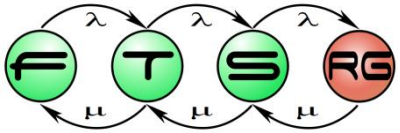
# Security Subsystem in Windows

Zoltán Micskei

http://www.mit.bme.hu/~micskeiz



# Copyright Notice

- These materials are part of the *Windows Operating System Internals Curriculum Development Kit*, developed by David A. Solomon and Mark E. Russinovich with Andreas Polze
- Microsoft has licensed these materials from David Solomon Expert Seminars, Inc. for distribution to academic organizations solely for use in academic environments (and not for commercial use)

- http://www.academicresourcecenter.net/curriculum/pfv.aspx?ID=6191

- 

# Questions

SID

HKLM

BSOD

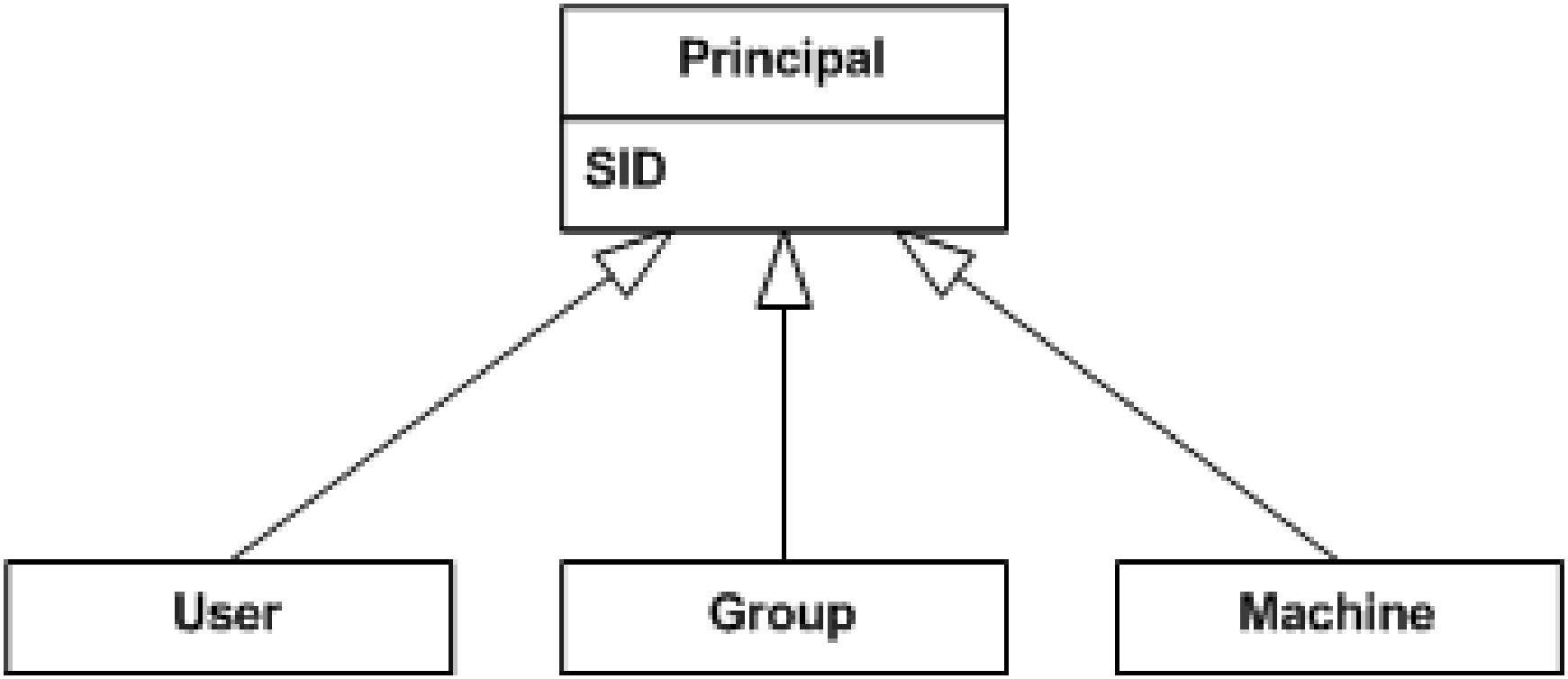
# Security tasks in Windows

- Authentication
  - Has / Knows / Is
  - E.g. logon screen, password popup
- Authorization
  - Principle: *Role* based access control
  - E.g. access control lists
- Auditing
  - Audit logging

# Security tasks in Windows

- **Authentication**
  - **Has / Knows / Is**
  - **E.g. logon screen, password popup**
- Authorization
  - Principle: *Role* based access control
  - E.g. access control lists
- Auditing
  - Audit logging

# Security entities in Windows



# Security Identifier (SID)

- Unique identifier
- E.g. SID of a machine:

`S-1-5-21-2052111302-1677128483-839522115`

- Users, groups:
  - <Machine SID>-<RID>
  - RID: relative identifier
- Well-known SIDs
  - Everyone: S-1-1-0
  - Administrator: S-1-5-domain-500
- Vista: services also get their own SIDs

