La sicurezza di Windows NT

Speaker:
Francesco Auriemma

Tratteremo

- **I componenti dell'architettura di sicurezza di Windows NT**
- **Le informazioni di sicurezza degli oggetti**
- **Le tecniche utilizzate per determinare l'accesso a una risorsa**
- **Come viene realizzato l'auditing di sicurezza**
- **Il logon interattivo**

La sicurezza

La sicurezza si riferisce alla protezione da danni, furti e usi non autorizzati di tutti i componenti hardware, software e dei dati memorizzati. Un piano di sicurezza che sia ben ideato, implementato e controllato facilita l'uso del computer e rende difficile o impossibile l'uso non autorizzato o il danno accidentale.

Il modello di sicurezza include componenti per controllare chi accede ai diversi oggetti, quali azioni un singolo utente può fare su un oggetto e quali eventi sono controllati.

Il modello di sicurezza di Windows NT è progettato per la sicurezza di livello C2, così come viene definito dal Dipartimento della Difesa Americano.

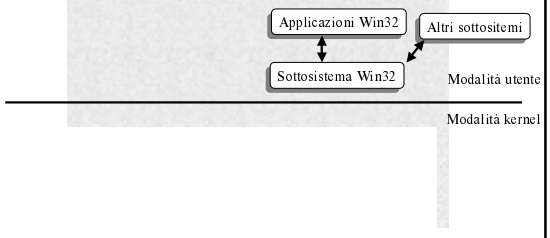
Modello C2

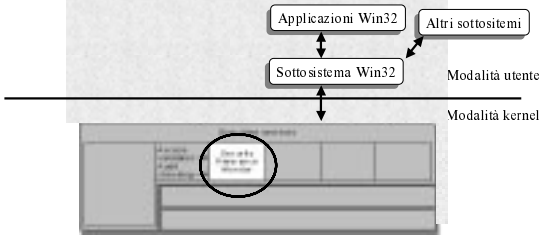
4 Gli amministratori di sistema devono essere in grado di controllare eventi collegati alla sicurezza. L'accesso a questi dati di controllo dev'essere limitato agli amministratori autorizzati.

5 Il sistema deve proteggere se stesso dall'interferenza o dalla manipolazione esterna come la modifica del sistema in esecuzione o dei file di sistema memorizzati su disco.

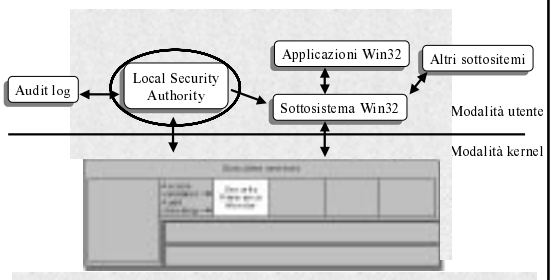
Questo mette in evidenza che la sicurezza sotto Windows NT è basata sull'utente

Architettura del modello di sicurezza

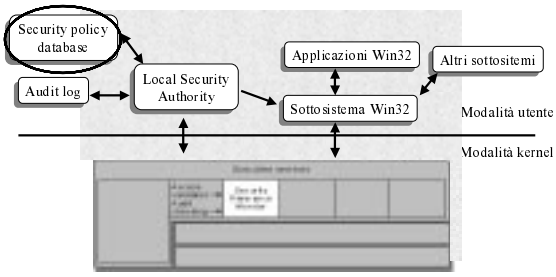




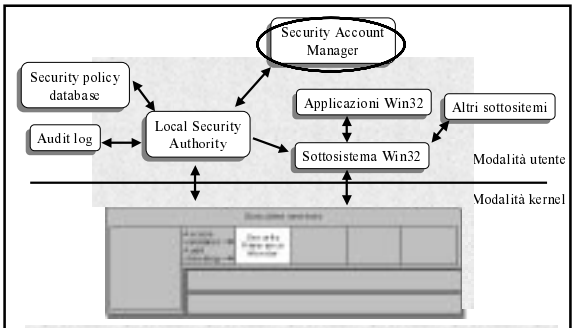
Security Reference Monitor (SRM) Questo componente verifica il permesso dell'utente di accedere a un oggetto e di eseguire una determinata azione. Esso offre dei servizi per assicurare che gli utenti e i processi che cercano di accedere a un oggetto abbiano i permessi necessari.



