

- somewhere a person is authentication factor, 718
- SONETs (Synchronous Optical Networks), 538–539
- source code analysis attacks
  - in cryptography, 370
- source code vulnerabilities, 1133–1134
- source files, protecting, 896
- source routing in firewalls, 966
- Soviet Union collapse, increase of attacks from, 134
- SOW (statements of work) in project management, 1081
- SOX (Sarbanes-Oxley Act), 20
- Spafford, Eugene H., 3
- spaghetti code, 1126
- Spanning Tree Protocol (STP), 657
- SPB (Shortest Path Bridging) protocol, 657
- spearphishing, 865
- Specht, Paul, 150
- special characters in passwords, 720
- Spectre attacks, 257, 372
- speed
  - biometric authentication, 726
  - TCP vs. UDP, 506
- SPF (Sender Policy Framework), 624
- spikes in electric power, 451
- Spiral methodology for software development, 1098–1099
- split knowledge, 34
- split tunnels in VPNs, 697
- splitting DNS, 530
- Splunk product, 979
- SPML (Service Provisioning Markup Language), 777–779
- spoofing
  - e-mail, 623
  - firewalls, 965
  - STRIDE model, 388
- spread spectrum wireless communications, 561–563
- sprinklers, 459–460
- sprints in Scrum methodology, 1102
- SRKs (storage root keys) in Trusted Platform Modules, 405
- SRS (Software Requirements Specification), 1083
- SS7 (Signaling System 7) protocol, 682
- SSD (static separation of duty) relations in RBAC, 773
- SSH (Secure Shell)
  - code repositories, 1144
  - communications channels, 701–702
- SSIDs (Service Set IDs), 565
- SSO (single sign-on)
  - identity management, 750–752
  - replay attacks, 372–373
- SSPs (signal switching points), 682
- staff, awareness programs for, 42
- stakeholders
  - enterprise architecture frameworks, 190
  - incident notifications, 1004
- standalone mode in WLANs, 565
- standard changes, 892
- Standard Generalized Markup Language (SGML), 776
- standard windows, 441
- standards
  - business continuity, 104–106
  - coding, 1135–1136
  - controls, 258
  - industry, 156–158
  - logs, 979
  - organizational, 29–31
  - WLANs, 565–574
- standby lighting, 912
- standby UPS systems, 453
- star integrity axiom in Biba model, 399
- star property rule in Bell-LaPadula, 398
- star topology, 488
- start bits, 646
- state actors, 60–61
- state tables
  - stateful firewalls, 949, 952
  - three-way-handshake process, 951
- stateful firewalls, 949–952
- stateful NAT, 533
- stateless inspection in packet-filtering firewalls, 948
- statements of work (SOW) in project management, 1081
- states
  - controls, 254–258
  - TCP connections, 951
- static analysis
  - antimalware software, 970
  - application security, 1139

- static application security
  - testing (SAST), 1139
- static electricity, 454
- static mapping in NAT, 532
- static routing protocols, 534–535
- static separation of duty (SSD) relations
  - in RBAC, 773
- statistical attacks in cryptography, 370
- statistical time-division multiplexing (STDM), 544
- steganography, 264–265
- stegomedium, 265
- Stevens, Ted, 469
- sticky notes in Kanban methodology, 1102–1103
- Stoll, Clifford, 643
- stop bits, 646
- storage, data, 232–233, 259–260
- storage facilities, 447–448
- storage keys in Trusted Platform Modules, 406
- storage root keys (SRKs) in Trusted Platform Modules, 405
- STP (shielded twisted pair) cable, 649
- STP (Spanning Tree Protocol), 657
- STPs (signal transfer points), 683
- strata in NTP, 831
- strategic alignment, 15–16
- stream ciphers in symmetric key cryptography, 333–334
- stream-symmetric ciphers, 575
- streaming protocols, 691
- strict liability category in civil law, 128
- STRIDE model, 387–388
- strong authentication, 718–719
- strong star property rule in Bell-LaPadula, 398
- structured walkthrough tests in disaster recovery plans, 1063
- subjects
  - ABAC, 774
  - data, 245
- subnet masks in IP addresses, 511–512
- subnets in IP addresses, 510–512
- substitution ciphers, 318
- sub-techniques in MITRE ATT&CK framework, 389
- succession planning, 1043
- Sullivan, Joseph, 20
- supernetting IP addresses, 512
- supervisor role, 24
- supervisory control and data acquisition (SCADA) systems, 290, 294
- supply chain risk management
  - attacks, 133
  - hardware, 98
  - minimum security requirements, 100
  - overview, 96–98
  - risk sources, 99–100
  - service level agreements, 101
  - services, 99
  - software, 99
  - upstream and downstream, 98
- supply system threats in site planning, 423
- support agreements, 672
- support staff, tasks and responsibilities, 886
- surges in electric power, 451
- surveillance
  - CPTED, 431–432
  - description, 913
  - digital forensics, 1019–1020
- suspending accounts, 860
- sustain stage in change management, 892
- Sutter Health of California breach, 255
- SVCs (switched virtual circuits), 549
- SWGDE (Scientific Working Group on Digital Evidence), 1009
- swipe cards for ownership-based authentication, 732–733
- switch controls in device locks, 921
- switch spoofing attacks, 632
- switched virtual circuits (SVCs), 549
- switches
  - characteristics, 665
  - layer 3 and 4, 659
  - overview, 657–658
  - VLANs, 630
- switching WANs, 545–547
- symbolic AI approach, 976–978
- symbolic links, 819, 821
- symmetric key cryptography
  - with asymmetric, 346–349
  - block ciphers, 330–333
  - description, 328
  - initialization vectors, 334–335
  - overview, 329–330
  - stream ciphers, 333–334
  - summary, 330

