

Index

Note to the reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

Numbers

3DES (Triple-DES), 159
8.3 filename convention, 39
10Base2, 81
10Base5, 81
10BaseT, 83, 116
802.1x authentication, 122
802.11 IEEE standard, 87
802.11x IEEE standard, 87

A

AAA server, 113
acceptable use policy, 211
acceptance, and risk assessment, 135
access control
 best practices, 99–101
 exam essentials, 110
 logical methods, 106–110
 models, 101–105
 DAC (Discretionary Access Control)
 method, 103–104
 MAC (Mandatory Access Control)
 model, 102–103
 Role-Based Access Control (RBAC)
 model, 104
 over physical environment, 11
access control list (ACL), 106
 for DAC, 103

access logs, 146
account expiration, 109
account lockout, 212
accounts, default, 79
Active Directory (AD), 115
 group policies and, 19
active sniffing, 58
ActiveX, 22
ad hoc mode, for wireless access points, 88
Address Resolution Protocol (ARP),
 poisoning, 48–49
administrative privileges, 3
Advanced Encryption Standard (AES), 159
adware, 8
agents, and DoS attack, 43
AH (Authentication Header), 177
ALE (annual loss expectancy), 136
algorithms, comparative strength of, 163
amplification network, 44
annual loss expectancy (ALE), 136
annualized rate of occurrence (ARO), 136
anomaly-based monitoring, 144
anomaly-detection IDS, 64, 65
anonymous FTP, 38–39
anti-spam software, 30
antivirus software, 4, 30
 logs, 147
 and VPN traffic, 118
Apple, Bootcamp, 31
application-level gateway firewall, 69

applications

- hardening, 15–16, 21–29
 - ActiveX, 22
 - browser, 23–24
 - buffer overflow, 24
 - cookies, 24–25
 - cross-site scripting (XSS), 27–28
 - input validation, 27
 - instant messaging (IM), 26–27
 - Java, 22
 - P2P, 27
 - scripts, 23
 - SMTP open relays, 25–26
 - limiting installs, 15
 - archive bit, 205
 - armored virus, 4
 - ARO (annualized rate of occurrence), 136
 - ARP poisoning, 48–49
 - assets identification, 135
 - assignment, and risk assessment, 135
 - asymmetric encryption, for digital
 - signatures, 163
 - asymmetric key, 160, 160–161
 - attack surface, 15
 - attenuation, 83
 - audit trails, 145
 - auditing, 145–147
 - exam essentials, 147
 - periodic, of system security, 147–149
 - authentication, 101, 110–112
 - attacker capture of, 42
 - components, 112–123
 - biometric reader, 112–113
 - Challenge Handshake
 - Authentication Protocol (CHAP), 120–121, 121
 - Kerberos, 119–120, 120
 - Lightweight Directory Access Protocol (LDAP), 115, 115
 - Password Authentication Protocol (PAP), 122
 - RADIUS (Remote Authentication Dial-In User Service), 113, 114
 - remote access policies, 116, 116–117
 - Remote Access Server (RAS), 114, 114–115
 - TACACS (Terminal Access Controller Access Control System), 122, 122
 - virtual private networks (VPNs), 117, 117–119, 118
 - exam essentials, 112, 122–123
 - vs. identification, 123–124
 - multi-factor, 111
 - mutual, 122
 - and non-repudiation, 162
 - for PPTP, 175–176
 - remote, 117
 - user names and passwords for, 107–108, 108
 - for workstation users, 18
- authentication factors, 14
- Authentication Header (AH), 177
- authority system, for certificates, 188
- authorization, 101
- availability, 161–162, 205
- awareness training, 214–215
 - on social engineering attacks, 220–221

B

- back doors, 78–79, 79
- backup generator, 200

backups, 204–205
bag and tag, 208
banner grab, 138
baseband, 81
 vs. broadband, 83
baselines, 142
behavior-based monitoring, 143–144
best practices, for access control, 99–101
biometrics
 locks, 126
 reader, 112–113
BIOS (basic input/output), 11–12
birthday attack, 78
 and hashing, 169
BitTorrent, 27
blind FTP, 39
block cipher, 159
Blowfish encryption system, 159
blue jacking, 89–90
bluesnarfing, 90
Bluetooth-capable devices, 89
BNC connectors, 81, 82
boink attack, 46
bonk attack, 46
boot sector viruses, 4
booting, off USB device, 12
botnets, 9, 44
bots, and DoS attack, 43
bounce network, 44
bridge trust structure, 188–189, 189
broadband, vs. baseband, 83
broadcast storm, 54
browser, 23–24
brute-force attack, 77, 139
buffer overflow, 24
business continuity planning, 203
business impact analysis, 204