DEMO

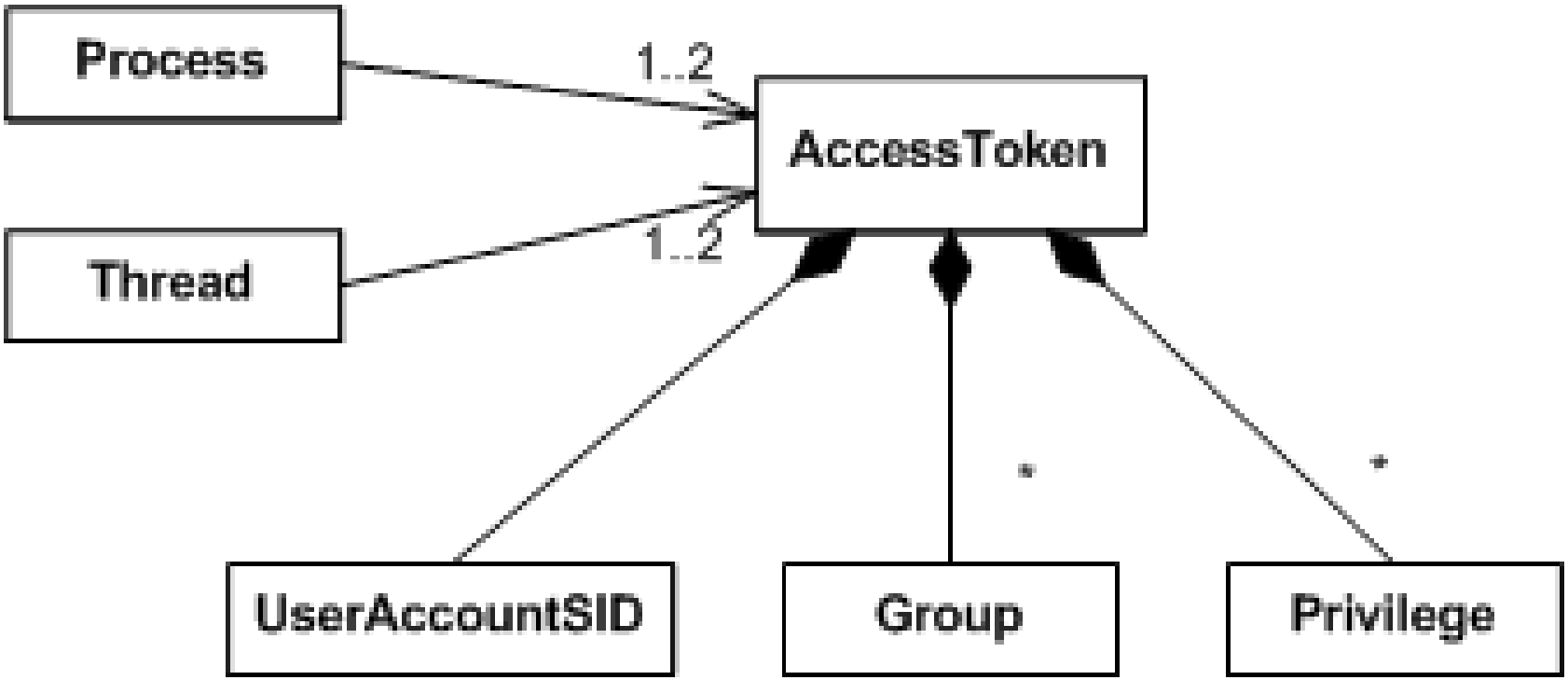
# Security identifier (SID)

- `psgetsid.exe machineName`
- `psgetsid.exe administrator`
- `psgetsid.exe <user>`

# Authentication

- Login
  - Through Winlogon's own desktop
  - Secure Attention Sequence: Ctrl + Alt + Del
  - Windows 8: Microsoft account, picture password
- Storing passwords:
  - Hash in the registry
- Network authentication
  - NTLM: NT LAN Manager
  - Kerberos: since Windows 2000, in domain environment

