Page references followed by italic t indicate material in tables.

A5/1 algorithm, 105
Access Control Lists (ACLs), 125
access controls, 122–125
   mandatory, 126
access tokens, 145–147
active cryptographic protocol attacks, 114
ActiveX, 165–166
   malware susceptibility, 159
Acxiom, 19
ADT Security Services, 386
Advanced Encryption Standard, See AES
adversaries. See also each term as a main index heading
   hackers, 43–46
   industrial espionage, 49–50
   infowarriors, 56–58
   lone criminals, 46–47
   malicious insiders, 47–49, 265–266
   national intelligence organizations, 54–56
   organized crime, 50–51
   police, 51–53
   press, 50
   risk tolerance, 42–43
   terrorists, 53–54
AES, 118
   described, 89, 100
   as hacking contest, 348
Alberti, Leon Battista, 88
airline accidents, greater visibility of relative security debacles, 391
Air Safety Reporting System, 391
AirTran, Web site hack in 1997, 37
Alibris, 49
AlterNIC, Network Solutions traffic redirect attack/protest, 181
American military, See United States military analysis
   of attacks, 376–377
   fault, 218, 221
   traffic, 34–35, 362
AND nodes, 320
   and defense in depth, 370
annual loss expectancy, 301–302
anomaly detection, 196–197
anonymity, 63–67
antitampering devices, 216
antivirus software, 153–154, 157–158
   at firewall, 201
application gateways, 192
Applied Cryptography, xxii, 394
Ariane 5 rocket mishap, 202–203
artificial intelligence, 362
assessment, of attacks, 376
assurance, 363, 373
asymmetric key encryption, 95. See also
   public-key encryption
   and PGP attack tree, 325–326
ATBASH cipher, 86

403
ATM fraud, 23, 40
  card retention after PIN timeout, 140–141
difficulty of prosecuting in England, 377–378
Hartford Connecticut fraud of 1993, 46–47
increasing sophistication of, 16
proactive solutions, 80–81
and secure failure, 371
security policies and countermeasures, 312–313
vulnerabilities, 281
AT&T, 1-800-COLLECT, 28
attacks, 14–15. See also specific kinds of attacks such as denial-of-service attacks, and specific attacks by perpetrator(s) and/or target(s)
action at a distance: global nature of Internet, 19–21
analyzing, 376–377
automation, 18–19, 21
changing nature of, 17–22
counterattacks, 380–383
criminal, 23–29
cryptographic protocols, 90–91, 113–115
detection, 374–376
inside origin: 70% of all attacks, 189
legal attacks, 40–41
need for vigilance, 378–379
need to prepare for worst, 395
need to publicize, 392
privacy violations, 29–36
proaction over reaction, 22
propagation of successful techniques, 21–22
publicity attacks, 36–39
recovery, 380
response, 377–378
steps to successful, 274–278
unchanging aspects of, 15–17
attack trees, 318–324
creating and using, 332–333
Pretty Good Privacy (PGP), 324–331
auction escrow services, 227
auditing, 9, 379–380
security needs, 77–78
Aum Shinrikyo, 90
authentication, 135–150, 283
and denial-of-service attacks, 183
security needs, 68–73
authentication protocols, 147–149
Authencode, 165
automated social engineering, 267–268
automatic program checkers, 362
automatic toll-collection systems, 32
automatic virus-detection centers, 159
automation, 18–19, 21
availability, 122
Avant!, 49
back doors, 241
Back Orifice, 156, 330
hacking tools infected with, 304
banking industry, 379–380
base rate fallacy, 195
Bell-LaPadula model, 125–126, 129
benefit denial, 375
beta testing, 204–205, 206
biometrics, 141–145
black boxes, 186
Blankenship, Lloyd, 382
Blowfish, 89
blue boxes, 186
boot-sector viruses, 152, 153
bots, 310
brand theft, 27–28
British military
  laptop theft from, 284
  security classifications, 63
brute-force attacks, 99–100
buffer overflows, 207–210, 363
bugs
  harmlessness of most software, 366
  software faulty code, 202–207, 210–211
Bugtraq list, 330
Bulgarian Telecommunications Company, distributed denial-of-service attack against, 185
burglar alarms, 197–198, 281
business privacy, 61
buzzword-compliant products, 102–103
byte code verifier, Java, 166
complexity
and faulty code, 204
and function creep, 359–360
as hindrance of security, 1–2
and security, 354–361
trend to in operating systems, 358t
trend to in source code, 357t
as worst enemy of security, 361
component-based software, 160–164
car alarms, denial-of-service attacks against, 39
cash card systems, 213
casino industry, 379
CD Universe, hacker credit card attack against, 37
cell phones, 386
A5/1 algorithm, 105
future improvements in digital, 353
organized crime applications, 51
pinpointing, 31
threat modeling, 304
CERT, 338–339
certificate authorities, 232–233
certificate revocation list (CRL), 231
certificates, 229–238
public-key, 225
CGI (common gateway interface), 172–174
CGI scripts, 172–174
check clearing, 213–214
check fraud, 23
Chinese Wall model, 127
choke points, 369–370
choosing, of security products, 349–352
chosen-plaintext attack, 91
Christmas.exe, 157
CIA, 54, 343
ciphertext only attack, 90
Cisco Systems, bug in switches, 203
Citibank, Russian hacker theft, 20, 391–392
Clark-Wilson model, 127
class loader, Java, 166
Clipper Chip, 241, 294, 304
code signing, 163, 165
Cohen, Fred, 152
collision in access, 111
Comité Liquidant ou Détournant les Ordinateurs (Computer Liquidation and Deterrence Committee), 24
criminal attacks, 23–29. See also organized crime
lone criminals, 46–47
speculations about causes of, 390
criminal investigation, and global nature of Internet, 20–21
critical infrastructure, 57
cross-site scripting, 174
cryptanalysis contests, 346–349
Index

