In 1988, Microsoft decided to develop and "new technology" (NT) portable Operating System. Originally designed to use OS/2 API, but was later changed to Win32 API. Key goals in design were: security, reliability, ease of use, Windows and POSIX application compatibility, high performance, extensibility, portability and international support. Structure consisted of a hybrid of layered/client-server design.
Security Subsystems

- **Winlogon**
  - Login process used for coordinating and providing interfaces for interactive login/logoff
  - Also manages desktops
- **Win32**
  - Makes Win32 API available to application programs
  - Provides GUI and all user input/output
- **Local Security Authority (LSA)**
  - Main responsibilities centered around security
  - Plays a major role in authentication and auditing (more details later)
  - Also upholds the local security policy (user privileges/access rights)
- **Security Accounts Manager (SAM)**
  - Manages information about accounts for users/groups either locally or domain wide
  - Contains information such as full name, home directory, last login time, username/password, SID, etc.
- **Security Reference Monitor (SRM)**
  - Runs in kernel mode
  - Responsible for enforcement of access validation and audit generation policies required by LSA

Windows NT Security Evaluation (TCSEC)

- **Windows NT has been certified at the C2-level by the U.S. government according to the Trusted Computer Systems Evaluation Criteria ("Orange Book")**
  - Provides a standard set of criteria and an evaluation procedure for judging the security that various computer products can provide
  - Split into four general divisions of security criteria, A, B, C and D with A being the highest assurance
  - B and C further broken down into classes C1, C2, B1, B2, and B3
- **Things to consider:**
  - Pretty low on the security model, but excels in other areas (e.g., trusted path & trusted facility management)
  - Not "out of the box" C2 compliant, must be setup (e.g., auditing disable by default)
  - Earned its C2 rating as a stand-alone system, not hooked up to a LAN
TCSEC (cont)

Windows NT Security Mechanisms

- Requirements for OS providing C2-level security are:
  - Object Reuse (Object Security) - prevent users from seeing data that another user has deleted or preventing access to memory that another user previously used/released
  - Zeros out the contents before giving access
  - Identification & Authentication - require unique identifier and password to identify a user before they are granted access to the system
  - Access Control - all OS shareable resources associate a block of information that specifies what operations users can perform on them
  - Auditing - monitor resources and record failed/successful attempts to access them

Security Objects

- Any data that needs to be shared or protected are stored as objects
  - Used to identify and subclass users, indicate permissible operations, and relate ownership and permissions to system objects
  - The Security Identifier (SID)
  - The Access Control Entry (ACE)
  - The Access Control List (ACL)
  - The Security Descriptor
  - The Access Token
- Each builds upon the other to provide specific security features
The Security Identifier

- A unique identifier used to identify an entity that performs actions on the system
  - Includes things such as users, local and domain groups, local computers, domains, and domain members
- A variable-length numeric value that consists of:
  - a SID revision number
  - a 48-bit identifier authority value (who issued the SID)
  - a variable number of 32-bit Relative Identifier (RID) (simply used to create unique SIDs)

The Security Identifier (cont)

The Access Control Entry

- Basic unit of permissions
- ACE contains:
  - two types (access allowed & access denied)
  - SID (the user and/or group the permission(s) are applied to)
  - access mask (indicates the permissions on the object)

Logical view of Access Control Entry

<table>
<thead>
<tr>
<th>ACE Type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SID</td>
<td></td>
</tr>
<tr>
<td>Access Mask</td>
<td></td>
</tr>
</tbody>
</table>
The Access Control List

- Describes all of the users and/or groups who are allowed or denied access to a particular object
  - Simply put, a list of ACEs

Logical view of Access Control List

| ACE | ACE | ACE | ... |

Access Control List (cont)

The Security Descriptor

- Information of an object that specifies who can perform what actions on the object
- Contains:
  - revision number
  - control flags
  - owner's SID
  - primary group SID
  - Discretionary Access Control List (DACL, optional)
  - System Access Control List (SACL, optional)
The Security Descriptor (cont)

The Access Token

- Essentially a complete description of a user from the viewpoint of NT
- Contains:
  - account SID
  - group SIDs
  - collective privileges
  - account name
- Attached to every process the user executes
Putting it all together: Access Control

Authentication Downfalls

- Password-based authentication is weak
- With physical access to the machine, the SAM file can be easily compromised
- MD4 hash algorithm
  - not collision free
  - susceptible to two-round attack
Is Windows NT “secure”?

- “Secure” is a complex concept
  - What properties protect against what attacks?
- More then just the OS
  - Many problems arise from applications, device drivers
- Security overlooked?
  - Missing range checks, invalid parameters (NTCrash)
  - Service Packs change half the OS
- Security by obscurity
  - SAM database
  - Authentication/encryption methods not well known, or even peer reviewed
- More factors to consider
  - Networking