Introduzione a Windows

Windows teoria
Parte 1

Ruggero Donida Labati

Laboratorio di Sistemi Operativi
Università degli Studi di Milano
Dipartimento di Informatica
A.A. 2024/2025

Panoramica della lezione

- Saranno introdotte le caratteristiche principali del sistema operativo Windows 10
- Verranno presentati i principi fondamentali di progettazione e i componenti del sistema operativo
- Saranno descritti gli algoritmi più importanti usati in Windows 10

Sommario (1/2)

1. Introduzione a Windows 10
   - Storia
   - Caratteristiche
2. Principi di progettazione
   - Sicurezza
   - Estensibilità
   - Portabilità
3. Componenti del sistema operativo
   - Architettura
   - Kernel
   - Power manager
   - Registro
   - Boot

Sommario (2/2)

4. Processi
   - Informazioni associate ai processi
   - Scheduling
   - Object manager
5. Memoria
   - Virtual memory manager
6. Gestione dell'I/O
   - I/O manager
   - Plug-and-Play (PnP) manager

1. Introduzione a Windows 10

- Storia
- Caratteristiche

Storia di Windows 10

- Nel 1998 Microsoft decise di sviluppare un SO «New Technology» (NT)
  - Supporto OS/2 e POSIX
  - Originariamente pensato per usare le API OS/2, successivamente cambiato utilizzando le API Win32
- Utilizzato come base per i SO a partire da Windows XP
  - XP
  - Vista
  - 7
  - 8
  - 10

Caratteristiche (1/3)

- Caratteristiche principali
  - 32/64 bit
  - Pre-emptive
  - Multitasking
  - Multi-utente
    - Utenti remoti
  - CPU Intel

Caratteristiche (2/3)

- Caratteristiche principali
  - Portabilità
  - Sicurezza
  - POSIX
  - Supporto multiprocessore
  - Estensibilità
  - Supporto internazionale
  - Compatibilità DOS e Win 9x

Caratteristiche (3/3)

- Caratteristiche principali
  - Architettura a micro-kernel
  - Versione diversificate
    - Hardware differente (laptop, desktop, server)
    - Prezzi diversi
  - Software
    - Windows App Store: nuovo metodo di distribuzione software
    - Windows Desktop Bridge: vecchi eseguibili

2. Principi di progettazione

- Sicurezza
- Estensibilità
- Portabilità
- Altri

Sicurezza (1/2)

- Principi di sicurezza
  - Access Control Lists (ACL)
    - Basate sugli attributi
    - Basate su claim
  - Livelli di integrità
  - Crittazione
    - File system
    - Comunicazioni

Sicurezza (2/2)

- Principi di sicurezza
  - Mitigazione degli exploit
    - Address-space layout randomization (ASLR)
    - Data Execution Prevention (DEP)
    - Control-Flow Guard (CFG)
    - Arbitrary Code Guard (ACG)
  - Firma digitale
  - Device guard
    - Controllo fine su quali software firmati possono girare

Estensibilità (1/2)

- Architettura a livelli
  - Remote procedure calls (RPCs)
  - Advanced local procedure calls (ALPCs)

Estensibilità (2/2)

- Local Procedure Call
  - Trasferisce richieste e risultati tra processi client e server all'interno della stessa macchina
  - Tre tipi di metodi per passaggio di messaggi
    - Messaggi piccoli (fino a 256 bytes): la coda dei messaggi è usata come storage intermedio, i messaggi sono copiati da un processo all'altro
    - Puntatore a zona di memoria condivisa creata per il canale di comunicazione
    - Quick LPC: usato da porzioni del sistema di display grafico di Win32

Portabilità

- Principi di portabilità
  - Windows 10 può essere portato da un'architettura ad un'altra con piccoli cambiamenti
    - Solo piccole porzioni CPU-specific sono scritte in assembly
  - Scritto in C e C++
  - Il codice platform-dependent è isolato in una dynamic link library (DLL) called the "hardware abstraction layer" (HAL)

