Index

A

adminWithPolicy, 256
Advanced encryption standard (AES), 29
Asymmetric algorithms, 9
Attestation identity keys (AIKs), 29, 101
Auditing commands
  audit log, 264, 267
  bit field, 264
  command audit, 265
  data, 268
  exclusive audit, 268
  PCR implementation, 265
  session audit, 266
  TPM2_GetCommandAuditDigest, 265
  TPM2_GetSessionAuditDigest, 265
  TPM2_SetCommandCode
    AuditStatus, 265
  TPM2_StartAuthSession, 265
Authenticated code module (ACM), 332
Authorizations
  ADMIN, 171
  audit usage, 168
  block diagram, 169
  command authorization area, 172
  command authorization structures, 174
  DUP, 172
  encrypt/decrypt usage, 168
  HMAC, 165
    authorizing commands, 192
    code implementation, 195
    data structure, 206
    entity creation, 191
    Nonces, 203
    RollNonces function, 194
    security, 205
    session key creation, 191
  password
    code implementation, 178
    command authorization block, 178
    lifecycle, 176
    TPM2_Create command, 177
    TPM2_CreatePrimary command, 177
    TPM2_HierarchyChangeAuth command, 177
    TPM2_NV_ChangeAuth command, 177
    TPM2_NV_DefineSpace command, 177
    TPM2_ObjectChangeAuth command, 177
  policy
    entity's policy digests, 211
    real policy session, 213
    time intervals, 209
    TPM2_NV_DefineSpace command, 212
    TPM2_NV_Write command, 214
    TPM2_PolicyAuthValue command, 213
  response authorization structures, 175
  specification, 167
  USER, 171

B

Boot sequence
  DRTM
    breakout measured launch, 336
    local applications, 339
    measured launch, 338
    SINIT ACM, 338
**INDEX**

<table>
<thead>
<tr>
<th>Boot sequence (cont.)</th>
<th>RSA (see Rivest, Shamir, and Adleman (RSA))</th>
</tr>
</thead>
<tbody>
<tr>
<td>termination, 339</td>
<td>attack classes, 7</td>
</tr>
<tr>
<td>trusted mode, 339</td>
<td>brute force (see Brute force)</td>
</tr>
<tr>
<td>SRTM</td>
<td>SHA-1 hash algorithm, 10</td>
</tr>
<tr>
<td>BIOS trust boundary, 338</td>
<td>weaknesses algorithms, 10</td>
</tr>
<tr>
<td>Microcode, 337</td>
<td>authentication/authorization ticket, 15</td>
</tr>
<tr>
<td>option ROMs, 338</td>
<td>block-mode encryption, 16</td>
</tr>
<tr>
<td>OS boot, 338</td>
<td>extend operation, 13</td>
</tr>
<tr>
<td>Startup ACM, 337</td>
<td>HMAC key, 12, 14</td>
</tr>
<tr>
<td>timeline, 336</td>
<td>KDFs, 14</td>
</tr>
<tr>
<td>Brute force</td>
<td>nonce, 17</td>
</tr>
<tr>
<td>asymmetric algorithms, 9</td>
<td>PCR, 13</td>
</tr>
<tr>
<td>attacks, 10</td>
<td>public key certification, 20</td>
</tr>
<tr>
<td>ECC, 9</td>
<td>secure hash, 12</td>
</tr>
<tr>
<td>key, 8</td>
<td>security protocols, 11</td>
</tr>
<tr>
<td>SHA, 9</td>
<td>symmetric-encryption key, 15</td>
</tr>
<tr>
<td>symmetric algorithms, 9</td>
<td></td>
</tr>
<tr>
<td>Business duplicable key (BDK), 253</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>Cryptographic service providers (CSPs), 40</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate authority (CA), 266</td>
<td></td>
</tr>
<tr>
<td>Certificate signing request (CSR), 130</td>
<td></td>
</tr>
<tr>
<td>Certified migratable keys (CMKs), 3, 31</td>
<td></td>
</tr>
<tr>
<td>Chain of trust, 332</td>
<td></td>
</tr>
<tr>
<td>Context management</td>
<td></td>
</tr>
<tr>
<td>error codes, 294</td>
<td></td>
</tr>
<tr>
<td>internal slots, 294</td>
<td></td>
</tr>
<tr>
<td>Microsoft simulator, 294</td>
<td></td>
</tr>
<tr>
<td>power and shutdown events, 296</td>
<td></td>
</tr>
<tr>
<td>resource manager</td>
<td></td>
</tr>
<tr>
<td>embedded, 291</td>
<td></td>
</tr>
<tr>
<td>proactive approach, 293</td>
<td></td>
</tr>
<tr>
<td>reactive approach, 293</td>
<td></td>
</tr>
<tr>
<td>single-user applications, 291</td>
<td></td>
</tr>
<tr>
<td>TPM response, 292</td>
<td></td>
</tr>
<tr>
<td>virtual-to-TPM handle mapping, 292</td>
<td></td>
</tr>
<tr>
<td>state diagrams, 297</td>
<td></td>
</tr>
<tr>
<td>TAB, 290</td>
<td></td>
</tr>
<tr>
<td>TPM2_ContextLoad command, 296</td>
<td></td>
</tr>
<tr>
<td>TPM2_ContextSave command, 295–296</td>
<td></td>
</tr>
<tr>
<td>TPM2_FlushContext command, 296</td>
<td></td>
</tr>
<tr>
<td>transient entities, 294</td>
<td></td>
</tr>
<tr>
<td>Core root of trust measurement (CRTM), 115, 152</td>
<td></td>
</tr>
<tr>
<td>Cryptographic algorithms</td>
<td></td>
</tr>
<tr>
<td>asymmetric keys, 18</td>
<td></td>
</tr>
<tr>
<td>ECC (see Elliptic curve cryptography (ECC)) function, 18</td>
<td></td>
</tr>
</tbody>
</table>