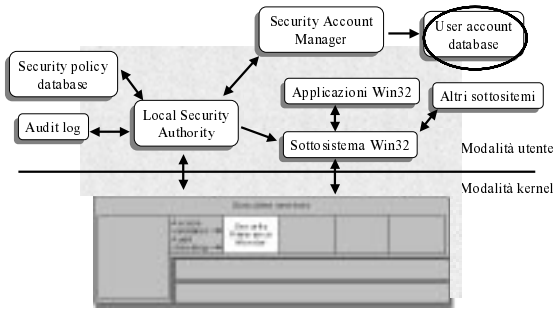
Local Security Authority (LSA). Questo componente genera gli access token, gestisce la sicurezza locale e offre dei servizi interattivi di autenticazione e convalida utente. Inoltre LSA controlla l'auditing e registra i messaggi di audit generati dal Security Reference Monitor.



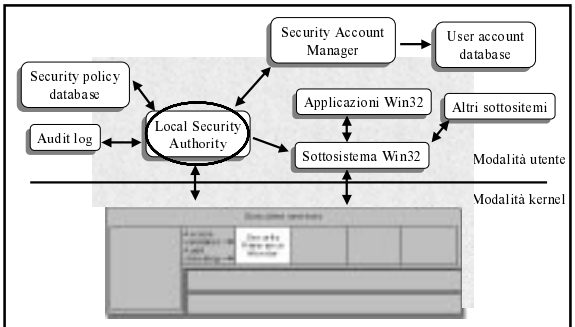
Database dei criteri di sicurezza LSA Un database che contiene le impostazioni dei criteri del sistema di sicurezza. Include informazioni come i domini affidabili per autenticare i tentativi di logon, chi ha le permission per accedere al sistema e come, a chi sono stati assegnati quali privilegi e che tipo di controllo (audit) viene effettuato.



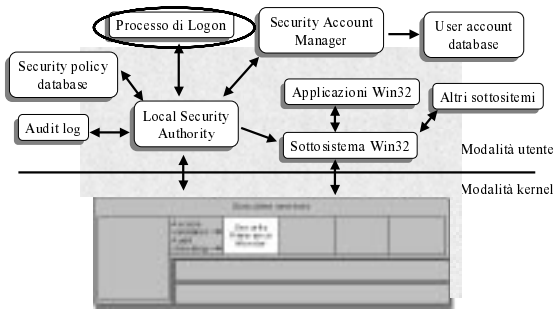
Server SAM Un Server SAM (Security Accounts Manager) è un insieme di subroutine responsabile della gestione del database che contiene i nomi utente e i gruppi definiti sul computer locale o in un dominio (se il sistema è un controllore di dominio).



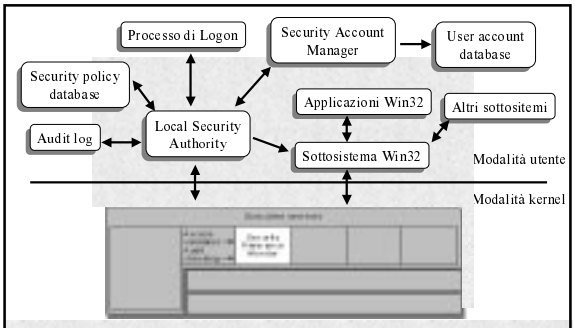
Database SAM Database (memorizzato nel registro sotto HKEY_LOCAL_MACHINE\SAM) che contiene gli utenti e i gruppi che sono stati definiti, unitamente alle loro password e altri attributi.



Pacchetto di autenticazione di default Una libreria a collegamento dinamico (DLL) chiamata MSV1_0.DLL.Questa DLL è responsabile del controllo di corrispondenza tra un nome utente e una password inseriti con quanto specificato nel database SAM.



Processo di logon Processo in modalità utente che esegue WINLOGON.EXE, il quale provvede alla cattura di nome utente e password per poi inviarli al server LSA per la verifica. Inoltre crea il processo iniziale della sessione utente



Questi componenti insieme sono conosciuti come sottosistema di sicurezza. Questo sottosistema viene chiamato ***Sottosistema Integrale,*** non sottosistema ambientale, perché agisce sull'intero sistema operativo Windows NT.

Local Procedure Call

Una ***chiamata a procedura locale*** (LPC) è uno strumento di comunicazione tra processi per il passaggio di messaggi ad alta velocità. Non è disponibile attraverso le API Win32 perché è un meccanismo interno disponibile solo ai componenti del sistema operativo Windows NT.

