SEC575 – Mobile Device Security & Ethical Hacking

Topics

Device Architecture & Application Interaction
- Mobile Probles & Opportunities 575.1–7-14
- SANS Integrated Lab Platform 575.1–15-25
- About iOS 575.1–28-48
- About Android 575.1–49-80
- Building Your Lab 575.1–81-97
- iOS Application Interaction 575.1–98-106
- Android Application Interaction ... 575.1–107-118

The Stolen Device Threat & Mobile Malware
- The Stolen Device Threat 575.2–4-26
- Jailbreaking iOS 575.2–28-45
- Rooting Android 575.2–47-61
- Data Storage on Android 575.2–63-82
- Data Storage on iOS 575.2–86-119
- Mitigating Malware 575.2–123-147

Static Application Analysis
- Introduction 575.3–4-5
- Manual Static Analysis 575.3–7-27
- Automating App Analysis 575.3–31-43
- Obfuscated Apps 575.3–47-72
- Third-Party App Platforms 575.3–76-103

Dynamic Mobile App Analysis & Manipulation
- Introduction 575.4–4
- Android Analysis with Drozer 575.4–6-13
- iOS Analysis with Needle 575.4–17-25
- Modifying Mobile Applications 575.4–27-43
- Mobile App Runtime Manip 575.4–47-84
- Runtime Manip with Objection 575.4–86-95
- Application Security Verification 575.4–99-142

Mobile Penetration Testing
- Introduction 575.5–4-8
- Network Activity Analysis 575.5–10-23
- Network Manipulation Attacks 575.5–27-48
- Network Traffic Manipulation 575.5–50-60
- SSL/TLS Attacks 575.5–62-79
- Intercepting SSL/TLS Traffic 575.5–81-107
- Leveraging Mobile Malware 575.5–111-136

Capture the Flag 575.6–2-15

Categories

Labs
- ADB Access 575.1–98
- Android App Static Analysis 575.3–29
- Android Backup Analysis 575.2–84
- Android Emulation 575.1–96
- Android IPC 575.1–121
- Android Malware Analysis 575.2–149
- Banking Transaction Manipulation 575.5–109
- Evil Bank 575.1–27
- Frida & Objection 575.4–97
- iPhone Data Analysis 575.2–121
- Manipulating Android Intents 575.4–15
- Manipulating Web Browser Activity 575.5–62
- Meterpreter RAT Deployment 575.5–138
- MobApp Network Traffic Analysis 575.5–25
- MobSF 575.3–45
- Modifying Android Applications 575.4–45
- Obfuscated Android App Analysis 575.3–74
- PhoneGap App Analysis 575.3–107
- Xamarin App Analysis 575.3–105

Tools
- ADB 575.1–92
- AMRPlayer 575.2–105
- Android SDK 575.1–86-87, 575.2–49, 53, 64, 575.4–41
- Android Studio 575.1–86-90, 575.3–49, 55-56, 58-68, 575.4–138
- Androsim 575.3–41-42
- APK Downloader 575.3–7
- ApkMonk 575.3–7, 78, 89, 96
- ApkOnline 575.3–7
- ApkPure 575.3–7
- ApkTool 575.4–31, 77, 575.5–96
- Appinst 575.2–44
- Apt-Get 575.2–43
- AXMLPrinter2 ..... 575.2–72
- Bettercap 575.5–43-47, 51, 69-70, 76-78
  - Filter 575.5–78
- BigBoss 575.2–43
- Binary Cookie Reader 575.2–98, 575.4–23
- Burp Suite 575.4–107, 575.5–53-56, 87-94, 103
  - Certificate 575.5–90-91, 94, 96
  - Decoder 575.5–21
  - Mobile Assistant 575.5–92-93, 100
  - Repeater 575.5–104-105
  - Site Map 575.5–55
- Bytecode Viewer 575.3–57
- Cain 575.5–32-37, 70, 103
- Chimera 575.2–36
- ClassDump 575.3–23-24, 575.4–49, 53, 59

