Übungsblatt 5

Übung zur Betriebssystemarchitektur
SS 2006

Michael Schöbel

HASSO-PLATTNER-INSTITUT
für Softwaresystemtechnik

Inhalt

- **Überprüfung von Zugriffsrechten unter Windows**
  - Security Descriptors
  - DACL
- **Windows Security API**
- **Übungsblatt 5**

Überprüfung von Zugriffsrechten unter Windows

- **Rechte werden durch den Security Reference Monitor beim Öffnen eines Objektes geprüft**
- **Drei Parameter**
  - Benötigte Zugriffsrechte
  - Token zur Identifikation des Benutzers
  - Security Descriptor des Objektes
- **Ausgabe: *Zugriff erlaubt* oder *Zugriff verweigert***

Benötigte Zugriffsrechte / Token

- **Benötigte Zugriffsrechte**
  - 32 Bit Wert, jedes Bit repräsentiert ein „Recht“
  - Welches Recht in welchem Bit kodiert ist, hängt vom Objekt ab
- **Token**
  - Repräsentiert einen Benutzer
    - Security Identifier (SID) des Benutzers
    - SIDs der Gruppen in denen der Benutzer enthalten ist
    - Liste der Privilegien des Benutzers
      - Systemoperationen
      - Z.B.: Backup/Restore, Debug, Shutdown
- **SID**
  - Format: S – Revision – Identifier Authority – Sub-Authority –.. – Relative ID
  - Vordefinierte SIDs (Beispiele)
    - World S-1-1-0 Administrators S-1-5-32-544
    - SYSTEM S-1-5-18

Security Descriptors

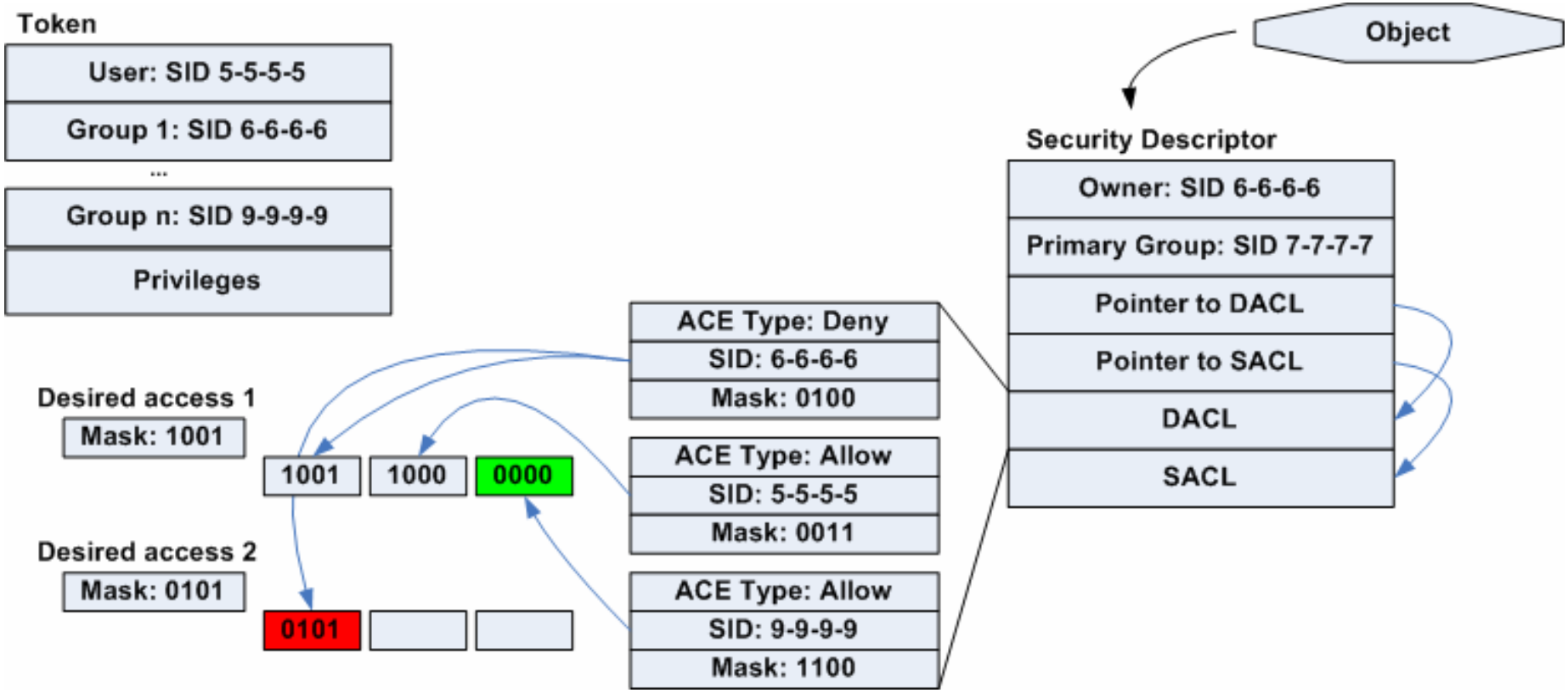
- **Sind Objekten zugeordnet**
- **Enthaltene Informationen:**
  - SID des Besitzers
  - Primäre Gruppe des Besitzers (POSIX)
  - Discretionary Access Control List
  - System Access Control List
- **Variable Größe, da DACL und SACL unterschiedlich viele Einträge enthalten können**

