

Windows NT Security

Every operating system provides some security mechanisms. The security mechanisms found in Windows NT are used to enforce: access control, integrity, accountability and auditing. Windows NT offer various enhancements to security compared to the Windows 9x family. It is critical that an operating system restricts users from accessing files and programs for which they do not have authorization. Windows NT was built from the start with security in mind compared to previous operating systems from Microsoft such as DOS where security was an after thought. Windows NT was built to incorporate networking, security and audit reporting as services with in the operating system (Blake).

DOD Security Evaluation

The Department of Defense (DOD) created the Trusted Computer System Evaluation Criteria, which is commonly referred to as the “Orange Book”. The “Orange Book” is used to evaluate the security of an operating system. The ratings for operating systems range from A to D. First, Class D system’s offers little security. Second, Class C rating is given to an operating system that provides discretionary access control. Third, a class B rating is given to a system that provides mandatory access control. Last, a class A rating is given to a system that has verified security, through the use of mathematical proofs and formulas. Many of the classes are also further subdivided depending on the on additional security requirements such as a C2 rating requires that the system provides discretionary access control, uses auditing and other additional requirements. The “Orange Book” classification essentially gives a means of measuring the assurance that can be placed in an operating system.

Windows NT was given a C2 rating based on the security it provides. Windows NT provides the resource kit tool C2Config to help configure the system to meet the C2 certification. If the OS is kept up to date by installing the current service packs and security patches the system will remain close to the C2 level certification (Russinovich).

To earn a C2 the operating system must provide secure logon, discretionary access control, auditing and object reuse protection (Russinovich). The secure logon is satisfied by NT having a unique user name and password to identify a user. An access control list (ACL) is used to specify the action a user is allowed to perform on an object. Auditing is used is used to record successful and failed attempts to access a resource. Last, object reuse protection prevents a user from accessing data in an object that has been deleted or accessing a memory location of another user (Russinovich).

Domains

Windows NT uses domains as a way to group a number of machines together. Domains are important in Windows NT because they allow a user to perform a single sign-on and access a number of different computers. In a Windows NT domain there is one Primary Domain Controller (PDC) and multiple Backup Domain Controllers (BDC). If the PDC were to fail, one of the BDC would be selected to be the new PDC and allow the domain

to continue to function. The Primary Domain Controller contains a central database called the Security Account Manager (SAM) Database which consists of accounts, passwords and access control lists (Davis & Lewis). The job of the PDC is to serve as an authenticator of the accounts it contains in its SAM database.

The SAM database can become very large. For this reason the organization can be split up into a number of domains. By splitting up the organization into domains it can also make administration easier. There are four ways to combine servers and workstations in NT: single domain, master domain, multiple master domains, and complete trust model. First, a single domain can be used by an organization with one domain. Next, the master domain is used for controlling user accounts and resource domains. A resource domain can contain file servers, application servers, etc. There are no user accounts in the resource domains (Davis & Lewis). Also, the multiple master domains contain more than one master domain controller in the system. Last, a trust model can be used to control the domains. In the trust model trusts are created so that domains can share resources.

Windows NT domains are built on the notion of trust. When a domain is created, it is an isolated unit that can not communicate with the other domains in the organization. To allow domains to interact with each other trust relationships must be established between domains. For instance, in an organization with a human resource department and accounting department each department can have its own domain. By default these two domains would not be able to share data. The solution to the problem is to establish a trust relationship between the two departments.

When a trust is established it creates a one way relationship. If domain X trust domain Y, then users of Domain Y can sign onto Domain X. In this case users in Domain X could not logon to Domain Y because domain Y has not given trust to domain X. Furthermore, the trust relationships are not transitive. One of the problems with the trust model is it becomes very complex as more trusts are added to the system. Also, it is difficult to administer a system with this trust model. Current versions of Windows have done away with this model. New versions of Windows use a new concept the Active Directory.

Security Sub-Systems

Windows NT has four basic components that are used in the NT security model (Blake).

1. Logon Process
2. Local Security Authority (LSA)
3. Security Account Manager (SAM)
4. Security Reference Monitor (SRM)

These four subsystems form the basis of security in Windows NT. Figure security-1 shows how these subsystems interact with each other.

