

Sistemi Operativi Windows - Architettura di Sistema.

Il seguente materiale è di proprietà di Stefano Pinardi ed è coperto da copyright ne è consentito l'uso agli studenti per soli motivi di studio, novembre 2021.

Capitolo 1 - Sezione 1: Processi e thread

Capitolo 1 - Sezione 2: L'autenticazione nel quadro architetturale

Capitolo 2 - Utente e Dominio

1.1 Architettura di Sistema – Un'introduzione

Il termine architettura di un sistema operativo denota complessivamente la struttura **totale** del sistema, se sia monolitico, virtualizzato, microkernel, i tipi servizi, le funzioni di accesso a memoria, alla rete, il modello a processi. Argomenti tutti che richiedono una lunga trattazione.

Questi argomenti vengono coperti altrove, e si intendono spiegati, basti qua sapere che mentre il sistema operativo Unix o Linux è detto modello monolitico, quello del sistema operativo Microsoft per eccellenza, il sistema operativo Windows, è un modello a microkernel.

Microkernel non si riferisce alla dimensione del kernel, piuttosto alla modalità di accesso alle risorse architetturali, e di suddivisione delle stesse tra kernel mode e user mode. Mentre in ambiente Unix e Linux quasi tutte le funzioni architetturali si trovano in modalità kernel, e tutti i processi vi accedono in modalità user, in Windows alcune funzioni architetturali – come i subsystem – funzionano già in modalità user.

Questo non significa che il sistema sia meno sicuro: l'accesso alle componenti kernel è sempre mediato da "stub", tra cui la NTDLL.DLL (vedi fig. 1.0) e da astrazioni che costringono il passaggio al modo kernel per accedere ai moduli kernel di sistema. Significa invece che il sistema è organizzato in modo più modulare e consente, se possibile e necessario, l'accesso ad alcune componenti in modo più diretto, altre in modo più mediato (ad es dai subsystem).

Per dare un quadro introduttivo generale, Windows è una famiglia di sistemi operativi che vanno dal Windows NT 3.51/4 alla ultima recente realizzazione di Windows 11. Questi sistemi prodotti sono tutti fondamentalmente basati sulla architettura Windows NT 3.51/4 progettato da D.N. Cutler tra il 1993 (NT 3.51) e il 1996 (NT 4.0).

Mentre molto cambia a livello di utente tra le varie realizzazione del sistema operativo, gli aspetti interni nel corso degli anni, la sua vera architettura non è variata: sono stati introdotti i meccanismi di plug & play, e quelli di autenticazione biometrica, e nella versione 2000 (XP) sono stati riscritti alcuni moduli

kernel relativi alla rete, ma il core è sempre il medesimo. Questo non deve fare pensare a un sistema antico o antiquato, Windows è nato come un sistema modulare by design, e la sua robustezza nel tempo è invece spunto di riflessione sulla lungimiranza di Cutler di aver disegnato un core logico e strutturato, che è ancora up-to-date e sulla qualità di questo design.

Parlando di definizioni, Windows è un sistema operativo **multitutente, multiprocess (multithread) con prelazione, mono e multiprocessore.**

Windows è progettato per lavorare su architetture diverse ad es Intelx86 e Alpha (hardware ora non più in produzione). L'astrazione dalla architettura hardware è garantita dall' HAL (hardware abstraction layer), anche se fondamentalmente, oggi come oggi, Windows gira quasi esclusivamente su architetture di tipo Intelx86, sigla che identifica un hardware progettato anche da costruttori non Intel (ad esempio AMD) ma compatibili con questa.

Quello che si intende dire, è che l'accesso alle componenti hardware sono servite al progettista e al programmatore di driver, con una visione unica che è quella offerta dalla HAL. L'architettura sottostante potrebbe essere di qualsiasi tipo. Questo garantisce la modularità anche a livello hardware del sistema.

Il kernel ha pieno accesso alle risorse hardware e software del computer ed esegue il codice in un proprio spazio di indirizzamento, che è separato da quello user, rendendo l'esecuzione protetta da accessi malevoli da parte di processi in user mode. Controlla lo scheduling, la priorità dei thread, la gestione della memoria e come già detto l'interazione con l'hardware attraverso i driver e l'HAL. Il kernel mode impedisce e alle applicazioni ma anche ai servizi in user mode di accedere ad aree critiche del sistema, i processi in user mode chiedono al kernel di effettuare le operazioni di architettura necessarie.

I vantaggi di questo design modulare per il sistemista professionale sono molteplici:

- *Manutenzione ridotta:* è possibile installare un server che svolga solo ed esclusivamente una funzione (AD DS, DHCP Server, DNS Server, File Services, Print Services, o Streaming Media Services).

