



# Index

---

- 3D rendering, 235, 302
- 3D studio, 296
- A**
- AC Tool, 40–46
- Advanced game hacking, 180–183, 293–319
- AFK (away-from-keyboard) combat, 230–234, 186
- Agro
  - drawing, macro for, 44–45
  - managing, 207–208
  - mode, macro for determining, 44
- Aimbots
  - Counter-Strike, 35, 26
  - description, 34–35
  - finding target coordinates, 131
  - and video cards, 131
- Aiming weapons, bot assistance. *See* Aimbots.
- Allal hazam, 73
- Alter data, 129
- Anti-debugging, 123–125
- Apple Computer, EULA, 85
- Architecture of games, 9–12
- Around the game, 132
- Artistic angles, modding, 306–307
- ASF software, 29
- Asheron's Call, 33
- Assembly language, reverse engineering. *See* Reverse engineering, assembly language.
- Assume Nothing, 249
- Attackers
  - affiliations of, 12
  - black hats, 326–327
  - clans, 12
  - philosophy of, 13
  - profile of, 12
  - TKC (Teamkill and Cheat) Community, 12
  - Vasily, 12, 15
  - white hats, 326–327
  - xqz, 12
- AT&T, 119
- Attacker-in-the-middle attack, 25–26, 131, 175
- Attacker's toolkit, 114
  - coverage tools, 117
  - decompilers, 114
  - disassemblers, 116
  - fault injection, 119
  - VM simulation, 122
- Attacks, monitoring, 207–208
- Auction cheats, 38–39
- Auto-join hack, 111
- Automating games. *See* Bots; Macros.
- Away-from-keyboard (AFK) combat, 230–234
- Azeroth, 5
- B**
- Banning, 16, 33, 89
- Battle.net, TOU (terms of use), 88–91
- BeingDebugged flag, 124
- Black hats, 326–327. *See also* Hackers.
- Blacklisting mobs, 203–207
- BlackSnow Interactive (BSI), 71
- Blizzard Entertainment. *See also* WoW.
- banning, 16
- BnetD lawsuit, 20, 76–77
- cheating, countermeasures, 49–51, 52–53
- EULA, 82–84
- game revenue, 20, 65–66
- message from Høglund, 62
- privacy issues, 49–51, 52–53
- spyware. *See* Warden
- TOU, 88–91
- versus EFF. *See* BnetD lawsuit.
- Warden, 49–51, 52–53
- Blunderbuss of flatulence, 27
- Blum, Richard, 264
- BnetD lawsuit, 76–77, 300
- Books and publications
  - Computer Security: Art and Science*, 10
  - "Dangerous Terms . . .", 86
  - Exploiting Software*, 9, 28, 88, 113, 215, 259
  - Hacker Disassembling Uncovered*, 264
  - "How to Hurt the Hackers . . .", 13
  - An Introduction to Genetic Algorithms*, 121
  - "Mastering Unreal Technology . . .", 312
  - "Mathematical Statistics and Online Poker," 37
  - Play Money*, 70
  - "Preventing Bots from Playing . . .", 46–47
  - Professional Assembly Language*, 264
  - Reversing: Secrets of Reverse Engineering*, 264

- Books and publications (*cont.*)  
*Rootkits*, 102, 228  
*The Shellcoder's Handbook*, 102, 113  
*Software Fault Injection*, 119  
*Software Security: Building Security In*, 11, 17, 93, 114, 324
- Boolean tests, reverse engineering, 269–271
- Boomerang, 114–115
- Bot herders, 102
- Botnets, 101–102
- Bots. *See also* Macros.  
 AFK (away-from-keyboard) combat, 230–234  
 aimbots, 34–35  
 assisted aiming, 34–35  
 building a, 21–23, 185–245  
 Combat Assist, 230–234  
 combat macros, 31–33  
 countermeasures  
   Blizzard Entertainment. *See* Warden.  
   captcha technique, 47  
   Governor, 51, 54–61  
   “Preventing Bots from Playing . . .”, 46–47  
   privacy issues, 49–51, 52–53, 61–62  
   PunkBuster, 48–49  
   reverse Turing test, 47  
   spyware, 48–51, 52–53, 61–62  
   Turing test, 22–23, 47  
   Warden, 49–51, 52–53, 61–62  
   WoW. *See* Warden.  
 data mining, 72–73  
 as debuggers  
   breakpoints, 214–219, 223–224  
   debugging loops, 209–214  
   disconnecting, 213–214  
   hardware breakpoints, 214–219  
   in-memory breakpoints, 214–219  
   overview, 208–209  
   privileges, 213–214  
   sampling from context, 219–223  
 SetDebugPrivilege, 213–214
- SetProcessKillOnExit, 213–214  
 siphoning, 223–224  
 as state machines, 187  
 definition, 21  
 giveaways, 35  
 kernel-assisted, 228–230  
 Lin2Rich, 33  
 macro bots, countermeasures, 137–139  
 online FAQ, 34  
 online mugging, 22  
 poker, 22, 36  
 reverse Turing test, 47  
 slaving, 35  
 superhuman aiming, 34–35  
 Thottbot, 72–73  
 Turing test, 22, 47  
 in Unreal Tournament, 34–35  
 user interface for, 234–244  
 uses for, 22  
 WinHoldEm, 36  
 ZelliusBot readme file, 34–35
- Bots, creating  
 closing with mobs, 189–190  
 event-driven design, 187  
 floating in the air, 189–190  
 player character movement  
   agro, managing, 207–208  
   attacks, monitoring, 207–208  
   blacklisting mobs, 203–207  
   direction calculation, 192–195  
   distance calculation, 193–194  
   distance from a mob, 198–199  
   fighting, 199–202  
   ignoring mobs, 203–207  
   looting mobs, 202–203  
   methods, 190  
   ping-ponging, 198–199  
   selecting mobs, 203–207  
   telehacking, 190–191, 195–198  
   teleportation. *See* Telehacking.  
