浅析Windows 2000的用户登录身份验证模型

马金钢　贺轶斐　(南京解放军理工大学气象学院　211101)

摘要：本文通过替换GINA DLL达到跟踪Windows 2000用户登录认证过程的目的，从跟踪纪录中我们可分析得出系统对用户的身份认证过程，很好的印证了Windows 2000的用户登录认证模型，加深了对该模型的认识。

关键词：GINA DLL　登录认证

Windows 2000以其良好的稳定性和安全性受到了人们的青睐，目前已逐渐在广大电脑使用者中间普及。Windows 2000安全系统是一个集成子系统，其组成部分有：本地安全授权(Local Security Authority)，安全访问监督(Security Reference Monitor)。另外，Windows 2000还提供以下安全机制：登录认证(Winlogon)，存取控制(Access Control)，存取标识(Access Token)，存取控制列表(Access Control List)。这些功能与安全账户管理、本地安全管理和安全访问监督相结合，提供了形成Windows 2000安全机制支柱的许多相互集成的性能。

登录认证通过是合法用户获得使用系统资源的前提条件，是Windows 2000安全的第一道屏障。登录认证是Windows 2000系统的一个组件，它管理用户登录认证过程，提供了交互式的图形界面。登录认证执行程序(Winlogon.exe)、图形化的登录认证动态链接库(GINA DLL)和网络服务提供者(Network Provider)三部分构成了登录认证组件。登录认证动态链接库是可被用户替换的部分，它集成了登录认证的核心部分。

1　建立新的登录认证动态链接库

默认情况下系统使用system32目录中的msgina.dll。用户可以修改注册表使用自己的GINA DLL，具体做法是在＼HKEY-LOCAL-MACHINE＼Software＼Microsoft＼Windows NT＼CurrentVersion＼Winlogon项中添加字符串值GinaDll，将其值设为用户的Dll文件名。注意应将用户自己的Dll文件拷贝到system32目录下。

在新的动态链接库中记录Winlogon.exe调用GINA DLL中的函数，然后调用msgina.dll中相应的函数，代码如下：

```
//gina32.cpp 文件
#define UNICODE
#include <windows.h>
#include <stdio.h>
#include <lm.h>
#include "Winwlx.h"
HMODULE i=NULL;
FARPROC a;
int (--stdcall *WlxWkstaLockedSAS1)(PVOID, DWORD);
.....(略)
BOOL WINAPI DllMain (HANDLE hInst,
ULONG ul-reason-for-call,
LPVOID lpReserved)
{  if(i==NULL) {
        i=LoadLibrary(L" msgina.dll");
// 装载原动态库
        SaveRecord(L" load msgina.dll"); }
// 纪录函数，下同
else return 1;
if(i!=NULL) {
    a=GetProcAddress(i," WlxWkstaLockedSAS");// 取得原同名函数地址
        WlxWkstaLockedSAS1=(int (--stdcall *)(PVOID,DWORD))a;
        .....(略)
    } else return 0;
    return 1;
}
int PASCAL FAR WlxWkstaLockedSAS(PVOID pWlxContext,DWORD dwSasType)
{SaveRecord(L" WlxWkstaLockedSAS");
// 记日志，当然也可以是您的模块
return WlxWkstaLockedSAS1(pWlxContext, dwSasType);
}
.....(略)
//gina32.def 文件
LIBRARY "gina32"
EXPORTS
WlxWkstaLockedSAS @1
.....(略)
```

在程序中实现了msgina.dll导出的18个以Wlx开头的函数，编译生成gina32.dll。

2　替换GINA DLL，根据调试输出分析Windows 2000登录认证过程

将上面编译生成的gina32.dll复制到system32目录中，修改注册表中GinaDll的数值为"gina32.dll"。重新启动计算机调试可得到调试的结果如下，其中分析说明部分是手动