SEC575 – Mobile Device Security & Ethical Hacking

CURL 575.2–43
Cycript 575.4–50-63, 121-122
Cydia 575.2–35-37, 42, 44
..... 575.5–92
App Store 575.2–41, 44
..... 575.4–21
Impactor 575.2–37-38
Substrate 575.4–49-50, 62, 110-111, 121
DevCraft 575.3–93
DEX2JAR 575.3–10
..... 575.4–77
DexGuard 575.3–69
..... 575.4–138
DexProtector 575.3–69
DotPeek 575.3–82-83, 87, 93
Drozer 575.4–6-13, 124, 126, 128, 131, 137
Agent 575.4–8-9
Console 575.4–9-13
DumpDecrypted 575.2–140
..... 575.3–18
..... 575.4–120
ECMAObfuscator 575.3–100
Elcomsoft Phone Breaker 575.4–118
Electra 575.2–36, 42
EPB 575.4–118
Ettercap 575.5–37-42, 69-71, 103
Certificate Impersonation 575.5–70-71
Configuration 575.5–70
ExifTool 575.2–113
Ez Texting 575.5–126
Fastboot 575.2–49
FFmpeg 575.2–105
Filza File Manager 575.2–44
Firebase Scanner 575.2–76
Framaroot 575.2–61
Frida 575.4–65-84, 86
..... 575.5–100
Capabilities 575.4–75
CLI 575.4–71-74, 76
Client 575.4–65, 70
Examples 575.4–77-83
Internals 575.4–70
Limitation 575.4–75
Non-Rooted Device 575.4–84
Server 575.4–65, 67-69, 84, 87
GDB 575.2–43
..... 575.4–48
Git 575.2–43
Google Find My Device 575.2–23
Google Voice 575.5–126
Hashcat 575.2–116
Hopper 575.3–26
..... 575.4–104
IDA Pro 575.3–26
..... 575.4–104
iExplorer 575.2–114-115
..... 575.4–115
iOS Find My iPhone 575.2–23
iOS SDK 575.1–85
iOS-Deploy 575.2–44
Iptables 575.5–52-53, 70, 95, 103
itunes_backup2hashcat 575.2–116
Jadx 575.3–10-12, 47, 54, 56, 71
..... 575.4–124, 131, 136
GUI 575.3–11, 54
JarSigner 575.4–40
..... 575.5–96
Java Decompiler 575.4–11
JDK 575.4–39
JScrambler 575.3–100
JustDecompile 575.3–93
Keychain Dumper 575.2–91
..... 575.4–117, 119
Kingo Root 575.2–61
Koodous 575.3–40
Lipo 575.3–20
Magisk 575.2–50
..... 575.4–64, 67
TrustUserCerts 575.5–97
Metasploit 575.5–116, 118-119
`adb_server_exec` 575.5–129
Handler 575.5–116
SOCKS Server 575.5–123
Meterpreter 575.5–116-123
Android Capabilities 575.5–119
APK 575.5–129-131
Persistence 575.5–123
Pivoting 575.5–123
RAT Permissions 575.5–119
Mitmproxy 575.5–58
Mobile Assistant 575.5–92-93, 100
MobSF 575.3–35-37
MsfVenom 575.5–117, 120-122
Needle 575.2–100
..... 575.4–17-25, 66, 103
NetworkMiner 575.5–18-20
Newsstand 575.5–132
Objection 575.4–66, 86-95
..... 575.5–100-101
CLI 575.4–88
Examples 575.4–92-95
Reconnaissance 575.4–90
OmniRAT 575.5–115
Server 575.5–115
OpenSSH 575.2–43
Otool 575.3–15, 22, 25
..... 575.4–103
Passionfruit 575.4–66
PhoneGap 575.3–95-102
Plist Editor 575.2–110
..... 575.4–23
Plist Substractor 575.2–96
Plutil 575.2–110
PowerVR 575.2–104
ProGuard 575.3–49, 52
..... 575.4–138

ProxyDroid 575.5–95
PVRTexTool 575.2–104
QARK 575.3–38-39
Qemu 575.1–86
Rasticrac 575.2–140
Rduck-pinbrute 575.2–18
Real APK Leecher 575.3–7
Rvictl 575.5–12-13
Sileo 575.2–36
App Store 575.2–42
Simplify 575.3–70-71
Smart Phone Flash Tool 575.2–57
SMSGANG 575.5–127
SQLite3 ..... 575.2–43
SQLiteSpy 575.2–74, 94, 112
..... 575.4–23
SSL Kill Switch 575.4–111-112
v2 ..... 575.5–100, 102
SslStrip 575.5–73-74, 78
SslStrip2 ..... 575.5–76-77
SSLUnpinning 575.5–100
SuperSU 575.2–50, 53, 55, 58
TcpDump 575.5–14
TWRP 575.2–48, 53, 57-58
Unc0ver 575.2–35-36, 38-40
Unity 575.3–77-81
VirusTotal 575.5–130-131
Visual Studio 575.3–93-94
WGet 575.2–43
Wireshark 575.5–15-16
XAgent 575.5–132
Xamarin 575.3–88-91
Xposed 575.4–64
Zip 575.2–43
ZipAlign 575.4–41

Terminal Commands

`adb` 575.1–92
`backup` 575.2–81
`connect` 575.1–92
..... 575.5–129
`devices` 575.1–92
..... 575.2–59
`forward` 575.4–9
`install` 575.1–92
..... 575.4–42, 139
..... 575.5–129
`logcat` 575.1–92
..... 575.2–79-80
..... 575.4–13, 127, 130
`pull` 575.3–7, 81
`push` 575.2–55, 60
..... 575.4–67
`root` 575.1–92
`shell am` 575.1–118
`shell service list` 575.1–112
`shell` 575.2–59
..... 575.4–67, 139
..... 575.5–129
`uninstall` 575.1–92
..... 575.4–42, 139
`android` 575.4–91-95
`hooking` 575.4–91-93
`intent` 575.4–91
`root` 575.4–95
`sslspinning` 575.4–95
`apktool`
`b` 575.3–101
..... 575.4–38
..... 575.5–131
`d` 575.4–31, 37
..... 575.5–131
`archtype` 575.3–20
`arp` 575.5–31
`bettercap` 575.5–45-46, 77
`class-dump` 575.3–23-24
`cycript` 575.4–52, 60, 122
`date` 575.2–94
`dd` 575.2–82
`debugdetect` 575.4–120
`diff` 575.4–115
`dmesg` 575.2–79
`dumpsys` 575.2–79
`egrep` 575.4–130
`emulator` 575.1–89
`ettercap` 575.5–38-40, 42, 71
`exiftool` 575.2–113
`fastboot` 575.2–49
`findstr` 575.3–12
`frida` 575.4–71, 73-74, 76
`gdb` 575.4–120
`grep` 575.3–9, 11-12, 97-99
`hashcat` 575.2–116
`id` 575.5–122
`ifconfig` 575.5–13
`ios hooking` 575.4–92
`iptables` 575.5–52, 70
`jadx` 575.3–11, 56
`jarsigner` 575.4–40, 139
..... 575.5–131
`java` 575.2–72
..... 575.4–137
`keychain-dumper` 575.2–91
..... 575.4–23, 117
`keytool` 575.4–39, 139-140
..... 575.5–131
`lipo` 575.3–20
`memory dump` 575.4–94
`msfconsole` 575.5–116
`msfvenom` 575.5–116, 121
`nmap` 575.5–129
`nm` 575.3–15
`objection` 575.4–87-95
..... 575.5–101
`ondeviceconsole` 575.4–21, 106
`openssl` 575.2–82

