Indice generale

Prefazione xiii

Introduzione xv

Destinatari del libro xvi
Prerequisiti xvi
Versioni di Android xvii
Organizzazione del libro xvii
Convenzioni xviii
Ringraziamenti xix
L’autore xix
Il revisore tecnico xx

Capitolo 1 Modello di sicurezza di Android 1

Architettura di Android 1
  Kernel di Linux 1
  Userspace nativo 2
  Dalvik VM 3
  Librerie di runtime Java 4
  Servizi di sistema 4
  Comunicazione tra processi 4
  Binder 5
  Librerie del framework Android 9
  Applicazioni 9
Modello di sicurezza di Android 11
  Sandboxing delle applicazioni 12
  Permessi 14
  IPC 14
  Firma del codice e chiavi della piattaforma 15
  Supporto multiutente 15
  SELinux 16
  Aggiornamenti del sistema 17

Boot verificato 17
Riepilogo 18

Capitolo 2 **Permessi 19**

Natura dei permessi 19
Richiesta dei permessi 20
Gestione dei permessi 21
Livelli di protezione dei permessi 22
Assegnazione dei permessi 24
Applicazione dei permessi 28
  Applicazione a livello di kernel 28
  Applicazione a livello di daemon nativo 29
  Applicazione a livello di framework 31
Permessi di sistema 35
  Permessi di firma 36
  Permessi di sviluppo 37
User ID condiviso 37
Permessi personalizzati 39
Componenti pubblici e privati 41
Permessi per activity e servizi 42
Permessi per i broadcast 42
Permessi per i content provider 44
  Permessi per i provider statici 44
  Permessi per i provider dinamici 45
Pending intent 46
Riepilogo 47

Capitolo 3 **Gestione dei package 49**

Formato dei package di applicazione Android 49
Firma del codice 50
  Firma del codice Java 51
  Firma del codice Android 56
Processo di installazione dei file APK 58
  Posizione di dati e package delle applicazioni 59
  Componenti attivi 59
  Installazione di un package locale 64
  Aggiornamento di un package 69
  Installazione di file APK crittografati 73
  Forward locking 76
  Implementazione del forward locking di Android 4.1 76
  App crittografate e Google Play 78
Verifica dei package 79
  Supporto di Android per la verifica dei package 79
  Implementazione di Google Play 81
Riepilogo 82

Capitolo 4 Gestione degli utenti 83

Panoramica sul supporto multiutente...83
Tipi di utenti 84
    Utente primario (proprietario)..85
    Utenti secondari 87
    Profili con restrizioni 87
    Utente guest...90
Gestione degli utenti...90
    Strumenti a riga di comando 90
    Stati utente e broadcast correlati..91
Metadati utente 91
    File dell'elenco utenti 92
    File dei metadati utente 92
    Directory di sistema utente 93
Gestione delle applicazioni per utente 94
    Directory dati delle applicazioni...94
    Condivisione delle applicazioni..96
Memoria esterna..98
    Implementazioni della memoria esterna 99
    Memoria esterna multiutente...99
    Permessi della memoria esterna...104
Altre funzionalità multiutente..106
Riepilogo 106

Capitolo 5 Provider di crittografia 107

Architettura dei provider JCA 107
    Provider del servizio di crittografia..108
Classi engine JCA 111
    Recupero dell'istanza di una classe engine.............................111
    Nomi degli algoritmi..111
    SecureRandom...112
    MessageDigest 113
    Signature 114
    Cipher..115
    Mac..118
    Key 119
    SecretKey e PBEKey 120
    PublicKey, PrivateKey e KeyPair 120
    KeySpec 120
    KeyFactory..121
    SecretKeyFactory...121
    KeyPairGenerator 122
    KeyGenerator 123
    KeyAgreement 123
    KeyStore..124

CertificateFactory e CertPath 127
CertPathValidator e CertPathBuilder 127
Provider JCA di Android...128
Provider Crypto di Harmony 128
Provider Bouncy Castle di Android...129
Provider AndroidOpenSSL 132
OpenSSL..132
Uso di un provider personalizzato 134
Spongy Castle..134
Riepilogo 135

Capitolo 6 Sicurezza di rete e PKI..137

Panoramica su PKI e SSL..138
Certificati a chiave pubblica 138
Trust diretto e CA private..139
Infrastruttura a chiave pubblica..140
Revoca dei certificati...142
Introduzione a JSSE 143
Socket sicuri..143
Autenticazione dei peer 144
Verifica del nome host 145
Implementazione JSSE di Android 147
Gestione e convalida dei certificati 147
Blacklisting dei certificati..153
Riesame del modello di trust PKI 157
Riepilogo 161

