Systémové programování Windows

Security Descriptor

Obsah

- Prohlížení oprávnění
- SECURITY_ATTRIBUTES
- Security Descriptor
- Default Security Descriptor
- Access Control List
- AccessPermission

Prohlížení oprávnění

- Soubory/adresáře

- http://www.sysinternals.com/
  - Sysinternals Suite: WinObj
    - BaseNamedObjects

SECURITY_ATTRIBUTES


```
typedef struct _SECURITY_ATTRIBUTES {
   DWORD  nLength;
   LPVOID lpSecurityDescriptor;
   BOOL   bInheritHandle;
} SECURITY_ATTRIBUTES,
```

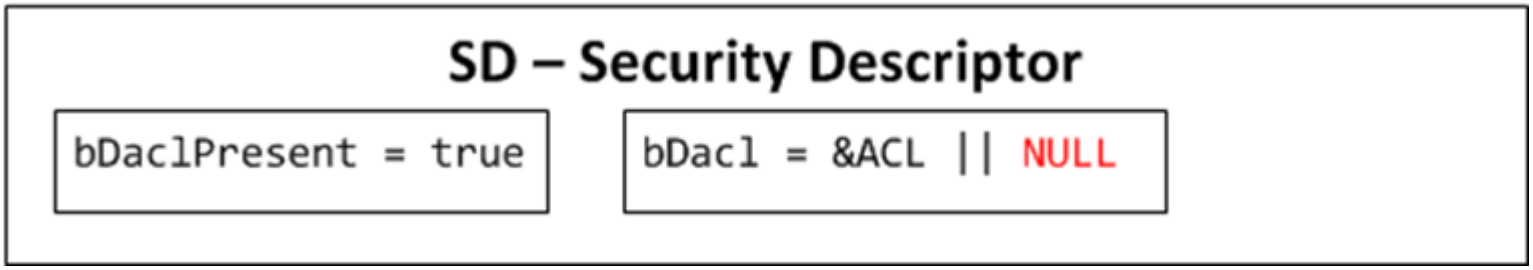
Default Security Descriptor

- Pokud není u objektu uveden Security Descriptor je použit tzv. Default Security Descriptor.

- Default Security Descriptor vychází z access tokenu aktuálního threadu.