Altri principi (1/3)

- Affidabilità
  - Meccanismi hardware per memoria virtuale
  - Meccanismi di protezione software per le risorse di sistema
- Compatibilità
  - Le applicazioni che supportano IEEE 1003.1 (POSIX) possono essere compilate per Windows 10 senza cambiare il sorgente

Altri principi (2/3)

- Prestazioni
  - I sottosistemi di Windows 10 possono comunicare tra di loro
    - Meccanismo di scambio di messaggi ad elevate prestazioni
  - Pre-emption di thread a bassa priorità
    - Risposta veloce ad eventi esterni
  - Multiprocessing simmetrico
- Supporto internazionale
  - National Language Support (NLS) API

Altri principi (3/3)

- Efficienza energetica
  - Dynamic tick
  - Process lifetime management
  - Desktop activity monitor
  - Connected standby

3. Componenti del sistema operativo

- Architettura
- Kernel
- Power manager
- Registro
- Boot

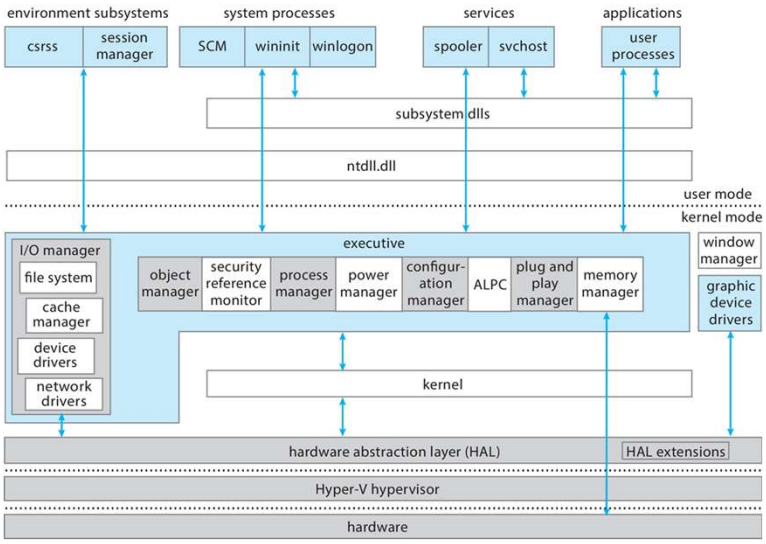
Architettura di Windows 10 (1/3)

- Architettura
  - Sistema di moduli organizzati in layer
  - Modalità protetta
    - Hardware abstraction layer (HAL)
    - Kernel
    - Executive
  - Modalità utente
    - Sottosistemi ambientali: Emulano diversi SO
    - Sottosistemi di protezione: funzioni di sicurezza

Architettura di Windows 10 (2/3)

- Virtual Trust Levels (VTLs)
  - Modalità sicura virtuale
  - Normal World (VTL 0) e Secure World (VTL 1)
    - Per ogni "world", ci sono modalità kernel e modalità utente
    - Secure World: kernel sicuro, executive, trustlets
  - Il layer più in basso gira in modalità processore "speciale"
    - VMX Root Mode (Intel)
    - Hyper-V hypervisor
    - Confine hardware tra "normale" e "sicuro"

Architettura di Windows 10 (3/3)



Kernel (1/2)

- Kernel di Windows 10
  - Fondamento per la modalità executive
  - Eccezione alla memoria e allo scheduling
    - Non viene mai tolto dalla memoria (no paging out)
    - Non viene mai pre-empted
- Quattro compiti principali
  - Scheduling dei thread
  - Gestione di interrupt ed eccezioni
  - Sincronizzazione del processore
  - Ripristino dopo una mancanza di corrente

Kernel (2/2)

- Orientato agli oggetti
  - Oggetti dispatcher
    - Dispatching, sicronizzazione (semafori, mutex, timer, …)
  - Oggetti di controllo
    - Chiamate di procedura asincrone, interrupt, eventi relativi alla corrente, processi
  - VSM Enclaves
    - Permette a codice firmato di terze parti di effettuare crittazioni

