La Sicurezza in Windows NT:

Speaker:
Ricco Daniela
Auriemma Francesco

1
- Descrizione generale dell'architettura del sistema e dell'interazione tra i suoi componenti.
- Descrizione del sottosistema di sicurezza locale.

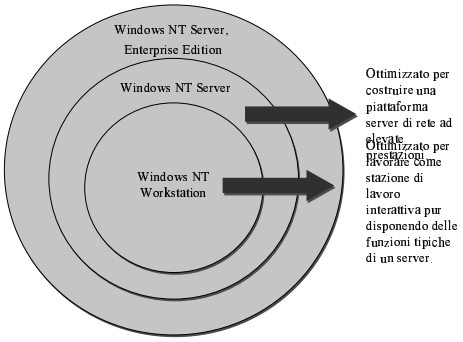
2
- Descrizione delle tecniche supportate dal sistema per l'organizzazione e la protezione delle risorse all'interno di una rete.
- Implementazione del meccanismo delle password all'interno del sistema.

Ci riferiremo a Windows NT 4.0 anche se sottolineeremo gli aspetti del sistema modificati in Windows 5.0

L'architettura di Windows NT

Esistono 3 edizioni di Windows NT:

*Windows NT Server, Enterprise Edition
*Windows NT Server
*Windows NT Workstation

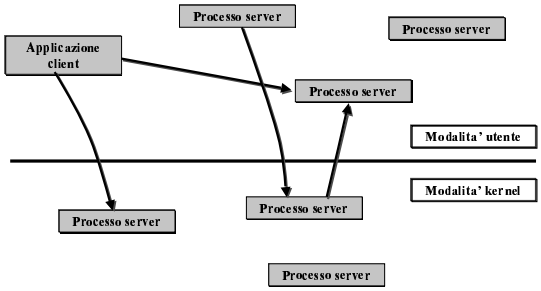


Windows NT è stato progettato combinando le caratteristiche di un sistema operativo a strati con quelle di un sistema client/server

La stratificazione consente:

Limitazione della quantità di codice che dispone di potere illimitato.

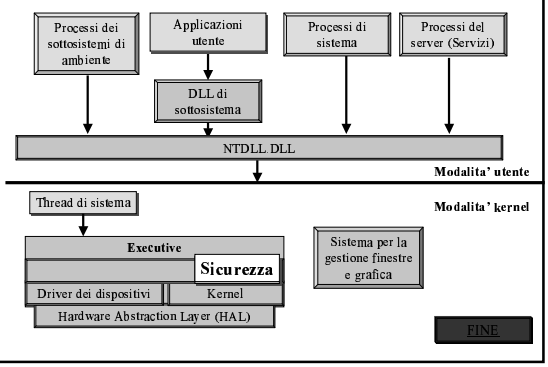
Architettura client/server



Modalità kernel e modalità utente

- I thread eseguiti in *modalità utente* hanno un privilegio piu' basso rispetto a quelli eseguiti in modalità kernel quindi vengono eseguiti in uno spazio di indirizzi privato, mentre
- ai thread eseguiti in *modalità kernel* e' permesso l'accesso a tutta la memoria dello spazio di sistema ed a tutte le istruzioni della CPU, quindi
- Windows NT non offre alcuna protezione per i componenti che sono eseguiti in *modalità kernel*.
- Un processo eseguito in *modalità utente* può passare alla *modalità kernel* quando deve effettuare una chiamata di sistema o accedere a strutture di dati interne al sistema. Alla fina dell'esecuzione del servizio, il processore viene commutato alla *modalità utente*.

L'architettura di Windows NT



Sottosistemi di ambiente

- Forniscono un ambiente di sistema operativo alle applicazioni utente.
- Ciascun sottosistema fornisce l'accesso a sottoinsiemi disgiunti di servizi di Windows NT.

Windows NT supporta tre sottosistemi di ambiente:

-Win32

-POSIX

-OS/2

•Win32 costituisce il sottosistema primario di Windows NT.

•Soltanto in esso sono sistemate le funzioni di visualizzazione dell'I/O (richiamate anche da POSIX e OS/2).