C

cables, shielding of, 218
callback, for dial-up modems, 115
Carlisle Adams/Stafford Tavares
 (CAST-128), 159
CD-Rs, 13
cell phones, 12–13
centralized key management, 156, 156
centralized logging, 146
centralized privilege management, 105
certificate authorities (CA), 181, 181,
 183–184
certificate policies, 184
certificate practice statement (CPS), 184
certificate revocation list (CRL), 186,
 186–187
certificates, 181
 information stored, 182
 issuance, 183
 obtaining, 182
 registration, 184
 single vs. dual sided, 165
 storage, 156–157
certification hold, 187
CGI (Common Gateway Interface), 23
chain of custody, 208
Challenge Handshake Authentication
 Protocol (CHAP), 120–121, 121
 authentication process, 121
change management, 212
chat (instant messaging), 26–27
circuit-level gateway firewall, 69
classifications, in MAC, 102
classifying information, 212
clearance level, in MAC environment, 103
cleartext, in SMTP, 25

clients, 18
 personal software firewall on, 29–30
 close circuit television (CCTV), 128
 closed ports, response from, 137
 closed wireless network, 89
 coax, 81
 coaxial cable, 81, 81–82
 cold site, 200
 .com file extension, 4
 Common Gateway Interface (CGI), 23
 common routers, 69
 companion virus, 4
 computer groups, 105–106
 computers, secure disposal, 211
 confidentiality, 102, 161
 configuration baselines, 20
 containment, 207, 209
 cookies, 24–25
 cracking passwords, 77
 CRL (Certificate Revocation List), 186, 186–187
 cross-certification, 188–189, 189
 cross-site scripting (XSS), 27–28
 cross-training, 100
 crossover error rate (CER), for biometric devices, 113
 cryptography, 155–167
 asymmetric key, 160, 160–161
 attacks against, 91
 comparative strength of algorithms, 163
 confidentiality, 161
 digital signatures, 163–164
 exam essentials, 165–167
 hashing, 168–170
 integrity and availability, 161–162
 key management, 155–157
 nonrepudiation, 162
 protocols, 173–180
 public key, 180–191

single vs. dual sided certificates, 165
 steganography, 157–158
 symmetric key, 158–159, 159
 Trusted Platform Module (TPM), 165
 whole disk encryption, 164
 WPA-2 for, 88

D

DAC (Discretionary Access Control)
 method, 103–104
 data center, 217
 data emanation, 88–89
 Data Encryption Standard (DES), 119, 159
 DDoS (distributed denial-of-service)
 attacks, 9
 decentralized key management, 156, 157
 decentralized privilege management, 105
 default accounts, 79
 default gateway, 60
 demilitarized zones (DMZ), 38, 51–52, 52, 70
 denial-of-service (DoS) attacks, 4, 43–46
 Denied settings in ACL, 103
 DES (Data Encryption Standard), 119, 159
 destroying keys, 187
 dictionary attack, 77–78, 139
 differential backup, 205
 Diffie-Hellman, 160
 digital signature
 in PGP, 171
 process, 172
 digital signatures, 163–164
 directory services, 115
 disaster recovery plans (DRPs), 199, 203–207
 exam essentials, 206–207
 exercises, 204

Discretionary Access Control (DAC)
 method, 103–104

diskettes, 13

disposal of computers, and security, 211

distributed denial-of-service (DDoS)
 attacks, 9, 43–44, 44

distributed reflective denial-of-service
 (DRDoS) attacks, 44

DMZ (demilitarized zones), 38, 51–52,
 52, 70

DNS (Domain Name Service)
 poisoning, 47–48
 resolving name into IP address, 47
 server logging, 146

documentation
 of change, 212
 for security, 211, 215

domain name kiting, 46–47

domain password policy, 107

domain tasting, 47

door access systems, 126–127

dual-homed firewall, 69, 70

dual-sided certificates, vs. single side, 165

due care policies, 213

due diligence, 213

due process, 213

dumpster-diving attacks, 13, 220
 countermeasure to, 211

DVDs, 13

E

e-mails, 7–8
 asymmetric encryption process, 175
 filter for spam, 6
 security issues, 25–26
 spam, 5