L'SRM e l'LSA comunicano utilizzando le LPC

Metodi di scambio dei messaggi

Le LPC sono progettate per permettere tre metodi di scambio di messaggi:

1. Un messaggio più piccolo di 256 byte può essere inviato chiamando una LPC con un buffer contenente il messaggio.
2. Se un messaggio è più grande di 256 byte, questo viene messo in una sezione condivisa alla quale i processi vengono mappati.
3. Quando un server vuole leggere o scrivere una quantità di dati superiore a quella che può trovare posto in una sezione condivisa, i dati possono essere letti o scritti direttamente dallo spazio degli indirizzi del client.

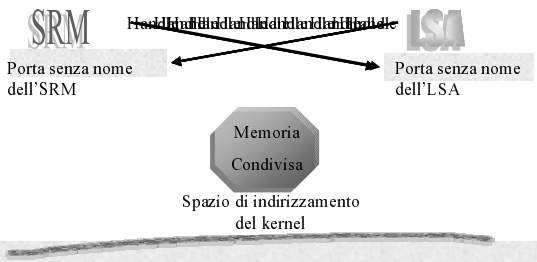
Porte LPC

- **Porta di connessione server.** Una porta con nome che è il punto di richiesta di connessione del server. I client si possono connettere al server connettendosi a questa porta.
- **Porta di comunicazione server.** Una porta senza nome che il server usa per comunicare con un client particolare. Il server ha una porta di questo tipo per ogni client attivo.
- **Porta di comunicazione client.** Una porta senza nome che un particolare thread client usa per comunicare con un particolare server.
- **Porta di comunicazione senza nome.** Una porta senza nome creata per essere usata da due thread nello stesso processo.

Come Funzionano?

1. Un server crea una porta di connessione server con nome.
2. Un client avanza una richiesta di connessione a questa porta.
3. Se la richiesta è accettata, vengono create due nuove porte senza nome: una porta di comunicazione client e una porta di comunicazione server.
4. Un client ottiene un handle alla porta di comunicazione client e il server ottiene un handle alla porta di comunicazione server.
5. Il client e il server useranno ora queste nuove porte per le loro comunicazioni.

Esempio



L'SRM crea una sezione di memoria condivisa per i messaggi più lunghi di 256 byte, passando un handle nella chiamata di collegamento.

Protezione degli oggetti

Gli oggetti che possono essere protetti in Windows NT comprendono file, dispositivi, mailslot, named pipe e pipe anonimi, processi, thread, eventi, mutex, semafori, timer waitable, token di accesso, windows station, desktop, condivisioni di rete, servizi, chiavi di registro e stampanti.

- Poiché le risorse del sistema, che vengono esportate alla modalità utente, vengono implementate come oggetti, il gestore degli oggetti rappresenta un punto di controllo importante per gli accessi di sicurezza.
- Per sapere chi può manipolare un oggetto, il sistema di sicurezza deve prima assicurarsi dell'identità di ogni utente.

Quali funzionalità consentono l'accesso?

- Account utente
- Autorizzazioni e Privilegi
- Gruppi di utenti
- Soggetti
- Informazioni di sicurezza sugli oggetti

Account utenti

Un amministratore crea un account utente assegnando un nome utente a un account, specificando i dati di identificazione dell'utente e definendo i diritti dell'utente nel sistema.
L'account comprende informazioni utente, l'appartenenza ai gruppi e informazioni sulla politica di sicurezza. Windows NT Server poi assegna un singolo identificatore di sicurezza (SID) al nuovo account.

- Quando un utente si collega, Windows NT crea un access token di sicurezza.
- Questo comprende un identificatore di sicurezza per l'utente e altre informazioni di sicurezza come il nome dell'utente e i nomi dei gruppi ai quali l'utente appartiene.
- Ogni processo, che viene eseguito per conto di questo utente, avrà una copia del suo access token.

Autorizzazioni e Privilegi

- Un Autorizzazione è una regola che determina quale azione un utente può eseguire su un oggetto, come l'autorizzazione di sospendere un thread o l'autorizzazione di leggere un file.
- Un Privilegio è un autorizzazione per un utente per eseguire determinate operazioni sul sistema, come il privilegio di effettuare il debug di applicazioni.

Come vengono realizzati?