..... 575.4–131
otool 575.3–15, 22, 25
..... 575.4–103
plutil 575.2–110
rvictl 575.4–113
..... 575.5–13
scp 575.5–14
sqlite3 ..... 575.4–115
strings 575.3–9, 92
..... 575.5–17
stty sane 42
tcpdump 575.4–113
..... 575.5–11, 13-14
unzip 575.3–81, 89, 97
..... 575.4–131, 137
zipalign 575.4–41

Files & Folders

.ab 575.2–81
.amr 575.2–105
.apk 575.2–67
/res/values/strings.xml 575.2–77
gradle.properties 575.2–77
local.properties 575.2–77
.armvX 575.3–20-23, 25
.binarycookies 575.2–98
.dylib 575.3–18
.mddata 575.2–109, 111-112
.plist 575.2–95-96, 109-110
..... 575.4–86
/cache 575.2–64
/data/ 575.2–64, 68-69
app 575.2–82
..... 575.3–7
data/ 575.2–66
*.calendar/calendar.db 575.2–68
*.contacts/contacts2.db 575.2–68
*.contacts/profile.db 575.2–68
*.downloads/downloads.db 575.2–68
*.maps/ 575.2–69
*.quicksearchbox/qsb-log.db 575.2–69
*.telephony/mmssms.db 575.2–68
*.telephony/telephony.db 575.2–68
*.userdictionary/user_dict.db .. 575.2–68
system/accounts.db 575.2–69
misc/wifi/wpa_supplicant.conf 575.2–68
/mnt 575.2–64
..... 575.3–7
/private/var/ 575.2–101
containers 575.2–103
containers/Bundle/Application/ ... 575.2–97
/.app/Info.plist 575.2–97
..... 575.4–104
<GUID>/Name.app/Name 575.3–17-18
mobile/Applications 575.2–102
mobile/Containers/ 575.2–102-104
Data/Applications 575.4–119
mobile/Library/ 575.2–93, 104-105
Add...ook/AddressBook.sqlitedb 575.2–93
Caches/Snapshots 575.2–104
Calendar/Calendar.sqlitedb 575.2–93
Keyboard/dynamic-text.dat 575.2–100
..... 575.4–23
Keyboard/UserDictionary.sqlite 575.2–93
Notes/notes.sqlite 575.2–93
Safari/Bookmarks.db 575.2–93
SMS/sms.db 575.2–93-94
Voicemail/voicemail.db 575.2–93, 105
wireless/Library/ 575.2–93
call_history.db 575.2–93
/system 575.2–64
/var/root/Library/ 575.2–106
Keyboard/dynamic-text.dat 575.2–106
AndroidManifest.xml 575.2–67
..... 575.3–8
..... 575.4–131, 137
..... 575.5–85, 119
FridaGadget.dylib 575.4–84
Info.plist 575.2–109-110, 142
..... 575.5–84
META-INF 575.2–67
..... 575.4–132, 139
Manifest.plist 575.2–109, 116
NOTICE 575.3–90
Status.plist 575.2–109
classes.dex 575.2–67
..... 575.3–8-9, 78
frida-agent.so 575.4–69, 84
@jdwp-control 575.4–137
libunity.so 575.3–81
network_security_config.xml ... 575.5–96, 99
res/ 575.2–67
resources.arsc 575.2–67
..... 575.3–8

A

AASA 575.1–103-104
Accessibility Attributes 575.2–90
..... 575.4–118
Accessibility Service 575.1–66
Abuse 575.2–134-136
Account Isolation 575.1–58
Action Extension 575.1–106-107
Activate Device Administrator 575.1–65
Activities 575.1–109, 111, 116-118
Extra 575.4–13, 127
Invocation 575.4–127
Thread 575.4–83
ADB 575.1–75, 92, 118
..... 575.2–48, 53, 59, 137
Adiantum 575.1–79
Admin Privilege 575.1–65
Adobe 575.3–95
AES 575.1–70
..... 575.2–73, 75, 81, 86
..... 575.4–136
AM 575.1–118
Android 575.1–50
Apps 575.1–54
Certificate 575.4–131
Manipulation 575.4–29, 43
Obfuscated 575.3–47, 49-50, 52
Report Card 575.4–124, 141
Retrieval 575.3–7
Signature 575.4–131, 139
Backup 575.2–81-82
Code Signing 575.1–67
..... 575.4–39-40, 139
Components 575.1–109, 116-117
..... 575.2–48
Exposure 575.4–7
Data Protection 575.1–70
Data Storage 575.2–70
Device Manager 575.2–144
Emulator 575.1–86, 91
..... 575.5–129
Encryption 575.1–70
Factory Reset 575.2–48
File System 575.2–64-82
Fragmentation 575.1–72-73
..... 575.2–128
IPC 575.1–110-118
..... 575.4–6
Permissions 575.1–115-116
Keystore 575.2–73, 75, 78
..... 575.4–135-136
Languages 575.1–54
Logs 575.2–79-80
Malware 575.2–128-137
Manifest 575.1–59-60, 64, 113-115, 117
..... 575.2–67, 77, 79, 131
..... 575.5–85
Binary Format 575.2–72
Market 575.3–12, 575.2–64
Obfuscation 575.3–49-54
Scope 575.3–51
OS Security 575.1–53, 68-69
Passcode 575.1–70
..... 575.2–17
Privileges 575.1–58-65
RAT 575.5–117-122
Deployment 575.5–124
Resources 575.2–67
Reverse Engineering 575.3–8
Example 575.3–80-87, 89-94, 96-102
SDK 575.1–54
..... 575.4–41
Security Library 575.2–71
Sensitive Code 575.3–12
Shared Preferences 575.2–71
Static Analysis 575.3–8-12, 34-35
Studio 575.1–86-90
..... 575.3–49, 55-56, 58-68
Tech Specs 575.1–51
Updates 575.1–71-78
..... 575.2–48-49
Versions 575.1–52
VM 575.1–54
Vulnerabilities 575.1–78
x86 ..... 575.1–91
Angry Birds 575.2–146
Anti-Reverse Engineering 575.4–138
Antivirus 575.2–143
Evasion 575.5–130-131
AOSP 575.2–48
AOT 575.1–56-57
AP 575.5–6, 98
Apache Cordova 575.3–95
API 17 ..... 575.2–77
API 18 ..... 575.2–78
..... 575.4–135
API 23 ..... 575.1–61, 63-64, 115
API 24 ..... 575.5–96
API 28 ..... 575.1–64
APK 575.1–90
..... 575.2–65
..... 575.3–8, 10, 70, 77
..... 575.4–64
Analysis 575.3–36, 38
Comparison 575.3–41
Deobfuscation 575.3–57-68
Source 575.3–56
Structure 575.2–67
Vulnerabilities 575.3–38-39
App Store 575.1–39, 43
..... 575.2–127, 140-141
..... 575.3–17
Certificates 575.2–140
AppFlyers 575.3–94
Apple ID 575.2–139
Apple Pay 575.2–107