Crypto-gram, 9

cryptographic algorithms, choosing, 115–119
cryptographic keys, 88
government access to, 240–243
key escrow, 240–241
key management, 90
cryptographic protocols, 107–112
attacks, 90–91, 113–115
choosing, 115–119
Internet, 112–113
proprietary, 117, 118
cryptography, 85–101. See also encryption;
MACs
as branch of mathematics, 102
buzzword-compliant products, 102–103
digital signatures, 96–98
future advances in, 353–354
future technologies, 361
key length, 99–101, 103–106
one-time pads, 106–107
one-way hash functions, 94
recognizing plaintext, 91–92
resources on, 8–9
cyberinsurance, 5–6
CyberPatrol, reverse engineering, 346
cyberspace crime, 15–16
ability to execute from anywhere, 19–21, 390
technique propagation, 22
cyber-squatting, 169–170
cyberstalking, 15
databases, 18–19, 33–34
database security, 18–19
Data Encryption Standard, See DES
data harvesting, 29, 30
Data Interception by Remote Transmission (DIRT), 156
data mining, 19
Data Protection Act of 1998 (EU), 60
Deep Crack, 100
default to insecure, 370–371
defense in depth, 370
Defense Intelligence Agency, 54
denial-of-service attacks, 38–39, 260. See also distributed denial-of-service attacks
lack of skill needed, 22
and network security, 181–184
DES, 119
differential-fault-analysis attack, 221
destructive attacks, 24
detection
and effective countermeasures, 279
dictionary attacks, 105, 137
differential-fault-analysis attack, 221
Diffie–Hellman keys, 101
digital embezzlement, 15
digital information erasure, 253–254
Digital Millennium Copyright Act (DMCA), 346
Digital Signature Algorithm (DSA), 97
Digital Signature Standard (DSS), 97
digital signatures, 96–98, 225
Digital Telephony Bill, 67
digital threats, 14–22. See also attacks
digital watermarking, 248–250
directional microphones, 30
DIRT (Data Interception by Remote Transmission), 156
discrete logarithm, 101
distinguished name, 233
distributed denial-of-service attacks, 24, 184–186
lack of skill needed, 22
Trojan horse use, 157
distributed firewalls, 201
distributed.net, 100
DNS security, 180–181
Domain Name Service (DNS), 180–181
dongle, 251
DoubleClick, 19
identity database, 33, 171–172
double-entry bookkeeping, 77
DSA, 97
Dudayev, Dzholar, killing by Russians after cell phone pinpointing, 31
duress code, 259
DVD attacks, 305, 311, 368, 386
and Sony product launch delay, 37
DVD Copy Control Association, 346, 382
dynamic linked libraries (DLLs), 161, 166
eBay
CGI script attack, 173
22-hour outage in 1999, 196
software bugs, 203
ECHELON, 35–36, 55–56
Electronic currency, 78–79
ElGamal algorithm, 95
Key length, 101
And PGP attack tree, 325–326, 327
Elliptic-curve algorithms, 95, 101
e-mail bombing, 182
e-mail-propagating malware, 157
e-mail security, 200
Policies, 307
Threat modeling, 295–296
Encrypted viruses, 154
Encryption, 86–90, 397. See also asymmetric key encryption; cryptography; symmetric key encryption and network defenses, 201
Packets, 179–180, 201
And virtual security, 284–285
Enigma, 91
Entrophy, 104
Equities issue, 342
Erasing digital information, 253–254
Europe, smart cards vs. credit cards, 316
Evaluation
Criteria for computer systems, 131–133
Of security products, 349–352
Excel macroviruses, 355
Exception handling, 258–260
Exploits, 45, 340
Export laws, 67–68
Face recognition, 31
Factoring, future breakthroughs in, 361
Fail-safe strategies, 204, 371
Default to insecure, 370–371
Fair elections, 289–293
Fault analysis, 218, 221
Faulty code, 202–205, 210–211