Un Autorizzazione è specificata in una struttura dati chiamata Access Control List o ACL che è normalmente associata ad un oggetto.
Un utente è rappresentato da un token di accesso. Quando un utente cerca di accedere a un oggetto sicuro, il suo access token viene confrontato con l'ACL dell'oggetto

I Privilegi sono codificati nell'access token, così nessun oggetto è associato con loro. La ragione per cui i privilegi sono codificati nell'access token è che molti di loro sovrascrivono le richieste di sicurezza.

Raggruppamento di utenti con bisogni simili

Gli amministratori normalmente raggruppano gli utenti in base alle loro esigenze lavorative.

Sono possibili due tipi di account di gruppo:

- Un Gruppo Locale può includere gli account utente e i gruppi globali provenienti da uno o più domini, raggruppati insieme sotto un unico nome di account.
  È possibile aggiungere al gruppo locale gli utenti e i gruppi globali esterni al dominio locale solo se appartengono ad un dominio trusted.
  Locale significa che è possibile concedere diritti e autorizzazioni a un gruppo per usare le risorse solo in un singolo dominio (locale).Un gruppo locale può contenere utenti e gruppi globali, ma non può contenere gruppi locali.

Soggetti

Uno degli scopi del modello di sicurezza di Windows NT è quello di assicurare che i programmi eseguiti da un utente non possiedano un accesso agli oggetti superiore a quello dell'utente.

- Quando un programma o un processo viene eseguito per conto dell'utente, si dice che viene eseguito nel ***contesto di sicurezza*** di quell'utente. Il contesto di sicurezza consiste di informazioni che descrivono i privilegi, gli account e i gruppi associati con un processo o con un thread.

Soggetti

Esistono due classi di soggetti all'interno dell'architettura di sicurezza di Windows NT:

Soggetti

Esistono due classi di soggetti all'interno dell'architettura di sicurezza di Windows NT:

- Soggetto semplice

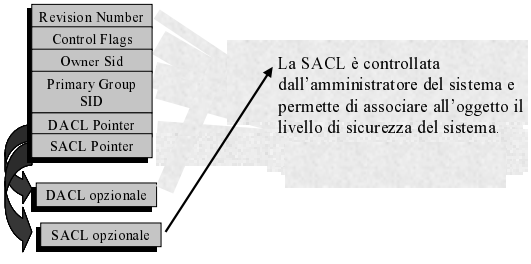
Soggetti

Esistono due classi di soggetti all'interno dell'architettura di sicurezza di Windows NT:

- Un Soggetto semplice è un processo a cui è stato assegnato un contesto di sicurezza quando l'utente corrispondente si è collegato. Esso non sta agendo nella capacità di un server protetto, che può avere altri soggetti come client.
- Un Soggetto Server, è un processo implementato come server protetto che possiede altri soggetti come client. In questo ruolo, normalmente un soggetto server ha il contesto di sicurezza di quei client disponibili all'uso quando agisce per conto loro.

Informazioni di sicurezza per gli oggetti

Un descrittore di sicurezza *(**Security Descriptor**)* descrive gli attributi di sicurezza di un oggetto che gli vengono associati nel momento in cui l'oggetto viene creato.



Struttura delle DACL

La **DACL** contiene un ingresso per ogni utente, gruppo locale o gruppo globale a cui è stato dato il permesso di accedere all'oggetto. Ognuno di questi ingressi è nella forma di un Access Control Entry (ACE).

Assunzioni

Quando un oggetto non ha una DACL, allora nessuna protezione è assegnata all'oggetto e ogni richiesta di accesso è permessa. Inizialmente l'SD di un oggetto è settato in modo che la sua DACL non abbia ACE, intendendo che nessun utente può accedere all'oggetto.

Struttura delle SACL

Una **SACL** è costruita in maniera del tutto simile a una DACL, ad eccezione che invece di definire degli accessi permessi o negati, la SACL specifica quali azioni un utente o un gruppo particolare deve effettuare affinché il sistema scriva gli eventi di controllo all'interno del NT Security log.

La maschera dell'header lista gli accessi che generano un evento quando l'utente o il gruppo, identificato con il SID, effettua l'accesso.

Come vengono assegnate le ACL?

Per determinare quale ACL assegnare a un nuovo oggetto, il sistema di sicurezza applica una di queste tre regole mutuamente esclusive.