Include:

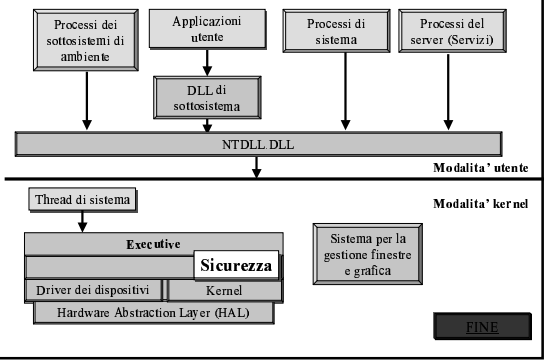
•Gestore delle finestre.

•Interfaccia GDI.

•I Driver dei dispositivi grafici.

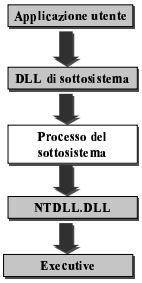
•Ogni sottosistema è costituito da:

L'architettura di Windows NT

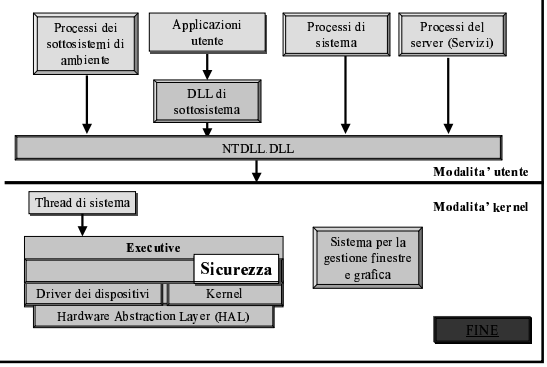


DLL (Dynamic Link Libraries)

•Nel caso in cui una applicazione effettui una chiamata relativa ad una funzione di una DLL di sottosistema, ci si può trovare di sistema delle delle situazioni relative al sottosistema.



L'architettura di Windows NT



NTDLL.DLL

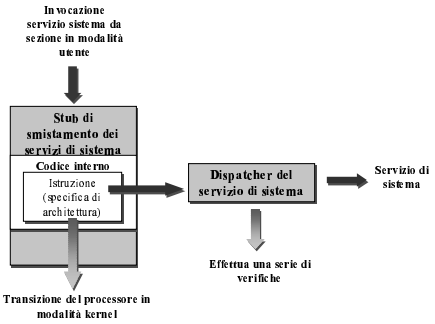
•E' una particolare libreria di sistema a collegamento dinamico utilizzata dalle DLL di sottosistema.

•Essa contiene due tipi di funzioni:

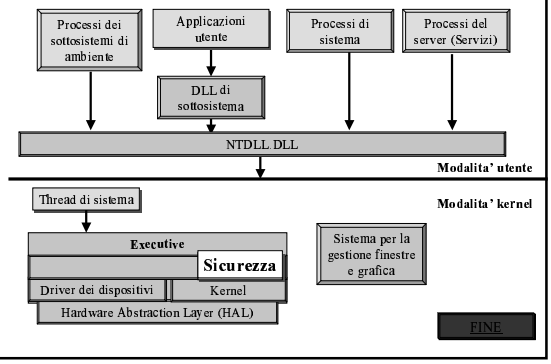
•Funzioni che forniscono l'interfaccia ai servizi di sistema dell'**Executive** che possono essere richiamate in modalità utente (*stub di smistamento dei servizi*).

•Funzioni di supporto come quelle che si occupano del caricamento delle immagini (.EXE) e quelle di comunicazione del processo del sottosistema Win32.

•Contiene anche il ***Dispatcher delle eccezioni***.



L'architettura di Windows NT



Executive: sezione superiore

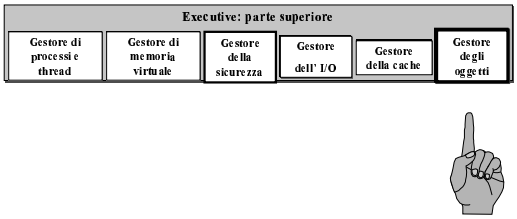
Comprende 4 tipi di funzioni:

•Funzioni richiamabili in modalita' utente per le quali l'interfaccia si trova in NTDLL.DLL.

•Funzioni richiamabili in modalita' utente ma che non sono disponibili attraverso funzioni di sottosistema documentate (tra esse vi sono le **LPC**).

•Funzioni richiamabili solo in modalita' kernel solatanto.

•Funzioni interne ad un componente.



Oggetti e Object manager

Windows NT implementa un modello ad oggetti per offrire un accesso coerente e sicuro a tutte le componenti del sistema.

