

Acknowledg **Contents at a Glance**

0. About this book
 1. Darwinism: The Evolution of MacOS and the *OS variants
 2. E Pluribus Unum: The Darwin Architecture
 3. Promenade: A tour of the *OS Filesystems
 4. Experience Points: UX and System Services
 5. Automatic for the People: Application Services
 6. Ex Machina: The Mach-O File Format
 7. In the Darkness, Bind Them: dyld internals
 8. Parts of the Process: Processes, Threads, and the Grand Central Dispatcher
 9. In Memoriam: Process and System Memory Management
 10. CFRun - RunLoopRun: The Runtime Environments
 11. The Message is the Medium: Mach IPC
 12. Mecum Porto: Mach Primitives
 13. The Alpha & Omega - launchd
 14. X is not a Procedure Call: XPC Internals
 15. Follow Me: Process Tracing & Debugging
 16. Het-Work: Darwin Networking
- Appendices**
- A. Spitting Image: MacOS & *OS Software Images

(Faint, illegible text from the reverse side of the page is visible in the background)

Table of Contents

0. About This Book	
1. Darwinism: The Evolution of *OS	1
o The Origin of Species	171
o Version Arithmetic	
o Darwin and Open Source	
o Darwin, UNIX and POSIX	
o Progenitor: NeXTSTEP	
o MacOS	
▪ 10.9 through 10.15(beta)	
o iOS and the i-Devices	
▪ iOS 5 through 13(beta)	
o TvOS and the Apple TV	
▪ The i-Device: Apple TV	
▪ Divergences from iOS	
▪ Jailbreaking	
o WatchOS and the Apple Watch	
▪ The i-Device: Apple Watch	
▪ Divergences from iOS	
▪ Jailbreaking	
o eOS/BridgeOS	
o The i-Device simulators	
o emulating iOS	
2. E Pluribus Unum: The Darwin Architecture	25
o Architecture, at a glance	
o Interlude: Property lists	
o Applications	
o Frameworks	
o Third Party Libraries	
o System Libraries	
o Kernel Interface	
▪ System Calls	
▪ Mach Traps	
▪ Machine Dependent (machdep) Calls	
▪ Diagnostic Calls (MacOS)	
▪ The comm page	
▪ Signals	

o	XNU (at a glance)	
▪	Mach & BSD	
▪	libkern	
▪	IOKit	
▪	The Platform Expert and ml_ APIs	
▪	Kernel extensions	
▪	Darwin Technologies (at a glance)	
3.	Promenade: A tour of the *OS Filesystems.....	55
o	Partitioning	
o	Filesystems	
o	Disk Images	
o	Disk Arbitration	
o	ACLs & Attributes	
▪	File flags	
▪	Extended Attributes	
▪	Transparent file compression	
▪	File forks (MacOS)	
o	Directories	
4.	Experience Points: UX and System Services.....	89
o	FSEvents	
o	Spotlight	
o	QuickLook	
o	System Information	
▪	Darwin: sysctl	
▪	MacOS: AppleSystemInfo.framework & system_profiler	
▪	*OS: MobileGestalt	
o	System Configuration	
o	Duet	
o	Printing	
o	Siri (assistantd) & Voice Control	
o	The User Interface	
5.	Automatic for the People: Application Services.....	137
o	Application Installation & LaunchServices	
o	Preferences	
o	Notifications	
▪	Darwin Notifications (/usr/bin/notifyd)	
▪	Distributed Notification Center (/usr/sbin/distnoted)	
▪	*OS: Notification proxying	
▪	Apple Push Notifications (APN)	

- o User Notifications
- o emond (MacOS)
- o Apple Events (MacOS)
 - AppleScript
 - Sending Events
- 6. Ex Machina: The Mach-O File format..... 173
 - o Overture: Fat Binaries
 - o General Mach-O Concepts
 - o Mach-O FileTypes
 - o Header Flags
 - o Load Commands
 - Load commands known to XNU
 - Load commands known to dyld
 - Load commands serving little or no purpose
 - Deprecated load commands
- 7. In the Darkness, Bind Them: dyld internals..... 195
 - o Program startup
 - o Linking
 - o dyld opcodes
 - Binding opcodes
 - Advantages of the opcode scheme
 - Rebasing opcodes
 - arm64e and dyld-625 (Darwin 18) changes
 - o Exports
 - o CoreSymbolication.framework
 - o Interposing
 - o The Shared Library Cache
 - o Darwin 17: dyldv3
 - o Programmatic manipulation of Mach-O objects
 - o Remote inspection of dyld state
 - o Debugging & tracing dyld operations
- 8. Parts of the Process: Threads and the Grand Central Dispatcher..... 233
 - o Processes
 - Process lifecycle
 - Process identifiers and grouping
 - Coalitions (Darwin 14+)
 - Credentials
 - Personae (*OS)
 - Signals