**D**

<table>
<thead>
<tr>
<th>Debugging</th>
<th>Decrypt/encrypt sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>authorization errors, 317</td>
<td>application-level structure, 277</td>
</tr>
<tr>
<td>bad parameters, 317</td>
<td>asynchronous calls, 285</td>
</tr>
<tr>
<td>high-level applications</td>
<td>asynchronous execution, 276</td>
</tr>
<tr>
<td>bad size, 320</td>
<td>authorization structures, 280, 282</td>
</tr>
<tr>
<td>debug process, 318</td>
<td>creating NV index, 280</td>
</tr>
<tr>
<td>disabled function, 319</td>
<td></td>
</tr>
<tr>
<td>FAPI, 311</td>
<td></td>
</tr>
<tr>
<td>hardware TPM advantages, 317</td>
<td></td>
</tr>
<tr>
<td>missing objects, 319</td>
<td></td>
</tr>
<tr>
<td>password authorization, 319</td>
<td></td>
</tr>
<tr>
<td>policy authorization, 320</td>
<td></td>
</tr>
<tr>
<td>wrong type, 319</td>
<td></td>
</tr>
<tr>
<td>low-level application</td>
<td></td>
</tr>
<tr>
<td>API, 311</td>
<td></td>
</tr>
<tr>
<td>complicated errors, 312, 315</td>
<td></td>
</tr>
<tr>
<td>debug trace analysis, 312–313</td>
<td></td>
</tr>
<tr>
<td>error code analysis, 312</td>
<td></td>
</tr>
<tr>
<td>hardest errors, 312</td>
<td></td>
</tr>
<tr>
<td>last resort, 315</td>
<td></td>
</tr>
<tr>
<td>RM, 311</td>
<td></td>
</tr>
<tr>
<td>TAB, 311</td>
<td></td>
</tr>
<tr>
<td>marshalling/unmarshalling errors, 317</td>
<td></td>
</tr>
</tbody>
</table>