Tutte le risorse di sistema che necessitano di condivisione e protezione e che sono rese visibili alle applicazioni in modalità utente, vengono implementate come oggetti.

Windows NT utilizza gli oggetti per ottenere tre importanti obiettivi:

- Fornire nomi leggibili alle risorse di sistema.
- Suddividere in maniera opportuna le risorse tra i processi.
- Implementare un meccanismo di protezione per proteggere le risorse da accessi non autorizzati dato che è possibile definire metodi sull'oggetto che possono essere invocati dall'esterno senza accedere ai componenti privati dello stesso.

Windows NT considera due tipi di oggetti:

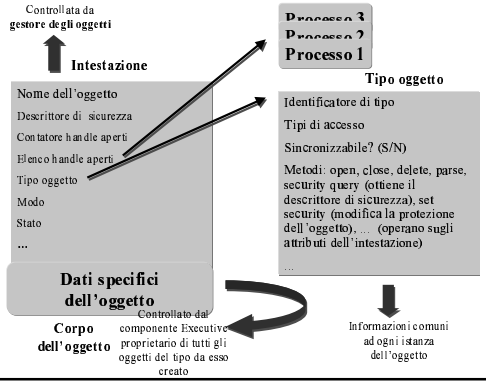
Oggetti executive Sono implementati dai componenti dello strato superiore dell'Executive (gestore della memoria, il gestore dei processi, ecc.).

Oggetti kernel Sono implementati dal Kernel. Forniscono capacità fondamentali quali la sincronizzazione. Molti oggetti executive incapsulano uno o più oggetti kernel.

L'Object manager

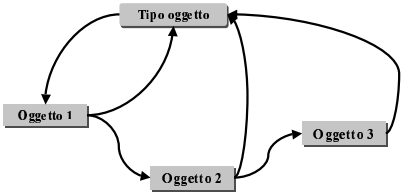
Object manager

Struttura di un oggetto



Il Tipo dell'oggetto

- Collega tutti gli oggetti di uno stesso tipo, permettendo al **Gestore degli oggetti** di localizzarli in maniera immediata.
- Non può essere manipolato in modalità utente.
- Alcuni degli attributi in esso definiti sono visibili anche attraverso le routine API Win32.

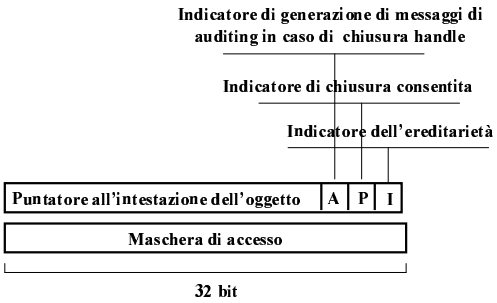


Gli handle ad un oggetto

- Rappresentano l'interfaccia all'oggetto a cui si riferiscono.
- Impediscono di accedere direttamente ad un oggetto da parte dei processi utente.
- I processi possono anche ereditarli al momento della loro creazione o possono riceverne duplicati da altri processi in un qualsiasi momento.
- Permettono al gestore degli oggetti di effettuare i dovuti controlli di accesso ad un oggetto.
- Costituiscono una interfaccia coerente agli oggetti (non c'è differenza per un processo, tra un handle ad un file, un handle ad un evento o un handle ad un thread.

Ad ogni processo è associata una tabella degli handle aperti.

Un handle rappresenta un indice in tale tabella.

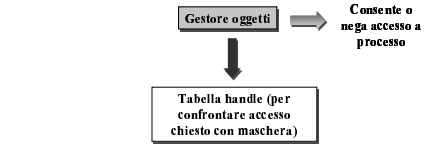


Come fa il sistema a conoscere il numero di handle ad un oggetto aperti?

Ogni volta che un processo apre un handle viene incrementato il contatore degli handle aperti per quell'oggetto.

Quando un processo termina di utilizzare un oggetto chiude l'handle ad esso ed il contatore degli handle viene decrementato.

Quando il contatore giunge a zero, l'oggetto viene rimosso, così nuovi processi non possono aprire un handle all'oggetto.