   telesticking, 198  
 state machines, 187–190  
 transition rules, 187  
 Wowzer engine, 224–228  
 Z-hacking, 189–190
- Boundaries, confusing, 99–101  
 Bragg, Marc, 87–88
- Brain in a vat, 122
- Branching operations, reverse engineering, 268–269, 272–274, 288–290
- Breakpoints  
 as cheats, 28  
 hardware, 214–219  
 in-memory, 214–219  
 samples, 223–224  
 using, 214–219
- Broemme, Maik, 315
- BSI (BlackSnow Interactive), 71
- Bubba's Warcraft Hack, 146
- Bufs, 231
- Bugs in games  
 chat message mods, 108  
 client-side game data mods, 108–109  
 drops, monitoring, 109–111  
 fear spell, 106–107  
 out-of-range values, 108  
 pathing, 104–107  
 reporting, 114  
 respawns, monitoring, 109–111  
 seven pernicious kingdoms, 93–95  
 time and state  
   character states, changing, 101–104  
   confusing boundaries, 99–101  
   introduced, 94  
   kingdom of, 94  
   lagging a game server, 101  
   playing for free, 97–98  
   race conditions, 95–97  
   server IP, finding, 101  
   state confusion, 102–104  
   unanticipated combinations, 102–104  
 travel management, 105–107  
 user interface mods, 107–108
- Busby, Jason, 312
- Butler, James, 102, 228
- Buying. *See* Trading in.
- C
- C++ objects, reverse engineering, 139, 248, 265, 285–286
- Call of Duty 2, 175

- Calling conventions, 282–283
  - Captcha technique, 47
  - Cash prizes, 72
  - Castranova, Edward, 67–68
  - cdecl calling, 283
  - CDs, copy protection, 80–82, 86–87. *See also* DMCA; DRM.
  - Cease and desist letters, 90–91
  - Character states, changing, 101–104
  - Charge, using continuously, 104
  - Chat message bugs, 108
  - Cheat codes, 7–8
  - Cheating. *See also* Bots; Bugs; Hacking; Macros.
    - attacker-in-the-middle attack, 25–26
    - auctions, 38–39
    - bots, 21
    - breakpoints, 28
    - criminal
      - duplicating currency, 6
      - money laundering, 73
      - murder in real life, 5
      - online mugging, 22
      - overview, 8
    - data siphoning, 36–39
    - DLL attacks, 27
    - forms of, 7–8
    - graphics-rendering driver attacks, 27
    - lurking, 36–39
    - motives for, 7–9
    - nine rules of online cheating, 13
    - packet interception, 25–27
    - poker, 28–31, 37–38
    - predicting the future, 28–31
    - proxy attacks, 25–27
    - pseudorandomness, 28–31
    - sources for, 21
    - statistics tracking, 37–38
    - system library attacks, 27–28
    - trading in, 8
    - triggers, 28
  - Cheating-Death, 27
  - Checklist, Security 327
  - Chunking functions, 284
  - Cigital, 8, 28, 323
  - Clans, 12
  - Client–server model, 9–12
  - Clients, game. *See* Game clients.
  - Closing with mobs, 189–190
  - CMP function, 268–269
  - Collusion, auctions, 39
  - Combat, 31–33, 199–202
  - Combat Assist bots, 230–234
  - Combat macros, 31–33
  - Compare operations, reverse engineering, 268
  - Comparing strings, 278
  - Consent to monitor, 83–84
  - Constructive activities, 326–327
  - Contractual obligations of EULAs, 85–86
  - Control flow graphs, 259, 261
  - Conversions. *See* Modding.
  - Copy protection, CDs, 80–82, 86–87. *See also* DMCA; DRM.
  - Copying
    - strings, 277
    - virtual objects, 6, 69
  - Copyright. *See also* Legal issues.
    - DMCA (Digital Millennium Copyright Act), 78, 86–87
    - DRM (digital rights management), 80–82
    - fair use, 77–78
  - Copyright Act, 77
  - Copyright Office, 77
  - Corpses
    - ethereal spirit form, 188
    - identifying, 149–150
    - resurrecting, 149–150
  - Cosmos. *See* Thottbot.