eavesdropping, and instant messaging, 27

ECC (Elliptic Curve Cryptography),
 161, 172

eDirectory, 115

EEPROM (electrically erasable
 programmable read-only memory), 11

EF (exposure factor), 136

egress filter, 72

El Gamal algorithm, 161

electrically erasable programmable read-
 only memory (EEPROM), 11

electromagnetic interference (EMI),
 shielding to prevent, 86

Elliptic Curve Cryptography (ECC), 161,
 172

emanations, 88–89

EMI (electromagnetic interference),
 shielding to prevent, 86

Encapsulating Security Payload (ESP), 177

encapsulation, by VPNs, 118

encryption
 for e-mail, 25
 weak, 90–91

end-user computers, 18

enterprise networks, 50

enterprise spam tools, 6

environmental controls, 217–218
 exam essentials, 218

ESP (Encapsulating Security Payload), 177

essential services on system, 16

ethical hacking, 141

evidence, gathering and protecting, 208

exam essentials
 access control, 110
 best practices, 100–101
 models, 104–105
 applications hardening, 28–29
 auditing, 147
 authentication, 112, 122–123

- cryptography, 165–167
 - protocols, 179–180
 - disaster recovery plans (DRPs), 206–207
 - environmental controls, 218
 - hardening applications, 28–29
 - hardening operating systems, 21
 - hardware risks, 14
 - hashing, 170
 - incident response procedures, 210
 - monitoring, 143, 144
 - network design, 61–62
 - network devices vulnerabilities, 80
 - network security, 73
 - organizational policies, 215–216
 - physical security, 128
 - protocols, 49–50
 - public key cryptography, 189–191
 - risk assessment, 136–137
 - security groups, 105–106
 - security threats, 10–11
 - on social engineering, 221
 - vulnerabilities assessment, 140
 - wireless networks, 91–92
- expiration date of certificate, 186, 187
- expiration of user accounts, 109
- exposure factor (EF), 136
- extranets, 52, 53
-
- F**
- facial recognition, 113
 - false acceptance rate (FAR; Type II) errors,
 - for biometric devices, 113
 - false positives, in IDS, 64
 - false rejection rate (FRR; Type I) errors,
 - for biometric devices, 113
 - FAT (File Allocation Table), 18
 - fault tolerance, 205
 - fiber-optic cable, 85, 85
 - file distribution, P2P for, 27
 - file resources, security controls for, 106
 - file swappers, 39
 - File Transfer Protocol (FTP), 38
 - anonymous, 38–39
 - packet sniffing, 39
 - SSL for, 177
 - filenames, 8.3 convention, 39
 - filtering, 137
 - filters
 - for firewalls, 68
 - Internet content, 72
 - fingerprints, 113
 - fire suppression, 217
 - fired employees, procedures for, 214
 - firewall policy, developing, 69
 - firewalls, 68–70
 - logs, 147
 - personal software, 29–30
 - and VPN traffic, 118
 - firmware, 74–75
 - first-party cookies, 25
 - first responders, 209
 - flash cards, 14
 - floppy disks, 13
 - forensics, 208
 - fraggle, 44
 - front running, domain name, 47
 - FTP. *See* File Transfer Protocol (FTP)
 - FTP upload, 39
 - full backup, 205
 - fuzzying attack, 27

G

GetAdmin, 3
GoDaddy.com, 47
government implementation of MAC, 102
graphics, text hidden inside, 157–158
group memberships, cumulative access
 based on, 104
group policies, 19, 106–107
 reviewing, 148

