操作系统安全简论(续上期)

Windows NT操作系统安全(二)

卿斯汉 (中科院信息安全技术工程研究中心主任 100080)

2.3 登录

用户登录Windows NT的过程比较繁琐，但每一步对建立一个安全环境和用户能够完成有用的工作都是必要的。用户本地登录与在域范围内登录到Windows NT计算机的步骤稍有不同，登录步骤如下：

(1) 用户按Ctrl+Alt+Del键，引起硬件中断，被操作系统捕获。这样使操作系统激活WinLogon进程。

(2) WinLogon进程通过调用标识与鉴别DLL，将登录窗口(帐号名和口令登录提示符)展示在用户面前。

(3) WinLogon进程发送帐号名和加密口令到本地安全认证(LSA)。如果用户帐号是Windows NT计算机的本地帐号，则本地安全认证访问安全帐号管理数据库。否则，本地安全认证就通过NetLogon服务建立一条安全通道访问主域服务器或备份域服务器的安全帐号管理模块(SAM)，鉴别登录请求。

(4) 如果用户具有有效的用户名和口令，则本地安全认证产生一个访问令牌，包括用户帐号SID和用户工作组SID。访问令牌也得到用户的特权(LUID)，然后该访问令牌传送回WinLogon进程。

(5) Winlogon进程传送访问令牌到Win32模块，同时发一请求，以便为用户建立登录进程。

(6) 登录进程建立用户环境，包括启动Desktop Explorer和显示背景等。

登录过程如图2所示：

如果要登录到网络上的Windows NT计算机(假定为服务器)，则步骤如下：

①用户将用户名和口令输入到网络客户机软件的登录窗口。

②该客户机软件打开NetBIOS连接到服务器上的NetLogon服务。该客户机软件对口令加密，发送登录证书到服务器的WinLogon进程。

③服务器的WinLogon进程发送帐号名和加密口令到本地安全认证(LSA)。如果用户帐号是Windows NT计算机的本地帐号，则本地安全认证访问安全帐号管理数据库。否则，本地安全认证通过NetLogon服务建立一条安全通道访问主域服务器或备份域服务器的安全帐号管理(SAM)，鉴别登录请求。

④如果用户具有有效的用户名和口令，则本地安全认证产生一个访问令牌，包括用户帐号SID和用户工作组SID。访问令牌也得到用户的特权(LUID)，然后该访问令牌传送回WinLogon进程。

⑤WinLogon进程传送访问令牌到Windows NT的Server服务，它将访问令牌与被客户机打开的NetBIOS连接联系起来。在具有访问令牌所建证书的服务器上，可完成任何在NetBIOS连接时所发送的其他操作(如读文件、打印请求等)。

网络登录过程如图3所示：

每次登录到Windows NT都产生一个访问令牌，访问令牌是用户帐号和工作组帐号的安全标示符(SID)及用户LUID(用户特权和工作组特权)组合而成的。访问令牌有两个目的：

→访问令牌保存全部安全信息，可以加速访问验证过程。当某个用户进程要访问某个对象时，安全子系统检查该进程的访问令牌，判断该用户的访问特权。

→每个进程均有一个与之相关联的访问令牌，因此，每个进程都可以在不影响其他代表该用户运行的进程的条件下，在某种可允许的范围内修改进程的安全特征。

2.4 资源访问控制

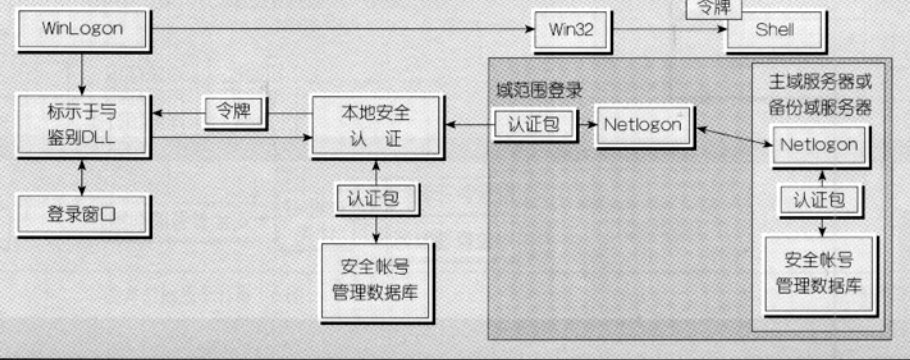
Windows NT的安全性达到了橘皮书C2级，实现了用户级自主访问控制。它的访问控制机制如图4所示。