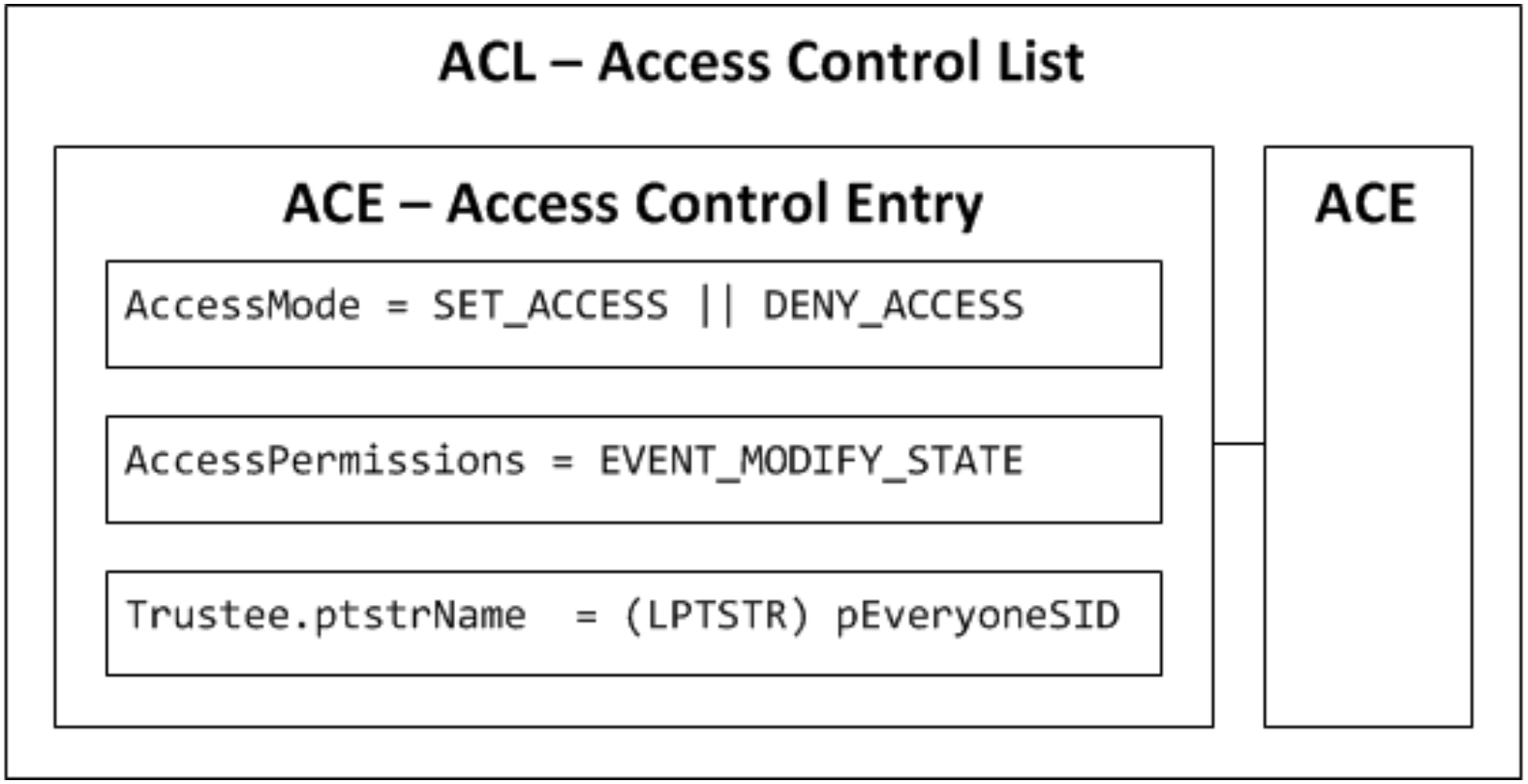
SECURITY_DESCRIPTOR

- Vnitřní struktura není veřejná
  - An owner security identifier (SID)
  - A discretionary access control list (DACL)




```
BOOL WINAPI SetSecurityDescriptorDacl(
      _Inout_   PSECURITY_DESCRIPTOR pSecurityDescriptor
      _In_      BOOL bDaclPresent,
      _In_opt_  PACL pDacl, //NULL - úplný přístup všem
                            //Prázdný - žádný přístup nikomu
      _In_      BOOL bDaclDefaulted);
```

Access Control List



AccessPermission

- **Eventy**
  - **EVENT_ALL_ACCESS** (0x1F0003)
  - **EVENT_MODIFY_STATE** (0x0002)

- **Mutexy**
  - **MUTEX_ALL_ACCESS** (0x1F0001)
  - **MUTEX_MODIFY_STATE** (0x0001)

- **FileMapping**
  - **FILE_MAP_READ** (0x0004)
  - **FILE_MAP_WRITE** (0x0002)

SDDL

- “D:(A;;0x100002;;;WD)(A;;KA;;;BA)”

  http://msdn.microsoft.com/en-us/library/windows/desktop/aa374928(v=vs.85).aspx

- ConvertStringSecurityDescriptorToSecurityDescriptor

```
(   _In_ LPCWSTR StringSecurityDescriptor,
    _In_ DWORD StringSDRevision, // SDDL_REVISION_1
    _Outptr_ PSECURITY_DESCRIPTOR * SecurityDescriptor,
    _Out_opt_ PULONG SecurityDescriptorSize );
```

- ConvertSecurityDescriptorToStringSecurityDescriptor

Díky za pozornost