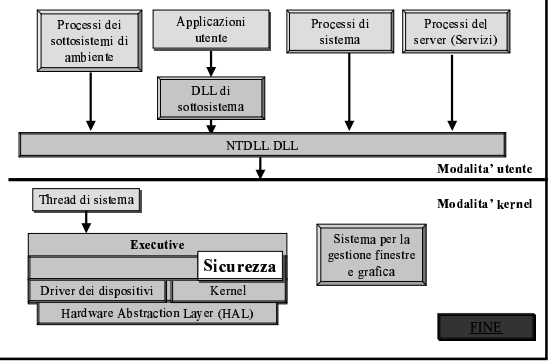


Security Reference Monitor

•E' responsabile dei controlli di sicurezza sugli accessi per quanto riguarda gli oggetti, la manipolazione dei diritti degli utenti e la generazione di eventuali messaggi conseguenti ai controlli di sicurezza effettuati.

•E' parte del sottosistema di sicurezza di Windows NT.

L'architettura di Windows NT



Executive: sezione inferiore
Kernel

Le funzioni principali che svolge sono le seguenti:

•Pianificazione e smistamento dei thread.

•Gestione e smistamento delle eccezioni.

•Gestione e smistamento degli interrupt.

•Sincronizzazione multiprocessore.

•Rende disponibile al resto dell'Executive gli **oggetti del kernel** (che in alcuni casi vengono anche esportati in modalita' utente).

QUINDI

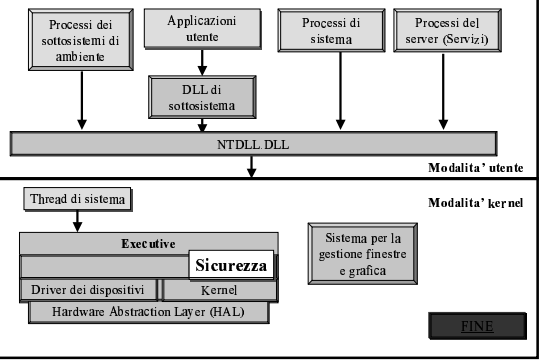
•Fornisce una base di funzioni primitive e meccanismi di s.o. ben definiti a basso livello che permettano ai componenti di piu' alto livello di svolgere quanto necessario.

•Astrae il resto dell'Executive e i Driver dei dispositivi dalle differenze esistenti tra le architetture hardware supportate da Windows NT.

N.B.

Implementa i meccanismi propri del s.o. ed evita scelte di tipo strategico tranne per cio' che riguarda la pianificazione e lo smistamento dei thread.

L'architettura di Windows NT



Executive: sezione inferiore

Driver di periferica o dei dispositivi

•Definiscono l'interfaccia tra il sistema di I/O e l'hardware pertinente.

•Sono scritti in C o C++.

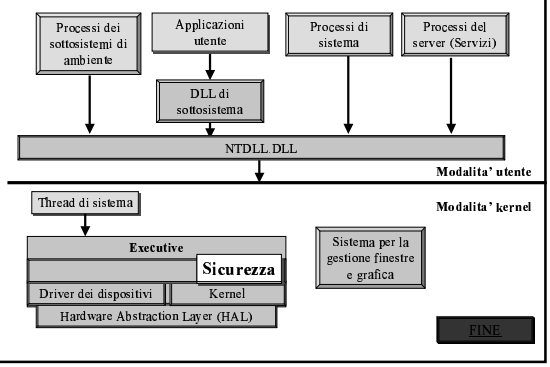
•Esistono quattro tipi di driver dei dispositivi:

- •Driver dei dispositivi hardware.
- •Driver del file system.
- •Driver di filtro.
- •Redirector e server di rete.

•Costituiscono l'unico modo di aggiungere codice in modalità kernel al sistema.

Occorre avere gli opportuni permessi di accesso al sistema per poterli installare.

L'architettura di Windows NT

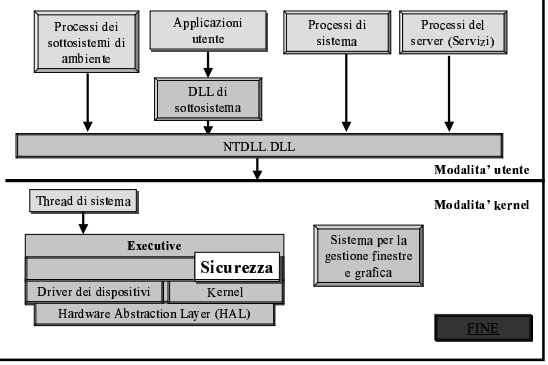


HAL (Hardware Abstraction Layer)

•E' l'elemento chiave che rende Windows NT portabile su diverse piattaforme hardware.