Attacks on, 205–207
FBI, 55
Florida wiretaps, 52
NuPrometheus League investigation, 382
Pinpointing of Oklahoma City bombing truck, 31
Position on key escrow, 240–241, 242
Pushes for stronger antiprivacy measures, 67–68
Social engineering attack of D.C. office, 266
FLOOZ.com, specialized currency, 79
FOUO classification (For Official Use Only), British military, 63
FRAUD, 23
And privacy violations, 17
Full-disclosure movement, 338–340
Functional testing, 335–336
Function creep, 359–360
GAK back door, 241–243
GPS, surveillance applications, 32
Hackers, 43–46
Activity follows academic year, 378
Prosecutions, 382–383
Hackers, Web site hack in 1995, 37
Hacking contests, 346–349
Hacking tools, 45, 277
Technique propagation, 22
Trading on Web, 304
Hardware security, 212–214
Side-channel attacks, 218–222, 248
Smart card attacks, 222–224
tamper-proof hardware, future breakthroughs in, 362
tamper resistance, 214–218
Hash functions
Key length, 100
One-way, 94
Heartbeats, 39
HIJACK, 222
Honey pots, 197–198
Host-based intrusion detection systems, 197
Hotmail CGI script bug, 173, 205
Human–computer interface, 260–262
Human–computer transference, 262–265
human factors, 255–256
  exception handling, 258–260
  risk analysis, 256–258
  social engineering, 266–269
IDEA, 89
identification, 135–150
  of attacks, 376
identity theft, 26–27
  as growth area for organized crime, 51
IKE (Internet Key Exchange), 112
ILOVEYOU worm, 155, 158, 262
  social engineering aspects, 268
in-band signaling, 186
industrial espionage, 49–50
  laptop theft, 284
infowarriors, 56–58
  terroristic, 53
insurance, 385–386
insurance companies
  and cyberinsurance, 5–6
  demand for improved security, 6
integrity, 73–77, 122
intellectual property theft, 24–26
interconnectedness, of complex systems, 174, 355
Internet. See also World Wide Web; specific
  Internet-related attacks
  complexity, 354
  FDA-type organization, 393
  future secure networking infrastructures, 362
  lack of borders, 19–21
  and least privilege, 368
  and mobile code, 164
  out-of-band signaling as defensive measure, 186–187
  public-key infrastructures, 238–239
Internet backbone, 178
Internet cryptographic protocols, 112–113
Internet Explorer
  fake update-based denial-of-service attack, 185
  subscription feature, 163
Internet Information Server, 363–364
Internet Key Exchange (IKE), 112
Internet Liberation Front, 182
Internet protocols, 176–177
Internet viruses, 153
Internet worms, 22
interpreted viruses, See macro viruses
intrusion detection systems, 194–197
IP addresses, 180
IPsec, 86, 112, 116–117, 201
IP security, 178–180
IP spoofing, 179
ISP filtering, 183
ITSEC, 132
Java, 166–167
Java 2, 163, 167
Java applets, 166
Java sandbox, 162, 166
  attacks against, 368
JavaScript, 165
Java security manager, 166–167
Java security model, 159, 206
Jurassic Park: The Lost World, Web site self-hack as publicity stunt, 37–38
Kashpureff, Eugene, 181
Kerberos, 148–149, 345, 382
Kerckhoffs, Auguste, 91
kernel bloat, 129
keyboard sniffer, 330
key escrow, 240–241
key freaks, 44
keys, See cryptographic keys
  keywords, 169
King, Steven, 311
knowledge partitioning, 378
known-plaintext attack, 90
lamers, 44
laptop theft, 284
Law Enforcement Access Field, 241
Layer Two Tunneling Protocol (L2TP), 112
least privilege, 368
legal attacks, 40–41
liability
  for businesses’ product security, 4–5
  software sold without, 365
  transfer of, 5–6
licensing, 394
Index