H

hacker, honeypot to attract, 71
hand geometry, 113
hard drives, 13
hardening
 applications, 21–29
 ActiveX, 22
 browser, 23–24
 buffer overflow, 24
 cookies, 24–25
 cross-site scripting (XSS), 27–28
 input validation, 27
 instant messaging (IM), 26–27
 Java, 22
 P2P, 27
 scripts, 23
 SMTP open relays, 25–26
 operating systems, 15–21
 configuration baselines, 20
 group policies, 19
 updates, 18
hardware, for cryptography key storage,
 157

hardware risks, 11–14
 BIOS, 11–12
 cell phones, 12–13
 exam essentials, 14
 network attached storage, 14
 removable media, 13–14
 USB drives, 12
hash value, 168
 for passwords, 108
hashing, 77, 78, 168–170
 exam essentials, 170
HIDS (host-based intrusion detection
 systems), 29, 63, 64, 65
high availability, 205
hijacking attacks, 802.1x authentication
 vulnerability to, 122
HIPAA (Health Insurance Portability and
 Accountability Act), 213
hiring policies, 214
hoax e-mail, 5
hoaxes, 6–7, 220
honeypot, 71, 71–72
host-based intrusion detection systems
 (HIDS), 29, 63, 64, 65
host ID, 59
HOSTS file, DNS poisoning and, 48
hot site, 199
hotfixes, 18
HTML (Hypertext Markup Language),
 176
HTTP (Hypertext Transfer Protocol),
 176–177
HTTPS (Hypertext Transport Protocol
 Secure), 176
human resource policies, 214
humidity control, 218

- Hunt, 42
 - HVAC management, 218
 - hybrid attacks, 139
 - Hyper-V, 31
 - Hypertext Markup Language (HTML), 176
 - Hypertext Transfer Protocol (HTTP), 176–177
 - Hypertext Transport Protocol Secure (HTTPS), 176
-
- I**
- ICANN (Internet Corporation for Assigned Names and Numbers), 47
 - ICMP (Internet Control Message Protocol), DoS attacks and, 43
 - ID badges, 126
 - IDEA (International Data Encryption Algorithm), 159
 - identification, vs. authentication, 123–124
 - IDSs (intrusion detection systems), 63–64
 - components, 66
 - firewall closing port, 67
 - and firewalls, 63
 - TCP resetting connections, 67
 - IKE (Internet Key Exchange), 178
 - IM (instant messaging), 26–27
 - IMAP (Internet Message Access Protocol), 25
 - implicit denials, 99
 - inbound filter, 72
 - incident response procedures, 207–210
 - chain of custody, 208
 - damage and loss control, 209
 - exam essentials, 210
 - first responders, 209
 - forensics, 208
 - reporting, disclosure, 209–210
 - incremental backup, 205
 - indirect control, of botnet, 9
 - information, classifying, 212
 - infrastructure mode, for wireless access points, 88
 - ingress filter, 57, 72
 - input validation, 27
 - instant messaging (IM), 26–27
 - integrity, 161
 - hashing to protect or verify, 168
 - International Data Encryption Algorithm (IDEA), 159
 - Internet content filter, 72
 - Internet Control Message Protocol (ICMP), DoS attacks and, 43
 - Internet Corporation for Assigned Names and Numbers (ICANN), 47
 - Internet Key Exchange (IKE), 178
 - Internet Message Access Protocol (IMAP), 25
 - Internet Protocol (IP), DoS attacks and, 43
 - Internet Security Association and Key Management Protocol (ISAKMP), 178
 - intranets, 52, 53
 - intrusion detection systems (IDSs), 63–64
 - components, 66
 - firewall closing port, 67
 - and firewalls, 63
 - TCP resetting connections, 67
 - and VPN traffic, 118
 - inventory of assets, 135
 - IP (Internet Protocol), DoS attacks and, 43
 - IP addresses, resolving DNS name into, 47
 - IP spoofing attacks, 57