  - Countermeasures
    - bots
      - captcha technique, 47
      - Governor, 51, 54–61
      - “Preventing Bots from Playing . . .”, 46–47
      - privacy issues, 49–51, 52–53, 61–62
      - PunkBuster, 48–49
      - reverse Turing test, 47
      - spyware, 48–51, 52–53, 61–62
      - Turing test, 22–23, 47
      - Warden, 49–51, 52–53, 61–62
    - data hacking, 129
    - macro bots, 137–139
    - reverse engineering, 122–126
    - software piracy, 19–20
  - Counter-Strike
    - aimbot, 35
    - graphics-rendering driver attacks, 27, 306–308
    - history of cheating, 12
    - load11, 28
    - proxy cheats, 25
    - as total conversion, 295
    - XQZ hack, 27, 35
  - Coverage tools, 117–120
  - Cracking, 75. *See also* Piracy.
  - Cracking crypto, 130
  - Criminal cheating. *See also* Cheating.
    - duplicating currency, 6
    - money laundering, 73
    - mugging, 22
    - murder in real life, 5
    - overview, 8
  - Customizing games. *See* Modding, Total conversion
- ## D
- Daedalus Project, 67
  - Data hacking
    - countermeasures, 129
    - data exposure, 129
    - moving data, 129–130
    - overview, 126–129
    - packet sniffing, 129–130
    - resting data, 129–130
    - video cards, 131
  - Data mining, 72–73
  - Data siphoning, 36–39
  - DBG\_EXCEPTION\_NOT\_HANDLED, 125
  - Debonneville, Alan, 70
  - Debuggers
    - anti-debugging, 123–125
    - bots as. *See* Bots, as debuggers.
    - drawing on the, 28
    - software testing, 117
  - Debugging loops, 209–214
  - Decompilers, 114–115, 156–164
  - Decrypting Warcraft packets, 317–318

- Defeating cheaters. *See* Countermeasures.
- Denial of service attack, 249
- Dependency Walker, 251–252
- Descartes, René, 122
- Destructive activities, 326–327
- Detours (Microsoft), 57
- Dibbell, Julian, 70
- Direct3D interception, 27, 131, 175
- DirectX, 175
- Direction, calculating, 192–195
- Disassemblers, 116–117
- Distance  
calculating, 193–194  
maintaining, 198–199
- DLLs  
attacks, 27  
hiding, 176–179  
injecting, 166–175  
injection, 54, 166–175  
reverse engineering  
relationships, 252–257
- DMCA (Digital Millennium Copyright Act), 78, 86–87. *See also* Copyright.
- Douglas, A. S., 3
- Donkey Kong, 105
- Doom, 3, 21
- DRM (digital rights management), 80–82. *See also* Copyright.
- Drops, monitoring, 109–111
- Ducheneaut, Nicolas, 47
- DUMPBIN, 252
- Dungeons and Dragons, 3
- Dupe bugs, 6, 69, 100
- Duplicating  
strings, 277  
virtual objects, 6, 69
- Dynamic tracing, 262–264
- E**
- eBay, ban on trading in virtual objects, 9, 71
- Economics, game worlds. *See* Virtual economies.
- EDSAC, 3
- EFF (Electronic Frontier Foundation)  
BnetD lawsuit, 76–77  
on EULAs, 86  
Warden, and privacy, 50
- Eilam, Eldad, 264
- Ellipse example, 269–270
- Emulation servers  
decrypting Warcraft packets, 317–318  
definition, 300  
disclaimers, 315  
hooking the packet engine, 317  
login process, 318–319  
MaNGOS, 302, 317–318  
protocol emulation, 316–318  
WoW, list of, 315
- Encryption, 26, 130, 179–180  
cracking, 130
- Enemies. *See* Mobs.
- Epic Games, 311
- Epilogue to functions, 282
- ESA (Entertainment Software Association), 90–91
- Ethereal spirit form, 188
- Ethics, xxii–xxiv, 63–63, 73
- EUCD (EU Copyright Directive), 78
- EULAs (End User License Agreements). *See also* Legal issues; TOU.  
Apple Computer, 85  
Blizzard Entertainment, 82–84  
common restrictions, 79  
consent to monitor, 83–84  
contractual obligations, 85–86  
definition, 79  
EFF comments on, 86  
FrontPage 2002, 84–85  
Gator Corporation, 84  
hacking restrictions, 87  
legality of, 83  
license checks, 76–77, 300–301  
malware with, 85  
Microsoft, 84–85  
property rights, 87–88  
restricting UI, 24–25  
reverse engineering, 86–87  
Sony, 80–82  
virus with, 85  
Warden, 82–84
- Eve Online, 7, 95, 266
- Even Balance, Inc., 48
- Event-driven bot design, 187
- EverQuest, GDP, 68
- Exception frames, 287–288
- Exception handlers, 286–288
- Exchange rates, 68–69
- Exploiting Software*, 9, 28, 88, 113, 215, 258
- F**
- Fair use, 77–78
- Farmers, 25. *See also* Grinding.