linking, 161
localization of attacks, 376
locks, 103
logic bombs, 156
lone criminals, 46–47
lotteries, 305
lottery terminals, 313–314
L0phtcrack, 137

macro viruses, 152, 153
MACs, 92–94
and digital signatures, 97–98
magnetic stripe cards, 315
mail bombing, 182
mailing lists, 330
malicious insiders, 47–49, 265–266
malicious software, 151–159
malware, 151, 157–160
Managed Security Monitoring, 387
mandatory access controls, 126
man-in-the-middle attacks, 114
Mars planet orbiter mishap, 203
MCI, 1–800–0PERATOR, 28
MD4, 94
medical anonymity, 66–67
Melissa virus, 32, 158, 262, 329, 382
memory cards, 314–316
Message Authentication Codes, See MACs
meta tags, 169
Microsoft Data Access Components, security flaw discovered in, 340
Microsoft Excel macroviruses, 355
Microsoft Outlook, 159, 172
Microsoft Outlook 2000, HTML-based malware susceptibility, 159
Microsoft scripting languages, 159
Microsoft Word
known-plaintext attacks, 90–91
macroviruses, 153, 355
military, See British military; United States military
misuse detection, 196
Mitnick, Kevin, 267, 382
mobile code, 164–167
modular code, 160–164
and complexity, 355
money laundering, 17, 51
Moore’s Law, 31
Morris worm, 154–155, 205, 209, 363
CERT founded after, 338
Multics, 129
multilevel security, 62–63, 125