# Authentication – Access token

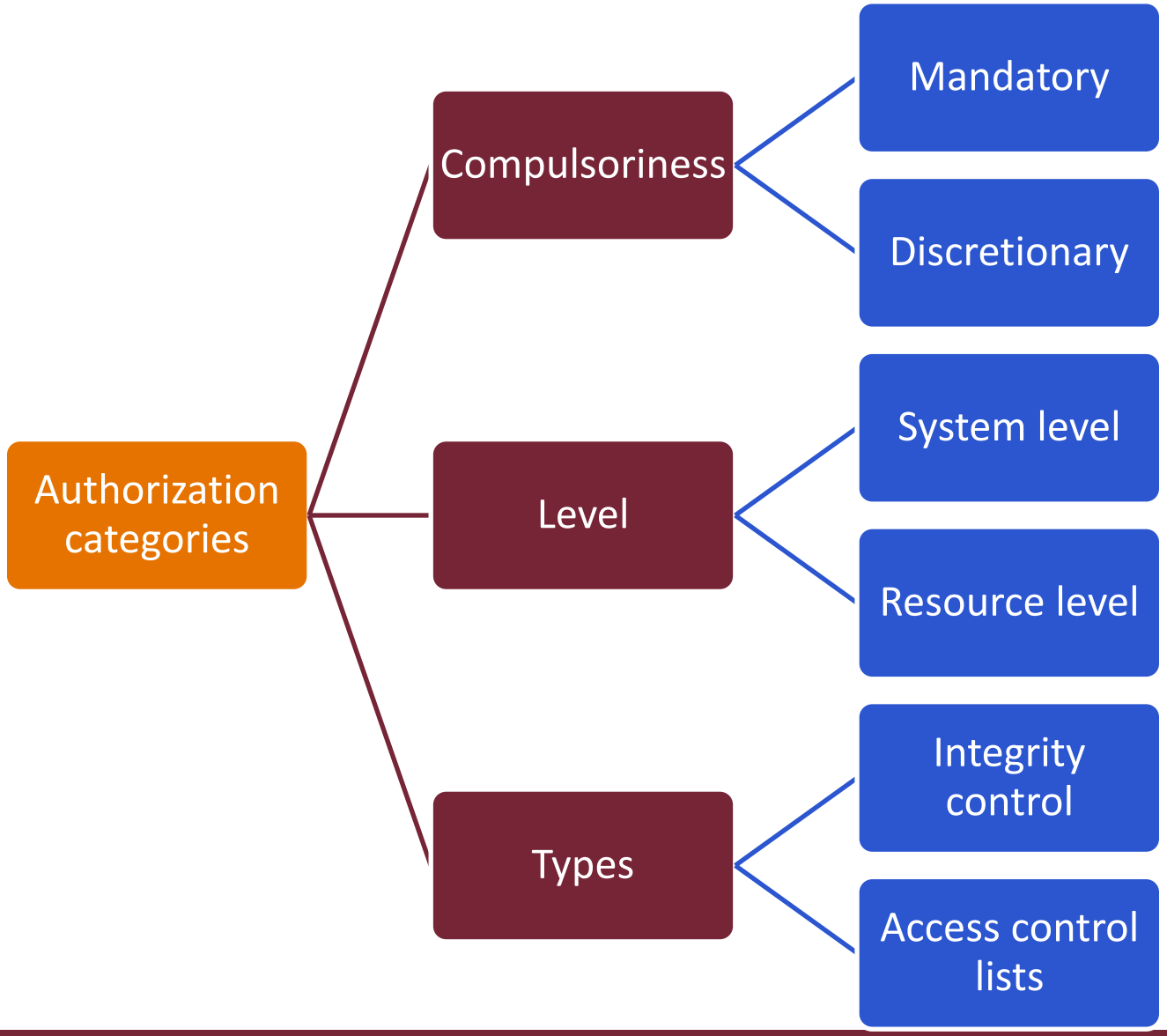



- Impersonation

# Security tasks in Windows

- Authentication
  - Has / Knows / Is
  - E.g. logon screen, password popup
- **Authorization**
  - **Principle: *Role* based access control**
  - **E.g. access control lists**
- Auditing
  - Audit logging

# Categorizing authorization (see prev. lecture)



# Authorization methods in Windows

- Mandatory Integrity Control
- System level privileges and rights
- Discretionary Access Control

# DEMO

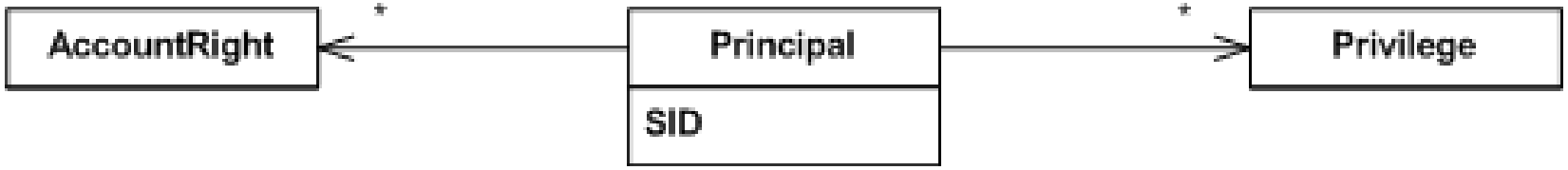
## Mandatory Integrity Control

- Vista feature
- `icacls /setintegritylevel H|M|L`
- Trying „No write up”
  - `psexec -l cmd.exe`: starts with low integrity
- e.g. Internet Explorer uses MIC

# Authorization methods in Windows

- Mandatory Integrity Control
- **System level privileges and rights**
- Discretionary Access Control

# System level authorization




- Privilege
  - operating system level
  - E.g.: shutdown machine, load device driver
  - Name: SeShutdownPrivilege, SeLoadDriverPrivilege
- Account right
  - who / how can or cannot login
  - E.g.: interactive, network logon…

