Contents at a glance

Part I: Defensive Techniques and Technologies

The missing documentation for Apple's proprietary security mechanisms

1. Authentication
2. MacOS Auditing
3. Authorization - KAuth
4. MACF - The Mandatory Access Control Framework
5. Code Signing
6. MacOS Software Restrictions
7. AppleMobileFileIntegrity
8. Sandboxing
9. MacOS System Integrity Protection
10. Privacy
11. Data Protection

Part II: E pur si rompe

A detailed exploration of vulnerabilities and their exploits

12. MacOS: Classic vulnerabilities in 10.10.x and 10.11.x
13. iOS: Jailbreaking
14. evasi0n (6.x)
15. evasi0n 7 (7.0.x)
16. Pangu Axe (7.1.x)
17. XuanYuan Sword (8.0-8.1)
18. TaiG (8.0-8.1.2)
19. TaiG (8.1.3-8.4)
20. Pangu 9 (9.0.x)
21. Pangu 9.3 (9.2-9.3.3)
22. Pegasus (9.0-9.3.4)
22½. Phœnix (9.0-9.3.5)
23. mach_portal (10.1.1)
24. Yalu (10.0-10.2)
25. async_wake (11.0-11.1.2) and the QiLin Toolkit

Appendix A: MacOS Hardening Guide

Appendix B: Darwin 18 security changes

Table of Contents

Part I: Defensive Techniques and Technologies

The missing documentation for Apple's proprietary security mechanisms

0. About This Book vii

1. Authentication 1
   - Password files (*OS)
   - SetUID and SetGID (MacOS)
   - The Pluggable Authentication Module (MacOS)
   - opendirectoryd (MacOS)
   - LocalAuthentication.framework
   - Apple IDs
   - External Accounts

2. MacOS Auditing 21
   - Design
   - Audit Sessions
   - Implementation
   - System Call Interface
   - OpenBSM APIs
   - Auditing Considerations

3. Authorization - KAuth 35
   - Design
   - Implementation
   - KAuth Identity Resolvers (MacOS)
   - Debugging KAuth

4. MACF - The Mandatory Access Control Framework 47
   - Background
   - MACF Policies
   - MACF Callouts
   - MACF System Calls

5. Code Signing 63
   - The Code Signature Format
   - Code Signature Requirements
   - Code Signature Enforcement
   - Code Signing Weaknesses
   - Code Signing APIs

6. MacOS Software Restrictions 91

- authd
- Gatekeeper
- libquarantine
- Quaratine.kext
- Quarantine in Action
- Managed Clients

7. AppleMobileFileIntegrity 119

- AppleMobileFileIntegrity.kext
- amfid
- Provisioning Profiles
- SIP Integration (MacOS)
- AMFI Trust Cache
- AMFI UserClient

8. Sandboxing 151

- Evolution of the Sandbox
- App Sandbox (MacOS)
- Mobile Containers (*OS)
- Sandbox Profiles
- User Mode APIs
- mac_syscall
- Sandbox.kext
- sandboxd (MacOS)
- ContainerManagerd (*OS)

9. MacOS System Integrity Protection 183

- Design
- Implementation
- APIs

10. Privacy 191

- Transparency, Consent and Control
- Unique Device Identifiers
- Differential Privacy (MacOS 12/iOS 10)

11. Data Protection 205

- Partition Level Encryption (MacOS)
- File Level Encryption (*OS)
- Obliteration (*OS)
- KeyBags (*OS)
- The AppleKeyStore.kext
- Keychains

Part II: Vulnerabilities and Exploitation

A detailed exploration of both the bugs and their exploits

12. MacOS: Classic vulnerabilities in 10.10.x and 10.11.x.................................... 233
   - 10.10.1: ntpd
   - 10.10.2: rootpipe
   - 10.10.3: Racing kextd
   - 10.10.4: DYLD_PRINT_TO_FILE
   - 10.10.5: DYLD_ROOT_PATH (muymacho)
   - 10.11.0: tpwn
   - 10.11.3: Mach race
   - 10.11.4: Lokihardt's Trifecta (pwn2own 2016)

13. iOS: Jailbreaking.. 255
   - The Jailbreaking Process
   - Kernel Patches
   - Kernel Patch Protection
   - Evolution of iOS Jailbreaks

14. evasi0n (6.x).. 283
   - The Loader
   - The Untether
   - Kernel Mode Exploits
   - Apple Fixes

15. evasi0n 7 (7.0.x).. 305
   - The Loader
   - The Untether
   - Kernel Mode Exploits
   - Apple Fixes

16. Pangu Axe (7.1.x) 323
   - The Loader
   - The Jailbreak Payload
   - The Untether
   - Kernel Mode Exploits
   - Apple Fixes

17. XuanYuan Sword (8.0-8.1).. 339
   - The Loader
   - User Mode Exploits
   - The Untether
   - Apple Fixes

18. TaiG (8.0-8.1.2)... 349
- The Loader
- User Mode Exploits
- The Untether
- Kernel Mode Exploits
- Apple Fixes

19. TaiG (8.1.3-8.4)... 373
- The Loader
- User Mode Exploits
- The Untether
- Kernel Mode Exploits
- Apple Fixes

20. Pangu 9 (9.0.x)... 387
- The Loader
- The Jailbreak Payload
- Kernel Mode Exploit
- Code Signing Bypass
- The Untether
- Pangu 9.1
- Apple Fixes

21. Pangu 9.3 (9.2-9.3.3)... 409
- Kernel Mode Exploit

22. Pegasus (9.0-9.3.4)... 415
- Exploit Flow
- Kernel Memory Read and KASLR Bypass
- Kernel Arbitrary Memory Write
- Persistence

22½. Phœnix (9.0-9.3.5)... 427
- The Info Leak
- mach_ports_register

23. mach_portal (10.1.1)... 437
- Exploit Flow
- Mach port name urefs handling
- Crashing powerd
- XNU UaF in set_dp_control_port
- Disabling Protections
- Apple Fixes

24. Yalu (10.0-10.2).. 451

- Primitives
- KPP Bypass
- Post Exploitation
- A deadly trap and recipe for disaster (10.2)
  - The exploit (Beer)
  - The exploit (Todesco & Grassi)

25. async_wake (11.0-11.1.2) and the QiLin Toolkit 471

- Bypassing KASLR
- Kernel Memory Corruption
- Post-Exploitation: The QiLin Toolkit

Appendix

A. MacOS Hardening Guide 497

B. Darwin 18 security changes 511