Apple System Log → ASL
Application Data 575.4–19, 575.2–66
Application Flaws 575.1–10
Application Report Card → Report Card
Application Security 575.4–99
Application Transport Security → ATS
APR 575.5–32, 34-36
APT 575.2–41
ARC 575.4–103
Architecture 575.3–19-20
ARM 575.1–30, 38, 51
..... 575.3–19, 25
..... 575.4–28
v5 ..... 575.3–19
v6 ..... 575.3–19
v7(s) 575.3–19
ARP Spoofing 575.5–28-29, 36, 38, 42, 46
Example 575.5–30-31
ART 575.1–53-54, 56-57
ASCII 575.5–17
ASL 575.1–43
..... 575.4–21, 106
ASLR 575.1–31, 35, 37, 68
..... 575.3–14
Assembly 575.4–28
ATS 575.5–84
Attack Surface 575.1–117, 119
..... 575.4–9-10, 126
Audit 575.4–99
Authentication Token 575.4–119
Autocorrect Keywords 575.2–68
Automated Analysis 575.3–31-43
Tools 575.3–34
When ? 575.3–33
Automatic Reference Counting → ARC
AVD 575.1–86-92
..... 575.4–9
Creation 575.1–91
Interaction 575.1–92
Management 575.1–89

B

Backdoor 575.2–5
Banned Applications 575.2–41
BCS 575.3–41
Big Endian 575.3–92
..... 575.5–17
Binary Cookies 575.2–98
..... 575.4–24
Binary Test 575.4–103
`BIND_ACCESSIBILITY_SERVICE` 575.2–134, 136
Bionic 575.1–38
BKS 575.2–78
BLU 575.2–52-58
Bluetooth 575.1–8
..... 575.2–21
Bolts 575.3–91
BOO 575.3–77
Bookmarks 575.2–93
Boot Loader 575.1–53
..... 575.2–34, 47, 48-49
Boot ROM 575.1–31, 53
..... 575.2–34
Bootstrapper 575.4–69
BouncyCastle 575.2–78
BPF 575.5–45-46
Broadcast Intents 575.1–118
Broadcast Receivers 575.1–109, 111, 114, 116-117
..... 575.4–126
Browser 575.5–72, 75
History 575.2–68
Brute Force 575.2–18
Bubbles API 575.1–79
Buffer Overflow 575.3–14
`BuildConfig.DEBUG` Flag 575.4–130
BYOD 575.1–8
..... 575.2–146
Bytecode 575.3–103

C

C# 575.3–77, 82-83, 88, 93
CA Trust 575.4–108, 110
..... 575.5–65
Cajino 575.3–41
Calendar 575.2–68, 93, 109
Canary Protection 575.4–103
Captive Portal 575.5–98
Carnal0wnage 575.5–145
Cellebrite 575.2–8, 12
Cellular Interface 575.5–10
Certificate Details 575.5–69
Certificate Impersonation 575.5–70-72
Certificate Pinning 575.4–108-112
`CFBundleURLSchemes` 575.4–104
CFR 575.3–57
CGI 575.5–106
Checksum 575.4–116
Chrome 575.5–59
Chrome for iOS 575.1–105
CIL 575.3–79, 82, 88, 91, 93, 103
Class Key 575.2–87
Cleartext Traffic → Unencrypted Traffic
`cleartextTrafficPermitted` Flag 575.5–85
Clickjacking Attack 575.2–135
Cloak & Dagger Attack 575.2–134-136
ClockworkMod 575.2–48
Cloud Systems 575.5–6
Code Signing 575.1–31, 39, 67
Command & Control 575.2–130, 132, 142
Computer Programs Directive 575.3–5
Contacts 575.2–68, 93, 109
Access 575.1–42
Contract 575.3–12
Content Providers 575.1–109, 113, 116-117

CoreData 575.2–92
Couchbase 575.2–92
COW 575.2–60
CPU-Agnostic Code 575.3–79
Credentials 575.2–68, 93
Theft 575.2–125
CSS 575.3–95, 97
..... 575.5–43
Cut the Rope 575.2–146
CVE 575.1–105
..... 575.2–60
Cyanogen 575.1–76
..... 575.2–48