350
DecryptResponseParam decrypts response parameters, 278
EncryptCommandParam encrypts command parameters, 278
EndAuthSession function, 278
function tests, 276
limitations, 272
location and size, 283
NV index deleted, 280
parameters, 271, 276
password session, 282
policy session, 281
pseudocode flow
  HMAC and policy sessions, 273
  lifecycles, 274
  password session, 273
RollNonces function, 278
setting command authorizations, 277
StartAuthSessionWithParams function, 278
synchronous call, 285
synchronous execution calls, 276
Tss2_Sys_ExecuteAsync, 284
Tss2_Sys_ExecuteFinish, 284
Tss2_Sys_GetEncryptParam, 286
Tss2_Sys_GetRspAuths, 284
Tss2_Sys_SetEncryptParam, 286
Undefine command, 279
write data array, 280
write operation, 284
XOR and CFB modes, 271, 273
Deprovisioning process, 308
Dictionary-attack logic, 308
Direct anonymous attestation (DAA), 2
Duplicable storage key (DSK), 258
Dynamic root of trust measurement (DRTM), 159, 332

Endorsement key (EK), 101, 323
End user license agreement (EULA), 158
Enhanced authorization (EA), 166
Enterprise key, 253
Entertainment key, 253
Execution environment
  software stacks
    TSS 2.0, 75
    TSS.net, 75
TPM
  binary version, 72
  Microsoft simulator, 71
  Platform command port, 72
  Python Script, 73
  source code, 72
  system API test code, 74
  TPM command port, 72
  TSS.net, 74
Extended authorization (EA) policies
  administrator role, 242
  approved policy, 247
  certified policies, 247
  command-based assertions, 233
  compound policies, 222, 237
  definition, 217
  end user role, 241
  flexible policy, 222
  home role, 242
  multi-assertion policy, 222
  multifactor authentication, 219, 234
  office role, 242
  policies and passwords, 218
  policy commands, 221
  PolicySession, 243
  simple assertion policy, 222
    digital signatures, 226
    external device, 231
    flexible (Wild Card) policy, 232
    locality of command, 228
    NV RAM location, 230
    passwords, 223
    PCRs, 227
    TPM internal state, 230
  simple assertions and multifactor assertions, 243
  TPM2_PolicyXXX commands, 220
  understudy role, 242
  wild card policy, 246

E
Electronic codebook (ECB) mode, 16
Elliptic curve cryptography (ECC), 9, 121
  ECDH algorithm, 20
  ECDSA algorithm, 20
Elliptic curve Diffie-Hellman (ECDH), 19
Elliptic curve digital signature algorithm (ECDSA), 19
  encryptionKeyIn parameter, 257
Feature API (FAPI), 320
ASYM_RESTRICTED_SIGNING_KEY, 81
ASYM_STORAGE_KEY, 81
callback function, 84–85
derendorsement key, 81
HMAC_KEY, 81
NV, 81
object ancestor, 80
password-handler function, 85
path descriptions, 80
policy commands, 84
profile file, 79
Sign command, 83
standard policy and authentications, 81
Feature Application Programming Interface (FAPI), 252
Financial key, 253
GetDecryptParam function, 89
getPollHandles function, 94
GPIO pins, 146
Hash message authentication code (HMAC)
authorization error, 315
keys, 14
Hierarchies
cryptographic primitive
digest primitives, 114
random number generator, 114
definition, 105
disabling method, 307
derendorsement hierarchy, 108
HMAC primitives, 116
NULL hierarchy, 113
platform hierarchy, 106
privacy
credential format, 109
privacy considerations, 111
proof value, 105
RSA primitives, 117
storage hierarchy, 107
TPM 1.2 SRK, 106
TPM 2.0, 105
UEFI, 107
Infrastructure Work Group (IWG), 157
Institute for Applied Information Processing and Communication (IAIK), 46
Integrity Measurement Architecture (IMA), 153, 157
Intel TXT
boot sequence (see Boot sequence)
components
BIOS ACM, 334
BIOS enabling for Intel TXT, 335
CPU and chipset hardware, 334
CPU microcode, 334
GETSEC, 335
high level applications, 335
Intel authenticated code modules (ACMs), 334
OS/middleware, 335
SINIT ACM, 334
TPM, 335
features, 333
NV indices, 340
PCRs, 340
servers platform, 333
Key derivation function (KDF), 14
Key duplication, 324
Key management system
tree (see Key tree)
Windows 8+, 259
Keys
authorization, 124
cache, 123
certification
digital signature, 131
fingerprint authorization, 131
hybrid index, 132
NV index, 132
signing key, 130–131
X.509 certificate, 130
commands, 119
context management vs. loading, 129
destruction, 125
duplication attributes, 126
generator, 120
hierarchy, 125
NULL hierarchy, 130
persistence, 123
primary key
ECC key, 134
endorsement key, 122
HMAC key, 133
key-derivation function, 121
persistent hierarchies, 121
persistent storage/volatile memory, 121
provisioning software, 120
RSA key, 132
SRK, 120
templates, 121
TPM commands, 122
TPM2_CreatePrimary(), 120
restricted decryption key, 128–129
symmetric and asymmetric keys attributes, 126
Key tree
algorithm set, 252
duplication, 253
SSL servers, 254

