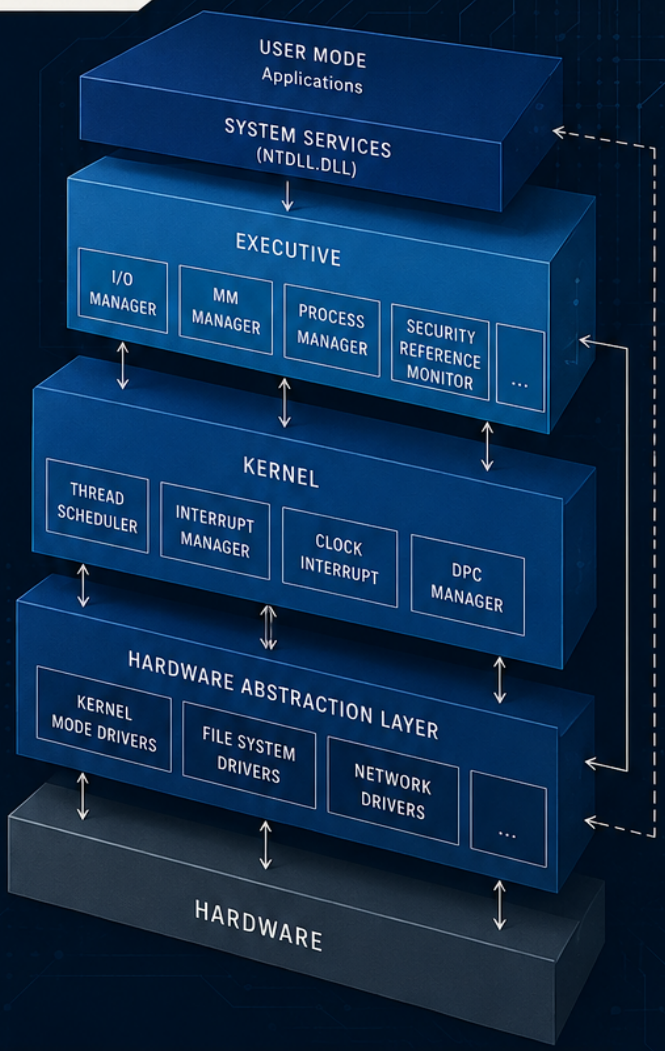
WINDOWS INTERNALS

ARCHITECTURE OF MODERN MICROSOFT OPERATING SYSTEMS

FROM BOOT TO SHUTDOWN

Kernel Design, Security, Virtualization, and Debugging in Windows 10, 11, and Server

- BOOT & INITIALIZATION
- KERNEL ARCHITECTURE
- MEMORY MANAGEMENT
- PROCESSES & THREADS
- I/O SYSTEM & FILE SYSTEMS
- SECURITY ARCHITECTURE
- VIRTUALIZATION
- DEBUGGING & DIAGNOSTICS
- EXPLOIT MITIGATIONS



JAKE SINOFSKY

Windows Internals: Architecture of Modern Microsoft Operating Systems

From Boot to Shutdown — Kernel Design, Security, Virtualization, and Debugging in Windows 10, 11, and Server

Steve T. Publications

This book is available at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperatingsystems

This version was published on 2026-07-09

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Contents

From Boot to Shutdown — Kernel Design, Security, Virtualization, and Debugging in Windows 10, 11, and Server

About this book: Modern Windows is the most widely deployed desktop operating system in the world, yet its internals remain opaque to all but a small community of kernel developers, security researchers, and systems programmers. This book bridges that gap. It provides a comprehensive, technically rigorous treatment of the Windows NT kernel architecture from power-on through shutdown, covering the boot process, kernel initialization, memory management, process and thread scheduling, I/O subsystem, file systems, security architecture, virtualization technologies, debugging tools, and modern exploit mitigations. Every chapter includes annotated code snippets, data structure layouts, WinDbg debugging sessions, practical experiments, and comparisons with Linux where illuminating. This book is intended as a graduate-level textbook and professional reference for operating system developers, systems programmers, security researchers, reverse engineers, malware analysts, digital forensics practitioners, and advanced computer science students.