Power manager

- Power manager in Windows 10
  - Rileva la situazione di corrente attuale
  - Mette il sistema nello stato di sleep o ibernazione
  - Controlla la CPU in base allo stato di corrente
    - Core parking
    - CPU throttling
    - CPU boosting
  - Controlla lo stato dei dispositivi in base allo stato di corrente
    - Es. risparmio energetico

Registro

- Configurazione del sistema operativo
  - Mantenuta in repository interni chiamati *hive*
  - Hive separati
    - Informazioni di sistema
    - Preferenze utente
    - Informazioni software
    - Sicurezza
    - Informazioni di boot
- Gestita dal registro
  - Gestore della configurazione per Windows 10
- Windows 10 crea un system restore point prima di fare cambiamenti al registro
  - Ripristino del sistema in caso di fallimenti

Boot

- Booting via firmware BIOS
  - Se la macchina è ibernata, si avvia winresume.efi
  - Power-on self-test (POST)
  - Booting
    - Kernel
    - Idle
    - System process
    - Secure system process
    - Session manager subsystem (SMSS)
- UEFI: *Secure Boot Feature*
  - Controllo dell'integrità con firma digitale di tutti i componenti in fase di avvio

4. Processi

- Informazioni associate ai processi
- Scheduling
- Object manager

Informazioni associate ai processi (1/3)

- Informazioni associate al processo
  - Spazio di indirizzamento in memoria virtuale
  - Affinity
  - Informazioni extra (es. priorità)

Informazioni associate ai processi (2/3)

- Thread
  - Sono l'unità di esecuzione schedulata dal dispatcher del kernel
  - Informazioni associate al thread
    - Priorità
    - Affinity
    - Accounting
  - Otto stati
    - Initializing, ready, deferred-ready, standby, running, waiting, transition, terminated

Informazioni associate ai processi (3/3)

- Due modalità di esecuzione
  - User-mode thread (UT)
  - Kernel-mode thread (KT)
- Ogni thread ha due stack
  - Uno per ogni modalità
  - Il kernel può cambiare stack e modalità CPU

Scheduling (1/6)

- Priorità
  - Dispacther usa 32 livelli di priorità per determinare l'ordine di esecuzione dei thread
  - Priorità divise in due classi
    - Real-time: priorità 16-31
    - Variable: priorità 0-15

Scheduling (2/6)

- Priorità
  - Windows 10 tende a fornire tempi di risposta brevi per applicazioni interattive (mouse, tastiera)
  - Permette a thread I/O-bound di tenere alta l'occupazione dei dispositivi di I/O
  - Occupa i cicli di CPU rimanenti con thread complete-bound

Scheduling (3/6)

- Attivazione dello scheduling in determinati momenti
  - Thread entra nello stato «ready» o «wait»
  - Thread termina
  - Un'applicazione cambia le informazioni associate ad un processo
    - Priorità del thread
    - Affinità del processore

Scheduling (4/6)

- Classi di priorità
  - I thread real-time hanno accesso «preferenziale» alla CPU
  - Windows 10 NON garantisce che un thread real-time inizierà l'esecuzione entro un certo limite di tempo
    - Soft real-time

Scheduling (5/6)

- Trap-handling
  - Il kernel fornisce un meccanismo di gestione di interrupt ed eccezioni
    - Generate sia lato hardware che software
  - Le eccezioni che non possono essere gestite dal trap handler sono gestite dall'exception dispatcher del kernel
  - Interrupt dispatcher
    - Modulo del kernel che gestisce gli interrupt, chiamando una interrupt service routine (es. driver) o una routine interna del kernel
  - Il kernel usa spin locks in memoria globale per garantire la mutua esclusione in sistemi multiprocessori