为了实现进程间的安全访问，Windows NT中的对象采用了安全性描述符(Security desciptor)。安全性描述符主要由用户SID (Owner)、工作组SID (Group)、访问控制列表(DACL)和系统访问控制列表(SACL)组成，安全性描述符如图5所示。

当某个进程要访问一个对象时，进程的SID与对象的访问控制列表比较，决定是否可以访问该对象。访问控制列表由访问控制项(ACE)组成，每个访问控制项标识用户和工作组对该对象的访问权限。一般情况下，访问控制列表有3个访问控制项，分别代表如下含义：拒绝对该对象的访问；允许对该对象读取和写入；允许执行该对象。访问控制列表首先列出拒绝访问的访问控制项，然后才是允许的访问控制项。对访问控制列表判断的规则如下：

(1) 从访问控制列表的头部开始，检查每个访问控制项，看是否显式地拒绝用户或工作组的访问。

图2 登录过程



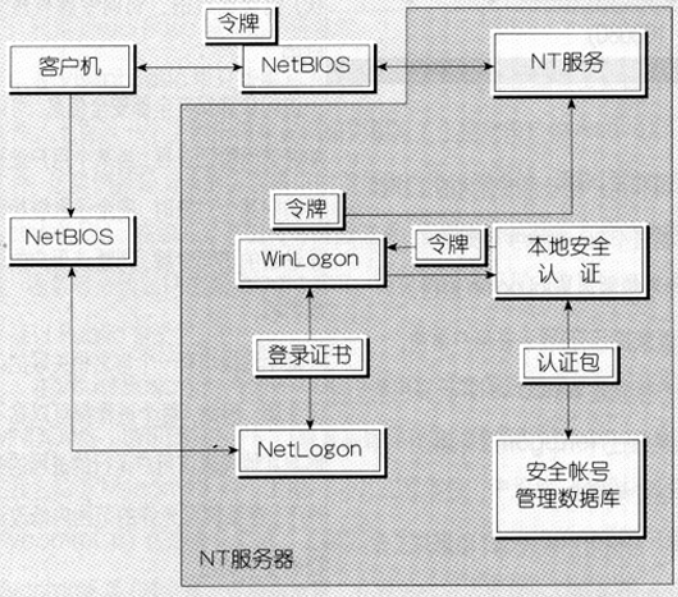


图3 网络登录Windows NT服务器的过程

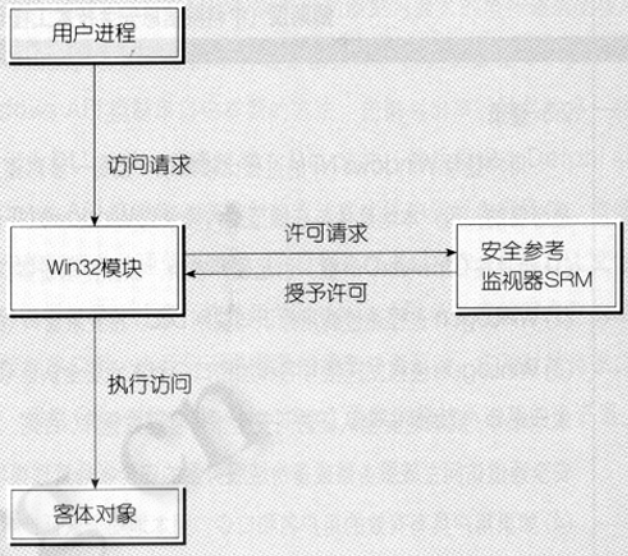


图4 Windows NT的客体访问示意图

(2) 继续检查，看进程所要求的访问类型是否显式地授予用户或工作组。

(3) 重复1、2步，直到遇到拒绝访问，或是累计到所有请求的权限均被满足为止。

(4) 如果对某个请求的访问权限在访问控制列表既没有授权也没有拒绝，则拒绝访问。因此，访问令牌和访问控制列表就是进程访问对象的"规则"。在Windows NT中，用户进程并不直接访问对象，Win32代表进程访问对象。这样做的主要原因是为了使程序较为简单，程序不必要知道如何直接控制每类对象，请操作系统去做此工作。另一好处是，由操作系统负责实施进程对对象的访问，可使对象更加安全。