D

Dalvik 575.1–53-56, 68
..... 575.3–8, 70
..... 575.4–29
Bytecode 575.4–30-38
Instructions 575.4–35
Types 575.4–34
Decompiler 575.3–10
Dark Matter 575.5–113
Data Encryption 575.1–40, 70
Data Exfiltration 575.5–132
Data Loss 575.2–6, 575.5–22
Data Storage 575.2–63
Database 575.2–65
Dead Code 575.3–70
Debug Detection 575.4–120-121, 137
Debug Mode 575.4–130
Debuggable Flag 575.2–79
..... 575.4–137
Decompilation 575.4–29-31, 48
Decompiler 575.3–57-58, 82
Default Gateway 575.5–29, 44
Defense Techniques 575.5–135
Deobfuscation 575.3–57-68
Deobfuscator 575.3–70
DEP 575.1–31, 35, 37, 68
DER 575.4–109
Developer Certificate 575.1–39
Developer Mode 575.5–124
Development Platforms 575.3–76, 88
Device-Specific Key 575.4–119
DEX 575.1–54
..... 575.2–65
..... 575.3–8, 10, 70
..... 575.4–30
DexGuard 575.3–69
..... 575.4–138
DexProtector 575.3–69
Dialer History 575.2–68, 93
Dictionary Preferences 575.2–93
Direct Exploit Delivery 575.5–27
Dirty Cow Exploit 575.2–60
Disassembler 575.3–26
..... 575.4–30
Disclosure 575.3–94, 100
..... 575.4–113, 128, 130, 133
..... 575.5–23
DLL 575.3–79, 89, 91-93
DMCA 575.2–30
..... 575.3–5
DNS 575.5–14, 19, 39, 45
DoS 575.1–37
..... 575.4–12
..... 575.5–28, 32, 36
Double-Free Threat 575.4–103
Duckyscript 575.2–18
Duktape 575.4–65, 70, 76
Dumping Attack 575.1–40
Dynamic Analysis 575.3–35, 37
..... 575.4–4

E

ECC 575.4–136
Eclipse 575.4–37, 138
ELF 575.1–51
Emails 575.2–68
..... 575.5–125
Emergency SOS 575.2–14, 20
Emulators 575.1–84
Encrypted Traffic 575.5–64
End-User Training 575.5–135
Engineer Mode 575.2–47
Enterprise Certificate 575.2–142
Entitlement 575.1–40
Epoch Time 575.2–94
EULA 575.2–32-33
..... 575.3–5
Exploit 575.5–111
APK 575.3–38
Delivery 575.5–128
Mitigation 575.1–68
Payload 575.5–116
Exploitation 575.5–4
Exported Attribute 575.1–117
Ext4 ..... 575.1–51
Extra 575.4–13
Ez Texting 575.5–126

F

Face ID 575.2–15, 107, 117
FaceTime 575.1–105
Fair Practice 575.3–5
FanReact 575.3–96-102
Faraday Bag 575.2–13
FAT 575.1–51
FBI 575.2–133
FernFlower 575.3–57
File Key 575.2–87

File Protection Classes 575.2–88
File System 575.4–115-116, 134
Encryption 575.1–31, 40
Firebase DB 575.2–76, 92
Flappy Bird 575.3–14
Flash Storage 575.1–40
Foncy 575.2–130-132
Forensic Acquisition 575.2–117
FourGoats 575.4–9
Fragments 575.1–109
Free Wi-Fi 575.5–98
Full Routing 575.5–35-36, 38

G

Gadgets 575.1–35
Garbage Collection 575.4–103
`getExtra` 575.4–11, 13, 127
GID 575.1–58
Go To Declaration 575.3–64
GoatDroid 575.4–9
Google Find My Device 575.2–23
Google Maps 575.2–68
Google Play Protect 575.2–144
Google SafetyNet 575.2–50
Google Voice 575.5–126
GPS 575.2–21, 23, 69, 113, 131
GPWN 575.5–143
GrayKey 575.2–8-13
Password Guessing 575.2–9
GUID 575.2–101

H

Hacking Team 575.5–113-115
HAL 575.1–75
Hardening Techniques 575.4–86
Bypass 575.4–95
Hardware Key 575.2–87
Hashing 575.5–21-22
Heap 575.1–118
HFSX 575.1–30
HIDL 575.1–75
HMAC 575.2–116
Host Fingerprinting 575.5–18
HSRP 575.5–29
HSTS 575.5–75-77
Bypass 575.5–76
HTML 575.5–43
HTML5 ..... 575.3–95, 97
HTTP 575.4–20, 133
..... 575.5–45
Parameter Tampering 575.5–103
Traffic Manipulation 575.5–73
HTTPS 575.5–70
Avoidance 575.5–72
Intercept 575.5–86-87, 96
Hub 575.5–11
Hybrid App Development 575.3–76

I

iBoot 575.2–34
ICCID 575.2–109
iCloud 575.2–107
Backup 575.2–107
Identity Management 575.1–14
Identity Validation 575.1–67
iFunBox 575.2–44
..... 575.4–115
IMAP 575.2–97
IMAPS 575.5–70
IMEI 575.2–109
..... 575.5–21-22
Impact 575.2–5
Implementation Check 575.4–121
Information Disclosure → Disclosure .....
Integer Overflow 575.3–14
Intents 575.1–109, 111, 114
..... 575.4–11-13
`ACTION_CALL` 575.3–12
`ACTION_VIEW` 575.4–83
Filter 575.1–114, 117
Populated 575.4–13
Invisible Grid Attack 575.2–135
Invisible Proxy 575.5–53-54
Invoke 575.4–34-35
iOS 575.1–29
App Store 575.2–44
Apps 575.1–32
Analysis 575.4–19-21
Disassembly 575.3–25-26
Encrypted 575.3–17-18
Extensions 575.1–106-107
Manipulation 575.4–28, 48, 63
Report Card 575.4–123
Retrieval 575.3–17
Unencrypted 575.3–21
Backup 575.2–107-118
..... 575.4–118
Encrypted 575.2–116
Password 575.2–116-117
Resources 575.2–109
Boot Process 575.2–34
Code Signing 575.1–39
Data Protection 575.1–40
..... 575.2–86-88
Data Storage 575.2–92
Encryption 575.1–40
File System 575.2–101-106
Find My iPhone 575.2–23
How To Store Passwords 575.4–119
IPC 575.1–100-107
Keychain 575.2–89-91
Accessibility Attributes 575.2–90

