Windows servers

The NT security model
NT networks
NT networks

• Networked NT machines can be:
NT networks

- Networked NT machines can be:
  - Primary Domain controller
    - Centralizes user database/authentication
NT networks

- Networked NT machines can be:
  - Primary Domain controller
    - Centralizes user database/authentication
  - Backup Domain controller
NT networks

- Networked NT machines can be:
  - Primary Domain controller
    - Centralizes user database/authentication
  - Backup Domain controller
  - Domain member
NT networks

- Networked NT machines can be:
  - Primary Domain controller
    - Centralizes user database/authentication
  - Backup Domain controller
  - Domain member
  - Non-domain member
NT networks

• Networked NT machines can be:
  – Primary Domain controller
    • Centralizes user database/authentication
  – Backup Domain controller
  – Domain member
  – Non-domain member

• Trusted domains
NT networks

- Networked NT machines can be:
  - Primary Domain controller
    - Centralizes user database/authentication
  - Backup Domain controller
  - Domain member
  - Non-domain member

- Trusted domains

- Trusting resources
Architecture

Architecture

- Modular

Architecture

- Modular
- OS interface (system calls) are available at:
  - Integral subsystems
  - Environment subsystems


Breno de Medeiros
Florida State University
Fall 2005
Architecture

- Modular
- OS interface (system calls) are available at:
  - Integral subsystems
  - Environment subsystems
- Both run in the “user mode” protection space


Breno de Medeiros  Florida State University  Fall 2005
Security viewpoint
Security viewpoint

• Four main components:
Security viewpoint

• Four main components:
  – Executive (kernel mode)
Security viewpoint

• Four main components:
  – Executive (kernel mode)
  – Protected Servers (user mode)
Security viewpoint

• Four main components:
  – Executive (kernel mode)
  – Protected Servers (user mode)
  – Network Subsystem (both kernel and user modes)
Security viewpoint

- Four main components:
  - Executive (kernel mode)
  - Protected Servers (user mode)
  - Network Subsystem (both kernel and user modes)
  - Administrator tools (user mode)
Handle tables
Handle tables

- Each process has a table of “object handles” which enable the process to access those resources
Handle tables

- Each process has a table of “object handles” which enable the process to access those resources
  - Maintained by object manager
Handle tables

• Each process has a table of “object handles” which enable the process to access those resources
  – Maintained by object manager
  – Each handle describes the type of access the process has to the object (read, write, etc)
Handle tables

• Each process has a table of “object handles” which enable the process to access those resources
  – Maintained by object manager
  – Each handle describes the type of access the process has to the object (read, write, etc)
  – The object manager ensures that access is only granted if compatible with the handle
Handle tables

• Each process has a table of “object handles” which enable the process to access those resources
  – Maintained by object manager
  – Each handle describes the type of access the process has to the object (read, write, etc)
  – The object manager ensures that access is only granted if compatible with the handle

• When a process requests a new resource for the first time, the Object Manager asks the Security Reference Monitor to decide if the process may acquire the handle.
File system protection
File system protection

- Windows NT systems support many file systems, including:
  - File Allocation Table (FAT) FS
  - NTFS
  - CD-ROM FS (CDFS)
  - Named Pipe File System (NPFS)
  - Mailslot File System (MSFS)
File system protection

- Windows NT systems support many file systems, including:
  - File Allocation Table (FAT) FS
  - NTFS
  - CD-ROM FS (CDFS)
  - Named Pipe File System (NPFS)
  - Mailslot File System (MSFS)
- Only the NTFS is protected by the access control system.
File system protection

- Windows NT systems support many file systems, including:
  - File Allocation Table (FAT) FS
  - NTFS
  - CD-ROM FS (CDFS)
  - Named Pipe File System (NPFS)
  - Mailslot File System (MSFS)

- Only the NTFS is protected by the access control system.