- Farming, macro for, 40–46
- Farms, 5
- Fast calling functions, 283
- Fault injection engines, 119–121
- Fear spell, bug, 106–107
- Felten, Ed, 78, 82
- Fighting movements, 199–202
- Finding the future, 28–31
- First Amendment goes down, 84
- First computer game, 3
- First4Internet, 81
- Floating in the air, 189–190
- Forests, modding, 311–314
- Fortify Software, 93
- Forwarding exceptions, 125
- Frame pointer omission, 284
- Freakonomics*, 68
- Free gaming, 97–98
- FriendGreetings virus, 85
- FrontPage 2002, EULA, 84–85
- Functions, reverse engineering  
calling conventions, 282–283  
cdecl calling, 283  
chunking, 284  
epilogue, 282  
exception frames, 287–288  
exception handlers, 286–288  
fast calling, 283  
frame pointer omission, 284  
imports and exports, 251–257  
inline, 284  
intrinsic, 283  
override-able, 285–286  
page optimization, 284  
prologue, 281–282  
standard calling, 283  
this pointer, 285–286  
variable reuse, 284–285  
working set tuning, 284
- Future of software, 17

- G**  
 Gamasutra, 71  
 Gambling online, legal restrictions, 66. *See also* Poker.  
 Game architecture, 9–12  
 Game clients  
   data mods, 108–109  
   definition, 10  
   modding, 302  
   rendering, 302  
   rewrites, 296–297  
   state, 10–11  
 Game objects. *See* Virtual objects.  
 Game servers  
   emulation. *See* Emulation servers.  
   IP, finding, 101  
   lagging a, 101  
   modding, 297–302  
   third party, 301. *See also* Emulation servers.  
 Gamer’s checklist. *See* Checklist, Security.  
 Gamers, number of, 3, 5  
 GameUSD.com, 68–69  
 Gaming market  
   chart of market share, 6  
   creating wealth, 5–6  
   estimated value of, 66  
   first computer game, 3  
   growth rate, 3, 66  
   history of, 3–4  
   most popular game, 5  
   online poker, 4  
 Gator Corporation, EULA, 84  
 Geographical considerations, 72  
 Getting around the game, 132–180  
   getting in the game, 139–164  
   getting outside the game, 179–180  
   getting over the game, 132–139  
   getting under the game, 164–179  
 Global values, reverse engineering, 267  
 Golle, Phillipe, 47  
 Governor, 51, 54–61, 138  
 Graphics rendering. *See* Rendering.  
 Graphviz, 119
- Grinding. *See also* Farmers.  
 automating, 24–25  
 definition, 24  
 macro for, 40–46  
 targeting free enemies, 32–33  
 Growth rate, gaming market, 3, 7, 66
- H**  
*Hacker Disassembling Uncovered*, 264  
 Hacking. *See also* Bugs; Cheating.  
   game data. *See* Data hacking.  
   legal definition, 87  
   motives for, 12–14, 15  
   nine rules of online cheating, 13  
   restrictions in EULAs, 87  
   scope of, 16–17  
 Half-Life, 295  
 Hardware breakpoints, 214–219  
 HBGary, 116  
 Health status, determining, 136–137, 188  
 Heightmaps, 307, 310, 312  
 Høglund, Greg, 102, 228  
 Høglund’s WoW\_Agro Macro, 40–46  
 Hotkeys, 133–134  
 HunterBot, 227
- I**  
 if else statements, 272–274  
 if statements, 272  
 IGE (Internet Gaming Entertainment), 70  
   connections to Thottbott, 72  
 Ignoring mobs, 203–207  
 In the game, 135–164  
 Inflation, in virtual economies, 69  
 Inline functions, 284  
 In-memory breakpoints, 214–219  
 Inspector, 116  
 INT3 (interrupt 3), 167–164  
 Intel notation, 266  
 Interposition. *See* attacker-in-the-middle  
 Intrinsic functions, 283
- An Introduction to Genetic Algorithms*, 121
- J**  
 Jedi knights, 294
- K**  
 Kaspersky, Kris, 264  
 Kernel hacking, 180–183, 228–230  
 Kernel-assisted bots, 228–230  
 Keystrokes, controlling, 132–133  
 Kiblinger, Robert, 70
- L**  
 Lagging a game server, 101  
 LAN party, 26, 76  
 Law/Lawyers. *See* Legal issues  
 LEA instruction, 267  
 Legal issues. *See also* Copy-right; EULAs; TOU.  
   BnetD lawsuit, 76–77  
   cease and desist letters, 90–91  
   EULAs, 83  
   modding, 319  
   online gambling restrictions, 66  
   server-side license checking, 76–77  
   threats, 89–91  
 Legend of Mir, 5  
 Levitt, Steven, 68  
 Licenses. *See* EULAs.  
 Lin2Rich, 33  
 Linden Lab, 87–88  
 Lineage, 23  
 Litchfield, David, 113  
 Load11, 28  
 Logical operators, reverse engineering, 274–275  
 Looping, reverse engineering, 276–277  
 Looting mobs, 202–203  
 Lurking, 36–39
- M**  
 Macro bots, countermeasures, 137–139  
 Macros, 24, 132. *See also* Bots.  