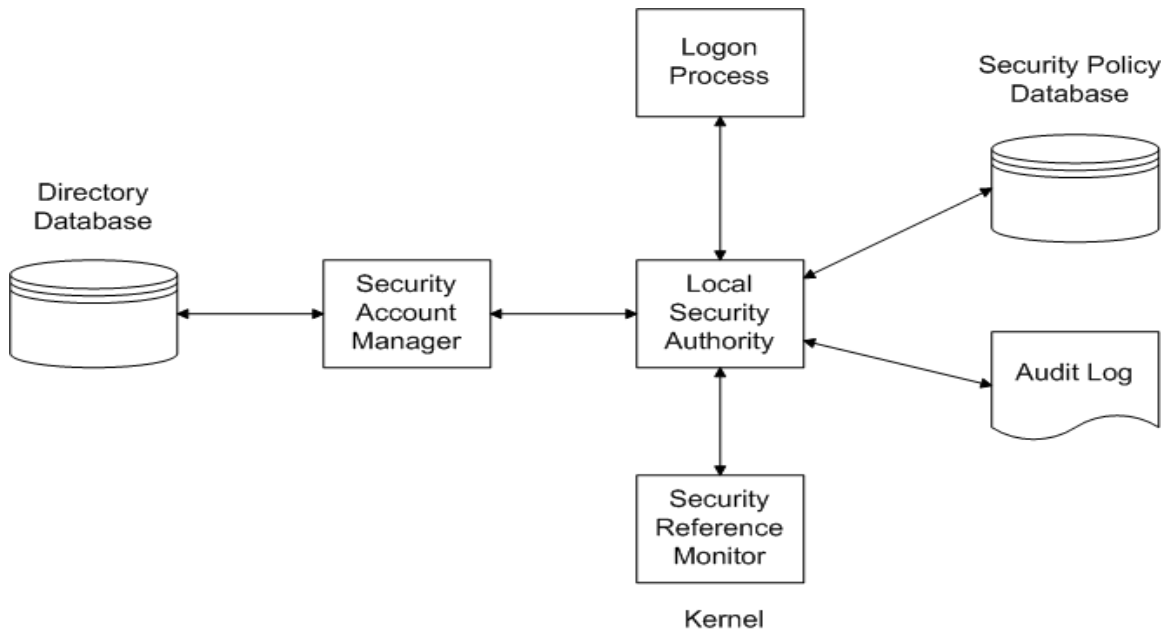


Figure: Security-1 Windows NT Security Sub-Systems (Davis & Lewis)

The **Logon Process** used by Windows NT is used to verify the authentication of a user. Authentication forms the foundation of NT security. NT uses two different methods for logging on based on whether the login is local computer vs. logging into a domain. To logon to a domain the netlogon service must be used. A user initiates the logon process by pressing CTRL-ALT-DELETE and then supplying a user id, a password and the domain they wish to logon to. If the id and password are valid the user is granted access to the system. If there is no match for the user name and password a user may still get access to the system. If the guest account is enabled the user is logged on to the guest account when the logon fails. It is probably a good idea to disable the guest account because it can be used as a first step used by an attacker to gain access the system. The figure below shows the logon process for Windows NT.