- *Ridotta superficie d'attacco*: l'installazione può essere minima, quindi meno applicazioni che possono essere soggette a bug.
- *Meno spazio e memoria occupati*: è possibile installare Windows in meno di un GB: meno applicazioni significano meno RAM occupata, con l'evidente vantaggio di poter installare più macchine virtuali, ognuna con una specifica funzione, su una stessa macchina fisica.

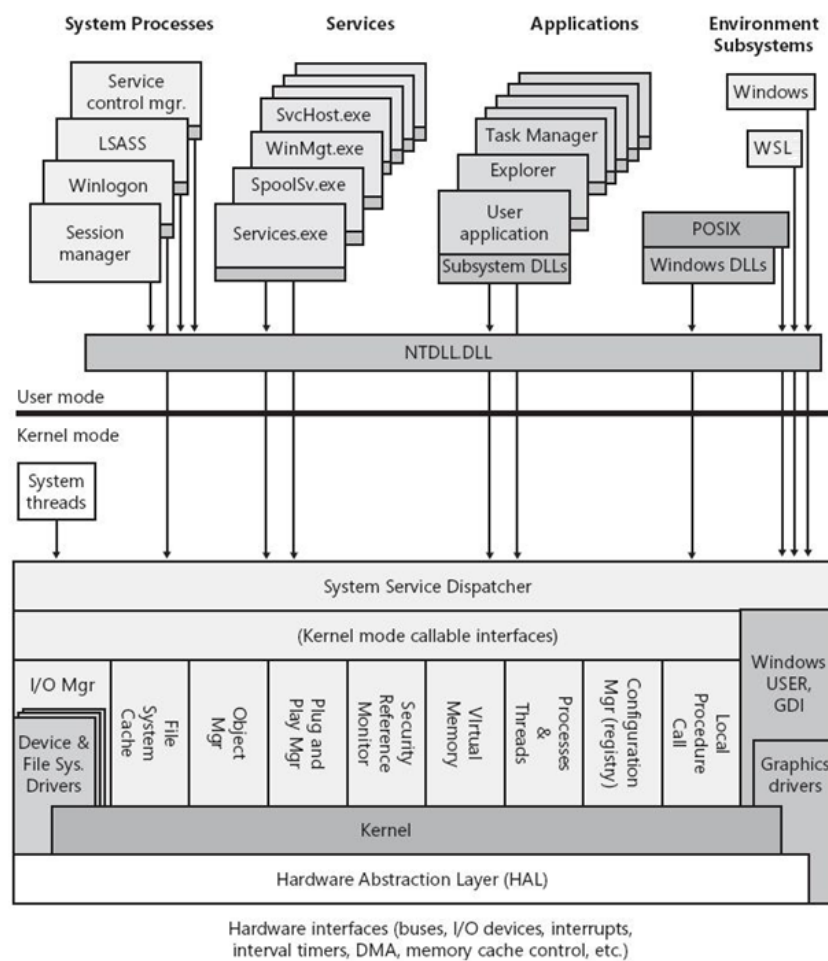


Fig 1.0 L'architettura interna di Windows è basata su quella originale di Windows NT 3.51/4.0 progettata da D.N. Cutler nel 1996 (immagine di D. Solomon e M.Russinovich © leggermente adattata)

Come dicevamo, una disamina adeguata di ciascuna di queste componenti e di tutta l'architettura richiede una trattazione diffusa e molto complessa, che richiederebbe un corso a se stante. E forse più di uno.

Quello che si intende qui mostrare sono alcune funzioni di Windows, inerenti all'architettura: come sono strutturate e come sono utilizzate. In particolare si intende mostrare il modello a processi e thread e di concorrenza, e il modo di autenticazione. Il primo perché il modello a processi è specifico di ogni sistema operativo e quello di Windows si differenzia – sul piano architetturale – dal modello Unix e Linux, e quindi riveste grande importanza in particolare sul piano programmatico conoscere queste differenze. Il secondo argomento, che può sembrare marginale, è importante perché il modello multiutente è intrinseco all'architettura al file system e questo richiede di parlare prima di tutto di accesso, accesso distribuito e di sicurezza, argomento di rilievo per qualsiasi installazione enterprise del sistema Windows e introduttivo all'Active Directory on premises. Non si parlerà di Active Directory argomento che esula questa esposizione. Per un excursus completo su Active directory on premises si rimanda il lettore interessato a “Active Directory come directory service” di Stefano Pinardi, Emanuele Colombo, Alessandro Aruanno, Duke Italia editore, ISBN:8886460155