Discretionary Access Control List

- **Besteht aus keinem oder mehreren Access Control Entries (ACE)**
  - Keine DACL vorhanden: Zugriff für alle erlaubt
  - Leere DACL vorhanden: Zugriff für alle verweigert
- **Access Control Entries**
  - Zwei Typen: „deny“ oder „allow“
  - Jeder ACE enthält:
    - Typ
    - SID auf den sich der Eintrag bezieht
    - Bit-Maske
- **ACEs werden sequentiell ausgewertet**

Überprüfung der Zugriffsrechte

- **Security Reference Monitor betrachtet nur Bitmuster**



Sonderfälle

- Der Besitzer eines Objektes hat immer WRITE_DACL und READ_DACL Rechter
- Ein Benutzer mit „take ownership“-Privileg kann Besitz von beliebigen Objekten übernehmen
- Ein Benutzer mit „backup“-Privileg kann jede Datei lesen
- Ein Benutzer mit „restore“-Privileg kann jede Datei schreiben

Windows Security API (I)

- **Aktueller Benutzer**

```
BOOL GetUserName(    LPTSTR lpBuffer,
                     LPDWORD lpcchBuffer )
```

- **Verarbeiten von SID**

```
BOOL LookupAccountSid(
                     LPCTSTR lpszSystem,
                     PSID psid,
                     LPTSTR lpszAccount,
                     LPDWORD lpcchName,
                     LPTSTR lpszReferencedDomain,
                     LPDWORD lpcchReferencedDomain,
                     PSID_NAME_USE psnu )
```

Windows Security API (II)

- **Lesen des Security Descriptors einer Datei**

```
BOOL GetFileSecurity(
                    LPCTSTR lpszFileName,
                    SECURITY_INFORMATION secInfo,
                    PSECURITY_DESCRIPTOR psd,
                    DWORD cbSd,
                    LPDWORD lpcbLengthNeeded )
```

Windows Security API (III)

- **DACL Informationen**

```
BOOL GetSecurityDescriptorDacl(
                        PSECURITY_DESCRIPTOR psd,
                        LPBOOL fDaclPresent,
                        PACL *pAcl,
                        LPBOOL lpfDaclDefaulted )
BOOL GetAclInformation(
                        PACL pAcl,
                        LPVOID pAclInformation,
                        DWORD cbAclInfo,
                        ACL_INFORMATION_CLASS dwAclInfoClass )
BOOL GetAce(            PACL pAcl,
                        DWORD dwAceIndex,
                        LPVOID *pAce )
```

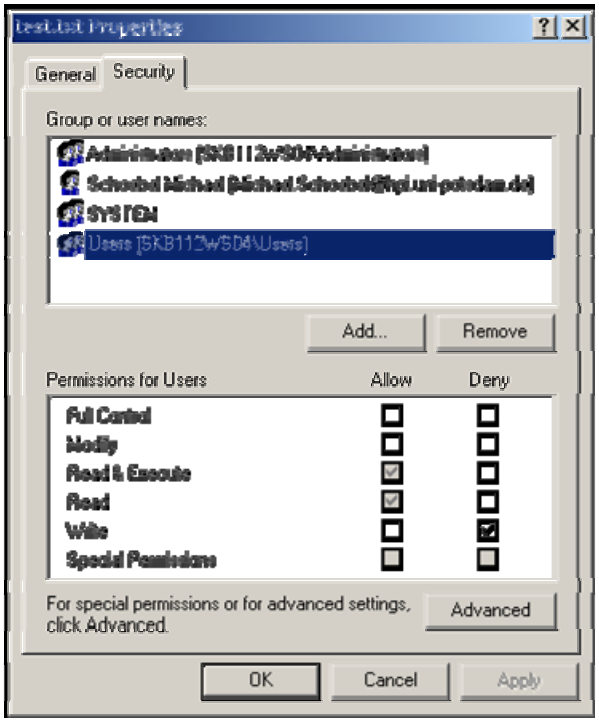
Windows Security API (IV)

- **ACE Datenstruktur**
  - Typen: PACCESS_ALLOWED_ACE, PACCESS_DENIED_ACE
  - Wichtige Felder:
    - **`Header.AceType`**
    - **`Mask`**
    - **`SidStart`**

- **Bei der Verwendung zu Beachten:**
  - **`#include <windows.h>`**
  - Programm zusammen mit **`advapi32.lib`** linken

Übungsaufgabe 5.5

- **Lesen von Security Descriptoren**
- **Ausgabe der DACL**



Referenzen

- **Mark Russinovich, David Solomon: „Windows Internals“**
- **Johnson M. Hart: „Win32 System Programming“**

- **MSDN**

  http://msdn.microsoft.com/library/default.asp?
  url=/library/en-us/secauthz/security/authorization_functions.asp