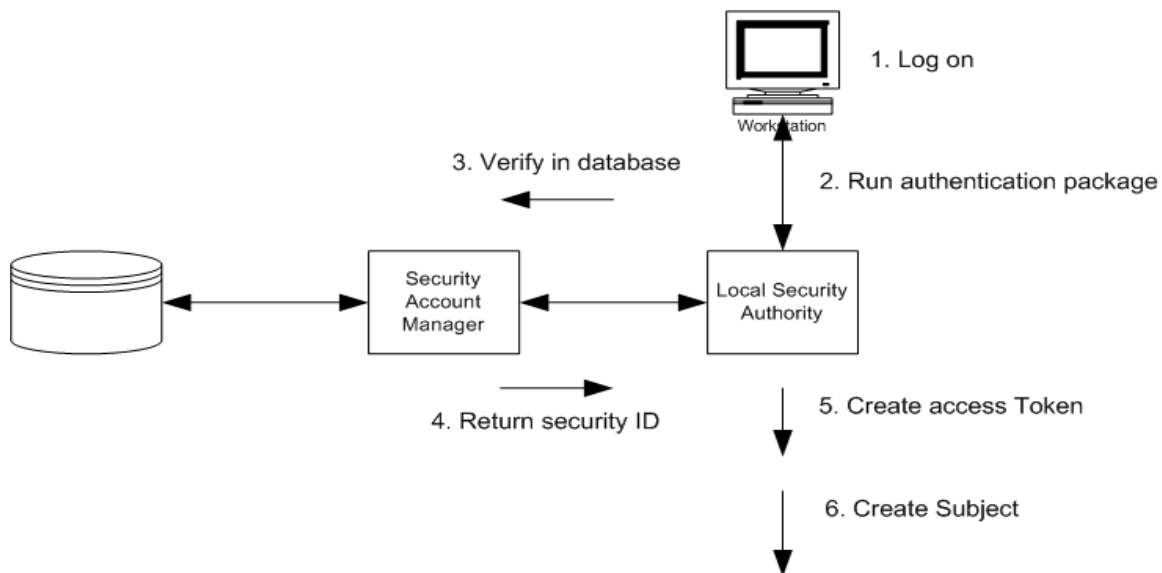


Figure: Security-2 Windows NT Logon Process (Davis & Lewis)

The **Local Security Authority** forms the groundwork of the security subsystem. The LSA is used to verify the logon process by sending requests to the SAM sub-system. Furthermore, the LSA is used to generate access tokens, and also administer the local security that is defined by the system (Blake). The LSA is also responsible for auditing events.

The **Security Account Manager** is responsible for maintaining the SAM database and providing an API to access the database (Davis & Lewis). The SAMs database contains information about the users and groups in the system. The SAM database is contained within the Windows NT registry. The Security Account Manager is responsible for validating a user id and password and return the SID of the user. The SAM database that is access may be either local or somewhere else on the network depending on the type of logon session.

The **Security Reference Monitor** is a kernel component that is used to control user requests to access objects in the system. The SRM enforces the access validation and audit generation (Davis & Lewis). Windows NT forbids the direct access to objects. Any access to an object must first be validated by the SRM. For example, if a user wants to access a specific file the SRM will be used to validate the request. The Security Reference Monitor enforces access validation and audit generation policy (Blake).

Security Objects

The resources in Windows NT are represented by objects. Some common objects in Windows NT are files and printers. A subject in Windows NT is a combination of a process that was created on behalf of a user and an access token (Blake). In Windows NT there are also a number of security objects, which are used to enforce the security in the operating system. There are five core objects which Windows NT uses.

1. The Security Identifier (SID)
2. The Access Control Entry (ACE)
3. The Access Control List (ACL)
4. The Security Descriptor
5. The Access Token

Windows NT uses the **Security Identifier** as a way of identifying objects in the system. Each of the following objects has a unique SID: users, local groups, domain groups, local computers, domains and domain members (Russinovich). The SID is a variable length numeric value containing a SID revision number, a 48-bit identifier authority value and 32-bit sub-authority value. Windows NT has a number of predefined SID's that can also be used. Two examples of SID's used by Windows NT are the Owner SID and Group SID. The Owner SID is for a user or group who owns an object. The Group SID is the primary group associated with an object. The Group SID is not used by the NT file system it is used for POSIX file systems (Blake). An example of an SID is S-1-5-21-3409648204-1077011011-4013025049-1005.

Access Control Entry is the most basic unit of permission available in Windows NT (Frost). The ACE contains the SID and a permission mask. The permission mask is used to indicate what permission is allowed or denied. The permission mask has both generic and specific rights. The generic rights are:

- DELETE
- READ_CONTROL
- WRITE_DAC
- WRITE_OWNER
- SYNCHRONIZE

Some of the specific rights that can be assigned in Windows NT are:

- FILE_READ_DATA
- FILE_LIST_DIRECTORY
- FILE_WRITE_DATA
- FILE_ADD_FILE
- FILE_APPEND_DATA
- FILE_ADD_SUBDIRECTORY
- FILE_EXECUTE
- FILE_TRAVERSE
- FILE_DELETE_CHILD
- FILE_READ_ATTRIBUTES
- FILE_WRITE_ATTRIBUTES

An Access Control entry is show in figure security-3.

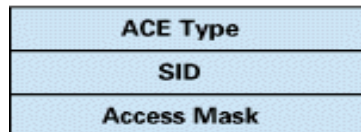


Figure: Security-3 Access Control Entry (Rusinovich)

The **Access Control List** is used to group ACE's. The Access Control List is used describe which users or groups are allow or restricted from accessing which objects. There are a number of problems with the ACL's in Windows NT. First, NT does not support a large number properties or operations on an object. Also, changes made to an ACL are not propagated to other ACL's in the system, so the management of ACLs can be difficult (swift).