IP-to-MAC address resolution, falsifying, 48–49

IPSec (Internet Protocol Security), 118, 177, 177–178

NAT-T to support, 56

iris scans, 113

ISAKMP (Internet Security Association and Key Management Protocol), 178

J

Java, 22

JavaScript, 23

job rotation, 100

Juggernaut, 42

K

KDC (Key Distribution Center), 119

Kerberos, 42, 112, 119–120, 120
authentication process, 120

key destruction, 187

Key Distribution Center (KDC), 119

key escrow, 185, 185–186

key management, 155–157

key recovery agent, 185–186

keyboard dynamics, 113

L

L2TP (Layer 2 Tunneling Protocol), 118, 175, 177

land attack, 46

LANMAN protocol, 170

Layer 2 Tunneling Protocol (L2TP), 118, 175, 177

LDAP (Lightweight Directory Access Protocol), 115, 115

leaf CA, 188

least privilege, 100, 104, 148

lifetime date, 186

Lightweight Directory Access Protocol (LDAP), 115, 115

location, disaster recovery plan and, 204

locks, for physical access control, 126

log files, 145

from firewalls, 147

logging procedures, 145–147

logic bombs, 10

logical access control methods, 106–110

logical tokens, 109

logon

security for credentials, 119

time of day restrictions for, 108

logs, of physical access, 125–126

M

M of N control, 186

MAC addresses, resolving IP addresses to, 48

MAC (Mandatory Access Control) model, 102–103

MAC value, 168

macro virus, 4

MagicJack, 61

maintenance hook, 78

malicious code, 4

e-mail delivery of, 8

logic bombs as, 10

man-in-the-middle attacks, 41–42, 42
 802.1x authentication vulnerability to, 122
mandatory vacations, 213
mantrap, 127, 127
mathematical attacks, 91
memory cards, 14
 for cell phones, 12
Message Digest 5 (MD5), 169
Microsoft
 Virtual PC, 31
 Virtual Server 2005, 31
military implementation of MAC, 102
MIME header, corrupted, 8
mitigation, 135
modems, 114, 114–115
monitoring, 145
 methods, 143–144
 tools, 142–143
multi-factor authentication, 111
multihomed firewall, 69
multipartite virus, 4
mutual authentication, 122
mutual certificate exchange, 165

N

NAC (network access control), 58–59
NAS (network attached storage), 14
NAT (Network Address Translation), 55, 55–56
NAT Traversal (NAT-T), 56
need-to-know policies, 103, 212
net use command, 40
NetBIOS (Network Basic Input Output System), and null sessions, 40
NetScout Sniffer, 138
NetWitness, 72
network access control (NAC), 58–59
Network Address Translation (NAT), 55, 55–56
network attached storage, 14
network components, 50–62
network design, exam essentials, 61–62
network device vulnerabilities, 76–80
 back doors, 78–79, 79
 birthday attack, 78
 brute-force attack, 77
 default accounts, 79
 dictionary attack, 77–78
 privilege escalation, 76
 weak password, 77
Network General, 72
network hardening, 73–74
network interconnections, 56–58
network intrusion prevention system (NIPS), 59, 63, 68
network mappers, 140
Network News Transfer Protocol (NNTP), SSL for, 177
network security, 63–73
 exam essentials, 73
 firewalls, 68–70
 honeypot, 71, 71–72
 Internet content filter, 72
 intrusion detection systems (IDSs), 63, 63–68
 network intrusion prevention system (NIPS), 68
 protocol analyzers, 72
 proxy servers, 70
New Technology File System (NTFS), 18
NIDS (network IDS), 63, 64, 64

nmap, 138
 NNTP (Network News Transfer Protocol), SSL for, 177
 nonessential services on system, identifying, 16
 nonrepudiation, 162, 171
 NTFS (New Technology File System), 18
 NTLM (NT LAN Manager), 170
 null sessions, 40–41

O

OBEX protocol, 89–90
 objects, in MAC environment, 103
 OCSP (Online Certificate Status Protocol), 182, 187
 one-time pad, 173
 one-time passwords, 109
 one-way certificate exchange, 165
 Online Certificate Status Protocol (OCSP), 182, 187
 open ports, response from, 137
 Open Vulnerability and Assessment Language (OVAL), 138
 open wireless network, 89
 operating systems
 hardening, 15–21
 configuration baselines, 20
 defining, 17
 group policies, 19
 rootkits and, 8
 virtualization technology and, 31
 organizational policies, 210–216
 acceptable use policy, 211
 change management, 212
 due care policies, 213
 due diligence, 213

 due process, 213
 exam essentials, 215–216
 human resource policies, 214
 mandatory vacations, 213
 password complexity, 211–212
 Personally Identifiable Information (PII), 213
 SLA (service-level agreement), 214
 outbound filter, 72
 OVAL (Open Vulnerability and Assessment Language), 138

P

P2P (peer to peer), 27
 packet filter firewalls, 69
 packet sequencing, to prevent replay attacks, 42
 packet sniffing
 of FTP traffic, 39
 and instant messaging, 27
 padded cell, 72
 palm scans, 113
 passphrase, 87, 164
 Password Authentication Protocol (PAP), 121, 122
 password cracking, 108, 139
 password guessing attack, 108
 password policy, 107
 passwords
 complexity, 211–212
 for default accounts, 79
 history, 212
 and user names, 107–108, 108
 weak, 77
 PAT (Port Address Translation), 56