575.4–118
Dump 575.4–118-119
Languages 575.1–32-33
Logs 575.2–99, 101
Malware 575.2–138-139
OS Security 575.1–31, 101-102
Passcode 575.2–7
Privileges 575.1–41-43
RAT 575.5–132
Reverse Engineering 575.3–13, 16
Simulator 575.1–85
Static Analysis 575.3–13
Support 575.1–46
Tech Specs 575.1–30
Trusted CA 575.5–91
Updates 575.1–44
Versions 575.1–46
IP Forwarding 575.5–70
IPA 575.2–37
575.3–77
Analysis 575.3–36
Install 575.2–44
575.4–19
iPad 575.1–29
IPC 575.1–100, 106, 115
575.4–126
iPhone 575.1–29
DevWiki 575.4–55
XS 575.1–38
iTouch 575.1–29
iTunes 575.2–37, 107-109, 111, 114, 117
575.4–118
575.5–12
Backup 575.2–107-108

J

Jabber 575.4–113-114
Jailbreak 575.1–38
575.2–5
Detection 575.4–21
Bypass 575.4–65, 79, 86, 95
Evasion 575.4–61
Signature 575.2–37
Jailbreaking 575.2–28, 145
Artifacts 575.2–106
Binary Identification 575.3–15
Boot 575.2–34
Details 575.2–33-45
Motivators 575.2–29-31
Recommendations 575.2–32
Revert 575.2–33
Runtime Manipulation 575.4–48-49
(Un)Tethered 575.2–33
JAR 575.3–10, 79
Java 575.1–54
575.3–83
575.4–29
575.4–64, 76
Decompiler 575.4–11
VM 575.4–76
`Java.perform` Call 575.4–76
`Java.use` Wrapper 575.4–77, 83
Javascript 575.3–77, 95, 97-98
575.4–50, 59, 65, 76
575.5–43, 45
Engine 575.1–36, 38
575.4–65
Nitro JIT RWX 575.1–39
Obfuscation 575.3–100, 102
Runtime 575.4–70
`jdwp-control` 575.4–137
JIT Compilation 575.1–36, 38-39, 55-57
JOP 575.1–38
JSON 575.2–76

K

Kaspersky Labs 575.2–133
Key Escrow Storage 575.2–101
Key Handling 575.4–136
Key Hierarchy 575.2–87
Key-Value 575.2–71
Keybag 575.2–101
Keyboard 575.1–45
Cache 575.2–100
Keychain 575.1–70
575.2–89-91, 101, 107
575.4–75, 86, 117
Dump 575.4–118-119
Keylogger 575.5–115, 132
Keyset 575.2–71
Keystore 575.4–39, 135-136
Khronos Texture → KTX
Kotlin 575.1–54
KTX 575.2–104

L

LAN 575.5–29
Mirror 575.5–23
Languages 575.1–32-33, 54
Legitimate Application 575.1–67
575.2–128
575.3–13, 41
LiberiOS Exploit 575.2–35
Library Preload 575.4–120
LineageOS 575.2–48
Linux Firewall 575.5–51
Little Endian 575.3–92
575.5–17
Local Certificate Copy 575.4–110
Local File Headers 575.4–41
Location Manager 575.3–12
Location Tracking Information 575.2–69
Lockdown Mode 575.2–20

Locked Bootloader 575.1–53
Locked Device 575.2–16
Loss Impact 575.2–5
Lost Device 575.2–23-25

M

MAC 575.1–38, 69
..... 575.5–19, 22
Mach-O 575.1–30
..... 575.3–16-17, 19, 23, 25
Machine Language 575.4–48
Mailing List 575.5–143
MainActivity 575.5–118-120
Malicious Certificates 575.5–99-100
Malware 575.2–123-124
..... 575.4–69
..... 575.5–111
Authors Motivator 575.2–126
Defense 575.2–143
Delivery Methods 575.2–127
MAM 575.5–135
Manipulation 575.4–27-29
Master Key 575.1–70
..... 575.2–71
MASVS 575.4–100-101, 142
MDM 575.1–65
..... 575.2–6, 16, 145
..... 575.5–135
Solutions 575.2–22
Memory Dump 575.4–94
Memory Management 575.4–103
Messaging 575.5–125
Metasploit 575.4–6, 17, 25
..... 575.5–116
Method Hooking 575.4–77-83
Method Swizzling 575.4–59
MIC 575.5–104
Microsoft 575.3–88, 94
MIPS 575.1–51
MITM 575.2–50
..... 575.3–99
..... 575.4–111
..... 575.5–28, 46, 50-52, 67
Limitations 575.5–59, 64
Tools 575.5–32, 37, 51-59
MO 575.1–29
..... 575.2–146
Mobile Application Management → MAM .....
Mobile Device Management → MDM .....
Mobile Operator → MO .....
Mobile Security Approach 575.1–13
MobileKeyBag 575.2–101
MobileMail 575.2–97
MobileSafari 575.1–39, 43, 100, 107
..... 575.2–142
MobileSync 575.2–108
`MODE_WORLD_READABLE` 575.2–77
MogoRoad 575.2–138
MoneyPack 575.2–133
Mono 575.3–88
Monolithic Kernel 575.1–51
MSTG 575.4–100
mTAN 575.2–125

N

Name Mangling 575.3–15
Name Resolution 575.5–14, 39
NAND 575.1–40
NAT 575.5–52
`nat` Table 575.5–52
NDA 575.1–73
.NET 575.3–88, 92
Network Activity Analysis → Traffic Analysis .....
Network Capture → Packet Capture .....
Network Fuzzing 575.5–50
Network Manipulation . 575.5–27-28, 37, 50, 56-57, 106
Network Security Configuration 575.5–85, 99-100
Network Tap 575.5–11
NFC 575.1–8, 50
Ninja Slider 575.3–8-9
No-Cert-Warning 575.5–75-76
Notes 575.2–93
Notification of Loss 575.2–19
`NSAllowsArbitraryLoads` 575.4–20
NSFileProtection 575.1–40
NSUserDefaults 575.2–92
..... 575.4–119
`NullPointerException` 575.4–127