The **Security Descriptor** is an object which used to store the security attributes of an object. The Security Descriptor contains five central elements (Frost). First, each descriptor has a header that tells the revision number and specifies control flags. The control flag specifies attributes, such as what memory layout the descriptor uses (Rusinovich). Second, the descriptor contains the SID of owner of the object. Third, it contains the SID of the group that owns the object. Fourth, the Security Descriptor contains a Discretionary ACL, which tells actions that users or groups may perform on an object. Fifth, System ACL tells what action taken by a user or group should be audited. When the security attributes of an object are changed it is done through the security descriptor. There are a number of functions built in NT for managing a Security Descriptor. Figure security-4 shows the fields that are contained in the security descriptor.

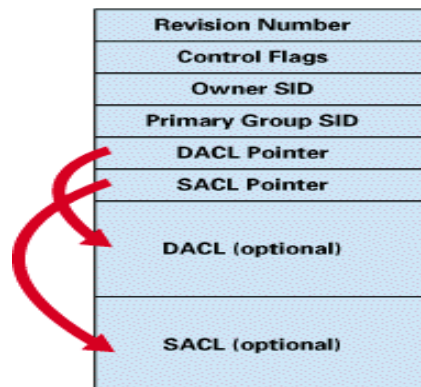


Figure: Security-4 Security Descriptor (Rusinovich)

An **access token** is used to identify each process. The access token contains information about a user. The access token is used to identify credentials for a specific process. Access tokens are created for a user when they logon to the system. Figure security-5 shows the fields that are contained in an access token. The access token contains the SID of the user, the SID's for the groups to which a user belongs and the permissions the user has. The access token is then appended to all the processes that a user creates when they are logged in. Access Validation is performed by the Security Reference Monitor comparing the SID in the access token with the ACL. The access token also contains a default primary group and default ACL which are used when a process creates a new object the new object will inherit default group and ACL. Token source describes the process that created the token. The authentication ID is commonly used to tell it is if a token to a logon session.

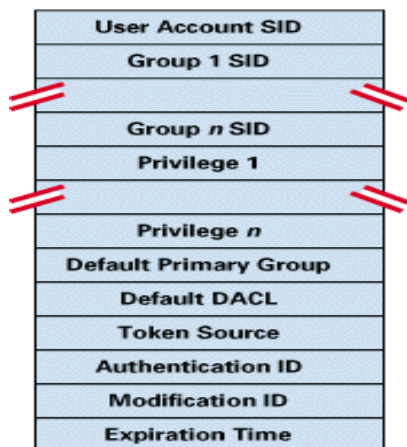


Figure: Security-5 Access Token (Rusinovich)

Access Request Process

When an access request takes place the Security Reference Monitor scans the list of Access Control Entries associated with an object. The Reference Monitor looks for any SID that matches an SID in a user access token. If any of the ACE entries for the user deny access to an object, then access is denied. Even if the user has other ACEs that

allow access to the object the permission will be denied. Figure security-6 shows that user Mark is denied access to an object because the writer group is denied access to the object even though Mark explicitly is granted read and write access to the object.