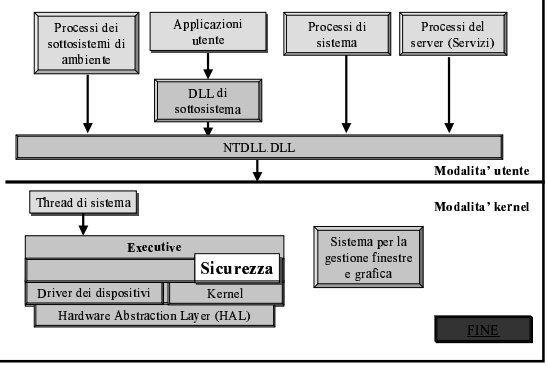
•E' costituito da uno strato di codice che isola il Kernel, i Driver di dispositivi ed il resto dell'Executive di Windows NT dalle particolarita' hardware specifiche della piattaforma.

L'architettura di Windows NT



Sistema di finestre e grafica

L'architettura di Windows NT



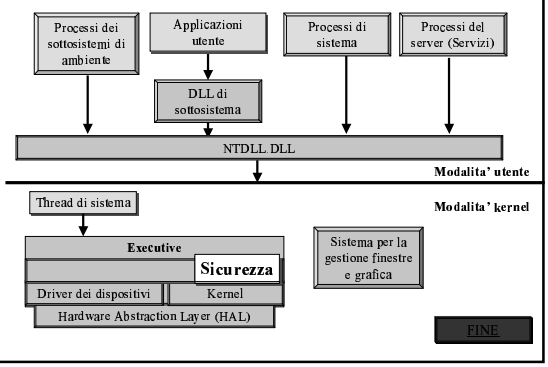
Servizi e Processi del Server

I Servizi sono delle immagini Win32 eseguite in modalità utente che richiamano particolari funzioni Win32 per interagire con il *Controller di servizio*. A seguito di tali richieste, il *Controller di servizio*, invoca l'esecuzione di particolari processi detti processi del server.

I Processi del server possono essere configurati in modo da partire automaticamente durante l'avvio del sistema; possono anche essere avviati manualmente.

Molti componenti di Windows NT sono implementati come Processi del server e tra essi il **servizio di log degli eventi** ed il **servizio di logon di rete** (*NetLogon.*)

L'architettura di Windows NT



Processi di sistema

Sono processi di supporto al sistema.

Fanno parte di ogni sistema Windows NT:

•*Processo Idle*. Contiene un thread per CPU per contabilizzare il tempo di inattività della CPU.

•*Processo System.* Ingloba i thread di sistema in modalità kernel.

•*Gestore della sessione.* Funge da interruttore e controllore tra applicazioni e debugger.

•Processo del sottosistema Win32.

•Processo di logon (*WINLOGON.EXE*).

•Server di autenticazione della protezione locale (*LSASS.EXE*) responsabile protezione per la sicurezza del sistema locale

•*Controller di servizio* e corrispondenti processi di servizio.

WINLOGON.EXE

•Gestisce le attività di logon e di logoff da parte degli utenti in modo interattivo.

•Viene avviato quando viene inserita un particolare combinazione di tasti (Ctrl-Alt-Delete).

Tutti gli aspetti di identificazione e di autenticazione di tale processo sono implementati in una DLL *GINA* (Graphical Identification and Authentication). Essa implementa l'interfaccia predefinita di logon di Windows.

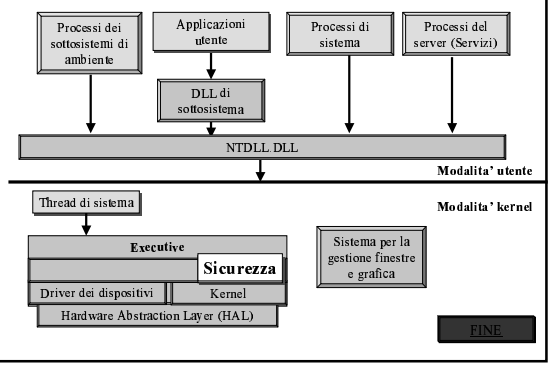
LSASS.EXE

•E' responsabile dei criteri di protezione per la sicurezza del sistema locale.

• L'autenticazione degli utenti.

• L'invio di messaggi per l'auditing della sicurezza all'*Event Log* (registro eventi).

L'architettura di Windows NT



FINE PRIMA PARTE