O

Obfuscator 575.3–69
..... 575.4–138
Object Obfuscation 575.4–138
Objective-C 575.1–32-34, 39, 54
..... 575.3–14-15
..... 575.4–48-50
@objc Header 575.4–62
Basics 575.4–51
Certificate Pinning 575.4–109
OCR 575.3–91
OEM 575.1–74
..... 575.2–47-49
OHA 575.1–50, 73
OkHttp 575.5–100
ooVoo 575.4–102-123
Operation Pawn Storm 575.5–132
OPML 575.5–144
OS X 575.1–30
OTA 575.1–44, 71
..... 575.2–101
OUI 575.5–19, 22
Ouija 575.3–80-87

Overlay 575.2–134-136
OWASP 575.4–9, 100
Ownership Model 575.1–29

P

PAC 575.1–38
  Bypass 575.1–38
Packet Capture 575.5–11, 14
Packet Sniffer 575.5–13, 45
Parental Control 575.2–143, 146
Passcode 575.1–70
  ..... 575.2–6, 109
  Bypass Attack 575.1–53
    ..... 575.2–7, 17
  Failed Guesses 575.2–17
  Recommendations 575.2–19
Passcode Key 575.2–87
Passwords 575.2–68, 93, 97
  Cracking 575.5–32
  Dumping 575.5–32
  Guessing 575.2–9, 106
  Reuse 575.5–64
  Sniffing 575.5–32, 37
  Storage 575.4–119
Patching 575.1–8
Pegasus Attack 575.5–133
Penetration Testing 575.5–4-8, 82
  Roles 575.5–8
Permission Groups 575.1–61
  Dangerous 575.1–64, 115
  Normal 575.1–63, 115
Persistence 575.5–123
Personal Information 575.4–106
Phishing 575.2–139
  ..... 575.5–111, 125-126
Phone Service Abuse 575.1–62
PhoneGap 575.3–47
  Security Issues 575.3–102
PIE 575.4–103
PII 575.4–106
Pillaging 575.5–4-5
PIN 575.2–8-9, 17-18, 21
  ..... 575.4–106
  Top-20 ..... 575.2–18
Pivoting 575.5–112
Plaintext Credentials 575.5–64
Plist 575.2–95-97
Pokemon Go 575.3–78
POP3 ..... 575.2–97
POP3S 575.5–70
Popup 575.2–139
Position Independent Executable → PIE .....
Post-Exploitation 575.5–4
PPTP 575.5–23
Prerouting 575.5–51-52, 70
Privilege Escalation 575.5–106, 119
PRNG 575.3–52
Process Builder 575.3–12
Process Isolation 575.1–55
Procyon 575.3–57
ProGuard 575.3–49, 52, 69
  ..... 575.4–138
Project Mainline 575.1–78
Protection Levels 575.1–115
Protocol Robustness Testing 575.5–50
Proxy 575.4–107
  ..... 575.5–11, 43
  Transparent → Invisible Proxy .....
`ptrace` 575.4–120
Public Key 575.4–139
PUP 575.5–130
Purchase Blocker 575.2–146
Purchase Systems 575.4–27

Q

Qemu 575.1–86, 89
QVOD 575.2–141

R

RAM 575.4–41
Ransomware 575.2–133
RAT 575.3–41
  ..... 575.5–111-116
  Capabilities 575.5–112
  Deployment 575.5–124
Realm DB 575.2–75, 92
Reconnaissance 575.5–4, 125
Recovery 575.2–48
Reflective Programming Language 575.4–49
Registered Protocols 575.4–20
Registers 575.4–33
Remote Access Trojan → RAT .....
Replay Attack 575.5–104-105
Report Card 575.4–101, 123-124, 141
`REQUIRES_INSTALL_PACKAGES` 575.2–137
Resistance 575.1–11
Restrictions Bypass 575.4–49
Reverse Engineering 575.1–30
  ..... 575.3–4-5, 79
  ..... 575.4–65, 104
  Obfuscated Application 575.3–47
  Platforms 575.3–76-103
RFID 575.1–8
Risk 575.5–4
  Posture 575.5–21
ROM 575.2–47-48
Root CA 575.5–65, 90-91, 98-99
Root Certificate 575.5–69
Root Exploit 575.5–119
Rooting 575.2–28, 47-61
  Detection Bypass 575.4–86, 95
  Motivators 575.2–29-31

Recommendations 575.2–32
Root Access 575.2–59
Rootkit 575.2–5
RootViewController 575.4–54
ROP 575.1–35, 37-38
RSA 575.4–136
RSS 575.5–144
Rubber Ducky 575.2–18
Rules Set 575.5–95
Running Services 575.5–27
Runtime Debugger 575.4–29
Runtime Manipulation 575.4–47, 65, 86, 121