NASA, Mars planet orbiter mishap, 203
national intelligence organizations, 54–56
National Reconnaissance Office, 54
National Security Agency, See NSA
Navajo code talkers, 87
Nazis, traffic analysis application against French, 34
NetCoalition.com, 60–61
Netscape Navigator, 341
random number generator flaw, 36, 105
SSL, 86, 112, 167–168, 170
network-based intrusion detection systems, 197
network defenses
burglar alarms, 197–198, 281
demilitarized zones, 193
e-mail security, 200
and encryption, 201
firewalls, 188–193
honey pots, 197–198
intrusion detection systems, 194–197
virtual private networks, 193–194
vulnerability scanners, 198–200
networked-computer security
malicious software, 151–159
mobile code, 164–167
modular code, 160–164
Web security, 167–175
network security, 176–178. See also denial-of-service attacks
as business problem, 2–4
and complexity, 354
DNS security, 180–181
enforcement of, 4–8
future developments, 186–187
insurance companies’ role in, 6–7
IP security, 178–180
monitoring center, 386–387
resources on, 8–10
Network Solutions
sex.com domain name stolen, 27
traffic redirect attack, 181
Nikrasch, Dennis, 218
null hypothesis, 116

Omnibus Counterterrorism Bill, 67
one-time pads, 106–107
one-way hash functions, 94
OpenPGP, 112
open source solutions, 343–346
open standards, 343–346
opt-out, of data collection, 60
Orange Book, 131–132
organized crime, 16, 50–51
Japanese pachinko machines, 304–305
merging with governments, 58
OR nodes, 321
and defense in depth, 370
out-of-band signaling, 186
outsourcing, of security processes, 386–388

pachinko machines, 304–305
Pacioli, Luca, 77
packet filters, 191
packets, 177–178
encryption, 179–180, 201
page jacking, 28, 169
PAL (permissive action link), 217
Panix, denial-of-service attack against, 181–182
paperless office, 256
PAPS (prescribed action protective system), 217
passive cryptographic protocol attacks, 113–114
password checker, timing attack, 219
passwords, 104–105, 136–141
truncating to avoid buffer overflow attacks, 209

password sniffing, 178–179
patches, need to use latest, 210–211
payload, of IP packets, 178
permissive action link (PAL), 217
personal information, 16–17
PGP (Pretty Good Privacy), 86, 135, 138
attack trees, 324–331
confidence in, 119
key length, 332
OpenPGP, 112
phone cloning, 113
phone phreaks, 18, 44, 186
physical security, 283–284
pinhole cameras, 31
Pinkerton Detective Agency, 381–382
pinpointing, 31
PKI, 225, 232
on Internet, 238–239
problems with traditional, 234–238
PKIX protocol, 113
plaintext
known-plaintext attack, 90
recognizing, 91–92
Plasticash (hypothetical stored-value smart card), 295–300
plug-ins, 167
Point-to-Point Tunneling Protocol (PPTP), 112, 117
police, 51–53
legal attacks by, 41
MDC-4800 Police Data Terminal, 118
personal information database use, 17
privacy violations by, 29
polymorphic viruses, 154
power attacks, 219–220
Practical Cryptography, 8–9
prescribed action protective system (PAPS), 217
press, 50
Pretty Good Privacy, See PGP
PrettyPark worm, 155
privacy
and government, 67–68
security needs, 59–62, 67–68
privacy violations, 16, 29–36
smart cards, 223
private investigators, 29
private keys, 96, 97
proaction, and reaction, 22
proactive solutions, 79–81
product testing and verification, 334–335
 after-the-fact security flaw discovery, 338–343
evaluation and selection, 349–352
 failure of, 335–338
 hacking contests, 346–349
 open source solutions, 343–346
 reverse engineering, 346, 383
 proprietary cryptography protocols, 116–119, 343–346, 363
 prosecution, 377–378
 of criminal attacks, 28–29
 and global nature of Internet, 20–21
 hackers, 382–383
 honey pots to gather information for, 198
 protection, and effective countermeasures, 279
 protection profile, 133
 proxy firewalls, 192
 pseudonymity, 64
 publicity attacks, 36–39
 and tamper resistance efforts, 216
 publicity seekers, 42
 public-key certificates, 225
 public-key encryption, 94–96
 key length, 101
 risk analysis, 258
 public-key infrastructures, See PKI
 public keys, 94–96, 97
 PURPLE code, 91
 quantum computers, 361–362
 random number generators, 98–99
 rational adversary, 43
 rational countermeasures, 286, 316–317
 reaction
 and effective countermeasures, 279
 proaction preferred to, 22
 recovery, 380
 red boxes, 186
 reference monitors, 128
 Registration Authority (RA), 234–235
 remote-cache services, 182
 response, to attacks, 377–378
 reverse engineering, 346, 383
 Riding the Bullet (Steven King), unprotected copies on Web, 311
 risk analysis, 256–258
 risk assessment, 301–302
 risk management, 383–386
 credit card industry as model, 398
 risk tolerance, 42–43
 root certificates, 236
 routers, 177–178
 well-configured, vs. firewalls, 192
 routing attacks, 179
 RSA, 95, 97, 119
 and PGP attack tree, 325–326, 327
 timing attack, 218
 RSA Security
 hacking contests, 348
 home page hijacking, 181
 safes, 279–280
 salami attack, 18
 salting, 141
 Sanders, Thompson, 70
 SATAN (Secure Administrator Tool for Analyzing Networks), 199–200
 scans, 24
 script kiddies, 44, 46
 search engines, and URL hacking, 168–169
 Secret classification, United States military, 62
 secret cryptography, 118
 Secure Compartmented Information Facilities (SCIFs), 220
 Secure Hash Standard (SHS), 94
 Secure networking infrastructures, 362
 SecurID cards, 118, 146
 security. See also adversaries; attacks; Internet; network security; World Wide Web
 after the fact flaw discovery, 338–343
 complexity as worst enemy of, 361
 context matters more than technology, 12–13
 enlisting users, 373
 erasing digital information, 253–254
 future of products, 353–366
 human factors in, 255–269
 implementation flaws more common than design flaws, 202
 improvement of, 2
Index