当一进程请求Win32执行对象的一种操作时，Win32借助安全参考监视器进行校验。安全参考监视器首先检查用户的特权，然后再将进程的访问令牌与对象的访问控制列表进行比较，决定进程是否可以访问该对象。另外，在Windows NT中，特权优于对象的权限，这就是为什么文件的拥有者把NO Access的权限给予Everyone，但是管理员(Administrator)帐号还是能够取得文件的拥有权。

Windows NT初始时禁止所有用户可能拥有的特权，而当进程需要某个特权时，才打开相应的特权。由于每个进程均有自己的访问令牌，其中包含用户的特权信息，因此，进程所打开的特权只在当前进程内有效，而不会影响其他进程。

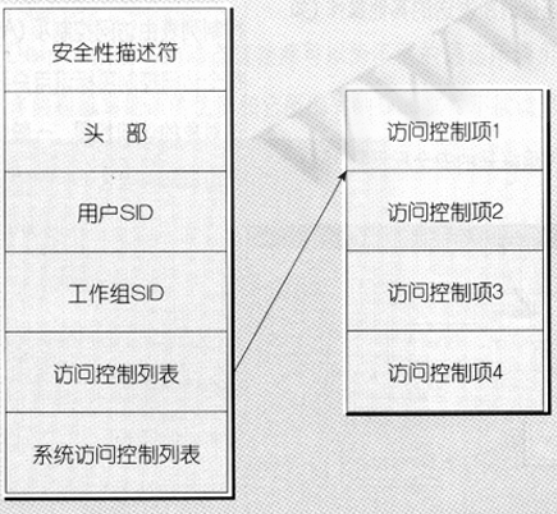


图5 安全性描述符的构成

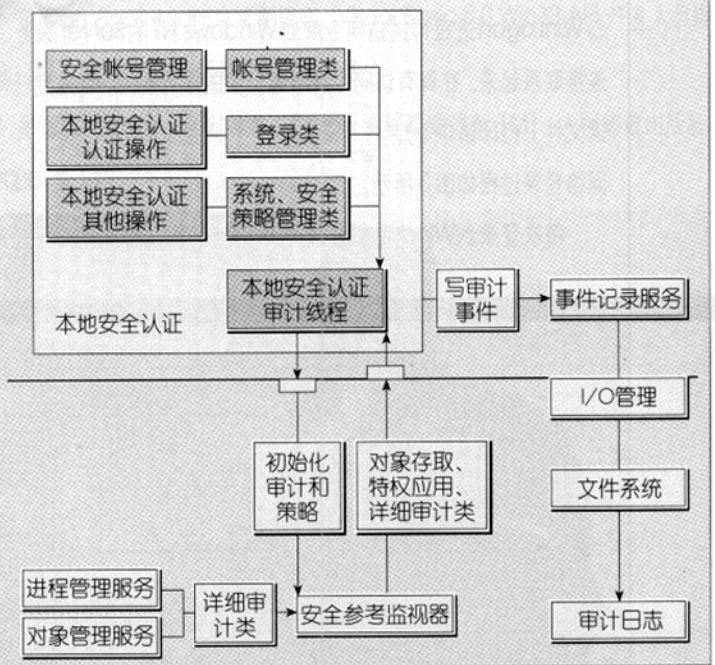


图6 审计子系统结构图

Windows NT安全子系统的另外一个重要特点是“假扮”。这种特点非常适用于客户机/服务器模式。当客户机和服务器通过远程过程调用连接时，服务器可以临时“假扮”成客户机身份，从而按照客户机的权限访问对象。当访问结束后，服务器恢复自己的真实身份。

2.5 Windows NT的审计子系统

配置Windows NT达到橘皮书C2级，必须要有审计功能。系统运行中产生3类日志：系统日志、应用程序日志和安全日志，可使用事件查看器浏览和按条件过滤显示。前两类日志任何人都能查看，它们是系统和应用程序生成的错误警告和其他信息；安全日志则对应审计数据，它只能由审计管理员查看和管理。前提是它必须存于NTFS文件系统中，使Windows NT的系统存取访问控制(SACL)生效。

Windows NT的审计子系统缺省是关闭的，审计管理员可以在服务器的域用户管理或工作站的用户管理中打开审计并设置审计事件类。事件分为7类：系统类、登录类、对象存取类、特权应用类、帐号管理类、安全策略管理类和详细审计类。对于每类事件，可以选择审计失败还是成功的事件或是二者都审计。对于对象存取事件类的审计，管理员还可以在资源管理器中进一步指定各文件和目录的具体审计标准，如读、写、修改、删除、运行等操作，也分为成功和失败两类进行选择。对注册表项及打印机等设备的审计类似。