- patches, 18
 - management, 19
- PBX (private branch exchange), 60, 61
- PDAs, cell phones as, 12
- penetration testing, vs. vulnerability scanning, 141
- performance baseline, 142–143
- performance logging, 146
- performance monitor, 142
- periodic audits of system security, 147–149
- personal software firewalls, 29–30
- Personally Identifiable Information (PII), 213
- PGP/MIME, 171
- PGP (Pretty Good Privacy), 25, 171–172
- phage virus, 4
- phishing, 220
- physical environment, access control over, 11
- physical security, 124–128, 125
 - door access systems, 126–127
 - exam essentials, 128
 - ID badges, 126
 - locks, 126
 - logs/lists, 125–126
 - mantrap, 127, 127
 - physical token, 127
 - video surveillance, 128
- physical token, 127
- piggybacking, 127
- PII (Personally Identifiable Information), 213
- ping flood, 46
- ping of death, 46
- PKI (public key infrastructure), 158–159, 180, 181–182, 183
- Point-to-Point Protocol (PPP), 175
- Point-to-Point Tunneling Protocol (PPTP), 118, 175–176
- polymorphic viruses, 4
- POP3 (Post Office Protocol), 25
- popup blocker, 30
- Port Address Translation (PAT), 56
- ports
 - 25 for SMTP, 25
 - 110 for POP3, 25
 - 143 for IMAP, 25
 - 443 for SSL, 174
 - 443 for TLS, 174
- post-admission philosophy, for NAC, 59
- Post Office Protocol (POP3), 25
- PPP (Point-to-Point Protocol), 175
- PPTP (Point-to-Point Tunneling Protocol), 118, 175–176
- pre-admission philosophy, for NAC, 59
- precomputed hash, 139
- Pretty Good Privacy (PGP), 25, 171–172
- principle of least privilege, 100, 104, 148
- print resources, security controls for, 106
- privacy, 213
- private branch exchange (PBX), 60, 61
- private IP addresses, NAT to convert to public, 55
- private key, 183
 - impact of loss, 185
- private key cryptography, 158
- privilege abuse, 148
- privilege escalation, 3–4, 76, 148
- privilege management, 99. *See also* access control
 - groups for, 105–106
- privileges, 148
- Project Athena, 119
- protocol analyzers, 72, 138

protocols

- antiquated, 37–39
- for cryptography, 173–180
- exam essentials, 49–50
- limiting installs, 15
- for VPN, 118

proxy firewall, 69, 69

proxy servers, 70

public IP addresses, NAT to convert

- private to, 55

public key cryptography, 160, 180–191

- certificate authorities (CA), 183–184
- certificate revocation list (CRL), 186, 187–188
- exam essentials, 189–191
- key escrow, 185, 185–186
- private key, 183
- public key, 182
- registration, 184
- trust models, 188–189

public key infrastructure (PKI), 158–159, 180, 181–182, 183

R

RA (registration authority), 182

RADIUS (Remote Authentication Dial-In User Service), 113, 114

- for VPN clients, 119

RAID (Redundant Array of Independent Disks), 201, 201

RBAC (Role-Based Access Control) model, 104

RBAC (Rule-Based Access Control), 104

RC5 (Rivest Cipher 5), 159

realm, 119

reconstitution, 9

redundancy planning, 199–203, 205

- backup generator, 200
- cold site, 200
- hot site, 199
- RAID (Redundant Array of Independent Disks), 201, 201
- redundant ISP, 202
- redundant servers, 202
- single point of failure, 200
- spare parts, 201–202
- UPS (uninterruptible power supply), 202
- warm site, 200

redundant ISP, 202

redundant servers, 202

registration authority (RA), 182

registration, to obtain certificate, 184

remote access policies, 116, 116–117

Remote Access Server (RAS), 114, 114–115

remote authentication, 117

Remote Authentication Dial-In User Service (RADIUS), 113, 114

remote calling, 60

removable media, 13–14

renewal of key or certificate, 187

replay attacks, 42, 43

Requests for Comments (RFCs)