   AC Tool, 40–46  
   attracting and killing monsters, 40–46

- Macros (*cont.*)  
 banning, 33, 39  
 combat, 31–33  
 countermeasures, 137–139  
 drawing agro, 44–45  
 farming, 40–46  
 hoglund's WoW\_Agro  
   Macro, 40–46  
 Lin2Rich, 33  
 TargetFreeEnemy, 32–33  
 tools for, 40–46  
 Magic crypto fairy dust, 323  
 Magic key sequences, 133–134  
 Malicious demon, 122  
 Malware, in EULAs, 85  
 Man in the middle. *See*  
   Attacker in the middle  
 MaNGOS, 302, 317–318  
 Market share, 5–6, 6  
 Mastering Unreal  
   Technology . . . , 312  
 “Mathematical Statistics and  
   Online Poker,” 37  
 McGraw, Gary, 93, 114, 119,  
   324  
 Media, customizing. *See*  
   Modding.  
 Media file formats, 314–315  
 Memory  
   cloaking, 181–183  
   manipulating, 27–28, 127  
   moveable, 140–141  
   process memory, reading  
     and writing, 162  
 Messages, generating, 139  
 Microsoft, 323  
 Middle market, 70–71  
 Middlemen, 70–71  
 Milkshape, 304  
 Mitchell, Melanie, 121  
 MMOs (massively multiplayer  
   online games)  
   chart of market shares, 6  
   growth rate, 3  
   sociology of players, 67–68  
 MMORPGs (MMO role  
   playing games), 3  
 Mobs  
   attracting monsters, macro  
     for, 40–46  
   blacklisting, 203–207  
   camping on monsters, macro  
     for, 40–46  
   character distance from,  
     193–194, 198–199  
   character orientation to,  
     192–195  
   closing with, 189–190  
   definition, 142  
   finding and killing, 188–189  
   free enemies, targeting,  
     32–33  
   ignoring, 203–207  
   killing monsters, macro for,  
     40–46  
   looting, 202–203  
   selecting, 203–207  
   sticking characters to,  
     104–105, 198  
 Modding  
   artistic angles, 306–307  
   client rendering, 302  
   client rewrites, 296–297  
   definition, 293  
   emulation servers  
     decrypting Warcraft  
       packets, 317–318  
     definition, 300  
     disclaimers, 315  
     hooking the packet engine,  
       317  
     login process, 318–319  
   MaNGOS, 302, 317–318  
   protocol emulation,  
     316–318  
     WoW, list of, 315  
   heightmaps, 307, 310, 312  
   legal issues, 319  
   license checks, 300–301  
   media file formats, 314–315  
   model construction,  
     302–305  
   nude hack, 294  
   overview, 293–295  
   private servers. *See*  
     Emulation servers.  
   procedural generation,  
     307  
   server rewrites, 297–302  
   stand-ins, 305  
   TC (total conversion),  
     295–296  
   terrain, 307–314  
   textures, 306–307  
   third party servers, 301  
   tools for, 302, 304, 311  
   wireframe rendering,  
     310–311  
 Model construction, modding,  
   302–305  
 Money. *See also* Revenue from  
   games; Virtual  
   economies.  
   laundering, 73  
   poker, 4  
   RMT (real money trading),  
     70–71  
   from virtual objects. *See*  
     Trading in virtual  
     objects.  
   WoW Gold, 4  
 Monsters. *See* Mobs.  
 Motives for cheating, 7–9  
 Mouse droppings. *See* Mouse  
   events.  
 Mouse events, controlling,  
   134–136  
 Moveable memory, 140  
 MOV instruction, 266  
 MPQ media format,  
   314–315  
 Mugging online, 22  
 Murder, resulting from  
   gaming, 5  
 MyWarCraftStudio, 304  
 N  
 National Academy of Sciences,  
   302  
 Newitz, Annalee, 86  
 Nine rules of online cheating,  
   13  
 NPCs (nonplayer characters),  
   142, 150–151  
 nProtect, 181  
 NtIllusion toolkit, 176–179  
 Nude hack, 294  
 NVIDIA cards, 165  
 O  
 O'Brien, Mike, 314  
 OGaming, 73  
 OGRE 3D rendering library,  
   235–244, 302  
 OllyDbg, 117  
 Online games. *See* Gaming.  
 Online poker. *See* Poker.  
 OpenGL interception, 27,  
   175  
 Orc speed racing, 296, 298  
 Out-of-range values, 108  
 Outside the game, 179–180  
 Over the game, 132–139  
 Override-able functions,  
   285–286

- P**
- Packets
    - encryption, 179–180
    - intercepting, 25–27
    - manipulation, 179–180
    - sniffing, 129–130
  - Packing, 123, 290–291
  - Pac-Man, 3
  - Page optimization, 284
  - Parrish, Zak, 312
  - Parser, attacking, 258
  - Parsing strings, 276–281
  - Patching, 141
  - Pathing bugs, 104–107
  - Pattern scanning, 258–261
  - Payment interception,
    - auctions, 39
  - PE header, parsing, 146–148
  - PEB (process environment block), altering, 123–125
  - Pernicious kingdoms, 93–95
  - Philosophy of hackers, 13
  - Photoshop, 310
  - Pierce, Brock, 70
  - Pimp My Game, 21
  - Ping-ponging, 198–199
  - Piracy
    - countermeasures, 19–20
    - history of, 19
    - online games, 20
    - TOU (terms of use), 89
  - Pixels, sampling, 43–44, 136–137
  - Play Money*, 70
  - Player character
    - attack mode. *See* Agro.
