员破译口令的组合，有的非法闯入者常用超长字符串破坏那些口令算法。

3.3 编程

真正危险的安全漏洞源于代码，这种数据的毁损往往是毁灭性的。

病毒。病毒的特点是随着它所附着的另一个程序在机器之间传播，并可进行自我复制，这种传播可通过从 BBS 上下载文件时进行，也可通过将新的资料输入机器的过程来进行，最著名的病毒之一——Internet 蠕虫，就是在整个网络上进行传播的。

代码炸弹。它的原理是到了设定的日期和钟点，被触发并开始破坏，但代码炸弹不像病毒那样四处传播。

特洛伊木马。它是包括病毒、代码炸弹、蠕虫和诸如此类的代码的通称。通常被安装到不知情的人的机器上，伪装成系统上已有的程序，到了一定的时候它就毁坏数据，破坏系统。

4 数据完整性和安全威胁的一般解决办法

4.1 提高数据完整性的工具

4.1.1 备份 恢复出错系统的通用做法是安装备份系统，如果用户丧失了系统的数据完整性，可用备份系统将最近的一次数据备份恢复到机器上。

4.1.2 镜像技术 该技术是指将数据原样从一台机器上拷贝到另一台机器上，即两个部件执行完全相同的工作。如果其中一个出现故障，另一个系统则继续工作。通常用于磁盘子系统中。

4.1.3 分级存储管理 该技术是一种能将软件从在线存储器上归档到近在线存储器上的自

动系统，也可进行相反的过程。它本质上并不将文件删除，而是在文件原来的地方留一个与原文件相同名字的标志文件，该标志文件占用比原文件小得多的空间。当用户想访问原文件时，该标志文件就自动地将原文件恢复过来。

4.2 减少数据安全威胁的工具

4.2.1 病毒检查 要经常用反病毒软件检查磁盘和系统，一旦查出病毒，应及时消除。

4.2.2 加密 加密是指对数据进行编码，但仍保持其可恢复的形式。当信息在网上传输被别人偷窃时，偷窃者必须解密才能知道信息的内容，否则毫无用途，这是一种常用技术。

4.2.3 执行身份鉴别 身份鉴别是指机器核实某人身份的过程，它包括两个问题：你是谁？你是你说的那个人吗？执行身份鉴别的常用方法是设置口令。口令需要常更换，这种方法可限制非法侵入者。

4.2.4 Internet 防火墙 防火墙是用来限制信息从外部网络进入内部网络间，它是网络中保护数据安全的常用措施。

5 未来对数据完整性和数据安全的考虑

计算机技术随着网络集成和无线通信技术的不断发展，对数据完整性和安全的威胁也不断增长，主要包括：

5.1 开关设备和虚拟网络

为适应不断增长的数据传输的需要，系统中已开始使用具有极高速度的开关集线器和其他的网络连接。这些开关主要是为网络上的个人计算机提供分离的连线区段间的数据传输进行控制，除此之外，还能利用它们建立虚拟网络。虚拟网络可通过集线器中的软件功能建立而不必改变集线器的硬件，但虚拟网络也会产生安全风险。除了要保证非授权用户无法访问未被授权的区段外，还要保证非授权用户不能用“特洛伊木马”程序来改变开关的配置，从而非法进入其它的网络区段。虚拟网络中的另一个安全问题是由于人为错误造成的集线器配置改变，使一些非授权用户获得了不能访问的文件和系统。

5.2 无线网络

无线网络中最明显的安全威胁是数据传输被无线电接收机拦截并被窃取，而最明显的数据完整性威胁是电磁干扰能导致数据在传输中被破坏，使用定向无线和特别的反射窗口遮盖物可减少从窗户中外泄的网络无线电传输。

5.3 公共网络和 Internet

Internet 以开放的原则工作，任何人只要愿意都可以访问它。如果用户有 Internet 上有一个网络服务器，都能闯入其他访问 Internet 的用户的系统，像 Gopher, Finger, Telnet, Ftp 和 E-mail 这样的常用工具都曾被黑客们用来访问他们未被授权阅读的信息。虽然有的用户已经

建立了“防火墙”，但仍然有技术高超的黑客非法侵入系统，破坏数据的完整性。
综上所述，在计算机技术迅猛发展的今天和未来，如何保证数据的安全和数据的完整性仍是整个计算机界（包括计算机专家和各种用户）所面临的主要问题，我们希望出现有关数据完整性和数据安全的存储管理标准，使用户能安全地使用各种信息产品。

参考文献

1 Marc Farley, Tom Stearns, and Jeffrey Hsu: LAN Times Guide to Security and Data Integrity, Published by McGraw Hill, Inc.

2 刘春平．小心：计算机病毒．中国计算机用户，1998-10-05