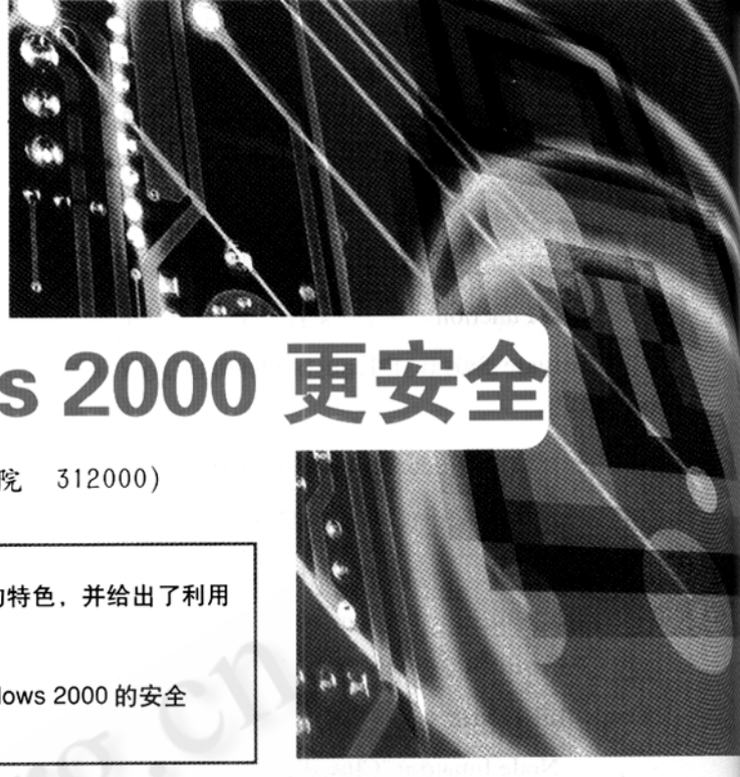

利用注册表使 Windows 2000 更安全

孟万化 （浙江绍兴文理学院 312000）

摘要：阐述了Windows2000的安全系统及其注册表编辑器的特色，并给出了利用Windows 2000注册表来提高Windows2000系统安全的实例。

关键词：注册表 事件 权限 子项 键值 Windows 2000Windows 2000的安全

1 Windows 2000的安全

Windows NT/2000具有一个完整的安全系统，它是操作系统不可分割的一部分，而且不能被禁用，这是与Windows 95/98所不同。Windows 2000的安全系统负责在用户登录系统时验证用户的身份；控制用户能够访问的资源、文件和应用程序；负责维护对用户活动期间生成的安全时间进行审核跟踪。

Windows 2000的安全分为三个主要的部分：用户的访问令牌，安全帐号管理器（Security Accounts Manager，SAM）的注册表项中有关每个用户访问权限的信息，以及对系统管理员有可能审核的安全事件的记录。

1.1 访问令牌

访问令牌是由Windows 2000安全系统创建的软件对象，它包含用户当前工作站以及网络中其他计算机上的特权信息。访问令牌包括的信息保存在注册表中，并可在注册表中直接进行操作。访问令牌包括下列信息：①用户安全ID（User Security ID，SID）；②所有者的SID；③用户特权；④组安全ID（Group Security ID）；⑤主组（Primary Group）的SID；⑥默认的访问控制列表（Access Control List，ACL）。

1.2 SAM注册表项

有关用户安全设置的信息保存在注册表配置单元HKEY_LOCAL_MACHINE的一个名为SAM（Security Accounts Manager）的子项中。SAM是Windows 2000负责验证来自各种系统工具用户界面的用户登录信息有效性的服务，同时还提供包含在每个用户访问令牌中的信息。SAM注册表中的信息通常不会被直接操作，而是通过某种管理工具进行操作。

1.3 审核

Windows 2000系统无论何时发生涉及安全的活动，都有可能产生安全事件，这些事件被依次写入一个日志文件，以利于系统管理员审核，及时发现问题，采取有效措施进行维护。这个日志文件由事件查看器控制，但是其设置是在注册表中，而且在需要时可以查看。安全事件包括：①创建新用户/组成员改变；②程序执行/资源被访问；③登录/注销；④安全策略变动；⑤特权的使用；⑥系统事件对安全造成影响。

Windows 2000的安全特性是在用户试图登录到Windows 2000工作站时开始的。输入到登录对话框中的信息一经确认，就被提交给本地安全授权（Local Security Authority，LSA），这是一种根据SAM数据库验证登录信息有效性的系统安全服务。一旦验证登录信息有效，那就会为这一用户创建一个访问令牌并激活，这个令牌与一个或多个可执行程序相结合创建一个主题，然后该主题开始访问系统。LSA使用注册表项来确定上述过程如何进行，因而这个过程可以通过直接操作注册表来变动（如登录过程中显示用户界面）。

