State array, AES, 56
Stateful inspection firewalls, 418–419
Statistical anomaly detection, 382
  profile-based, 384
    counter, 385
    gauge, 385
    interval timer, 385
    mean and standard deviation, 385–386
    resource utilization, 385
  threshold analysis, 384
Stealth virus, 346
Stream ciphers, 63–67
  defined, 48
  design considerations, 64
  keystream, 64
  plaintext processing, cryptography, 48
  RC4 algorithm, 65–67
  structure of, 63–65
Stuxnet worm, 355, 359
Subject field, 144, 147
Subkey, Kerberos, 137
Substitution bytes, AES, 56
Symmetric encryption, 46–52
  block cipher, design of, 50
  block size, 50
  ciphertext, 47
  computationally secure, 49
  cryptanalysis, 48–50
  cryptography, 48
  decryption algorithm, 47
  encryption algorithm, 46
  Feistel cipher structure, 50–52
  key size, 51
  plaintext, 46, 48–49
  principles of, 46–52
  requirements of, 47
  round function, 50
  rounds, number of, 50
  secret key, 46
  subkey generation algorithm, 52

T

Tablets, 227
Target discovery
  hit list, 371
  random, 371
  scanning or fingerprinting, 371
  topological, 371
Third-generation scanner, 362
Threats. *See also* Attack(s)
  active attacks, 27
  denial-of-service (DoS) attack, 30
  masquerade, 27
  modification of information, 27
  network security, 124
  passive attack, 25–27
  release of contents, 25
  replay, 27
  service, 41
  traffic analysis, 26
Threshold random walk (TRW) scan detection, 366
Ticket-granting server (TGS), 126
Ticket-granting service exchange, 136–137
Ticket lifetime, 134–135
Time series model, 386
Times, Kerberos, 136
Timestamp authentication, 127, 137
Tiny fragment attacks, 417–418
Traffic analysis, 26
Traffic flow confidentiality (TFC), 316
Traffic processing, IP, 312–314
Traffic security, 230
Transport Layer Protocol, SSH, 209–213
Transport Layer Security (TLS), 65, 91, 165, 190–207
  alert protocol, 191
  cipher spec, 194–197
  cryptographic computations, 202–204
  handshake protocol, 197–202
  message authentication code (MAC), 211–212
  padding, 194
  pseudorandom function (PRF), 203–204
  record protocol, 192–194
Transport-level security, 187–219
  HTTPS, 188, 207–208
  Secure Shell (SSH), 188, 207–208
  Socket Layer (SSL), 190
  Transport Layer Security (TLS), 190–207
  Web considerations, 188–190
Transport mode, IP, 308–309, 317–320
Triple Data Encryption Standard (3DES), 54–55
Trojan horses, 354–355
Tunnel mode, IP, 308–309, 320–321

U

UNIX implementations, 399–400
Unknown risk profile, 178
User credential compromise, 39
User credential guessing, 39
User identity, 413
User terminal and user (UT/U), 38

V

Virtual local area networks (VLANs), 163
Virtual private network (VPN), 230, 425–426
Viruses
  concealment strategy
    encrypted virus, 346
    metamorphic virus, 346
    mutation engine, 346
    polymorphic virus, 346
    stealth virus, 346
  nature of
    dormant phase, 343
    execution phase, 343
    infection mechanism, 343
    payload, 343
    propagation phase, 343
    triggering phase, 343
    trigger, logic bomb, 343

structure
compression virus, 344, 345
simple virus, 344
traditional machine-executable virus code, 343
target, classification by
boot sector infector, 346
file infector, 346
macro virus, 346
multipartite virus, 346
Vulnerability, passwords
electronic monitoring, 397
exploiting
multiple password use, 397
user mistakes, 397
offline dictionary attack, 396
password guessing against single user, 397
popular password attack, 396–397
specific account attack, 396
workstation hijacking, 397

W

Web security, 184–185, 188–190. *See also* Internet security
Web sites, 188, 189
Wide area network (WAN), 411, 423
Wi-Fi hotspots, 224
Wi-Fi Protected Access (WPA), 231, 237
Wireless Ethernet Compatibility Alliance (WECA), 231
Wireless networking components, 224
Wireless network security, 222–250
IEEE 802.11i LAN, 236–250
IEEE 802.11 LAN, 230–236
Robust Security Network (RSN), 237
Wi-Fi Protected Access (WPA), 237
Wired Equivalent Privacy (WEP), 237
wireless security, 223–226
Wireless network threats, 224–225
accidental association, 224
ad hoc networks, 224
denial of service (DoS), 225
identity theft (MAC spoofing), 224
malicious association, 224
man-in-the middle attacks, 224
network injection, 225
nontraditional networks, 224
Wireless security, 223–226
accessibility, 223
access points, 225
channel, 223
measures, 225
mobility, 223
networks, 224–226
resources, 223
threats, network, 224–225
transmissions, 224–225
encryption, 225
signal-hiding techniques, 225
Workstation hijacking, 397
Worm propagation model, 349–350
Worm technology, state of
metamorphic, 351
multiexploit, 351
multiplatform, 351
polymorphic, 351
transport vehicles, 351
zero-day exploit, 351