S

Safari 575.1–36, 39
Safe Browsing 575.2–144
Sandbox Directory 575.1–40
..... 575.2–101
Sandboxing 575.1–31, 41, 55
..... 575.2–143
SANS Integrated Lab Platform 575.1–15-20, 25
SAW 575.1–79
Scanning 575.5–4, 575.2–144
SCEP 575.5–65
Scope 575.3–64
..... 575.5–78-79
Screenshots 575.2–104
SD 575.1–53
SDK 575.1–85-87
Search Terms 575.2–68
Security Assessment 575.4–101
Security Controls 575.4–86, 100
Bypass 575.4–95
Security Levels 575.4–100-101
SELinux 575.1–69
Sensitive Information 575.1–66, 107
..... 575.2–138
..... 575.4–106
..... 575.5–21
SEP 575.2–9, 86
Server-side Controls 575.1–8
Server-Side Filtering 575.3–102
ServiceManager 575.1–112
Services 575.1–109, 111-112, 116-117
Session Data 575.4–22
..... 575.5–18
Session Timeout 575.5–104
SHA1 ..... 575.2–108-109
Shared Libraries 575.4–19
Side Loading 575.2–145
Sidejacking Attack 575.4–24
Signature Validation 575.4–139-140
Signed Applications 575.2–64
..... 575.4–39-40
Signing Keys 575.4–39
Simulators 575.1–84
Slashdot 575.5–77
Smali 575.4–30-32, 37
VM 575.3–70
Smart Lock 575.2–20-21
SMS 575.2–68, 93-94, 109, 125-126, 138
Auto-Send 575.2–126, 138
Manager 575.3–12
Phishing 575.5–126
Short Code 575.2–126, 129-130, 132, 138, 146
Spoofing 575.5–127
Snap Length 575.5–14
Snapshots 575.2–104
SNMP 575.5–40
SoC 575.1–30
Social Engineering 575.5–98
Socket 575.3–12
..... 575.4–137
SOP 575.5–45
Span Port 575.5–11
SpringBoard 575.2–44, 142
..... 575.4–49
SQL Injection 575.3–99
..... 575.5–106
SQLCipher 575.2–73
SQLite DB 575.2–73, 92-93, 119
..... 575.4–86
Data Decoding 575.2–94
SSL 575.4–111, 113
Attacks 575.5–64, 103
Connection Validation 575.5–65
Enforcement 575.5–83
Interception 575.5–81
MITM 575.5–69-71, 75
Pinning 575.4–65, 79, 86, 95
..... 575.5–59, 81
Bypass 575.5–93, 101
Explained 575.5–100
SslStrip Attack 575.5–74, 79
Stack Canary 575.4–103
Stack Overflow 575.3–48, 63
Stagefright 575.1–78, 575.5–128
Static Analysis 575.3–4, 13, 34, 37, 38
..... 575.4–4
Stolen Device 575.2–4
Stored Data 575.5–112
Storm8 ..... 575.2–138
Strict Transport Security 575.5–75
SuiConFo 575.2–130
Support Lifetime 575.1–46
Svpeng 575.2–133
Swift 575.1–32-34
..... 575.3–14-15
..... 575.4–51, 62
@objc Header 575.4–62
Syslog 575.4–21
System Store 575.5–97
System-on-Chip 575.1–30
SYSTEM_ALERT_WINDOW 575.2–134

T

Table of Critical Addresses 575.4–121
TAC 575.5–22
Task Switching 575.2–104
TCP Stream 575.5–15
TcpDump 575.1–89
Telephony Manager 575.3–12
Telerik 575.3–93
Tesseract 575.3–91
Theft 575.1–8
Third-Party Applications 575.2–137
..... 575.3–76
Threats 575.1–8-9, 14
..... 575.2–4
Tink 575.3–89-94
TLS 575.4–107-109, 113
..... 575.5–84
Attacks 575.5–64, 103
Eavesdropping 575.4–111
Enforcement 575.5–83
Interception 575.5–81
Touch ID 575.2–107, 117
Touch ID Bypass 575.4–86, 95
TowelRoot Exploit 575.4–134
Traffic Analysis 575.4–112, 133
..... 575.5–10, 15
Traffic Duplication 575.5–12
Training 575.2–146
Treble 575.1–74-77
Trojan 575.2–129-130
Trusted CA 575.5–65, 90, 94
Trusted Execution Environment 575.2–78
TrustManager 575.4–95
TTL 575.5–19
Two-Factor Authentication 575.2–125
TWRP 575.2–48, 53

U

UDID 575.5–12-13
UIApp 575.4–54
UID 575.1–58
UIWebView 575.1–36
Unencrypted Traffic 575.5–83-85
Unicode 575.5–17
Unity 575.3–47, 77-81
Compiled Binaries 575.3–78
Universal Links 575.1–103-104
Unknown Sources 575.2–137, 145
..... 575.5–124
Unlocking 575.2–28
Motivators 575.2–29-31
Recommendations 575.2–32
Unrestricted Device 575.2–28-31, 33
Legality 575.2–30
Recommendations 575.2–32
Untrusted Certificate 575.5–66-68, 89
Update 575.1–57
URL Schemes 575.1–100-103
`content://` 575.1–113
Identification 575.4–104
Vulnerability 575.1–105
USB 575.4–73
..... 575.5–12
Debugging 575.2–54
On-the-Go Adapter 575.2–18
Restricted Mode 575.2–10-13
`useCleartextTraffic` Flag 575.5–85
User Dictionary 575.2–106
Userland Exploit 575.2–47, 51

V

V8 ..... 575.4–65, 70, 76
VFAT 575.1–51
VirusTotal 575.5–130-131
Visibility 575.1–14
VMI 575.5–135
Voicemail 575.2–93, 105
VRRP 575.5–29
Vulnerability Period 575.1–8

W

W^X 575.1–35
Web Application Attacks 575.5–82
Web Scanner 575.5–53
WebKit 575.1–38
WebViews 575.2–98
WEP 575.2–68
WHFSViewController 575.4–54-55, 61
WiFi 575.1–8
Windows Firewall 575.5–32-33
Wipe 575.2–17
Policy 575.2–26
Wireless Infrastructure 575.5–6
Wordlist 575.2–106
Workforce 575.1–11
WPA 575.2–68

X

Xamarin 575.3–47, 88-91
Xcode 575.1–39, 85
..... 575.2–96, 99, 140
..... 575.3–16, 25
..... 575.4–103, 106, 113
..... 575.5–12
Device Organizer 575.4–106
XDA Developers 575.2–61
XML 575.2–71-72, 95, 110
XMPP 575.4–113-114
XNU 575.1–30
XSS 575.1–105
..... 575.5–106

Y

YAFFS 575.1–51
Yispecter 575.2–141-142

Z

ZeuS 575.2–125
Zillow 575.4–125-141
ZIP Alignment 575.4–41
Zitmo 575.2–125
Zoom-In 575.2–104
Zygote 575.1–53, 110