МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

КУРГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра «Безопасность информационных и автоматизированных систем»

API – ФУНКЦИИ ДЛЯ РАБОТЫ С ПРИВИЛЕГИЯМИ

Методические указания
к выполнению лабораторной работы
по дисциплине «Безопасность операционных систем»
для студентов специальностей 090105, 090303, 090900

Курган 2012

Кафедра: «Безопасность информационных и автоматизированных систем»

Дисциплина: «Безопасность операционных систем» (специальность 090105, 090303, 090900)

Составил: ст. преподаватель А.Г. Рабушко

Утверждены на заседании кафедры « 21 » октября 2011 г.

Рекомендованы методическим советом университета « 21» ноября 2011 г.

ПРИБОРЫ, ОБОРУДОВАНИЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1 Операционная система (Microsoft Windows Xp).
2 Используемая среда программирования (Visual Studio C++).

ЦЕЛЬ РАБОТЫ

Программный доступ к привилегиям процесса.

ТЕОРЕТИЧЕСКОЕ ВВЕДЕНИЕ

Для различных версий операционной системы определяется различное число привилегий. В случае Windows XP имена можно найти в файле winnt.h.

```
#define SE_CREATE_TOKEN_NAME
  TEXT("SeCreateTokenPrivilege")
#define SE_ASSIGNPRIMARYTOKEN_NAME
TEXT("SeAssignPrimaryTokenPrivilege")
#define SE_LOCK_MEMORY_NAME
TEXT("SeLockMemoryPrivilege")
#define SE_INCREASE_QUOTA_NAME
TEXT("SeIncreaseQuotaPrivilege")
#define SE_UNSOLICITED_INPUT_NAME
TEXT("SeUnsolicitedInputPrivilege")
#define SE_MACHINE_ACCOUNT_NAME
TEXT("SeMachineAccountPrivilege")
#define SE_TCB_NAME
TEXT("SeTcbPrivilege")
#define SE_SECURITY_NAME
 TEXT("SeSecurityPrivilege")
#define SE_TAKE_OWNERSHIP_NAME
TEXT("SeTakeOwnershipPrivilege")
#define SE_LOAD_DRIVER_NAME
 TEXT("SeLoadDriverPrivilege")
#define SE_SYSTEM_PROFILE_NAME          TEXT("SeSystemProfilePrivilege")
#define SE_SYSTEMTIME_NAME
TEXT("SeSystemtimePrivilege")
#define SE_PROF_SINGLE_PROCESS_NAME
TEXT("SeProfileSingleProcessPrivilege")
#define SE_INC_BASE_PRIORITY_NAME
TEXT("SeIncreaseBasePriorityPrivilege")
#define SE_CREATE_PAGEFILE_NAME
TEXT("SeCreatePagefilePrivilege")
#define SE_CREATE_PERMANENT_NAME
TEXT("SeCreatePermanentPrivilege")
#define SE_BACKUP_NAME
TEXT("SeBackupPrivilege")
#define SE_RESTORE_NAME
```

```
TEXT("SeRestorePrivilege")
#define SE_SHUTDOWN_NAME
TEXT("SeShutdownPrivilege")
#define SE_DEBUG_NAME
TEXT("SeDebugPrivilege")
#define SE_AUDIT_NAME
TEXT("SeAuditPrivilege")
#define SE_SYSTEM_ENVIRONMENT_NAME
TEXT("SeSystemEnvironmentPrivilege")
#define SE_CHANGE_NOTIFY_NAME          TEXT("SeChangeNotifyPrivilege")
#define SE_REMOTE_SHUTDOWN_NAME
TEXT("SeRemoteShutdownPrivilege")
#define SE_UNDOCK_NAME
TEXT("SeUndockPrivilege")
#define SE_SYNC_AGENT_NAME
 TEXT("SeSyncAgentPrivilege")
#define SE_ENABLE_DELEGATION_NAME
TEXT("SeEnableDelegationPrivilege")
#define SE_MANAGE_VOLUME_NAME
TEXT("SeManageVolumePrivilege")
#define SE_IMPERSONATE_NAME
TEXT("SeImpersonatePrivilege")
#define SE_CREATE_GLOBAL_NAME          TEXT("SeCreateGlobalPrivilege")
```

В ядре привилегии представляются структурой LUID:

```
typedef struct _LUID {
   DWORD LowPart;
   LONG HighPart;
} LUID, *PLUID;
```

Как правило, наличия привилегии в токене доступа процесса недостаточно. Для того, чтобы ее роль осуществилась, привилегия должна быть приведена во включенное состояние.

ПОРЯДОК ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

Для выполнения лабораторной работы необходимо:

Получить хэндл процесса с помощью функции

```
HANDLE WINAPI OpenProcess(
  __in        DWORD dwDesiredAccess,
  __in        BOOL bInheritHandle,
  __in        DWORD dwProcessId
);
```

Если речь идет о текущем процессе, в качестве третьего параметра можно воспользоваться результатом фукции GetCurrentProcessId().