security (Continued)
and key length, 103–106
layers, 84
need for cost effectiveness of, 365–366
need to question constantly, 373
problem of complexity for, 1–2
process not a product, 273, 395
and software complexity, 354–361
technologies to watch, 361–363
upper-management perspectives on, 272
weakest link, 369
security by obscurity, 344, 371
security kernels, 127–130
security manager, Java, 166–167
security models, 125–127
future of, 133
security needs
anonymity, 63–67
audits, 77–78
authentication, 68–73
electronic currency, 78–79
integrity, 73–77
multilevel security, 62–63
privacy, 59–62, 67–68
proactive solutions, 79–81
security policies, 307–309
security processes
detection and response, 374–380
outsourcing, 386–388
principles of, 367–373
risk management, 383–386
security tactics, 308
security tools
ineffectiveness of, 1
security tricks, 240–254
seeds, 99
Sendmail, UNIX breakins via, 205
Server Side Includes (SSIs), 173–174
session keys, 96
SET protocol, 78, 113
shadow password file, 140
Shannon, Claude, 92
shared libraries, 161
ShareFun, 157
shrinkage, 383–384
side-channel attacks, 218–222, 248
signature, viruses, 158
simplicity, 372–373
single sign-on, 149–150
slot machines
secure perimeter, 217–218
threat modeling, 305
smart card attacks, 218, 219, 222–224
active cryptographic protocol attacks, 114
French card attack, 341
recovery from, 380
smart cards, 213, 224
and memory cards, 314–316
stored-value, 296–301
S/MIME protocol, 86, 112, 119
Smith, David, 32, 382
snake oil, 119, 351
social engineering, 266–269
software piracy, 25, 252–253
software reliability, 202
buffer overflows, 207–210
faulty code, 202–207, 210–211
software vendors
firewall use by, 3
lack of security investments by, 3
SORM-2, 56
sound-based side-channel attack, 221
spam, 200
SPKI protocol, 113
SSL (Netscape Navigator), 86, 112, 167–168, 170
stack smashing (buffer overflows), 207
steganography, 245–246
Steve Jackson Games, 382
stored-value smart cards, 296–301
Stowger, Almon, 27
subliminal channels, 246–248
supernotes, Iranian counterfeit $100 bills, 21
surveillance, 30–33
ECHELON, 35–36, 55–56
Swisher stock price integrity incident, 73–74
symmetric encryption algorithms, 89, 117–118
symmetric key encryption, 86–90
and PGP attack tree, 326
SYN flooding, 38, 182, 341
SYN packets, 181
system high, 125
systems
interconnectedness of complex, 355
life cycle, 286
tamper-evident systems, 216
tamperproof hardware, 213, 214–215, 281, 362
tamper resistance, 214–218, 316, 353
targeted privacy attacks, 29–30
TCP/IP, 176
technique propagation, 21–22
telephone security threat modeling, 293–295
TEMPEST, 220, 222, 235, 330
terrorists, 24, 53–54
threat modeling, 288–289, 302–303, 318
fair elections, 289–293
secure e-mail, 295–296
secure telephones, 293–295
stored-value smart cards, 296–301
wrong threat, 303–306
threats, 14–22. See also attacks
ticker symbol smashing, 169
timing attacks, 218, 220, 326
TLS (Transport Layer Security), 112, 116
Top Secret classification, United States military, 62
trade secrets, 61
traffic analysis, 34–35, 362
Transport Layer Security (TLS), 112, 167
Trin00 distributed denial-of-service attack, 45–46
Triple-DES, 89, 100, 117, 118
Trojan horses, 151, 155–157
trust, 394–395
trusted client software, 309–312
trusted computing bases, 128
trusted third parties, 226–227
trust model, 308
typo pirates, 28, 169