Introduction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Chapter 1: The Windows Boot Process — From Power-On to Desktop

UEFI Firmware and the Handoff to Bootmgr

Boot Configuration Data (BCD) and Dual-Boot Architecture

Kernel Loading: winload.efi, Registry Hives, and Driver Initialization

Session Manager Subsystem (smss.exe) and the First User-Mode Process

Winlogon, Services Control Manager, and Desktop Startup

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Common Boot Failures and Recovery Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Chapter 2: The Windows Kernel Architecture — Kernel, Executive, and HAL

Historical Context: OS/2, NT 1.0, and the Hybrid Microkernel Design

The Kernel Proper (ntoskrnl.exe): Threads, Synchronization, IPC, Interrupts

The Executive Subsystems: Object Manager, I/O Manager, Security Reference Monitor, Memory Manager, Process/Thread Manager, Cache Manager, Configuration Manager, Power Manager

Hardware Abstraction Layer (HAL): ACPI, Multiprocessor Support, and Abstracted Hardware Interfaces

Kernel Mode vs. User Mode: Privilege Levels, Ring 0/Ring 3, and the Transition Boundary

Chapter 3: System Calls, Interrupts, and Exception Handling

The System Call Interface: Nt* API Functions and the syscall Instruction

System Call Dispatch: KiSystemService, Fast Calls, and Argument Copying

Hardware Interrupt Processing: IDT, ISR/DPC Model, and Interrupt DPCs

Software Exceptions: Structured Exception Handling (SEH), Vectorized EH, and Exception Propagation

Debug Exceptions and the Kernel Debugger Interface

Comparison with Linux syscalls and interrupt handling

Chapter 4: Process and Thread Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

EPROCESS and ETHREAD Internal Structures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Process Creation: NtCreateProcess, PEB/TEB, and DLL Loading

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Thread Creation and the Thread Environment Block (TEB)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Context Switching: KTHREAD, Save/Restore, and Stack Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Job Objects and Process Groups

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Comparison with Linux task_struct, fork/exec Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Chapter 5: The Windows Scheduler — Preemption, Priority, and Quantum Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Priority Levels and Priority Classes (Idle, Below Normal, Normal, Above Normal, High, Real-Time)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Time Quantum Allocation and Dynamic Priority Boosting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Multiprocessor Scheduling: Processor Affinity, NUMA Awareness, and the Ready Queue

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

I/O Completion Ports and Asynchronous I/O Scheduling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Real-Time Threads and Starvation Prevention

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Comparison with Linux CFS Scheduler

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Chapter 6: Virtual Memory Management — Address Spaces, Paging, and Physical Memory

Virtual Address Space Layout: User Mode vs. Kernel Mode Split

Page Tables: CR3, PML4/PDP/Directory/Page Table Hierarchy, and Hardware Support

Page Fault Handling: Demand Paging, Copy-on-Write, and Hard/Soft Faults

Working Set Management: Eviction, Trimming, and the Standby List

Physical Memory Manager: PFN Database, Memory Partitions, and NUMA Nodes

Shared Sections, Mapped Files, and Section Objects

Chapter 7: Synchronization Primitives and Interprocess Communication

Kernel Synchronization: Mutexes, Semaphores, Events, and Critical Sections

Wait Mechanisms: KeWaitForSingleObject, Alertable Waits, and Timeout Handling

Interlocked Operations and Atomic Instructions (CMPXCHG, LOCK prefix)

Interprocess Communication: Mailslots, Named Pipes, LPC/ALPC, Shared Memory

Reader/Writer Locks, Slim Reader/Writer (SRW), and Spinlocks

Deadlock Detection, Debugging Synchronization Issues

Chapter 8: The I/O Manager and Driver Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