审计数据以二进制结构文件形式存于物理磁盘，每条记录包括事件发生时间、事件源、事件号和所属类别、机器名、用户名和事件本身的详细描述。

用户登录到系统时，WinLogon进程为用户创建访问令牌，包含用户及所属组的安全标识符(SID)，作为用户的身份标识。文件等客体则含有自主访问控制列表(DACL)，标明谁有权访问，还含有系统访问控制列表(SACL)，标明哪些主体的访问需要被记录。用户进程访问客体对象时，通过WIN32子系统向核心请求访问服务，核心的安全参考监视器(SRM)将访问令牌与客体的DACL进行比较，确定是否拥有访问权限，同时检查客体的SACL，确定本次访问是否落在既定的审计范围内，是则送至审计子系统。整个审计过程可用图6表示：

审计数据如图7所示，这是Windows2000事件查看器中列出的部分登录事件，其中用户lhf的一次登录失败。

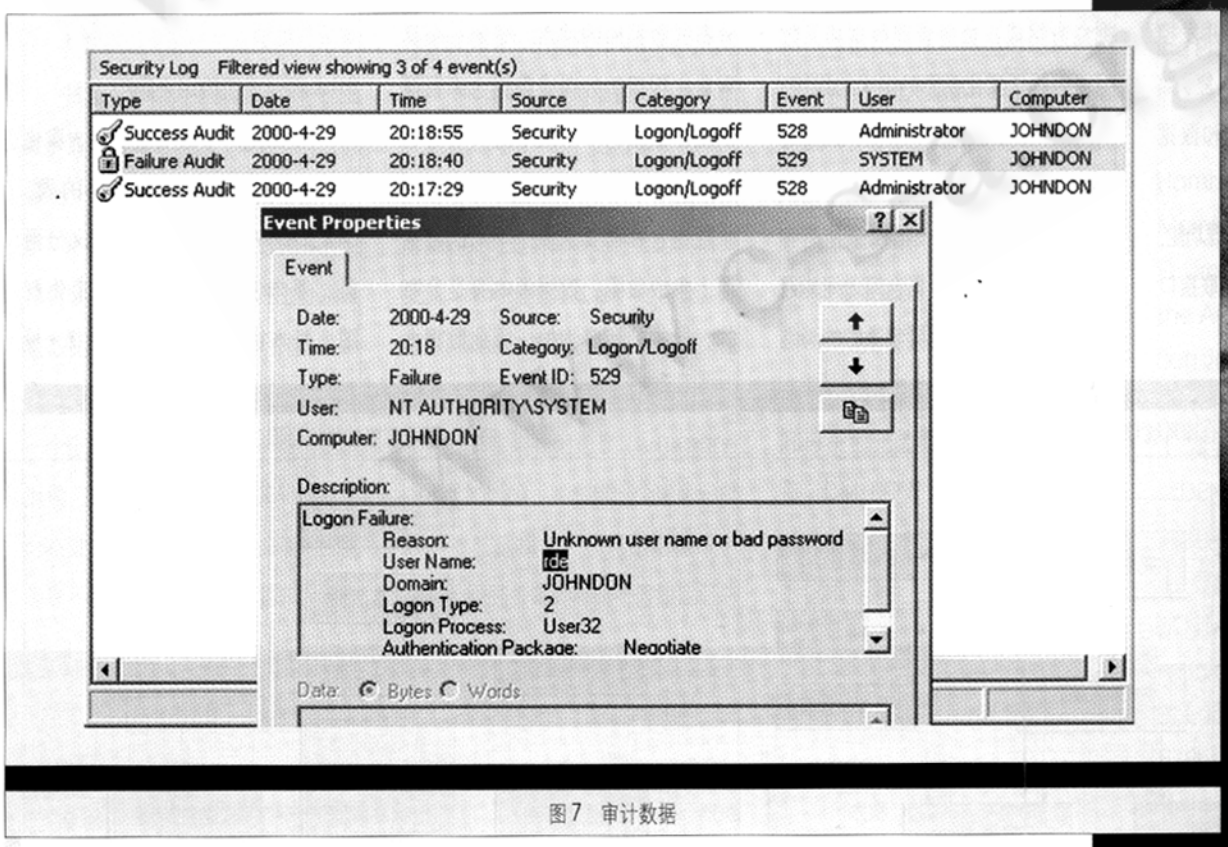


图7 审计数据