3

Se non si verifica nessuno dei primi due casi, il sistema di sicurezza recupera l'ACL di default dal token di accesso del chiamante e la applica al nuovo oggetto.

Access Tokens

Il Security Reference Monitor utilizza i token (o ***access tokens***) per definire il contesto di sicurezza di un processo o di un thread.

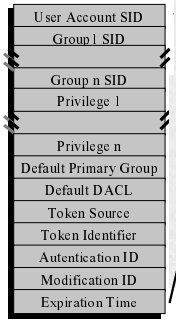
Internamente la struttura del token di accesso in modalità kernel è un oggetto allocato dal gestore degli oggetti al quale punta il blocco del processo executive o il blocco thread.

Associazione dei token ai processi

- Ogni processo ha un token di accesso primario ereditato dal proprio processo di creazione.
- Durante il logon, il processo LSASS verifica che il nome utente e la password corrispondano alle informazioni memorizzate nel SAM.
- Se il controllo ha esito positivo, viene inviato un token di accesso a WinLogon, il quale assegna tale token al processo iniziale della sessione utente.

Per default un thread non riceve un token di accesso, a meno che non lo richieda utilizzando la funzione di Win32 ImpersonateSelf, che clona il token di accesso primario del processo a cui appartiene e lo associa al thread.

Struttura di un token



Il campo ***Expiration Time*** che è presente ma non utilizzato sin da NT 3.1. Presumibilmente Microsoft aveva dato la possibilità ai token di essere validi per un periodo di tempo prima di espirare.

Impersonation

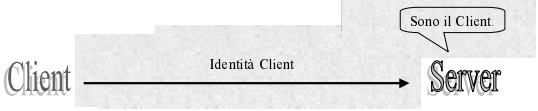
In NT, un server esporta risorse come file, stampanti e database. Un client che vuole accedere a una risorsa invia una richiesta al server. Quando il server riceve la richiesta, deve garantire che il client abbia i permessi per eseguire le operazioni sulla risorsa.

esempio

La personificazione permette a un server di notificare all'SRM che il server sta temporaneamente adottando il profilo di sicurezza di un client che ha effettuato la richiesta di una risorsa. Il server può allora accedere alle risorse da parte del client e l'SRM può controllare la validità dell'accesso.

Impersonation

Per prevenire misure di personificazione, NT non permette a un server di effettuare la personificazione senza il consenso del client, il quale può specificare il livello di personificazione che il server può raggiungere:



Delegation impersonation, il livello più permissivo, che permette al server di personificare il client sui sistemi locali e remoti.

Determinazione dell'accesso

Determinazione dell'accesso

4

Ogni ACE della DACL viene esaminato, a partire dal primo.
Se la SID nell'ACE corrisponde a un SID abilitato nel token di accesso del chiamante, l'ACE viene elaborato.
Se si tratta di un ACE ad accesso consentito, i diritti della maschera di accesso nell'ACE sono consentiti.
Se sono stati consentiti tutti i diritti di accesso richiesti, il controllo dell'accesso viene portato a buon fine.
Se si tratta di un ACE ad accesso negato e uno dei diritti di accesso richiesti si trova tra i diritti di accesso negato, l'accesso all'oggetto viene negato

5

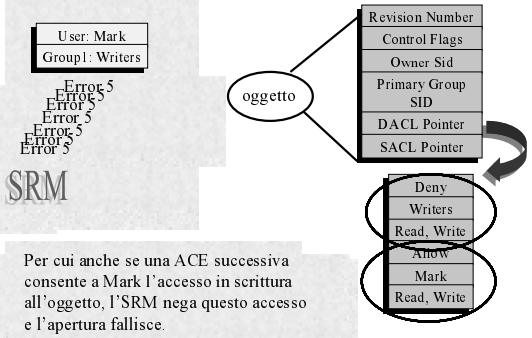
Se viene raggiunta la fine della DACL e qualcuno dei diritti di accesso richiesti non è stato consentito, l'accesso viene negato.

Osservazioni

Entrambi gli algoritmi di convalida degli accessi sono basati sul fatto che gli ACE ad accesso negato vengono posizionati prima degli ACE ad accesso consentito.

Poiché non sarebbe efficiente per il sistema di sicurezza elaborare la DACL ogni volta che un processo utilizza un handle, questo controllo avviene solo all'apertura e non ad ogni utilizzo di un handle.