# DEMO

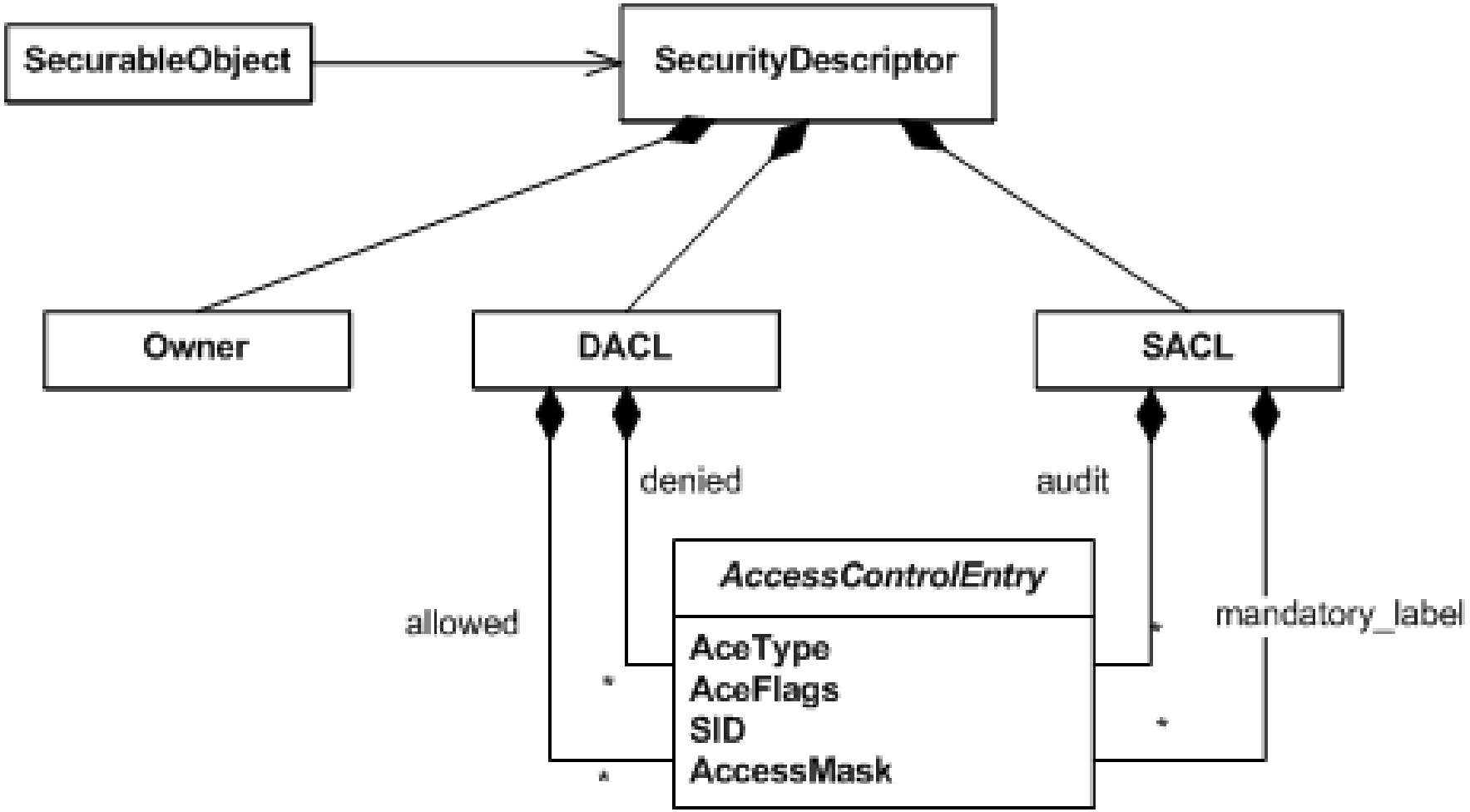
Privileges
Local Security Policy

- Privileges
  - `whomai /priv`
  - Local Policy: User rights
- Local Security Policy
  - Password policy
  - Account locking
  - Security options

