信息系统中信息的安全保密措施

边小凡 （河北大学计算中心） 顾劲松 （华北电力学院计算中心）

摘要：本文介绍了在信息系统的分析、设计、程序编制各阶段中保证信息安全的一些措施。笔者将自己开发信息系统时对信息的安全保密管采取的一些措施予以介绍，供同行参考。

一、信息的安全保密应有统筹规划

信息系统中的信息要在整个系统内传输和处理，是一种可共享的资源，因此信息的安全与保密是涉及系统各方面的全局性的问题。全局性问题只有统筹规划才能合理有效的解决，也就是说在系统分析规划阶段就应充分考虑，在此阶段应仔细考虑如下几个问题：

1.对信息的使用范围、保密等级应严格分类。

这种分类应与信息的存储和功能模块的划分结合在一起进行，既要保证信息存储处理的合理与方便，又要注意信息的保密与安全。这二者之间时有冲突，应视实际要求的不同采取不同的策略。有时或许要牺牲些方便性，以换取更高的安全保密性。

2.设计信息保护体系

在信息分类的基础上，充分利用操作系统或数据库管理系统等系统软件的信息保护功能设计信息保护体系，设计可分三步进行。

首先根据各种操作的性质及其所涉及的信息范围和权限，把它们划归不同的系统用户。这可以和子系统的划分统筹考虑。一般一个子系统可以划分成一个或几个系统用户。例如高校管理信息系统中的校办子系统可划分为报表打印和校长查询两个系统用户。前者涉及的信息范围窄，仅可存取与打印综合报表有关的信息，对部分信息有更新权。后者涉及的范围宽，可以查询系统内的任何信息，但无更新权。

其次划分信息集并确定其属主。这里所说的信息集在文件系统中指的是数据文件，在数据库管理系统中即指各种实体，例如关系。信息集的划分除考虑信息的属性、存储处理的方便外，还应考虑安全保密因素。安全保密程序不同的信息最好不要混放。一般建立信息集的系统用户即为该信息集的属主。属主对信息集具有至高无上的权力，并可赋给或收回其它用户对该信息集的各种权力。

最后，确定各系统用户对各种信息集的权限，即确定某一信息集可由哪些系统用户进行何种操作。一般多用户操作系统的文件保护功能只能把用户分成属主、同组和其它(OWNER, GROUP, WORLD)三类，且不能对文件内某些记录或字段分类操作。某些数据库管理系统，例如 ORACLE，提供了更为完善的信息保护功能，某个用户可对实体的部分记录或部分字段进行分类操作，应充分利用。系统软件的不足，可用应用软件的功能来补充。

完成以上三步之后，就有了一个初步的信息安全体系。

3.建立必要的审计功能

为了保证信息的安全，除了采取一切必要的手段防止信息被窃取或破坏外，还应有一定的审计手段，一旦信息被窃取或破坏后，能够及时发现和补救，找出系统的薄弱环节。审计措施在系统分析和设计阶段就应仔细考虑，以确定审计的主要对象和具体措施。审计不能滥用，否则会增加系统不必要的开销。审计措施有多种，可以随时审计，也可以定期(事后)审计。譬如可采用：

(1)双轨运行法：例如，财会帐目管理中记帐、冲帐等主要操作，必须两个人在不同的终端上完成，一个人记X的帐须经另一个人审核通过才能生效。

(2)轨迹法：系统中的一切重要操作都自动记录在案，即留有轨迹。这些记录定期由专职人员进行检查(审计)，以监督运行情况。对重要文件的每一次更新都由系统自动记入日志文件，文件内容包括更新日期、用户名、更新前的内容等。检查日志文件即可看到文件更新的情

况。

审计的实施也可借助系统软件提供的功能。因为某些操作系统本身提供日志功能，把每个系统用户的开机时间，使用资源，甚至各种操作都记录在案。有的数据库管理系统提供了更强有力的审计功能，它可以把整个数据库的操作情况按管理员的要求记录下来。例如，某个用户操作失败（如存取无权访问的实体等）的次数及操作内容，对某个实体的更新或查询情况等。一般来说，系统软件提供的这种功能开销是很大的，不但占用 CPU 时间，而且要占用大量的存储空间。因此使用时要权衡利弊，不能滥用。

4.网络环境下的特殊措施

在网络环境下，除考虑信息传输的可靠性外，还应对网络高层协议的开发提出要求，以防非法操作者对信息的破坏或读取。当网络的某节点向本地节点发送或请求读取信息时，应首先判断其合法性。可采用在每个节点上存放一些权限表。表中记录着每个远程节点可向本节点存取信息的权限，权限表的参考格式如下：

节点名	信息集名	权限	口令
node1	info1	read	123
node2	info2	update	AAA
node3	info1	write	BCD
:	:	:	:

如果需要控制信息集中某部分信息（例如某些字段或符合某条件的记录等）的操作权限，表中还可以加入字段名或相应的条件信息。

当某节点收到访问请求时，根据节点名和要访问的信息集名判断其操作是否合法，口令正确与否。若非法则拒绝访问，并记录在案，并返回出错信息。

二、系统实现时信息的安全保密措施

系统分析和设计阶段规划的信息保护体系，要在文件或数据库设计和程序设计时具体实现。在程序设计中，为完成信息保护体系的要求，可以采用很多措施。下面介绍几种：

1.动态菜单

所谓动态菜单就是同一个菜单从不同权限的系统用户进入系统，看到的将是不同的菜单提示，从而实现不同的操作。例如，某银行对财会业务处理系统设立三类用户：记帐、平帐和系统管理，而这三类用户进入系统主菜单时分别看到的是主菜单 1、2、3。

主菜单 1	主菜单 2	主菜单 3
1.记分户帐	1.平帐	1.系统备份
2.查询	2.打印分户帐	2.系统恢复
3.修改口令	3.查询	3.查询
4.退出	4.修改口令	4.修改口令
	5.退出	5.退出

使用动态菜单，可以使整个系统统一在一个菜单树下，但从不同权限的用户进入，又可以完成不同的操作，同时又不给操作员被限制的感觉，又防止了非法操作。

2.窗口封锁技术

该技术就是从某一系统用户进入系统只能按相应的窗口提示进行操作，其它操作都不能做，永远不会出现操作系统提示符。进而还可以限制某一终端只能以某一系统用户的名字进入系统，用其它用户名登录无效，这些可以通过使用系统登录文件和将 CTRL-C 等强行终止键屏蔽来实现。

3.口令

这是常用的保护措施之一。除利用多用户操作系统提供的口令功能外，某些极重要的操作之前还可再加口令保护，例如人事信息修改前，再询问一次口令。口令值最好不要嵌入程序，应隐蔽到某数据文件中，否则修改口令就要修改程序，这是很不方便的。

4.签名

这种方法在银行或财会记帐程序中经常使用。方法是分配给每个记帐员一个系统用户名，该用户的口令仅需该记帐员掌握，且可随时修改。记帐员每次记帐都用自己的系统用户名登录进入系统，每记一笔帐，系统自动在该笔帐后边签上一个特殊的名字。这样，一旦发现帐目有错就可查到由谁负责。

参考文献：

*[1]*曹文君，“提高微机数据库信息安全保密性的措施”，《电脑应用时代》，*1988* 年第三期。

*[2]*中科院成都计算所情报室，《软件加密与解密技术及其应用。实例专辑》，*1989* 年。