- 1918 on private IP addresses, 56
- 2661 on L2TP, 175

restoration after disaster, 206

retinal scans, 113

retroviruses, 4

reverse engineering, and hashing, 169

reverse hash matching, 77, 78, 169

revocation, of certificate, 186

risk assessment, 135–137, 204

- exam essentials, 136–137

risk, from users, 99
 Rivest Cipher 5 (RC5), 159
 Rivest-Shamir-Adleman (RSA), 160
 robot network, 9
 rogue access points, 90
 rogue DNS servers, 48
 Role-Based Access Control (RBAC)
 model, 104
 rootkits, 8–9
 rotating jobs, 100
 routers, 56, 57
 RSA (Rivest-Shamir-Adleman), 160
 RST packet, 137
 Rule-Based Access Control (RBAC), 104

S

S/FTP (Secure FTP), 38
 S-HTTP (secure HTTP), 176
 S/MIME (Secure Multipurpose Internet
 Mail Extensions), 25, 174–175
 schemes, in disaster recovery plan, 205–
 206
 scripts, 23
 secret key cryptography, 158
 secure disposal of computers, 211
 Secure FTP (S/FTP), 38
 secure HTTP (S-HTTP), 176
 Secure Multipurpose Internet Mail
 Extensions (S/MIME), 25, 174–175
 Secure Shell (SSH), 178
 Unix version, 179
 Secure Sockets Layer (SSL), 174, 177
 security. *See also* physical security
 for PBX systems, 60
 periodic audits, 147–149
 routers for, 57
 security applications
 implementing, 29–30
 procedures for, 145–146
 security association manager, 178
 security baseline, 20
 security breach, 207
 security domains, 102
 security templates, 20
 security threats, 3–11
 adware, 8
 botnets, 9, 44
 e-mails, 7–8
 exam essentials, 10–11
 hoaxes, 6–7
 logic bombs, 10
 privilege escalation, 3–4
 rootkits, 8–9
 spam, 5–6
 spyware, 5
 Trojan horse, 5
 viruses, 4
 worms, 4–5
 security zones, 51
 segmentation, routers for, 57
 sensitivity labels, 102, 103
 separation of duties, 100
 server cage, 217
 server vault, 217
 servers, 18
 clustering, 206, 206
 service-level agreement (SLA), 214
 service packs, 18
 services, limiting installs, 15
 SHA (Secure Hash Algorithm), 169
 shielded twisted pair (STP), 84, 84, 85
 specifications, 84–85
 shielding, 85
 of cables, 218

- shoulder surfing, 220
 - shredded documents, 220
 - signature-based monitoring, 144
 - signature detection, for IDS, 64, 65
 - signed applets, 22
 - Simple Mail Transfer Protocol (SMTP), 25
 - single factor authentication, 111
 - single loss expectancy (SLE), 136
 - single point of failure, 200
 - avoiding, 205
 - single-sided certificates, vs. dual sided, 165
 - single sign-on (SSO), 112
 - Kerberos as, 119
 - site surveys, 88
 - Skype, 61
 - SLA (service-level agreement), 214
 - SLE (single loss expectancy), 136
 - small home or SOHO networks, 50
 - smart cards, 14, 126
 - smartcard authentication process, 109, 109
 - SMTP (Simple Mail Transfer Protocol), 25
 - SMTP open relays, 25–26
 - smurf attack, 44, 45
 - sniffing attacks, switches as defense
 - against, 58
 - social engineering, 5, 218–221
 - protecting against, 219–220
 - software
 - for cryptography key storage, 157
 - firewalls, 29–30
 - vulnerability points, 15
 - spam, 5–6
 - spoofing and, 41
 - spam response policy, 7
 - spare parts, 201–202
 - spoofed e-mail, 6
 - spoofing attacks, 41
 - spyware, 5
 - SSH (Secure Shell), 178
 - Unix version, 179
 - SSID broadcast, 89
 - SSL (Secure Sockets Layer), 174, 177
 - FTP over, 38
 - stateful inspection firewalls, 69
 - stealth viruses, 4
 - steganography, 157–158
 - storage and retention policies, 148
 - STP (shielded twisted pair), 84, 84, 85
 - specifications, 84–85
 - stream cipher, 159
 - strong authentication, 111
 - subjects, in MAC environment, 103
 - subnet mask, 59–60
 - subnets, 51, 59–60
 - subordinate CAs, 188
 - Sun Microsystems, 22
 - suspension, of certificate, 187
 - switches, 57–58, 58
 - symmetric encryption, for digital
 - signatures, 163–164, 164
 - symmetric key, 158–159, 159
 - SYN flood attack, 45, 45
 - system logging, 146
 - system scanning, 145
 - systems monitor, 142
-
- T**
- T-connector (BNC), 82
 - T-Sight, 42
 - TACACS (Terminal Access Controller Access Control System), 122, 122
 - tape, 13
 - TCP (Transmission Control Protocol), DoS
 - attacks and, 43