M
Measured boot, 332
Migratable key, 257
Monitor mode, 344

N
National Institute of Standards and Technology (NIST), 30
Nonpersistent entity, 100
NULL hierarchy, 98
NV index
access controls, 144
bit field, 141
counter, 141
extend, 142
hybrid index, 143
names, 147
ordinary
certificate stating, 139
common password, 139
HMAC key, 140
platform authorization, 138
public key, 140
password, 149
TCG registry, 146
TPM 1.2 features, 137
TPM2_NV_Extend, 149
TPM2_NV_GlobalWriteLock, 149
TPM2_NV_Increment writes, 149
TPM2_NV_ReadLock locks, 149
TPM2_NV_SetBits, 149
TPM2_NV_WriteLock, 149
TPM2_NV_Write writes, 149
user-defined index, 137
written index, 145
NVRAM index, 99

O
Owner authorization, 35

P, Q
P_ECCP256 profile, 80
PEI phase, 332
Permanent entity
dictionary attack lockout reset, 98
ephemeral hierarchy, 98
password authorization session, 99
PCR, 98
persistent hierarchies, 97
platform NV enable, 99
reserved handles, 99
Persistent entity, 101
Personal duplicable key (PDK), 253
Personal key, 253
Personally identifiable information (PII), 28
Platform Configuration Registers (PCRs), 2, 13, 28, 41, 98, 128, 219, 221, 227
allocation, 152
attestation/quote, 151
algorithms, 160
attributes, 159
authorization and policy, 160
cryptographic proof, 156
EULA, 158
event-log file format, 157

353
Platform Configuration
   Registers (PCRs) (cont.)
   - quote data, 158
   - Trusted Computing concept, 157

Authorization
   - BIOS, 155–156
   - full-disk encryption applications, 154
   - OS level, 156
   - OS security, 154
   - sealing, 154–155
   - TPM2_PolicyAuthorize, 154
   - unseal, 155
   - VPN private key, 155

Commands, 153
   - CRTM, 152
   - debug, 153
   - extend, 151
   - IMA policy, 153
   - metadata, 153
   - NV extend indexes, 153
   - PC Client platform, 153
   - SHA-1 algorithm, 151
   - software state, 151
   - TPM implementation, 151

Platform security processor (PSP), 346
Platform Trust Services (PTS), 157
Pluggable authentication modules (PAMs), 329
PolicyAuthorize, 254
Private key mechanism, 25
Provisioning operation
   - certificate, X.509 format, 305
eDeprovisioning, 308
   - end user, 307
   - OEM platform, 306
   - primary endorsement key, 305
   - primary key, 305
   - TPM manufacturer, 305

P_RSA2048SHA1 profile, 80
P_RSA2048SHA256 profile, 80
Public key certification, 20