Esempio



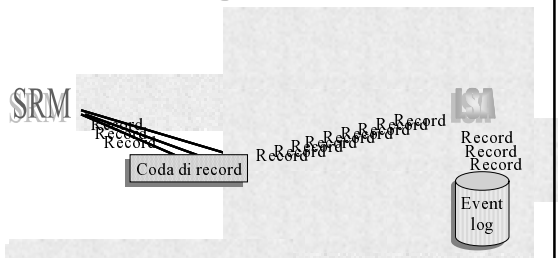
Per cui anche se una ACE successiva consente a Mark l'accesso in scrittura all'oggetto, l'SRM nega questo accesso e l'apertura fallisce.

Auditing di sicurezza

Il gestore degli oggetti può generare eventi di audit come risultato di un controllo dell'accesso.
Il codice in modalità kernel è sempre autorizzato a generare un evento di audit, tuttavia i processi che richiamano i servizi del sistema di controllo devono avere il privilegio SeAuditPrivilege per generare correttamente i record di audit.
Questo requisito impedisce a un programma malintenzionato in modalità utente di ingolfare il Security log.

La decisione di controllare un tipo particolare di evento di sicurezza è basato sui criteri di audit del sistema locale. Tali criteri, chiamati ***criteri di sicurezza locale***, fanno parte dei criteri di sicurezza seguiti dall'LSA.

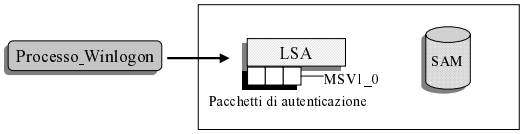
Auditing di sicurezza



LSA ha il compito di ricevere i record di audit dalla coda dell'SRM, di modificarli e di inviarli all'Event Log.

Logon interattivo

Il logon si verifica tramite l'interazione fra il processo di logon (WinLogon), l'LSA, uno o più pacchetti di autenticazione e il SAM.



Winlogon

WinLogon è un processo fidato (trusted) che ha il compito di gestire le interazioni utente relative alla sicurezza:

Il processo ***WinLogon*** deve garantire che le operazioni di sicurezza non siano visibili agli altri processi attivi. Per esempio, WinLogon si assicura che un processo non fidato non possa ottenere il controllo del desktop durante una di queste operazioni e di conseguenza ottenere l'accesso alla password.

WinLogon è l'unico processo che intercetta le richieste di logon dalla tastiera. Effettua chiamate all'LSA per autenticare l'utente che cerca di collegarsi.

Inizializzazione di WinLogon

Durante l'inizializzazione del sistema, prima che vengano attivate le applicazioni utente, WinLogon esegue alcune procedure per assicurarsi il controllo della workstation quando il sistema è pronto per l'utente:

4

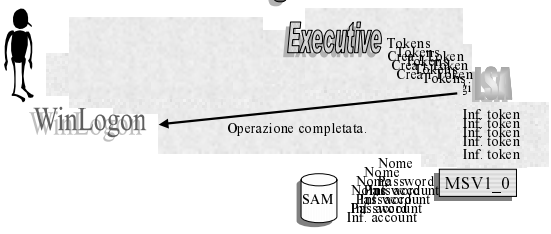
Richiama LsaLookupAuthenticationPackage per ottenere un ID associativo (association ID) per MSV1_0, che verrà utilizzato per le operazioni di autenticazione durante un tentativo di logon.

Inizializzazione di WinLogon

WinLogon esegue quindi certe operazioni Windows per impostare l'ambiente a finestre:

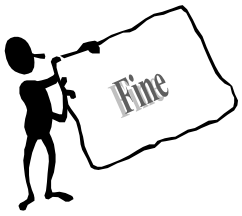
1. Inizializza e registra una struttura di dati di classe finestra che associa una procedura WinLogon con la finestra creata successivamente.
2. Registra la sequenza di tasti di accesso SAS (Secure Attention Sequence) associandola alla finestra appena creata, garantendo così che la window procedure di WinLogon venga chiamata ogni volta che l'utente inserisce la SAS.
3. Registra la finestra in modo che venga richiamata la procedura ad essa associata se un utente si scollega o scade il periodo del salvaschermo.

Fasi del logon utente



A questo punto l'LSA informa WinLogon del completamento dell'operazione e invia un handle al token di accesso, il LUID per la sessione di logon e le informazioni di profilo, se presenti,inviate da MSV1_0.

La sicurezza in locale di Windows NT



Grazie per l'attenzione