TCP/IP hijacking, 39–40, 40
 telecom, 61
 telephony, 60–61
 Telnet
 SSH as alternative, 178
 SSL for, 177
 temperature control, 218
 TEMPEST project, 88
 Terminal Access Controller Access
 Control System (TACACS), 122, 122
 terminals, 18
 terminating coaxial cable, 83, 83
 termination policies, 214
 TGT (ticket granting ticket), 119
 theft identification, 136
 ThickNet, 81
 ThinNet, 81
 third party cookies, 25
 ticket granting ticket (TGT), 119
 time of day restrictions, for user
 logon, 108
 timestamps, to prevent replay attacks, 42
 TLS (Transport Layer Security), 174
 tokens, 109
 TPM (Trusted Platform Module), 165
 transfer, and risk assessment, 135
 Transmission Control Protocol (TCP), DoS
 attacks and, 43
 transmission media, 80–86
 Transport Layer Security (TLS), 174
 transport mode, for IPSec, 177, 178
 Triple-DES (3DES), 159
 Trojan horse, 5
 trust models, 188–189
 hierarchical, 188
 Trusted Platform Module (TPM), 165
 tunnel mode, for IPSec, 177, 177
 tunneling, 55

tunneling protocols, 118
 twisted pair cable, 83, 116
 two-factor authentication, 111, 111
 two-way certificate exchange, 165
 Twofish, 159

U

UDP (User Datagram Protocol), DoS
 attacks and, 43
 uninterruptible power supply (UPS), 202
 unshielded twisted pair (UTP), 84, 84
 specifications, 84–85
 USB drives, 12
 user access and rights review, 148
 user accounts, automatic expiration, 109
 User Datagram Protocol (UDP), DoS
 attacks and, 43
 user groups, 105–106
 user names, and passwords, 107–108, 108
 user privileges, 99
 users
 education, 214–215
 on social engineering attacks, 220–
 221
 risk from, 99
 time of day restrictions for logon, 108
 UTP (unshielded twisted pair), 84, 84
 specifications, 84–85

V

vacations, mandatory, 213
 valid to date, for key or certificate, 187
 vampire tap, 81, 82, 83, 86

vCard (virtual business card), 89
VeriSign, 184
video surveillance, 128
virtual local area networks (VLAN),
 53–55, 54
Virtual PC, 31
virtual private networks (VPNs), 117, 117,
 117–119, 118
 open port in firewall for, 70
virtualization technology, 31
viruses, 4
VLAN (virtual local area networks),
 53–55, 54
VMWare, 31
voice recognition, 113
VoIP (voice over IP), 31
VPN. *See* virtual private networks (VPNs)
vulnerabilities, 136
 assessment, 137–140
 password crackers, 139
 port scanners, 137–138
 protocol analyzers, 138
 vulnerability scanners, 138
vulnerability scanning, vs. penetration
 testing, 141

W

war dialing, 89, 115
war driving, 89
warm site, 200
weak encryption, 90–91
weak keys, 90–91
weak password, 77
web browser, 23–24

web servers, 176
 cookies from, 24–25
well-known accounts, 79
whole disk encryption, 164
Wi-Fi Protected Access (WPA), 87
Wired Equivalent Privacy (WEP), 87
wireless cells, 86
wireless networks
 exam essentials, 91–92
 SSID broadcast, 89
 vulnerabilities, 86–92
Wireshark, 72, 138
work factor, and algorithm strength, 163
workstations, 18
worms, 4–5
WPA (Wi-Fi Protected Access), 87

X

x.500 standard, 115
X.exe, 3
XMAS scan, 137
XSS (cross-site scripting), 27–28
XTACACS, 122

Z

Zimmerman, Phil, 171
zombies, and DoS attack, 43
zone file, false data in, 48
zone transfers requests, logging, 146