Random number generator (RNG), 27
Resource manager (RM), 95
   - embedded, 291
   - proactive approach, 293
   - reactive approach, 293
   - single-user applications, 291

TPM response, 292
   - virtual-to-TPM handle mapping, 292

Rivest, Shamir, and Adleman (RSA), 9
digital signature, 19
encryption keys, 18
Root of trust for measurement (RTM), 332

SEC phase, 332
Secure hash algorithm (SHA), 9
Security problems
   - data backup, 327
   - firmware lock, 330
   - IDevIDs, 323
   - key generation, 327
   - key import, 325
   - privilege separation, 328
   - server’s Logon, 329

Sessions vs. authorization
   - audit usage, 168
   - block diagram, 169
   - encrypt/decrypt usage, 168
   - HMAC, 165–166
      - bound sessions, 188
      - key-derivation function, 182
      - key (K), 182
      - vs. policy sessions, 189
      - salted session, 187, 189
      - sessionKey, 183, 185
      - TPM2_StartAuthSession command, 182–183
      - TPM2_StartAuthSession handles and parameters, 187
      - unbound sessions, 188
      - unsalted session, 187, 189
      - password, 165–166
      - policy, 166
      - bound sessions, 188
      - vs. HMAC, 189
      - key-derivation function, 182
      - key (K), 182
      - salted session, 187, 189
      - sessionKey, 183, 185
      - TPM2_StartAuthSession command, 182–183
      - TPM2_StartAuthSession handles and parameters, 187
      - unbound sessions, 188
      - unsalted session, 187, 189
      - session creation variations, 164

354
specification, 167
use modifiers, 164
Signing scheme, 18
Single storage root key (SRK), 45
Startup definition, 301
Static root of trust (SRTM), 332
Storage root key (SRK), 35, 101, 120, 328
Symmetric algorithms, 9
System API (SAPI)
asynchronous test, 92
command
completion functions, 90
context allocation functions, 86
execution functions, 89
preparation functions, 88
one-call API test, 92
specification, 85
synchronous test, 92
test code, 93