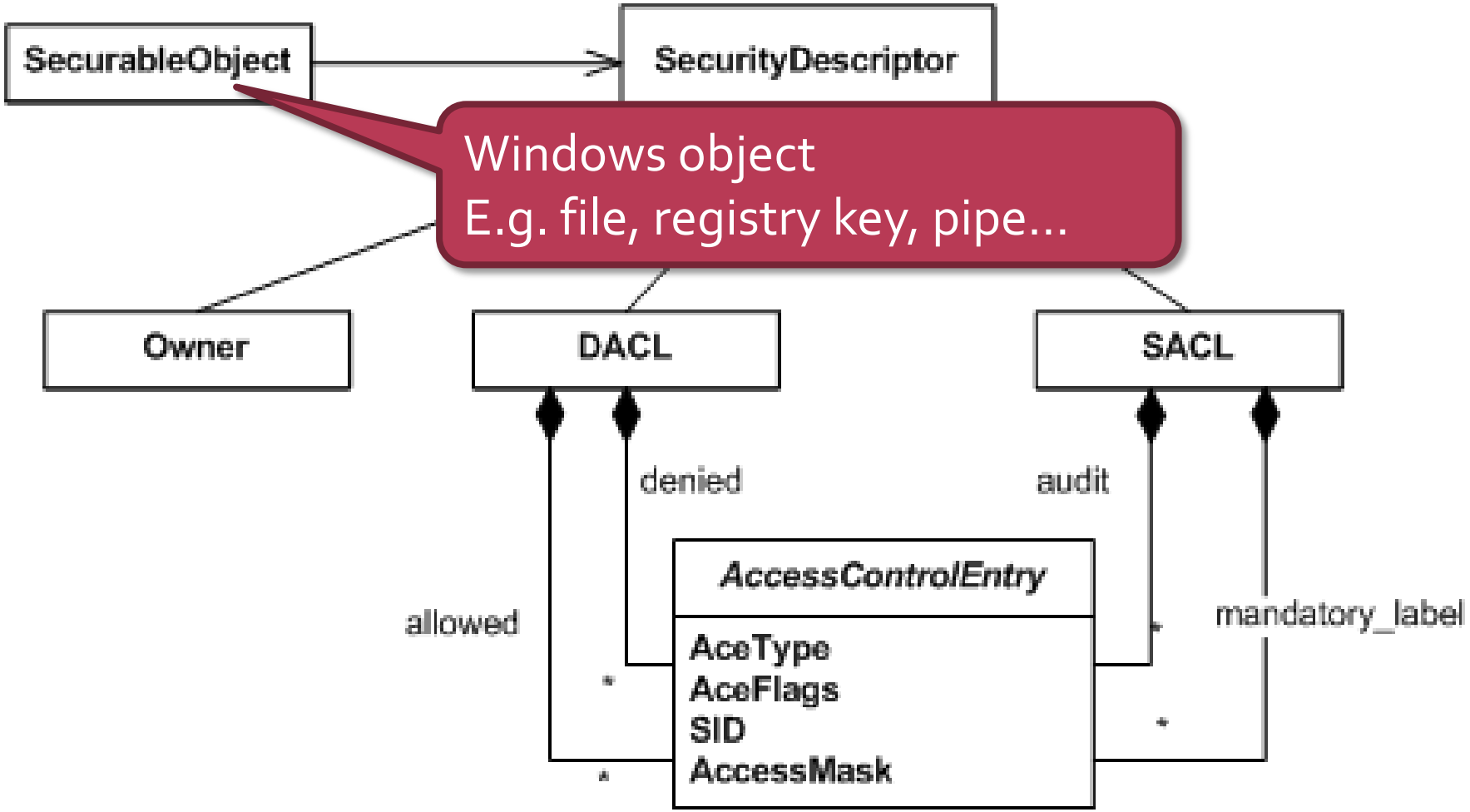
# Authorization methods in Windows

- Mandatory Integrity Control
- System level privileges and rights
- **Discretionary Access Control**