- o PThreads (glance)
 - Non-POSIX extensions
 - Initialization
 - Thread lifecycle
 - Introspection
 - What's in a pthread_t
 - Thread Specific Data (TSD)
 - Synchronization objects
 - Thread Local Variables (TLV)
 - Thread priorities and QoS class
 - Process, task & thread policies
- o Interlude: KEvents and KQueues
- o Grand Central Dispatcher
 - Blocks
 - Queues
 - Queue attributes
 - Queue maintenance
 - Dispatching blocks
 - Continuations
 - Dispatch Objects
 - Dispatch Sources
 - Introspection
 - kdebug codes
- 4. Experience Points: UX and System Services..... 275
 - o FSEvents
 - o Spotlight
 - o QuickLook
 - o System Information
- 9. In Memoriam: Process Memory Management..... 275
 - o On the same page
 - o Memory Management APIs
 - POSIX/BSD APIs
 - mach vm_map
 - memory tags
 - o libmalloc
 - The scalable (default) zone
 - Custom Zones
 - Zone APIs
 - In the Zone
 - Magazines
 - Hoard improvements
 - The Nano zone
 - The Nanov2 zone (Darwin 18+)
 - The Purgeable zone and libcache
 - Debugging

o	libplatform (os_alloc_once)	12
o	Swap		
▪	Dynamic paging (MacOS)		
▪	Compressed RAM		
o	Under pressure:		
▪	MacOS: MemoryStatus		
▪	*OS: Jetsam		
▪	Programmatic API		
▪	Detecting and responding to memory pressure		
▪	*OS: mmaintenanced		
10.	CFRun - RunLoopRun: The Runtime Environments	307
o	CoreFoundation		
▪	CF* Objects		
▪	CFRunLoop Internals		
o	Objective-C		
▪	Objective-C library initialization		
▪	Runtime support information		
▪	Type encoding		
▪	Classes and instances		
▪	Sending messages		
▪	Message passing internals		
▪	Other compiler directives		
▪	Reflection		
▪	Method swizzling		
▪	Tracing Objective-C		
o	Swift		
▪	Compiling		
▪	Mach-O sections		
▪	Reverse engineering Swift binaries		
▪	Closures		
▪	Mangling		
11.	The Message is the Medium: Mach IPC (the user mode view)	337
o	A little history		
o	Ma-xioms		
o	Scenarios		
o	Mach Port APIs		
o	Message format		
o	Sending and receiving messages		
o	The Mach Interface Generator		
o	SkyWalk		

12. Mecum Porto: Mach Primitives.....	367
o Ports as object abstractions	
o The host	
o The host_priv	
o The task	
o The thread	
o The lesser objects	
▪ The clock	
▪ The processor and processor set	
o Exception ports	
13. The Alpha & Omega - Launchd	389
o Born Again: Launchd's reincarnation in libxpc	
o The many faces of launchd	
▪ atd (scheduled execution)	
▪ crond (scheduled recurring execution)	
▪ inetd/xinetd (socket handoff)	
▪ Triggered execution	
o Interlude: UserEventAgent	
o Agents & Daemons	
▪ The <code>__TEXT.__bs_plist</code> property list	
o Domains	
o launchctl	
o APIs	
▪ The XPC bootstrap pipe	
▪ liblaunch.dylib	
▪ ServiceManagement.framework	
14. X is not a Procedure Call: XPC internals	411
o Design Rationale	
o Implementation details	
o XPC Object APIs	
▪ XPC data types	
▪ Object representation	
o XPC Transport APIs	
▪ XPC pipes	
▪ NSXPC*	
▪ GCD Integration	
o Remote XPC	
▪ The Nano2 zone (Darwin 18+)	
▪ The Purgeable zone and libcache	
▪ Debugging	

- o XPC services
 - xpc_main
 - Transactions
 - Starting services
 - XPC caches
- o XPC activities
- o Tracing XPC

15. Follow Me: Process Tracing and Debugging.....work on "Mac OS X Internals" has been 439

- o proc_info
- o stackshot
- o sysdiagnose(1)
- o os_log(3)
 - logd
 - Kernel use of os_log
 - /var/db/diagnostics
 - diagnosticd
- o aggregated (*OS)
- o DTrace (MacOS)
- o kdebug
 - Controlling kdebug
 - producing kdebug messages from user mode
- o ktrace
 - sysctl
 - tailspin
- o kperf
 - Controlling kperf
 - kpc
- o Hangs and Crashes
 - spindump(8)
 - Core dumps
 - Crash reporting

16. Her-Work: Darwin Networking chose instead to start "tabula rasa" and rewrite 477

- o Darwin Extensions of the BSD Socket APIs
- o Networking Configuration
- o Networking Statistics
- o Network Agents
- o Firewalling (ALF and PF)
- o Packet Filtering (BPF)
- o Network Extension Control Policies (NECP)
- o SkyWalk