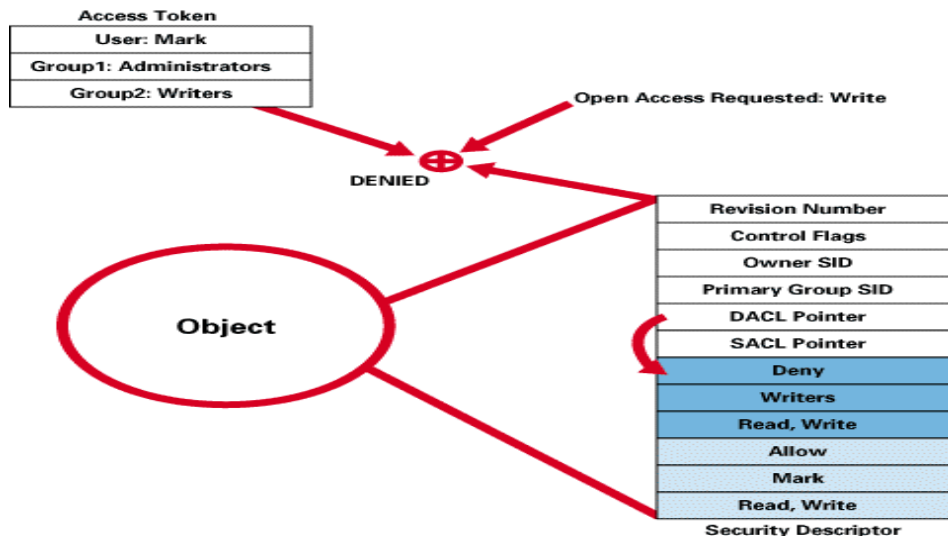


Figure: Security-6 Access Request (Rusinovich)

Auditing

An auditing mechanism monitors and records the executed operations so that possible unauthorized use of a resource can be observed. Auditing can also be used to make the users in the system accountable for their actions. Windows NT uses auditing to provide a way to record the successful and unsuccessful access to objects. This provides the system administrator a way of identifying any security violations, such as an intrusion into the system. With audit logs it is possible for an administrator to reconstruct the events that caused an intrusion to take place.

In Windows NT there are three logs that are used for auditing they are: the application log, the system log and the security log. The following are some common events that can be tracked:

1. Logon and logoff
2. Restart and shutdown
3. Security policy changes
4. Process tracking
5. Use of user rights
6. File and object access

Windows NT offer a fine level of granularity for auditing. The OS allows certain files or directories to be audited. Also, the audit mechanism can be used to record certain users or groups actions. By default the auditing is turned off in Windows NT. An organization should use there security policy to decide what events audits. By no means should an organization use the default setting and have auditing completely turned off. Without auditing an organization would have no means of knowing that the system was used in an unauthorized manner or compromised.

One of the problems with logging events is the amount of data that is generated. If everything is logged a tremendous amount of I/O will take place, degrading the performance of the system. Another problem with Windows NT auditing is the operating system offers little help in analyzing the logs. It is highly recommended that third party tools are utilized to analyze the log files.

Security Vulnerabilities

A large number of vulnerabilities have been found in Windows NT. A common method of attack used on Windows NT is a buffer overflow attack. On windowsecurity.com they state, "The vulnerabilities are due primarily to implementation errors and bugs not inherent architectural weaknesses, indicating a lack of maturity in early versions of the operating system." By default Windows NT is not very secure. There are a number of steps that can be taken to improve the security. For instance, guest accounts should be disabled. Also, the default access rights of the "everyone group" should be changed. By default Windows NT gives this group full access rights. Users should have the least amount of privileges needed to accomplish their specific task. Furthermore, any of the services that are not required should be turned off. Last, there are a large number of registry edits that can be used to improve the security of Windows NT. The web page <http://sabernet.home.comcast.net/papers/WindowsNT.html> lists a number of registry edits that can be used to improve security. By hardening Windows NT the operating system can become much more secure. These are a few of the steps that can be taken to improve security.

References

- Admin, "Network Strategy Report: Windows NT Security" October, 16, 2002.
http://www.secinf.net/windows_security/Network_Strategy_Report_Windows_NT_Security.html
- Blake, Sonya. "The Clark-Wilson Security Model" May 17, 2000.
<http://www.lib.iup.edu/comscisec/SANSpapers/blake.htm>
- Davis, Peter and Lewis, Barry. Teach Yourself Windows NT Server in 14 Days. Sams Publishing. Indianapolis Indiana. 1997.
- Frost, Jim. "An Overview of Windows NT Security" May, 4 1995.
<http://world.std.com/~jimf/nt-security/nt-security.html>
- Russinovich, Matt. "Windows NT Security, Part 1". Windows Network Magazine.
<http://www.winntmag.com/Articles/Print.cfm?ArticleID=3143>
- Russinovich, Matt. "Windows NT Security, Part 2". Windows Network Magazine.
<http://www.winntmag.com/Articles/Print.cfm?ArticleID=3492>
- Sutton, Steve. "An Intro to Windows NT Security" October, 16 2002.
http://secinf.net/windows_security/An_Intro_to_Windows_NT_Security.html
- Swift, Michael. (Et al) "Improving the Granularity of Access Control in Windows NT" Microsoft Corporation. Redmond, WA. 2001.