Windows 2000支持多台通过Netlogon服务连接到网络上的工作站使用一个安全数据库。Netlogon需要基于域的网络和主域控制器（Primary Domain Controller，PDC），在登录对话框中会显示一个额外的编辑控件，允许输入用来进行Netlogon验证的域名。Netlogon的各种特性可以通过直接操作注册表来控制。

安全问题还会在用户从一台工作站注销并有可能关机时发生。例如，某些用户可能只会显示注销对话框，而另一些用户会在对话框中出现关闭工作或关闭电源的选项。注册表中包含有控制这些特性的条目，可以通过直接操作注册表来控制。

2 Windows 2000的注册表管理

注册表实际上是一个庞大的数据库，其中容纳了应用程序和计算机系统的全部配置信息、中文Windows 2000系统和应用程序的初始化信息、应用程序和文档文件的关联关系、硬件设备的说明、状态和属性以及各种状态信息和数据等，它在系统的启动、运行与操作过程中起着重要的作用。管理Windows 2000注册表的方法很多，一般可以采用使用“注册表编辑器”直接修改、用户修改“控制面板”中的配置图标、用户安装新的驱动程序和应用程序、使用“系统策略编辑器”和使用注册表修改工具（如“超级兔子魔法设置2.94”For Windows 2000、豪侠99等）等方法。

注册表编辑器是管理Windows 2000注册表最常用的工具，它本身还具有保存和恢复整个注册表或所选项和值的树的高级功能。Windows 2000提供了两种类型的注册表编辑器，一种是16位的regedit.exe，另一种是32位注册表编辑器Regedt32.exe。regedit.exe是从原来的windows 95/98继承下来的，它与Windows 95/98的注册表编辑器的外观与操作方式相似，Windows2000之所以还保留这个程序，考虑的是熟悉Windows 95/98注册表编辑器的用户，但是由于使用环境不同了，即使仍然是16位的编辑器，也和Windows 95/98有较大区别：打开以后，主键变为5个了，而不是原来Windows95/98中的六个。这五个主键是：

① HKEY_LOCAL_MACHINE；

② HKEY_USER；

③ HKEY_CURRENT_USER；

④ HKEY_CLASSES_ROOT；

⑤ HKEY_CURRENT_CONFIG.

经比较，就知道少了一个主键，多数主键之下的第一层子键比Windows 95/98少，且更为简捷合理。另一个明显的区别就是菜单中多了“连接网络注册表”和“断开网络注册表”两项。Regedit简单易用，但是功能相对有限，支持的数据类型只有两种：字符串（REG_SZ）及二进制（REG_BINARY）。32位注册表编辑器Regedt32.exe是专为Windows 2000设计的注册表修改工具，它位于%Windir%＼System32文件夹中，界面与功能都要优于16位的编辑器。在“开始”菜单里，没有对应的图标或者菜单选项可供直接调用。当然，您既可以使用Windows资源管理器将它拖到桌面上创建一个快捷方式，也可以使用“开始”菜单中的“运行”命令启动注册表编辑器。

Regedt32编辑器的界面和Regedit编辑器的界面不同，Regedt32编辑器共有五个子窗口，每个子窗口对应于一个本地机器的主键。Regedit中的每个主键，在Regedt32中都占用一个子窗口，子窗口中每个主键之下的分支与原来也有很大不同，主要是其分组方法和键值放置位置上，与Windows95/98的注册表结构有较大的变动，但每个主键名称和储存的信息和Windows95/98中的规定是一样的。Regedt32编辑器的菜单中，新增加的主要的有“安全”，可以用来设定对注册表修改的权限。另外是为操作或显示方便，有“选项”、“窗口”、“目录树”。在“注册表”菜单项下主要新增的有“加载配置单元”和“卸载配置单元”命令项，可以将保存为文件的配置元加载到注册表中，或从系统删除加载的配置元。“加载配置元”和“卸载配置元”只影响HKEY_USERS和HKEY_LOCAL_MACHINE预定义项，而且只有在选定这些预定义项时才成为活动状态。当配置元加载到注册表时，配置元成为这些预定义项的一个子项。Windows 2000注册表条目共有11种可识别的数据类型，而每一种原始数据格式类型在Regedt32.exe中都有一个专门的编辑器，Regedt32编辑器中的键值编辑器使用极为方便。

3 ZK(直接修改注册表使系统更加安全的几个应用ZK)

如何让计算机系统更好地、安全地运行，是每一个系统管理员或用户都在思考的问题。Windows 2000注册表的有些有关安全条目和值不能用Regedit编辑器直接修改，必须使用Regedt32编辑器才能直接改动。下面列举利用Regedt32编辑器修改Windows2000注册表实现对系统的安全控制的的几个实用技巧。

3.1 安全权限

Windows2000对不同级别的用户，所赋予的修改注册表权限也有所不同，但可以修改这种权限。首先运行注册表编辑器Regedt32打开注册表，选定一个确定的主键或子键，鼠标左键单击菜单中的“安全”项，在下拉菜单中选取“权限…”命令项，在对话框中默认显示的安全权限分为好几种，而且在不同的键值下，出现的种类一般也有所不同，但每个键所具有的种类是：权限最高系统管理员、超级用户、系统用户，还可能出现的有：建立者和受限制用户。无论哪一种用户，权限是“读取”或“完全控制”。根据需要对每一项可以选“允许”，也可以选“拒绝”。其适用范围是该层键值以及从属于更下层的键值。另外，也可以添加新用户和设定权限。