TestSession, 223
TPM. See Trusted platform module (TPM)
TPM 1.2
device identification, 24
ciphering, 26
key storage, 26
NVRAM storage, 27
platform configuration registers, 28
privacy enablement, 28
random number generator, 27
resource identification, 36
specification, 23
TPM 2.0
algorithm agility, 29
clever policy, 33
EA, 32
flexible management, 35
non-brittle PCRs, 34
quicker loading key, 34
resource identification, 36
symmetric-key operation, 34
TPM 2.0 specifications
Auth role, 59
command fields, 58
communit use, 65
data structures
canonicalization, 62
diendarness, 63
hashAl, 62
TPMU HA Union, 62
typedef struct, 62
typedef union, 62
union, 61
definitions
byte stream, 54
canonicalized data, 54
command byte stream, 54
enhanced authorization, 53
handle, 53
HMAC authorization, 53
marshalled data, 54
response byte stream, 55
session, 53
unmarshalled data, 54
header file structure, 66
library
architecture, 52
commands, 52
structures, 52
supporting routines, 53
notation syntax, 63
parameters, 59
platform-specific, 69
ramped up strategies
Dave, 68
Ken, 68
Will, 66
response fields, 57, 60
response parameters, 60
table decorations, 64
TPM2B_DATA Structure, 61
TPM2_Create Command, 58
TPM2_Create Response, 59
TPM2_Startup command (see TPM2_ Startup command)
TPM2_Startup Response, 57
TPMT_HA Structure, 61
TPM2_Clear, 257
TPM2_CreatePrimary, 256, 258
TPM2_Duplicate, 255
TPM2_Duplicate command, 325
TPM2_DuplicationSelect, 253
TPM2_EvictControl command, 330
TPM2_Import, 257
TPM2_Import command, 325
TPM2_Load, 255
TPM2_Load command, 329
TPM2_LoadExternal command, 327, 330
TPM2_PolicyDuplicateSelect, 324
TPM2_Startup command, 56
   command
      code, 57
      fields, 57
      and response, 56
detailed actions, 56
   general description, 56
TPM2_VerifySignature, 254
TPM access broker (TAB), 95
TPM Base Services (TBS), 41
Trusted platform module (TPM)
   Name
      HMAC calculation, 102
      NV index, 103
      paranoid security analyst, 102
      public area, 103
   non-persistent entity, 100
   non-volatile entity, 99
   objects, 100
   permanent entity
dictionary attack lockout reset, 98
   ephemeral hierarchy, 98
   password authorization session, 99
   PCR, 98
   persistent hierarchies, 97
   platform NV enable, 99
   reserved handles, 99
   persistent entity, 101
TPM Software Stack (TSS)
device driver, 96
   feature API (FAPI)
      ASYM_RESTRICTED_SIGNING_KEY, 81–82
      ASYM_STORAGE_KEY, 81
      callback function, 84–85
      endorsement key, 81
      HMAC_KEY, 81
      NV, 81
      object ancestor, 80
      password-handler function, 85
      path descriptions, 80
      policy commands, 84
      profile file, 79
      Sign command, 83
      standard policy and authentications, 81
      user’s default configuration, 82
   SAPI
      asynchronous test code, 92
      command completion functions, 90
command context allocation functions, 86
command execution functions, 89
command preparation functions, 88
one-call API test code, 92
resource manager, 95
specification, 85
synchronous test code, 92
test code, 93
TPM2_GetTestResult command, 86
TPM2_Startup command, 86
schematic diagram, 79
   TAB, 95
   TCTI, 94
TPMT_SENSITIVE area, 326
TPMU_PUBLIC_ID, 326
TPMU_PUBLIC_PARMS, 326
Trusted computing base (TCB), 332
Trusted Computing Group (TCG), 1
Trusted Network Connect (TNC), 157
Trusted platform module (TPM)
   AMD Secure Processor
      AMD platform, 348
      hardware validated boot (HVB), 347
      SKINIT, 348
   applications
      back-end management function, 45
      BitLocker, 44, 48
      CAPI and PKCS, 40
      cryptographic devices, 46
      functions, 41
      IBM file and folder encryption, 49
      manageability solutions, 49
      programming interface, 39
      SRK, 45
      TBS interface, 41
      TrouSerS, 41
      TSS.Net and TSS.C++, 46
      Wave System, 47
      web-based applications, 45
      WMI, 42
   ARM TrustZone, 341
      architectural feature, 341
      mobile devices, 345
      monitor, 344
      NS bit, 343
      protection target, 342
      secure interrupts handling, 345
      secure monitor call (SMC), 344
      system security, 343
auditing commands (see Auditing commands)
CMKs, 3
dictionary attack, 2
direct anonymous attestation, 2
Intel TXT (see Intel TXT)
PCRs, 2
privacy certificate authority, 2
provisioning (see Provisioning operation)
PSP
   ARM TrustZone architecture, 346
      components, 346
security, 1–2
security coprocessor, 3
smart-card chips, 2
startup, 301
startup events
   CLEAR and STATE options, 302
      initialization, 303
   PCRs initialization, 303
   Reset, 302
   Restart, 302
   Resume, 302
   TPM2_Shutdown with CLEAR option, 302–303
TPM2_Shutdown with STATE option, 302–303
TPM 2.0 development
   asymmetric key, 4
   authoritative emulator, 5
   enhanced authorization, 5
   SHA-1, 3
   symmetric key, 4
TrustZone, 341
Tss2_Sys_ExecuteAsync method, 89
Tss2_Sys_ExecuteFinish function, 90
Tss2_Sys_Execute method, 90
Tss2_Sys_GetDecryptParam function, 89
Tss2_Sys_SetCmdAuths function, 89
Tss2_Sys_SetDecryptParam function, 89

U, V
Unified extensible firmware interface (UEFI), 107, 332
userWithAuth, 256

W, X, Y, Z
Windows Management Instrumentation (WMI), 42