Scheduling (6/6)

interrupt levels	types of interrupts
31	machine check or bus error
30	power fail
29	interprocessor notification (request another processor to act; e.g., dispatch a process or update the TLB)
28	clock (used to keep track of time)
27	profile
3–26	traditional PC IRQ hardware interrupts
2	dispatch and deferred procedure call (DPC) (kernel)
1	asynchronous procedure call (APC)
0	passive

Object manager (1/3)

- Windows 10 usa oggetti per servizi e le entità
  - Object manager: supervisiona l'uso di tutti gli oggetti
    - Genera un handle per l'oggetto
    - Controlla la sicurezza associata all'oggetto
    - Tiene traccia di quali processi usano l'oggetto
- Quasi tutti gli oggetti possono avere un nome
  - Permanente
  - Temporaneo
  - Eccezioni: processi, thread
- I nomi sono strutturati come percorsi
  - Windows 10: symbolic links, simili ai symbolic links di UNIX
  - Permettono a più alias di riferirsi allo stesso file

Object manager (2/3)

- Oggetti manipolati con set standard di metodi
  - Create, Open, Close, Delete, Query name, Security
  - Ogni oggetto è protetto da una Access Control List
- Un processo ottiene l'handle per un oggetto
  - Creando un oggetto
  - Aprendo un oggetto esistente
  - Handle duplicato da un altro processo
  - Ereditando l'handle dal processo padre

Object manager (3/3)

- Security Reference Monitor
  - Meccanismo uniforme per effettuare il controllo e l'audit dell'accesso a runtime, per ogni entità del sistema
  - Quando un processo apre un handle per un oggetto, il SRM controlla il *security token* del processo e l'access control list dell'oggetto
    - Controllare se il processo ha i privilegi necessari

5. Memoria

- Virtual memory manager

Virtual memory manager (1/6)

- Progettato assumendo che l'hardware supporti i meccanismi necessari
  - Mapping virtuale-fisico
  - Meccanismo di paginazione
  - Coerenza della cache
  - Virtual addressing aliasing
- VM manager in Windows 10
  - Schema basato sulla paginazione
  - Dimensione delle pagine dipende dall'hardware
    - 4KB, 2MB, 1GB

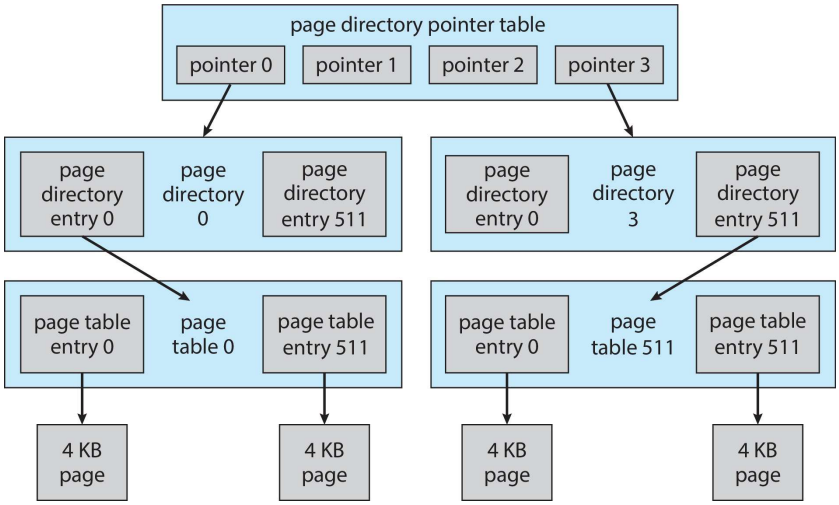
Virtual memory manager (2/6)

- Allocazione della memoria con meccanismo in 2 passi
  1. Riserva porzione dello spazio di indirizzamento del processo
  2. Effettua l'allocazione assegnando lo spazio nel file di paginazione del sistema

Virtual memory manager (3/6)