- Use FAT only in diskettes
Configuration Manager
Configuration Manager

- Keeps the configuration registry
Configuration Manager

- Keeps the configuration registry
- Stores system configuration information, including the password database (SAM), hardware and initialization information, and OS configuration information
Configuration Manager

- Keeps the configuration registry
- Stores system configuration information, including the password database (SAM), hardware and initialization information, and OS configuration information
- Entries in the registry are called keys
Security-related servers

- Winlogon
- Session Manager
- Local Security Authority
- Security Accounts Manager (SAM)
- Service Controller
- Event Logger
Local Security Authority
Local Security Authority

- Local Security Authority Subsystem Service (LSASS)
Local Security Authority

- Local Security Authority Subsystem Service (LSASS)
  - Invoked at login time, it verifies the user authentication and grants the system access token (SAT), which is used to start the initial shell and is inherited by all programs spawned during this login session
Local Security Authority

- Local Security Authority Subsystem Service (LSASS)
  - Invoked at login time, it verifies the user authentication and grants the system access token (SAT), which is used to start the initial shell and is inherited by all programs spawned during this login session
  - Performs audit functions
Local Security Authority

- Local Security Authority Subsystem Service (LSASS)
  - Invoked at login time, it verifies the user authentication and grants the system access token (SAT), which is used to start the initial shell and is inherited by all programs spawned during this login session
  - Performs audit functions
  - Operates in user mode
Security Account Manager (SAM)
Security Account Manager (SAM)

- User mode component
Security Account Manager (SAM)

- User mode component
- Maintains the user account database required by the LSA
Security Account Manager (SAM)

- User mode component
- Maintains the user account database required by the LSA
- Therefore the login sequence requires the following intermediation by security-related services:
Security Account Manager (SAM)

- User mode component
- Maintains the user account database required by the LSA
- Therefore the login sequence requires the following intermediation by security-related services:
  - Winlogon ↔ LSA ↔ SAM
SAM and authentication
SAM and authentication

- It is possible to configure a special computer called a *domain controller* to consolidate the SAM database in a single server.
SAM and authentication

• It is possible to configure a special computer called a domain controller to consolidate the SAM database in a single server.

• Secure Attention Sequence: <CTRL> + <ALT> + <DEL> cannot be captured by user-level programs
  – The system invokes Winlogon, which starts a graphical application (GINA), to handle local and remote connection requests (via the LSA and SAM)
Protection (Access Control)

- Windows NT and later provide discretionary access control (DAC). The unit of control is called an ACE (access control entry). The format of ACEs is as follows:

<table>
<thead>
<tr>
<th>ACE Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inheritance Control Flags (Boolean flags)</td>
<td>• OBJECT_INHERIT_ACE</td>
</tr>
<tr>
<td></td>
<td>• CONTAINER_INHERIT_ACE</td>
</tr>
<tr>
<td></td>
<td>• NO_PROPAGATE_INHERIT_ACE</td>
</tr>
<tr>
<td></td>
<td>• INHERIT_ONLY_ACE</td>
</tr>
<tr>
<td>ACE Type</td>
<td>• ACCESS_ALLOWED_ACE</td>
</tr>
<tr>
<td></td>
<td>• ACCESS_DENIED_ACE</td>
</tr>
<tr>
<td></td>
<td>• SYSTEM_AUDIT_ACE</td>
</tr>
<tr>
<td>ACE Type-Specific</td>
<td>• SUCCESSFUL_ACCESS_ACE_FLAG</td>
</tr>
<tr>
<td></td>
<td>• FAILED_ACCESS_ACE_FLAG</td>
</tr>
<tr>
<td></td>
<td>• Access Mask</td>
</tr>
<tr>
<td></td>
<td>• SID</td>
</tr>
</tbody>
</table>
Picture from Final Evaluation of Windows NT Workstations
by Science Applications International Corp./ Ctr. for Information Security

Breno de Medeiros
Florida State University
Fall 2005
Windows passwords
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
- Password aging
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
- Password aging
- Minimum password length
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
  - Password aging
  - Minimum password length
  - Password uniqueness
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
  - Password aging
  - Minimum password length
  - Password uniqueness
  - Account lockout features
    - Number of failed logon attempts
    - How long to lockout an account
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
  - Password aging
  - Minimum password length
  - Password uniqueness
  - Account lockout features
    - Number of failed logon attempts
    - How long to lockout an account