    - block, 153–154
    - camera angle, 151–153
    - data, 155
    - data structures, 142–144, 153–154
    - definition, 142
    - drawing attention to. *See* Agro.
    - movement
      - agro, managing, 207–208
      - attacks, monitoring, 207–208
      - blacklisting mobs, 203–207
      - direction calculation, 192–195
      - distance calculation, 193–194
      - distance from a mob, 198–199
      - fighting, 199–202
      - ignoring mobs, 203–207
      - looting mobs, 202–203
      - methods, 190
      - ping-ponging, 198–199
      - selecting mobs, 203–207
      - telehacking, 190–191, 195–198
      - telesticking, 198
      - objects, 142
  - Playing for free, 97–98
  - Playing for profit, 71–72. *See also* Revenue from games; Virtual economies.
  - PlayOn Project, 67
  - Pointers
    - finding, 156–164
    - reverse engineering, 276–277
  - Poker
    - bots, 22, 36
    - Cigital hack, 28–31
    - creating wealth, 4
    - game economy, 4
    - growth rate, 7
    - legal restrictions, 66
    - revenue from, 7, 66–67
    - shuffling algorithm, 28–31
    - statistics tracking, 37–38
    - teaching economics with, 68
  - Predicting the future, 28–31
  - Presence of Mind, making permanent, 104
  - “Preventing Bots from Playing Online Games”, 46–47
  - Preventing cheating. *See* Countermeasures.
  - Pritchard, Matt, 13
  - Privacy issues
    - Blizzard Entertainment, 49–51, 52–53, 61–62
    - bot countermeasures, 49–51, 52–53, 61–62
    - PartyPoker.com, 138
    - Sony rootkits, 80–82
    - Warden, 49–51, 52–53, 61–62
  - Privileges, debugger, 213–214
  - PRNGs (pseudorandom number generators), 28–31
  - Procedural generation, 307
  - Process environment block (PEB), altering, 123–125
  - Process Explorer (sysinternals), 249
  - Process lists, hiding from, 138
  - Process memory, reading and writing, 162
  - Professional Assembly Language*, 264
  - Program map, 262–263
  - Project Entropia, 70
  - Prologue to functions, 281–282
  - Property rights, EULAs, 87–88
  - Protocol emulation, 316–318
  - Proxy attacks, 25–27
    - operating a, 25–27, 130
  - Pseudorandomness, 28–31
  - Publications. *See* Books and publications.
  - PunkBuster, 48–49, 181
  - Puzzle contests, 72
  - PvP compat, 198
  - Python, 264, 266
- Q**
- QA (quality assurance). *See* Software testing.
- R**
- Race conditions, 11, 95–97
  - Randomize(), 29
  - Real money trading (RMT), 70–71
  - Realms, 5
  - Rendering
    - 3D, 235
    - game clients, 302
    - hacks
      - attacker-in-the-middle DLLs, 175
      - Direct3D interception, 175
      - DLLs, hiding, 176–179
      - DLLs, injecting, 166–175
      - driver attacks, 27
      - injecting new code, 166–174
      - object locations, 164–165
      - OpenGL interception, 175
      - transparent walls, 165
      - Trojan replacement, 175
      - wall hacking, 165
    - OGRE 3D rendering library, 235–244
    - wireframe, 310–311

- Repetitious play. *See* Grinding.  
 Respawns, monitoring,  
     109–111  
 Resurrecting a corpse,  
     149–150, 188  
 Revenue from games. *See also*  
     Virtual economies.  
     Blizzard Entertainment,  
         20  
     estimated total value, 3, 66  
     growth rate, 3, 66  
     poker, 7, 66–67  
     revenue streams, 65–66  
     RMT (real money trading),  
         70–71  
 Reverse engineering, 247–291  
     anti-debugging, 123–125  
     assumptions, 249  
     control flow graphs, 259,  
         261  
     copy protection, 86–87  
     countermeasures, 122–126  
     Dependency Walker,  
         251–252  
     description, 248–251  
     DLL relationships, 252–257  
     dynamic tracing, 262–264  
     EULAs, 86–87  
     forbidding, 86–87  
     forwarding exceptions,  
         125  
     function imports and  
         exports, 251–257  
     grouping into packages,  
         249–251  
     package boundaries,  
         252–254  
     packing, 123, 290–291  
     pattern scanning, 258–261  
     PEB (process environment  
         block), altering,  
         123–125  
     self-modifying code,  
         290–291  
     single-step timing, 126  
     sketching the system, 249  
     static tracing, 257–262  
     string analysis, 257  
     unpackers, 123  
 Reverse engineering, assembly  
     language  
     basic data movement,  
         266–267  
     basic logic, 267–275  
     Boolean tests, 269–271  
     branching operations,  
         268–269, 272–274,  
         288–290  
     C++ objects, 285–286  
     CMP function, 268–269  
     compare operations, 268  
     description, 264–266  
     functions  
         calling conventions,  
             282–283  
         cdecl calling, 283  
         chunking, 284  
         epilogue, 282  
         exception frames,  
             287–288  
         exception handlers,  
             286–288  
         fast calling, 283  
         frame pointer omission,  
             284  
         inline, 284  
         intrinsic, 283  
         override-able, 285–286  
         page optimization, 284  
         prologue, 281–282  
         standard calling, 283  
         this pointer, 285–286  
         variable reuse, 284–285  
         working set tuning, 284  
     global values, 267  
     if else statements,  
         272–274  
     if statements, 272  
     Intel notation, 266  
     LEA instruction, 267  
     logical operators, 274–275  
     looping, 276–277  
     MOV instruction, 266  
     pointers, incrementing,  
         276–277  
     strings  
         comparing, 278  
         copying, 277  
         parsing, 276–281  
         scanning for metacharac-  
             ters, 278–281  
     switch statements, 288–290  
     switch trees, 289–290  
     table switch statements,  
         288–290  
     TEST operations, 268–269  
     true/false tests, 269–271  
     Reverse Turing test, 47  
     Reversing. *See* Reverse  
         engineering  
     *Reversing: Secrets of Reverse  
         Engineering*, 264  
     Ripping CDs, prohibiting.  