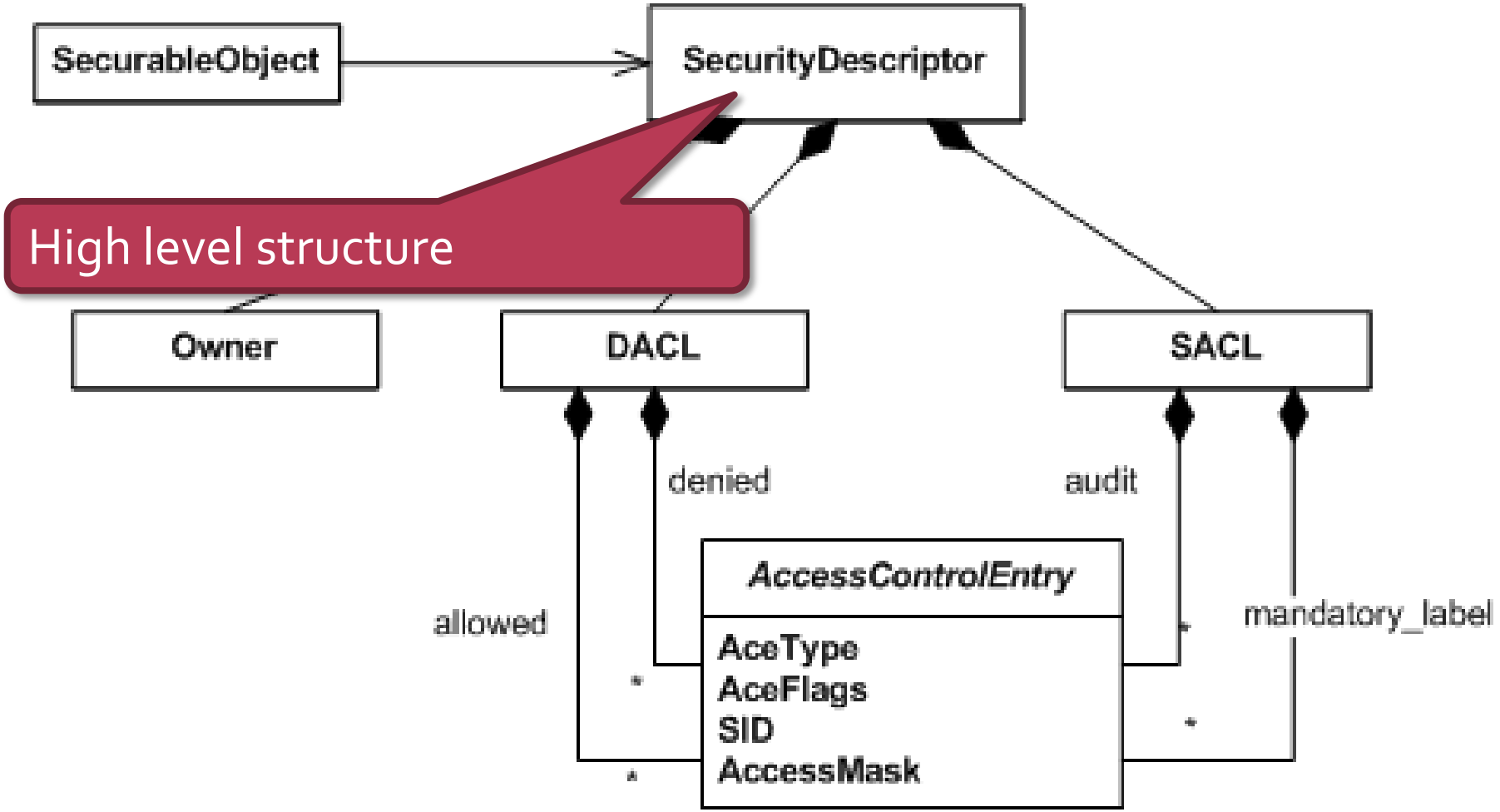
# Access control lists



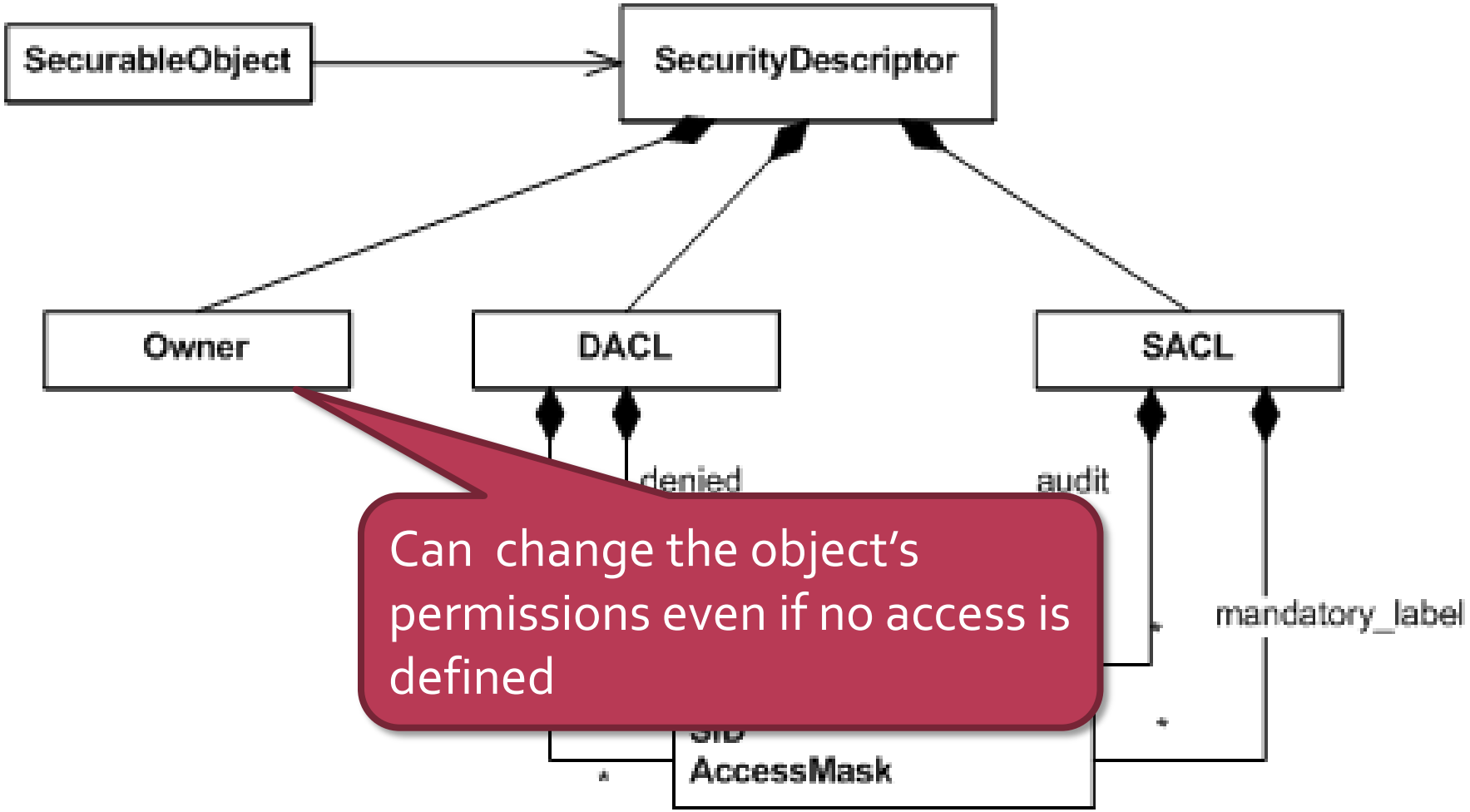
# Access control lists



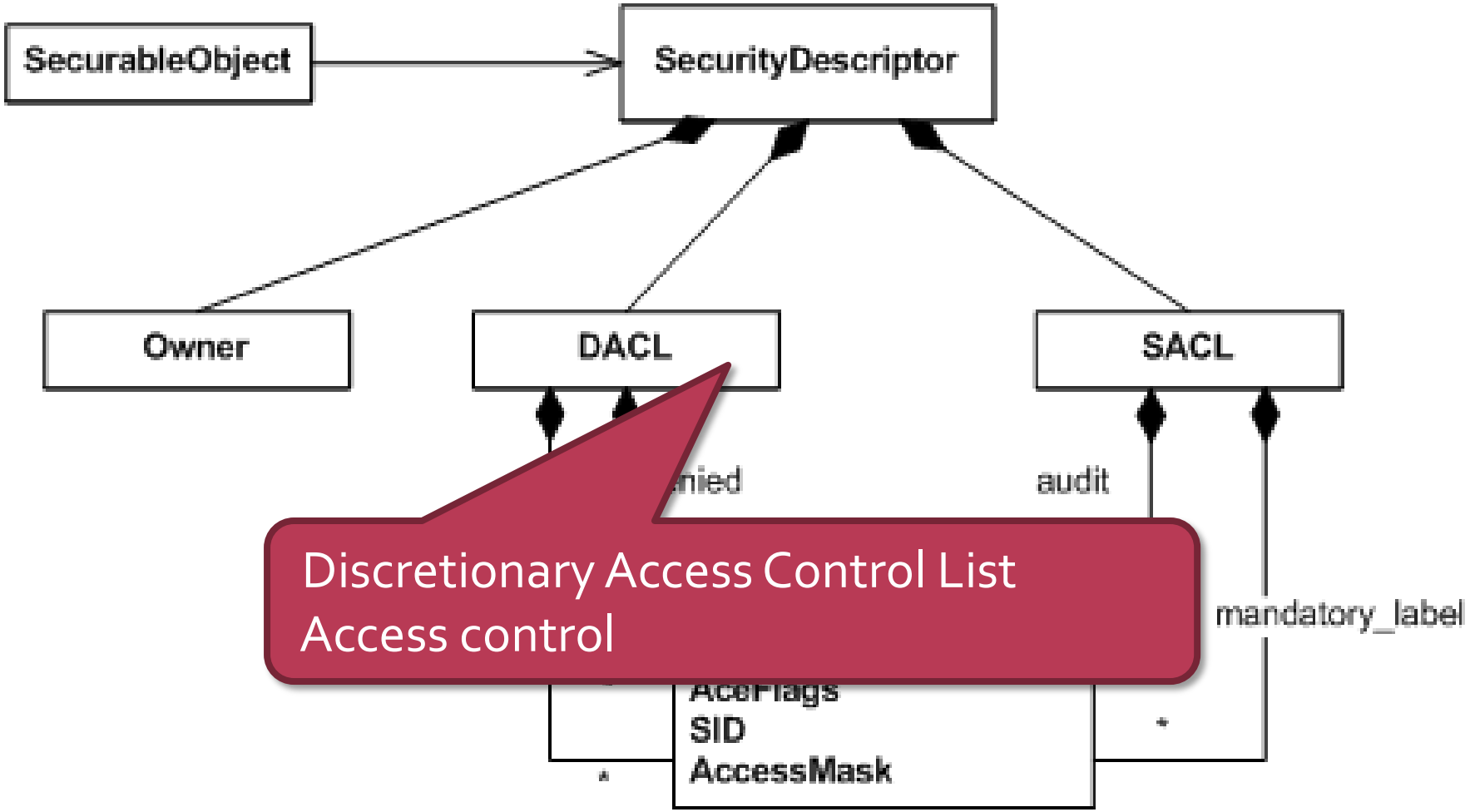
# Access control lists



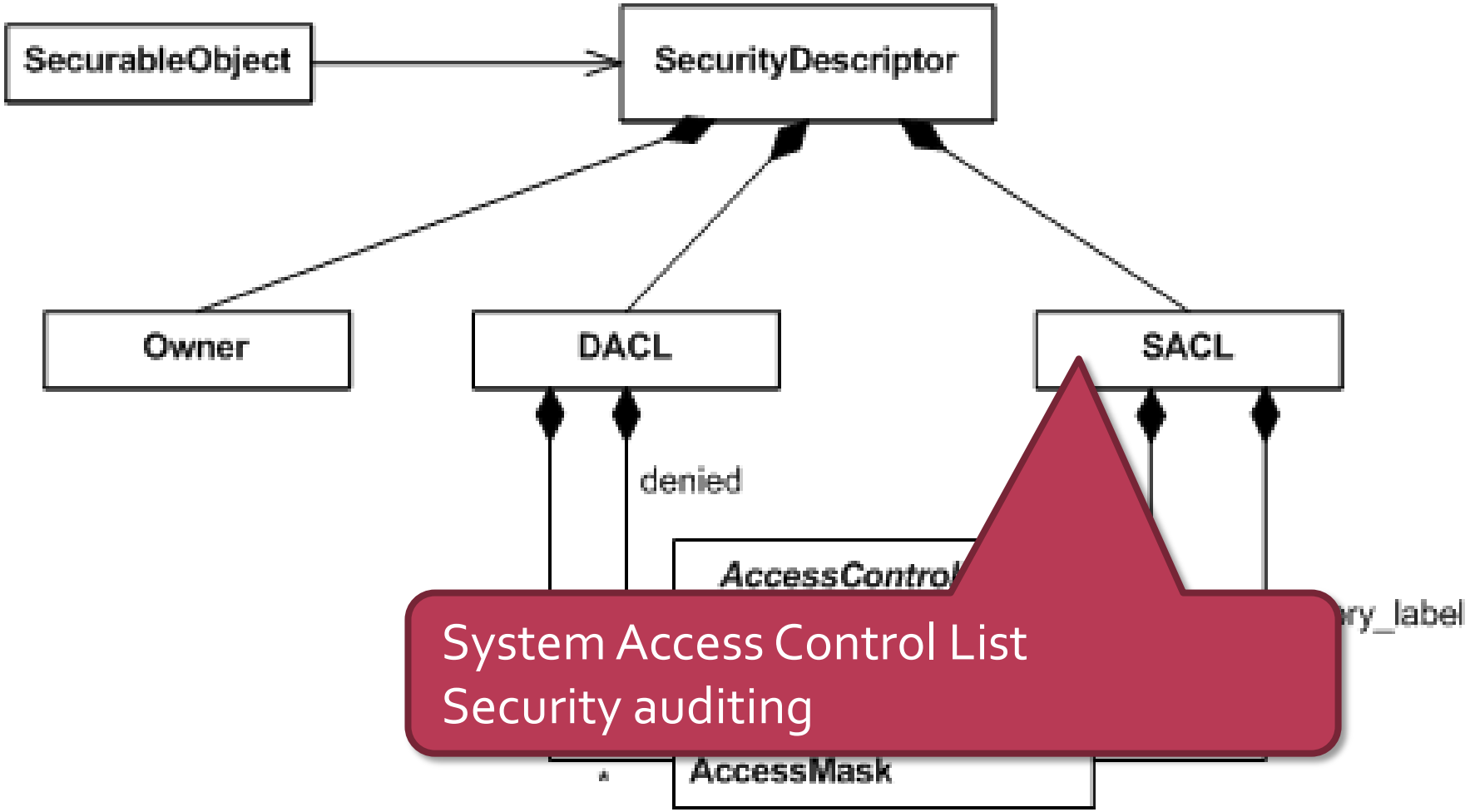
# Access control lists



# Access control lists

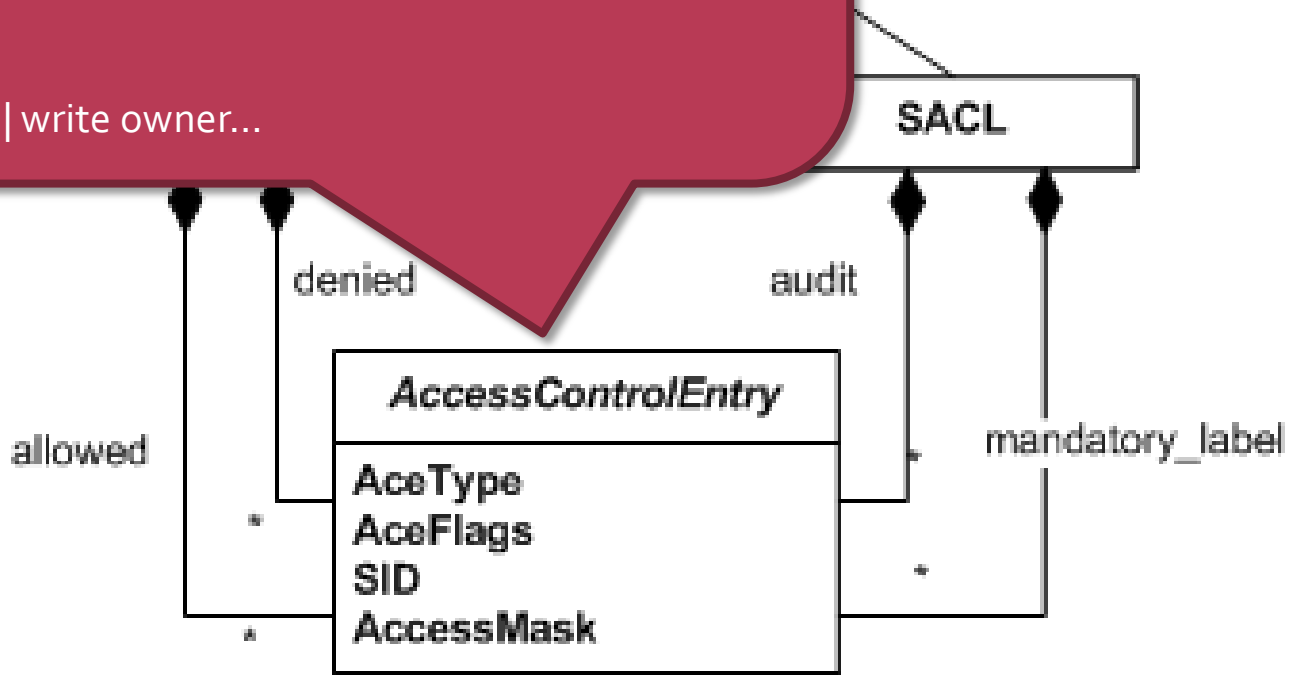


# Access control lists



# Access control lists

Type
allow, deny, audit
Flag
E.g. inheritance
SID
who to apply
Mask
execute | delete | write owner…



# Access control lists - Example

Object C:\temp

Descriptor

Owner: Administrator

DACL

ACE1: allow, inherits, Administrators, list folders | create files

ACE2: allow, not inherited, Users, list folders | read attributes

SACL

# Access control lists

- Inheritance flag
  - For container type objects (e.g. folder)
  - Child object inherits the ACE