Далее, по хэндлу процесса получить хэндл токена:

```
BOOL WINAPI OpenProcessToken(
  __in         HANDLE ProcessHandle,
  __in         DWORD DesiredAccess,
  __out        PHANDLE TokenHandle
);
```

Для получения списка привилегий в токене вызывается функция

```
BOOL WINAPI GetTokenInformation(
  __in         HANDLE TokenHandle,
  __in         TOKEN_INFORMATION_CLASS TokenInformationClass,
  __out_opt    LPVOID TokenInformation,
  __in         DWORD TokenInformationLength,
  __out        PDWORD ReturnLength
);
```

где в качестве второго параметра используется константа **TokenPrivileges**:

```
typedef enum _TOKEN_INFORMATION_CLASS {
   TokenUser = 1,
   TokenGroups,
   TokenPrivileges,
   TokenOwner,
   TokenPrimaryGroup,
   TokenDefaultDacl,
   TokenSource,
   TokenType,
   TokenImpersonationLevel,
   TokenStatistics,
   TokenRestrictedSids,
   TokenSessionId,
   TokenGroupsAndPrivileges,
   TokenSessionReference,
   TokenSandBoxInert,
   TokenAuditPolicy,
   TokenOrigin,
   MaxTokenInfoClass  // MaxTokenInfoClass should always be the last enum
} TOKEN_INFORMATION_CLASS, *PTOKEN_INFORMATION_CLASS;
```

Выходной буфер форматируется в соответствие со структурой:

```
typedef struct _TOKEN_PRIVILEGES {
```

```
    DWORD PrivilegeCount;
    LUID_AND_ATTRIBUTES Privileges[ANYSIZE_ARRAY];
} TOKEN_PRIVILEGES, *PTOKEN_PRIVILEGES;
typedef struct _LUID_AND_ATTRIBUTES {
    LUID Luid;
    DWORD Attributes;
 } LUID_AND_ATTRIBUTES, * PLUID_AND_ATTRIBUTES;
```

Определены следующие состояния привилегий:

```
#define SE_PRIVILEGE_ENABLED_BY_DEFAULT (0x00000001L)
#define SE_PRIVILEGE_ENABLED            (0x00000002L)
#define SE_PRIVILEGE_REMOVED            (0X00000004L)
#define SE_PRIVILEGE_USED_FOR_ACCESS    (0x80000000L)
```

Получить по имени привилегии ее LUID можно с помощью:

```
WINADVAPI
BOOL
WINAPI
LookupPrivilegeValue(
    __in_opt LPCSTR lpSystemName,
    __in     LPCSTR lpName,
    __out    PLUID   lpLuid
    );
```

Обратная операция:

```
WINADVAPI
BOOL
WINAPI
LookupPrivilegeName(
    __in_opt LPCSTR lpSystemName,
    __in     PLUID   lpLuid,
    __out    LPSTR lpName,
    __inout  LPDWORD cchName
    );
```

Для переведения привилегии токена во включенное состояние используется функция:

```
WINADVAPI
BOOL
WINAPI
AdjustTokenPrivileges (
    __in            HANDLE TokenHandle,
    __in            BOOL DisableAllPrivileges,
```

```
__in_opt    PTOKEN_PRIVILEGES NewState,
__in        DWORD BufferLength,
__out_opt   PTOKEN_PRIVILEGES PreviousState,
__out_opt   PDWORD ReturnLength
);
```

СПИСОК ЗАДАНИЙ

1 Получить привилегии процесса exlporer.exe.

2 Получить привилегии процесса winlogon.exe.

3 Получить привилегии процесса svchost.exe -k LocalService.

4 Проверить наличие привилегии SE_TCB_NAME процесса exlporer.exe.

5 Проверить наличие привилегии SE_TCB_NAME процесса winlogon.exe.

6 Проверить наличие привилегии SE_TCB_NAME процесса.

7 svchost.exe -k LocalService.

8 Проверить состояние привилегии SeRemoteShutdownPrivilege процесса exlporer.exe.

9 Проверить состояние привилегии SeRemoteShutdownPrivilege процесса winlogon.exe.

10 Проверить состояние привилегии SeRemoteShutdownPrivilege svchost.exe -k LocalService.

11 Включить в текущем процессе привилегию SeRemoteShutdownPrivilege.

12 Включить в текущем процессе привилегию SeTakeOwnershipPrivilege.

13 Включить в текущем процессе привилегию SeLoadDriverPrivilege.

14 Включить в текущем процессе привилегию SeLoadDriverPrivilege.

СПИСОК ЛИТЕРАТУРЫ

1. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows. Мастер-класс. – СПб.: Изд-во «Питер», 2005.
2. Дейтел Х.М., Дейтел П.Дж, Чофнес Д.Р. Операционные системы. Ч. 2: Распределенные системы, сети, безопасность. – М.: Бином, 2006.
3. Дейтел Х.М., Дейтел П.Дж, Чофнес Д.Р. Операционные системы. Ч. 1: Основы и принципы. – М.: Бином, 2006.
4. Гордеев А.В. Операционные системы: учебник для вузов. – СПб.: Питер, 2004. – 416 с.
5. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2001. – 544 с.
6. Кастер, Х. Основы Windows NT и NTFS. Русская редакция. – М., 1996.
7. Проскурин, В.Г. Защита в операционных системах. – М.: Радио и связь, 2000.

Рабушко Артур Германович

API – ФУНКЦИИ ДЛЯ РАБОТЫ С ПРИВИЛЕГИЯМИ

Методические указания
к выполнению лабораторной работы
по дисциплине «Безопасность операционных систем»
для студентов специальностей 090105, 090303, 090900

Редактор Е.А. Устюгова

Подписано к печати	Формат 60×84 1/16	Бумага тип. №1
Печать трафаретная	Усл. печ.л. 0,75	Уч.-изд.л.0,75
Заказ	Тираж э/в	Цена свободная

РИЦ Курганского государственного университета.
640669, г. Курган, ул. Гоголя, 25.
Курганский государственный университет.