- Better password protection is offered through passfilt.dll:
Windows passwords

• Password policies can be established using the UserManager administration tool, which supports the following:
  • Password aging
  • Minimum password length
  • Password uniqueness
  • Account lockout features
    – Number of failed logon attempts
    – How long to lockout an account

• Better password protection is offered through passfilt.dll:
  • Passwords must be at least six characters long
Windows passwords

- Password policies can be established using the UserManager administration tool, which supports the following:
  - Password aging
  - Minimum password length
  - Password uniqueness
  - Account lockout features
    - Number of failed logon attempts
    - How long to lockout an account
- Better password protection is offered through passfilt.dll:
  - Passwords must be at least six characters long
  - Passwords must contain at least three of the following four classes of characters:
    - Upper case letters
    - Lower case letters
    - Numbers
    - Non-alphanumeric characters (punctuation symbols)
Windows passwords

• Password policies can be established using the UserManager administration tool, which supports the following:
  • Password aging
  • Minimum password length
  • Password uniqueness
  • Account lockout features
    – Number of failed logon attempts
    – How long to lockout an account
• Better password protection is offered through passfilt.dll:
  • Passwords must be at least six characters long
  • Passwords must contain at least three of the following four classes of characters:
    – Upper case letters
    – Lower case letters
    – Numbers
    – Non-alphanumeric characters (punctuation symbols)
• Passwords can not match your username or part of your full name listed for the account.
Windows passwords
Windows passwords

- The original Windows password hashing scheme (LM):
  - Up to 14-character long passwords (all uppercase).
  - Computed as two independent hashes on 7-character values.
  - Highly vulnerable to dictionary based attacks, such as L0phtrack.
Windows passwords

- The original Windows password hashing scheme (LM):
  - Up to 14-character long passwords (all uppercase).
  - Computed as two independent hashes on 7-character values
  - Highly vulnerable to dictionary based attacks, such as L0phtrack
- NTLM uses 14 characters for a single hash
Windows passwords

- The original Windows password hashing scheme (LM):
  - Up to 14-character long passwords (all uppercase).
  - Computed as two independent hashes on 7-character values
  - Highly vulnerable to dictionary based attacks, such as L0phtrack
- NTLM uses 14 characters for a single hash
- LM hash still exported by default for compatibility with older machines in same network (i.e., placed in the SAM).
Windows passwords

- The original Windows password hashing scheme (LM):
  - Up to 14-character long passwords (all uppercase).
  - Computed as two independent hashes on 7-character values
  - Highly vulnerable to dictionary based attacks, such as L0phtrack
- NTLM uses 14 characters for a single hash
- LM hash still exported by default for compatibility with older machines in same network (i.e., placed in the SAM).
- NTLMv2 accepts longer than 14 characters, and in that case the exported values for LanManager are incorrect (backward incompatibility).
  - Encrypts password hashes before storing them in the SAM
Windows passwords

- The original Windows password hashing scheme (LM):
  - Up to 14-character long passwords (all uppercase).
  - Computed as two independent hashes on 7-character values
  - Highly vulnerable to dictionary based attacks, such as L0phtrack
- NTLM uses 14 characters for a single hash
- LM hash still exported by default for compatibility with older machines in same network (i.e., placed in the SAM).
- NTLMv2 accepts longer than 14 characters, and in that case the exported values for LanManager are incorrect (backward incompatibility).
  - Encrypts password hashes before storing them in the SAM
- Enforce 15 characters as minimum password length and disable LAM authentication
Password hash challenge-and-response
Password hash challenge-and-response

- Windows machines use hash-based challenge and response mechanisms
Password hash challenge-and-response

- Windows machines use hash-based challenge and response mechanisms
- This implies that while passwords are required for local login, password hashes can be used for remote authentication
Password hash challenge-and-response

- Windows machines use hash-based challenge and response mechanisms
- This implies that while passwords are required for local login, password hashes can be used for remote authentication
- It also means that, by eavesdropping the network and capturing challenge/response pairs, an adversary can collect information to perform dictionary and/or brute-force attacks on the password.