Capitolo 7 Archiviazione delle credenziali 163

Credenziali EAP per VPN e Wi-Fi 164
Certificati e chiavi di autenticazione 164
Archivio delle credenziali di sistema 165
Implementazioni dell'archivio delle credenziali 166
Servizio keystore...166
Tipi e versioni di key blob 168
Restrizioni di accesso 168
Implementazione del modulo keymaster
e del servizio keystore 168
Implementazione con supporto hardware di Nexus 4.............169
Integrazione nel framework 172
API pubbliche 172
API KeyChain 172
Implementazione dell'API KeyChain...178
Controllo dell'accesso al keystore 178
Provider keystore di Android..180
Riepilogo 181

Capitolo 8 Gestione degli account online 183

Panoramica sulla gestione degli account in Android 183
Implementazione della gestione degli account 184
  AccountManagerService e AccountManager 184
  Moduli autenticatori 185
  Cache del modulo autenticatore 186
  Permessi e operazioni di AccountManagerService 187
  Database degli account 189
  Supporto multiutente 193
  Aggiunta di un modulo autenticatore.....................................194
Supporto per gli account Google 197
  Servizio di login Google 198
  Autorizzazione e autenticazione per i servizi Google..............200
  Google Play Services 203
Riepilogo 205

Capitolo 9 Sicurezza aziendale 207

Amministrazione del dispositivo 208
  Implementazione 209
  Aggiunta di un amministratore del dispositivo 215
  Integrazione degli account aziendali.......................................218
Supporto VPN 220
  PPTP 221
  L2TP/IPSec 222
  IPSec Xauth 222
  VPN basate su SSL 222
  VPN legacy 223
  VPN basate sulle applicazioni...229
  Supporto multiutente 232
EAP Wi-Fi...234
  Metodi di autenticazione EAP 235
  Architettura Wi-Fi di Android...236
  Gestione delle credenziali EAP 237
  Aggiunta di una rete EAP con WifiManager 240
Riepilogo 242

Capitolo 10 Sicurezza del dispositivo..243

Controllo dell'installazione e dell'avvio del sistema operativo.......244
  Bootloader 244
  Recovery..245
Boot verificato...246
  Informazioni generali su dm-verity..246
  Implementazione in Android 247
  Abilitazione del boot verificato 248

Crittografia del disco 250
  Modalità di cifratura 251
  Derivazione della chiave 252
  Password di crittografia del disco 253
  Modifica della password di crittografia del disco 254
  Abilitazione della crittografia 255
  Avvio di un dispositivo crittografato 257
Sicurezza dello schermo 260
  Implementazione della schermata di blocco 261
  Metodi di sblocco del keyguard 262
  Protezione contro gli attacchi di forza bruta 270
Debug USB sicuro 271
  Panoramica su ADB 271
  Esigenza di ADB sicuri 273
  Protezione di ADB 273
  Implementazione sicura di ADB 275
  Chiavi di autenticazione ADB 276
  Verifica del fingerprint della chiave host 276
Backup in Android 277
  Panoramica sul backup in Android 277
  Formato di file di backup 279
  Crittografia del backup 280
  Controllo dell'ambito del backup 281
Riepilogo 282

Capitolo 11 NFC ed elementi sicuri 283

Panoramica su NFC 283
Supporto NFC in Android 284
  Modalità Reader/Writer 284
  Modalità Peer-to-Peer 288
  Modalità di emulazione delle card 288
Elementi sicuri 289
  Fattori di forma SE nei dispositivi mobili 290
  Accesso ai SE incorporati 292
  Ambiente di esecuzione SE di Android 295
  UICC come elementi sicuri 298
Emulazione di card software 302
  Architettura HCE di Android 4.4 303
  Routing APDU 303
  Scrittura di un servizio HCE 307
  Sicurezza delle applicazioni HCE 309
Riepilogo 310

Capitolo 12 SELinux

Capitolo 12 SELinux 311
Introduzione a SELinux 312
  Architettura di SELinux 312
  Mandatory Access Control 313
  Modalità di SELinux 314
  Contesti di protezione 314
  Assegnazione e persistenza del contesto di protezione 315
  Policy di sicurezza 316
  Istruzioni per le policy 316
  Regole di transizione dei tipi 319
  Regole di transizione dei domini 319
  Regole dei vettori di accesso 320
Implementazione in Android 322
  Modifiche al kernel 322
  Modifiche allo userspace 323
  File di policy del dispositivo 330
  Registrazione degli eventi delle policy 331
Policy SELinux di Android 4.4 331
  Informazioni generali sulle policy 331
  Applicazione dei domini 333
  Domini unconfined 334
  Domini delle app 335
Riepilogo 337

Capitolo 13 Aggiornamenti di sistema e accesso root 339
Bootloader 340
  Sblocco del bootloader 340
  Modalità fastboot 342
Recovery 344
  Recovery stock 344
  Recovery personalizzati 353
Accesso root 355
  Accesso root sulle build di engineering 356
Accesso root sulle build di produzione 359
  Rooting mediante modifica dell'immagine di boot o di sistema 359
  Rooting mediante flashing di un package OTA 360
  Rooting tramite exploit 366
Riepilogo 366

Indice analitico 367