3.2 安全事件

Windows 2000 提供了把有关安全的事件写入日志文件的能力。而注册表包含控制这个日志文件怎样创建和维护的设置。

(1) 启动注册表编辑器Regedt32，将所有的配置单元分别显示在不同的层叠子窗口中。

(2) 选择“窗口”菜单项HKEY_LOCAL_MACHINE，其子窗口显示。

(3) 使用左窗口的树型控件定位到 SYSTEM ＼ CurrentControlSet ＼ Services ＼ EventLog ＼

Security子项。单击该子项选取，在右窗口中显示其值。对于定位在不同的值的条目，进行相应的修改或设置，就可以达到相关安全事件的控制。下表列举出一些安全事件相关的条目（如果没有表中的条目可以进行创建）：

条目	功能
File	用来保存安全事件日志文件的路径和文件名
MaxSize	安全事件日志文件的最大容量（缺省值512KB）
Retention	事件保存在日志文件中的秒数（缺省值604800秒，即7天）
Sources	事件记录到安全事件日志中的所有服务、应用程序、应用程序组的名称
[appname] ＼Even MessageFile	包含文档的路径和文件名，这文档包含有安全事件日志文件标识符的事件描述
[appname] ＼ Category MessageFile	包含文档的路径和文件名，这文档包含对安全事件日志文件标识符的类别描述
[appname] ＼ Types Supported	包含这一应用程序在安全事件日志文件标识符中使用的事件类型值

表 1 与安全事件相关的条目

注：表中 [appname] 表示应用程序或服务名称的子项。

3.3 安全 Netlogon 服务

Windows 2000 网络一部分的工作站可以使用远程数据库进行登录验证。有许多注册表条目可以控制Netlogon的操作。

(1) 启动注册表编辑器Regedt32，将所有的配置单元分别显示在不同的层叠子窗口中。

(2) 选择“窗口”菜单项HKEY_LOCAL_MACHINE，其子窗口显示。

(3) 使用左窗口的树型控件定位到 SYSTEM ＼ CurrentControlSet ＼ Services ＼ Netlogon ＼ Parameters 子项。单击该子项选取，在右窗口中显示其值。对于定位在不同的值的条目，进行相应的修改或设置，就可以得到相关 Netlogon 的控制。例如：

① 访问控制用于登录的脚本的路径：定位到值 Scripts 的条目，使用字符串编辑器把Scripts的值改为包含登录脚本的文件夹的完整的路径名。

② 防止经由网桥/路由器的信箱消息阻塞：定位到值MailslotDuplicateTimeout 的条目，使用 Dword 编辑器把MailslotDuplicateTimeout 的值改为0。

3.4 注销或关机安全

可以通过注册表条目创建或修改其值，使得当用户准备从Windows 2000 中注销或关机时，在“注销”或“关机”对话框中确定显示的选项，达到系统安全、快速地注销或关机的目的。现以设置“关闭系统”选项为例：

(1) 启动注册表编辑器Regedt32，将所有的配置单元分别显示在不同的层叠子窗口中。

(2) 选择“窗口”菜单项HKEY_CURRENT_USERS，其子窗口显示。

(3) 使用左窗口的树型控件定位到Software＼Microsoft＼Windows＼CurrentVersion＼Explorer子键分支。

(4) 在此子键分支中查找或创建一个键值名ShutdownSetting，其类型为REG_SZ，值可以设置为的数值有：1（关机）、2（重新启动系统）和3（关闭所有程序，并以其他身份登录系统）。

(5) 注销当前用户，重新登录即可生效。

4 结束语

利用注册表设置 Windows 2000 系统的安全性，还可从计算机的操作者的角度来考虑。计算机操作者一般分为三大类：第一类是系统管理员，拥有对系统的绝对控制权，一般来说没有必要对系统管理员的权限进行限制；第二类是一般用户，他们使用计算机完成各种工作，必须获得一定的权限，但也要防止他们超越权限或破坏系统；第三类是非法用户，他们根本无权使用计算机，对他们一定要将系统的一切功能全部屏蔽，使之无机可入。这样，对于不同的用户，进行适当的权限设置，既保证了用户的安全，又禁止用户越权操作，防止非法用户“入侵”，确保系统安全。这方面有许多注册表应用技巧，由于篇幅的限制，不一一列举了。本文只介绍少许应用注册表的实例，其目的主要还是在于显示注册表对 Windows2000 系统的安全的神奇作用。同时也想抛砖引玉，希望大家积累自己需要的注册表使用实例，通过对注册表的修改，使计算机用户对系统的安全实现控制。■

参考文献

曹国均等，WINDOWS 2000 中文版注册表使用开发与实例 [M]，北京清华大学出版社，2000。