I/O Request Packets (IRP): Structure, Stack Locations, and Completion Routines

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

The Driver Object and Device Object Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Dispatch Routines: Major Function Codes and IOCTL Handling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Filter Drivers: Upper/Lower Filters and Stream Inspectors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Plug and Play Manager: Device Enumeration, Power Management, and Resource Assignment

Windows Driver Kit (WDK): KMDF, UMDF, and Modern Driver Development

Chapter 9: Storage Stack, File Systems, and NTFS Internals

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

The Storage Stack: Classpnp, Disk.sys, Storport, and SCSI/Storage Miniport Drivers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Filter Manager and Volume Snapshots (VSS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

NTFS File System Architecture: MFT, B-Trees, Resident vs. Non-Resident Attributes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

NTFS Data Structures: Boot Sector, Master File Table, Attribute Lists, Security Descriptors

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

ReFS, FAT32, exFAT, and the File System Filter Framework

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Storage Spaces, Tiered Storage, and DirectStorage

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Chapter 10: Networking Stack — From TCP/IP to Winsock

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

The TCP/IP Protocol Stack: Tcpip.sys, NDIS, and Protocol Drivers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Network Driver Interface Specification (NDIS): Miniport Drivers and Filter Drivers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Winsock 2 API: Socket Implementation, Overlapped I/O, and IOCP Integration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

TCP Connection State Machine and Performance Tuning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

Windows Filtering Platform (WFP) and Firewall Architecture

SDN, Hyper-V Virtual Switch, and Container Networking

Chapter 11: Security Architecture — Tokens, Privileges, Authentication, and Mitigations

Access Tokens: Structure, Privileges, Mandatory Levels, and Impersonation

Security Reference Monitor (SRM): ACL Evaluation, Object Security Descriptors, and Access Checks

Local Security Authority (LSASS): Authentication Packages, Kerberos, NTLM, and Credential Management

Integrity Levels and Mandatory Integrity Control (MIC)

Modern Exploit Mitigations: DEP, ASLR, CFG, Stack Cookies, and Guard Pages

Kernel Exploit Mitigations: PatchGuard, KASLR, and Pool Vulnerability Protection

Chapter 12: Virtualization — Hyper-V, Containers, and WSL

Hyper-V Architecture: Root Partition, Child Partitions, Virtual Processor Scheduling, and vGPU

Hardware Virtualization: Intel VT-x/AMD-V, Nested Paging/EPT, and Direct Execution

Windows Containers: Process Isolation, Hyper-V Isolation, and the Container Runtime

Windows Subsystem for Linux (WSL): WSL1 Translation Layer, WSL2 Lightweight VM, and Interop

Device Emulation, Paravirtualization, and SR-IOV

Chapter 13: Debugging, Performance Analysis, and Crash Dump Forensics

WinDbg Fundamentals: Breakpoints, Symbol Loading, Extension Commands (exts), and Debugger Scripts

Kernel Debugging: Serial/1394/USB/Network Debugging and Live Kernel Dump

Event Tracing for Windows (ETW): Providers, Sessions, Manifests, and Analysis with PerfView/Xperf

Crash Dump Analysis: Full/Memory/Hiberfil Dumps, Analyzing BSODs, and Common Bug Checks

Performance Counters, Sampling Profilers, and Memory Leak Detection

Practical Case Studies: Real Debugging Scenarios and Forensic Investigations

Chapter 14: Modern Security — VBS, HVCI, Credential Guard, and the Future

Virtualization-Based Security (VBS): Isolated Memory Regions and Secure Launch

Hypervisor-Protected Code Integrity (HVCI): Kernel Mode Signing Enforcement and DMA Protection

Credential Guard: Protected LSASS, Secure Boot Chain, and Identity Protection

Windows Defender Application Control (WDAC) and Attack Surface Reduction Rules

Secure Boot, TPM Integration, and Measured Boot

Future Directions: Confined Virtualization, Pluton SoC, and Zero Trust Architecture

Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/windowsinternalsarchitectureofmodernmicrosoftoperat