Unclassified classification, United States military, 62
Underwriters Laboratory model, 393–394
unicity distance, 92
Uniform Computer Information Transactions Act (UCITA), 346
United States military. See also NSA
counterattack plan after potential
Russian nuclear strikes, 381
intercepts Japanese message discussing
Pearl Harbor, 35
micro air vehicles, 31
Navajo code talkers, 87
Navy NSA-distributed keys, 89
Navy procedures to prevent social engineering, 268
nuclear weapons control system: tamper resistance, 217
Patriot missile unpredictability, 372
pizza deliveries preceding Iraq bombing, 34
security levels, 62–63
Serbian hackers attack, 57
Soviet Embassy denial-of-service attack in D.C., 39
TEMPEST shielding, 220, 222
U.S. Embassy in Moscow bugged, 286
University of Minnesota, distributed denial-of-service attack against, 184
UNIX
and C1 security, 131–132
kernel bloat, 129
password files, 140
permission system, 124, 368
unpredictability, leveraging, 371–372
URL hacking, 168–170
Usenet postings, 19
users, enlisting security processes, 373
van Eck radiation, 31, 220
VeriFone, 69–70
VeriSign, 232
version-rollback attack, 304
video piracy, 25–26
Video Privacy Protection Act, 25–26
vigilance, against attacks, 378–379
virtual private networks (VPNs), 193–194, 364
cryptography, 86, 113
digital security, 284–285
viruses, See computer viruses
Visa
brand theft attempt against, 27
SET protocol, 78
voice recognition, 31
von Neumann, John, 98
vulnerability landscape, 282–286
vulnerability scanners, 198–200, 210, 342
Walker, John, 378
warez, 25, 252
watermarking, 248–250
Web privacy, 172–175
Web scripts, 172–175
Web spoofing, 170
Windows 2000, 210
  hacking contest, 347
  kernel bloat, 130
  security holes, 207
Windows NT
  kernel bloat, 129–130
  L0phtcrack, 137
  permission system, 124, 368
  security flaw discovered in Microsoft
    Data Access Components, 340

Index

  security holes, 207
  software architecture, 161
  user-remembered passwords, 105

World Wide Web
  publicity attack site defacings, 37–38
  security, 167–175

Worm.ExploitZip worm, 158, 262
worms, 151, 154–155
  Morris worm, 154–155, 205, 209, 363

Y2K, 395

zeroization, 254
zombies, 184–185