         *See* Copy protection,  
         CDs.  
     RMT (real money trading),  
         70–71  
     Rootkits, 139  
     *Rootkits*, 102, 228  
     Rules of online cheating, 13  
     Russinovich, Mark, 81
- S**
- Scripting. *See* Bots; Macros.  
 Second Life, 70, 87–88, 323  
 Security  
     best practices, 324–326  
     black hats, 326–327  
     building in, 322–327  
     checklist, 327–328  
     constructive activities,  
         326–327  
     destructive activities,  
         326–327  
     for everyday games, 327  
     gamer’s checklist, 327–328  
     software. *See* Software  
         security  
     touchpoints, 324–326  
     white hats, 326–327  
 Selecting mobs, 203–207  
 Self-modifying code, 290–291  
 Selling. *See* Trading in.  
 Servers. *See* Game servers.  
 Server-side license checking,  
     76–77  
 SetDebugPrivilege,  
     213–214  
 SetProcessKillOnExit,  
     213–214  
 Seven pernicious kingdoms,  
     93–95  
 Shell code, 102  
*The Shellcoder’s Handbook*,  
     102, 113  
 Skill bidding, 39  
 Shuffling algorithm, 28–31  
 Single-step timing, 126  
 Siphoning, 223–224  
 Slaving, 35  
 Snyder, Jack, 90–91  
 Sociology of players, 67–68  
 Software, piracy. *See* Piracy.  
*Software Fault Injection*, 119  
 Software security, 17, 321–329



- Software Security: Building Security In*, 11, 17, 93, 114, 324
- Software Security Group. *See* Cigital
- Software testing  
 coverage tools, 117–120  
 debuggers, 117  
 decompilers, 114–115  
 disassemblers, 116–117  
 fault injection engines, 119–121  
 generic, 99  
 malicious, 113–114  
 measuring test completeness, 117–120  
 virtual machine simulators, 122
- Sony, 80–82  
 rootkit debacle, 81–82
- SourceForge, 90–91
- SpeedTree, 311
- Spyware, bot countermeasures, 48–51, 52–53, 61–62
- Standard function calling, 283
- Stand-ins, 305
- Star Wars Galaxies, 6, 71
- State  
 bugs. *See* Time and state bugs.  
 boundary confusion, 99–101  
 client-side, 10–11  
 over time, 11  
 race conditions, 11  
 transition rules, 187
- State machines, bot design, 187–190
- Static tracing, 257–262
- Statistics tracking, 37–38
- Stopping cheaters. *See* Countermeasures.
- String analysis, 257
- Strings, reverse engineering  
 comparing, 278  
 copying, 277  
 parsing, 276–281  
 scanning for metacharacters, 278–281
- Superhuman aiming. *See* Aimbots.
- Swanson, Jason, 37
- Sweatshops, 71, 73
- Switch statements, 288–290
- Switch trees, 289–290
- System library attacks, 27–28
- Sysinternals, 249
- T
- Table switch statements, 288–290
- Target coordinates, finding, 131
- TargetFreeEnemy, 32–33
- TC (total conversion), 295–296
- Telehacking, 105, 190–191, 195–198
- Teleportation. *See* Telehacking.
- Telesticking, 198
- Teletubbies, 294
- Termination rights, TOU (terms of use), 89
- Terms of use (TOU). *See* TOU.
- Terragen, 311
- Terrain, modding, 307–314
- TEST operations, 268–269
- Testing software. *See* Software testing.
- Texas hold ‘em, 28–31
- Textures, modding, 306–307
- Think like a bad guy, 99
- Third party servers, 301
- this pointer, 285–286
- Thottbot, 37, 72–73  
 connection to IGE, 72
- 3D rendering, 235
- Tic-Tac-Toe, 3
- Time and state bugs, 11  
 character states, changing, 101–104  
 confusing boundaries, 99–101  
 kingdom of, 94  
 lagging a game server, 101  
 playing for free, 97–98  
 race conditions, 95–97  
 server IP, finding, 101  
 unanticipated combinations, 102–104
- TKC (Teamkill and Cheat) Community, 12
- Total conversion (TC), 295–296
- Torque, 302
- TOS (terms of service). *See* TOU.
- TOU (terms of use). *See also* EULAs.