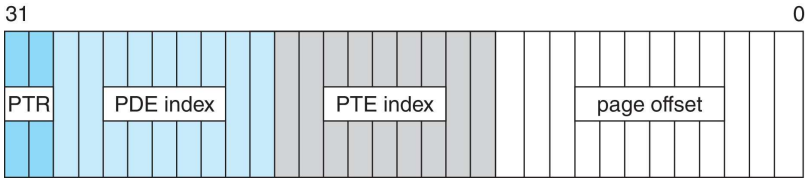
- VM manager: uso di diverse strutture dati
  - Ogni processo: directory delle pagine che contiene 1024 page directory entries (PDE), ognuna di 4 bytes
  - Ogni entry nella directory delle pagine: puntatore ad una tabella delle pagine con 1024 page table entries (PTE) di 4 bytes
  - Ogni PTE: punta ad un page frame di 4 KB nella memoria fisica
- Intero a 10 bit: può rappresentare valori da 0 a 1023, usato per selezionare le entry nelle directory
  - Per tradurre un puntatore nello spazio di indirizzamento virtuale in un byte nella memoria fisica

Virtual memory manager (4/6)



Virtual memory manager (5/6)

- Traduzione indirizzi da virtuale a fisica
  - 2 bit per PTR
  - 9 bit per PDE
  - 9 bit per PTE
  - 12 bit per byte offset



Virtual memory manager (6/6)

- Una pagina può essere in uno dei seguenti 6 stati
  - Valid
  - Zeroed
  - Free
  - Standby
  - Modified
  - Bad

6. Gestione dell'I/O

- I/O manager
- Plug-and-Play (PnP) manager

I/O manager (1/3)

- Responsabile di
  - File system
  - Gestione della cache
  - Driver di dispositivo
  - Driver di rete
- Tiene traccia
  - Quali file system sono caricati
  - Buffer per richieste I/O

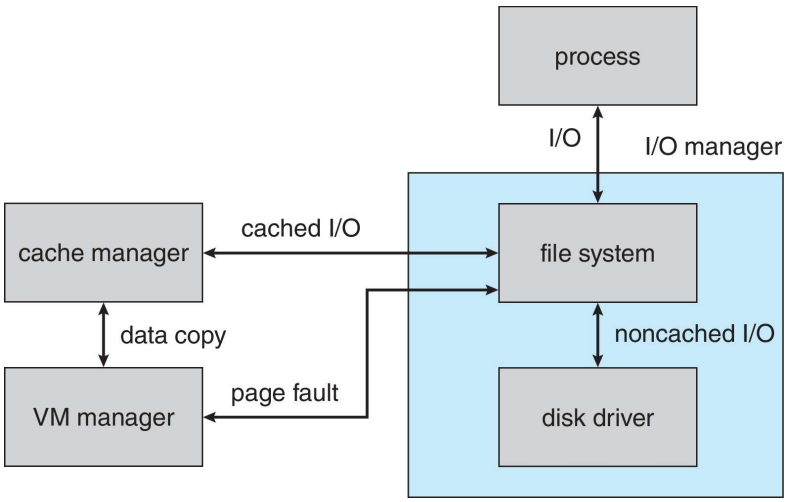
I/O manager (2/3)

- Gestisce l'I/O mappato in memoria
  - In collaborazione con il VM manager
- Controlla il cache manager di Windows 10
  - Gestisce la cache per l'intero sistema di I/O
- Supporta operazioni sincrone e asincrone
  - Time-out per driver
  - Meccanismi di scambio informazioni tra driver diversi

I/O manager (3/3)

- Driver
  - Howrdare o non hardware (e.g. IPv6)
  - Port / Miniport
  - Class / Miniclass
  - Kernel-mode driver /User-mode driver
  - Windows Driver Fundation model (github)

I/O manager (3/3)



Plug-and-Play (PnP) manager

- Plug-and-Play (PnP) manager
  - Usato per rilevare cambiamenti nella configurazione hardware e adattare il sistema di conseguenza
  - Quando un nuovo dispositivo è aggiunto (es. PCI, USB) il PnP manager carica il driver corrispondente
  - Tiene traccia delle risorse usate da ciascun dispositivo