添加的。

load msgina.dll

WlxNegotiate [IN] dwWinLogonVersion: 65539;[OUT] pdwDllVersion:0

// 判断执行文件和 GINA DLL 的版本是否相符

WlxInitialize [IN] lpWinsta:WinSta0 // 初始化 GINA DLL 环境

WlxDisplayStatusMessage //显示状态信息

WlxDisplayStatusMessage

WlxDisplayStatusMessage

WlxRemoveStatusMessage // 停止状态信息的显示

WlxRemoveStatusMessage

WlxDisplaySASNotice // 等待用户按下 CTRL+ALT+DEL 触发 SAS 事件

WlxRemoveStatusMessage

WlxLoggedOutSAS // 等待用户提供验证信息进行身份确认

WlxDisplayStatusMessage

WlxDisplayStatusMessage

WlxRemoveStatusMessage

WlxRemoveStatusMessage

WlxActivateUserShell [IN] pszDesktop Name:WinSta0 \ Default

// 启动用户命令解释程序

WlxRemoveStatusMessage // 至此，系统启动成功，用户获得控制权。下面锁定计算机

WlxLoggedOnSAS // 显示对话框与用户交互，判断用户是否要锁定计算机

WlxDisplayLockedNotice // 显示计算机已锁定的信息，锁定成功。下面解锁

WlxWkstaLockedSAS // 创建对话框提供用户在此验证身份，成功则解锁。下面关机

WlxIsLogoffOk //判断用户注销是否成功

WlxRemoveStatusMessage

WlxDisplayStatusMessage

WlxDisplayStatusMessage

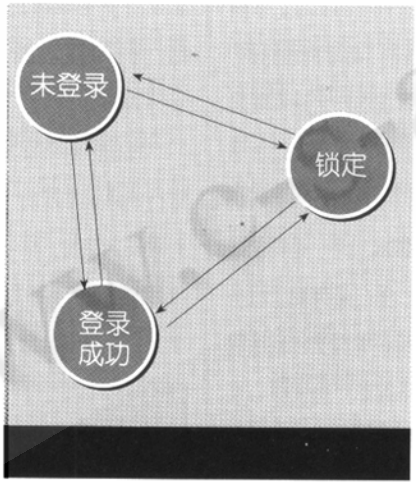
WlxShutdown // 显示关机信息

WlxDisplayStatusMessage

WlxRemoveStatusMessage

3 总结理解 Windows 2000 的登录认证模型

由上述分析可以看出，GINA DLL 是整个登录认证系统的核心，Winlogon 是通过调用 GINA DLL 来完成整个登录认证过程的。在登录认证过程中，Winlogon 组件有三个状态：未登录状态(Logged-out State)、登录成功状态(Logged-on State)、锁定状态(Workstation-locked State)，如下图所示：(箭头表示过渡关系)



3.1 未登录状态

当组件处于未登录状态时，用户需提供身份认证信息以使自己迅速得到认证。如果用户提供了正确的认证信息，用户将登录成功，命令解释程序（如 Explore.exe）将在操作桌面上运行。组件转变为登录成功状态。

3.2 登录成功状态

当组件处于登录成功状态时，用户可以与命令解释程序和其他活动的应用程序交互，可以做自己的工作。从登录成功状态，用户既可以停止所有的工作而注销自己，也可以锁定计算机暂时离开所有工作。如果用户决定注销自己时，登录认证组件将结束所有与此次登录有关的进程，计算机可由其他用户使用。而如果用户只是想锁定计算机，登录认证组件将转变为锁定状态。

3.3 锁定状态

当用户处于锁定状态时，如果用户没有提供与最初登录成功时使用的身份认证信息一致的信息解锁计算机或者管理员没有强制用户注销时，计算机将一直显示一个安全桌面。如果计算机被解锁，操作桌面将显示，所有的工作将继续进行。但是当管理员提供管理员的认证信息解锁计算机时，上次登录的用户的所有进程都会被停止，登录认证组件转变为未登录状态。

4 结束语

深入了解了登录身份认证模型后，我们可以完全替换GINA DLL以实现一些特有的功能。如记录用户使用计算机的时间及次数，记录用户的登录认证信息以确认合法用户等等。

参考文献

1 David J.Kruglinski等著，Visual C++6.0 技术内幕（第五版）(M)，北京希望电子出版社，1999.5。

2 the MSDN Library，Microsoft Corporation，2000.7。