- Battle.net, 88–91
- Blizzard Entertainment, 88–91  
 definition, 88  
 piracy, 89  
 termination rights, 89
- Tool chains, 304
- Touchpoints of software security, 324–326
- Tracking virtual objects, 139–140
- Trading in virtual objects  
 annual worldwide sales, 70  
 cheats, 8  
 eBay ban on, 71  
 methods, 9  
 middlemen, 70–71  
 projected growth, 70  
 record sale price, 70
- Transition rules for state change, 187
- Transparent walls, 165
- Travel management bugs, 105–107
- Trees, modding, 311–314
- Triggers, 28
- Trinity of Trouble, 322
- Trojan replacement, 175
- True/false tests, reverse engineering, 269–271
- Turing test, 22–23, 47
- U
- Under the game, 164–179
- Ultima Online, 70  
 inflation story, 69
- UML, 249
- Unpackers, 123, 290
- Unreal, 186, 311–314
- Unreal Tournament, 34–35
- UO Treasures, 70
- User interface  
 altering, 107–108  
 for bots, 23–25, 234–244  
 bugs, 107–108  
 customizing. *See* Modding.  
 health status, determining, 136–137  
 hotkeys, 133–134  
 keystrokes, controlling, 132–133  
 macro bots, countermeasures, 137–139

- User interface (*cont.*)  
 magic key sequences,  
 133–134  
 messages, generating, 139  
 MMORPGs, 23–24  
 mouse events, controlling,  
 134–136  
 overview, 24  
 process lists, hiding from,  
 138  
 rootkits, 139  
 sampling pixels, 136–137  
 source for, 23  
 using, 23–25  
 window names, changing,  
 138
- Utilities. *See* Macros.
- V**  
 Value, 16, 295  
 Van Eenwyk, Joel, 312  
 Vanguard, 250  
 Variable function reuse,  
 284–285  
 Vasily, 12, 15  
 Video cards  
 and aimbots, 131  
 data hacking, 131  
 object locations, 164–165  
 target coordinates, 131  
 Virtual economies. *See also*  
 Revenue from games;  
 Trading in virtual  
 objects.  
 cash prizes, 72  
 creating wealth, 5–6, 9  
 data mining, 72–73  
 EverQuest, GDP, 68  
 exchange rates, 68–69  
 geographical considerations,  
 72  
 inflation, 69  
 middlemen, 70–71  
 money laundering, 73  
 online poker, 4  
 playing for profit, 71–72  
 puzzle contests, 72  
*versus* real economies, 68–69  
 RMT (real money trading),  
 70–71  
 trading in cheats, 8  
 turning virtual objects into  
 real money, 9  
 WoW, 5  
 Virtual machine (VM)  
 simulators, 122  
 Virtual objects  
 copying, 6, 69  
 duplicating, 6, 69  
 finding game code  
 corpse identification,  
 149–150  
 NPC breakpoints,  
 150–151  
 overview, 148–149  
 player character block,  
 153–154  
 player character camera  
 angle, 151–153  
 player character data,  
 155  
 pointers, 156–164  
 process memory, reading  
 and writing, 162  
 resurrecting a corpse,  
 149–150  
 mobs, 142  
 moveable memory,  
 140–141  
 NPCs (nonplayer  
 characters), 142  
 ownership, 83, 87  
 patching, 141  
 PE header, parsing, 146–148  
 player characters, 142  
 player data structures,  
 142–144, 153–154  
 player objects, 142  
 reading files from disk,  
 144–146  
 tracking, 139–140  
 trading in. *See* Trading in  
 virtual objects.  
 value of, 68  
 Windows registry,  
 144–146  
 Virus EULA, 85  
 Vista (Microsoft), 27  
 VM (virtual machine)  
 simulators, 122
- W**  
 Wall hacking, 165, 175  
 Warden  
 critique of, 61–62  
 defeating, 57, 54–61, 138  
 description, 49–51  
 EULA, 82–84  
 as spyware, 52–53  
 Wealth, creating, 5–6, 9  
 White hats, 326–327. *See also*  
 Hackers.  
 Wii, Nintendo, 19  
 Window names, changing, 138  
 Windows registry, virtual  
 objects, 144–146  
 WinHoldEm, 36  
 Wireframe rendering, 310–311  
 Working set tuning, 284  
 WoW (World of Warcraft). *See*  
*also* Blizzard  
 Entertainment.  
 Agro macro, 40–45  
 Azeroth, 5  
 game economy, 5  
 game revenue, 20  
 market share, 5, 6  
 number of players, 5  
 privacy issues, 49–51,  
 52–53, 61–62  
 realms, 5  
 revenue streams, 65–66  
 Warden, 49–51, 52–53,  
 61–62  
 WoW Decompiler, 156–164  
 WoWEmu, 302  
 WowMapView, 90–91, 296  
 WoWModelView, 296, 304  
 WoWSniffer, 130  
 Wowzer engine, 224–228
- X**  
 XCP2, 81–82  
 xqz, 12  
 XQZ hack, 27, 35
- Z**  
 Z-hacking, 189–190  
 ZHeckBot, 224–228  
 ZelliusBot, 34–35, 186  
 Zoltan, Szego, 90–91