X

X.509 certificate, 139–146
certificate revocation list (CRL), 144
certificates, 140–142
certification authority (CA), 147
forward certificate, 143
introduction to, 139
issuer attributes, 146
key information, 145–146
path constraints, 146
policy information, 145–146
reverse certificate, 143
revocation of certificates, 144
subject attributes, 145
user's certificate, obtaining, 142–144
version 3, 144–145
X.800 standard recommendations, 24, 25, 27, 29–32

THE WILLIAM STALLINGS BOOKS ON COMPUTER

DATA AND COMPUTER COMMUNICATIONS, TENTH EDITION

A comprehensive survey that has become the standard in the field, covering (1) data communications, including transmission, media, signal encoding, link control, and multiplexing; (2) communication networks, including wired and wireless WANs and LANs; (3) the TCP/IP protocol suite, including IPv6, TCP, MIME, and HTTP, as well as a detailed treatment of network security. **Received the 2007 Text and Academic Authors Association (TAA) award for the best Computer Science and Engineering Textbook of the year.**

WIRELESS COMMUNICATION NETWORKS AND SYSTEMS (WITH CORY BEARD)

A comprehensive, state-of-the art survey. Covers fundamental wireless communications topics, including antennas and propagation, signal encoding techniques, spread spectrum, and error correction techniques. Examines satellite, cellular, wireless local loop networks and wireless LANs, including Bluetooth and 802.11. Covers wireless mobile networks and applications.

COMPUTER SECURITY, THIRD EDITION (WITH LAWRIE BROWN)

A comprehensive treatment of computer security technology, including algorithms, protocols, and applications. Covers cryptography, authentication, access control, database security, cloud security, intrusion detection and prevention, malicious software, denial of service, firewalls, software security, physical security, human factors, auditing, legal and ethical aspects, and trusted systems. **Received the 2008 TAA award for the best Computer Science and Engineering Textbook of the year.**

OPERATING SYSTEMS, EIGHTH EDITION

A state-of-the art survey of operating system principles. Covers fundamental technology as well as contemporary design issues, such as threads, SMPs, multicore, real-time systems, multiprocessor scheduling, embedded OSs, distributed systems, clusters, security, and object-oriented design. **Third, fourth and sixth editions received the TAA award for the best Computer Science and Engineering Textbook of the year.**

AND DATA COMMUNICATIONS TECHNOLOGY

FOUNDATIONS OF MODERN NETWORKING: SDN, NFV, QOE, IOT, AND CLOUD

An in-depth up-to-date survey and tutorial on Software Defined Networking, Network Functions Virtualization, Quality of Experience, Internet of Things, and Cloud Computing and Networking. Examines standards, technologies, and deployment issues. Also treats security and career topics.

CRYPTOGRAPHY AND NETWORK SECURITY, SEVENTH EDITION

A tutorial and survey on network security technology. Each of the basic building blocks of network security, including conventional and public-key cryptography, authentication, and digital signatures, are covered. Provides a thorough mathematical background for such algorithms as AES and RSA. The book covers important network security tools and applications, including S/MIME, IP Security, Kerberos, SSL/TLS, network access control, and Wi-Fi security. In addition, methods for countering hackers and viruses are explored. **Second edition received the TAA award for the best Computer Science and Engineering Textbook of 1999.**

BUSINESS DATA COMMUNICATIONS, SEVENTH EDITION (WITH TOM CASE)

A comprehensive presentation of data communications and telecommunications from a business perspective. Covers voice, data, image, and video communications and applications technology and includes a number of case studies. Topics covered include data communications, TCP/IP, cloud computing, Internet protocols and applications, LANs and WANs, network security, and network management.

COMPUTER ORGANIZATION AND ARCHITECTURE, TENTH EDITION

A unified view of this broad field. Covers fundamentals such as CPU, control unit, microprogramming, instruction set, I/O, and memory. Also covers advanced topics such as multicore, superscalar, and parallel organization. **Five-time winner of the TAA award for the best Computer Science and Engineering Textbook of the year.**