- Evaluation method
  - Several ACE can apply to a given SID
  - UNION of all the permission from the ACEs
  - Exception: deny ACE, it overcomes everything

# DEMO

Authorization –
Access control lists

- Basic permissions
- Inheritance
  - Limiting inheritance
- Take ownership
- Effective permissions
  - Union, except
  - Deny ACE
- Debugging: Process Monitor

# Security tasks in Windows

- Authentication
  - Has / Knows / Is
  - E.g. logon screen, password popup
- Authorization
  - Principle: *Role* based access control
  - E.g. access control lists
- **Auditing**
  - **Audit logging**

# Eventlog

- System, application, security events
- Event:
  - Type, time, source, ID, description
- Overwrite events:
  - Never, x day older, circular

DEMO

# Auditing

- Auditing policy
- Content of the security log
- Use of permissions

**DEMO**

# User Account Control, Runas

- Dangers of running as Administrator
- Working limited user
  - Windows XP: Run as… and runas command
  - Showing Run as..: left SHIFT + right click
- Vista solution: UAC

DEMO

# Group Policy

- Computer settings
  - Security options
  - System componets, e.g. Windows Update
- User settings
  - Applications
  - Windows interface
- Templates
- Administrative templates
- ~2500 settings

# Troubleshooting

# DEMO

## Blue Screen of Death (BSOD)

- If there is no other choice…
- Don’t hate the messenger☺

- KeBugCheckEx function, Bugcheck.h
- Error reporting
- Creating memory dump
- Analyzing minidump in WinDgb

DEMO

# Problem solving

- Event log errors:
  - Help & Support
  - EventID.net
  - Knowledge Base articles

# Special startup modes

- Hit F8 before the Windows logo