

# Systemové 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

---

## SA – SECURITY\_ATTRIBUTES

SecurityDescriptor = &SD

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



# Default Security Descriptor

---

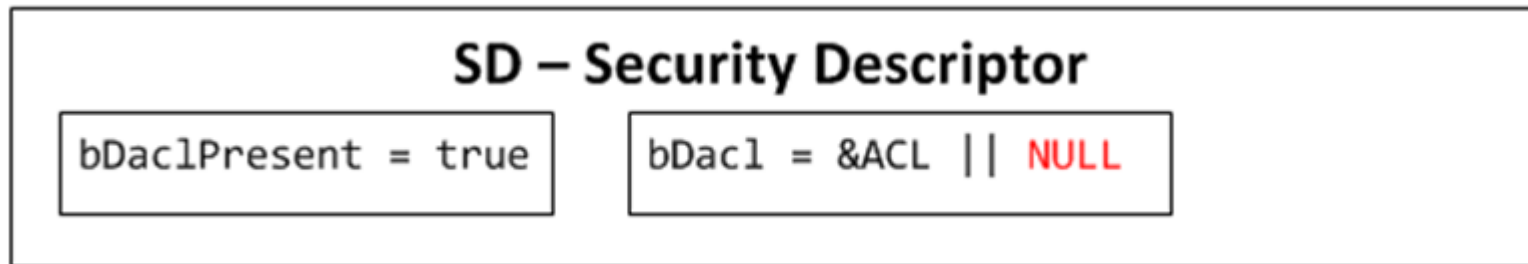
- ▶ Pokud není u objektu uveden Security Descriptor je použit tzv. Default Security Descriptor.
- ▶ Default Security Descriptor vychází z access tokenu aktuálního threadu.



# SECURITY\_DESCRIPTOR

---

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



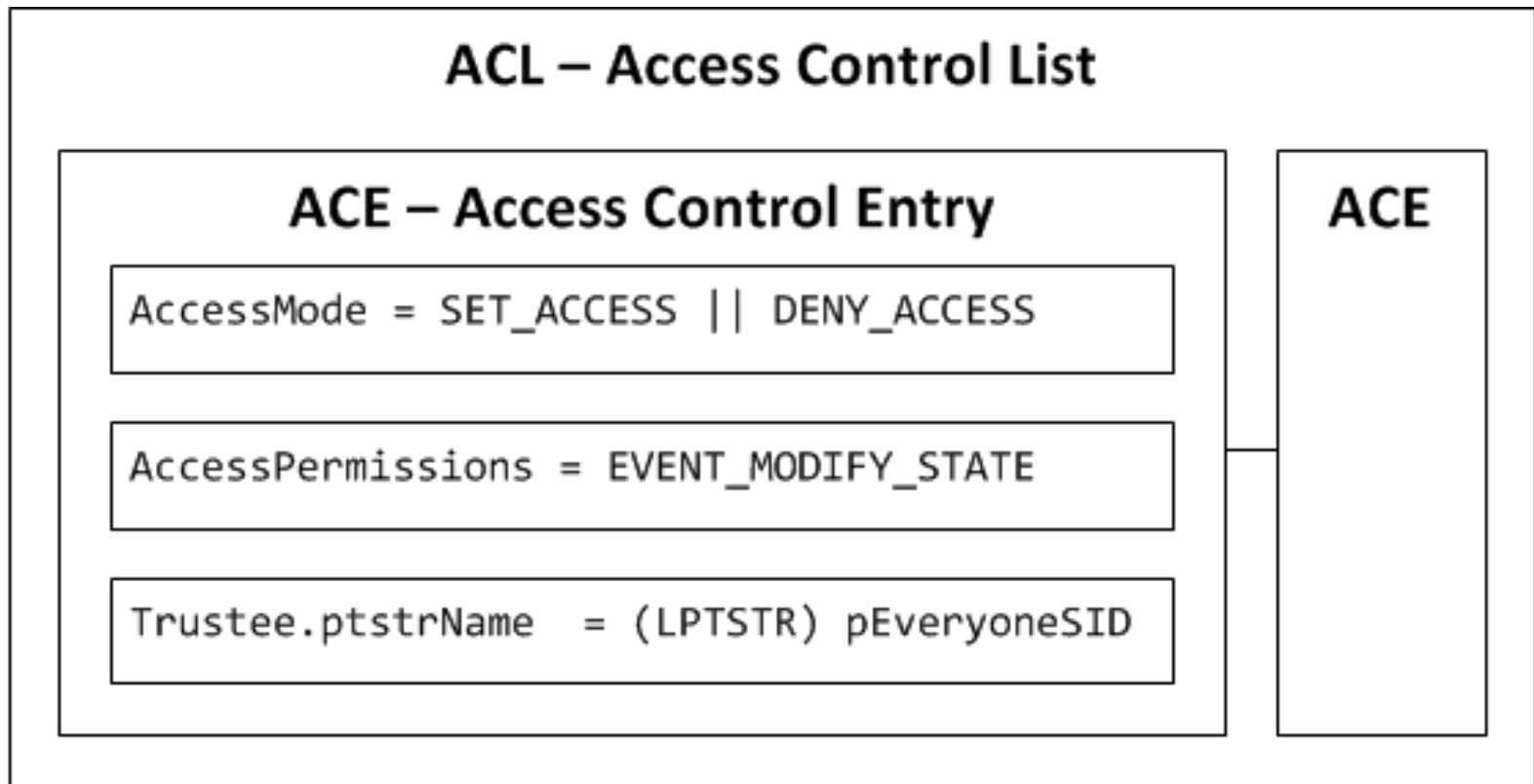
- ▶ 

```
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)
- 





---

Díky za pozornost