- symmetric services in DSL, 684
- SYN/ACK packets, 508
- SYN floods, 508
- SYN packets, 508, 949–951
- SYN-RECEIVED state in TCP connections, 951
- SYN-SENT state in TCP connections, 951
- synchronization
  - NTP, 830
  - passwords, 737
- Synchronous Optical Networks (SONETs), 538–539
- synchronous replication, 1039
- synchronous token devices for one-time passwords, 730–731
- synchronous transmission, 645–647
- synthetic transactions, 832
- system access control, 802
- system account access review, 798
- system administrators, tasks and responsibilities, 886
- system architectures
  - chapter questions, 311–315
  - chapter review, 310–311
  - client-based, 284
  - cloud-based, 301–305
  - database, 285–286
  - distributed, 307–309
  - high-performance computing, 288–289
  - industrial control systems, 289–296
  - overview, 283
  - pervasive, 305–307
  - server-based, 284–285
  - virtualized systems, 296–301
- system authentication, 579
- system images, 896
- system-level event audits, 742
- system owners, 23–24
- system resilience in availability, 1051
- system sensing access control readers, 925
- system-specific controls in Risk Management Framework, 175
- system-specific policies, 29
- system testing, 818

## T

- T-carriers for WANs, 541–542
- tables
  - forwarding, 656–657
  - rainbow, 721–722

- stateful firewalls, 949, 952
- three-way-handshake process, 951
- tabletop exercises (TTXs) in disaster recovery plans, 1063–1064
- TACACS (Terminal Access Controller Access Control System), 790–793
- TACS (Total Access Communication System), 584
- tactics in MITRE ATT&CK framework, 389
- tailoring controls, 258
- tamper-resistant property in reference monitors, 766
- tampering category in STRIDE model, 388
- tape vaulting for backups, 1039
- tapes for backups, 860
- Target company breach, 96–97
- target hardening vs. CPTED, 428
- targeted penetration tests, 826–827
- targets of attacks, 474
- tar pits, 976
- taxonomies in data retention, 236
- TCG (Trusted Computing Group), 404
- TCP. *See* Transmission Control Protocol (TCP)
- TCP/IP (Transmission Control Protocol/Internet Protocol) suite, 471, 502–503
- TDF (transborder data flow), 146–147
- TDM (time-division multiplexing), 541–542
- TDMA (time division multiple access)
  - GTS, 570
  - mobile communications, 584
- teams
  - backup administrators, 1035
  - business continuity planning, 1030
  - disaster recovery plans, 1056
  - incident response, 991, 1000–1001
  - risk analysis, 76, 78
  - risk assessment, 66–67
  - risk management, 56–57
  - software development, 1080
- technical controls
  - assessments. *See* testing
  - risk responses, 83, 86–87
- technical reports, 872–873
- technical sensors in incident detection, 995
- technological communication protocols, 646
- TEEs (trusted execution environments), 408–411
- telephone calls in PBXs, 665–667

- Telephone Records and Privacy Protection Act, 865
- telephones in disaster recovery plans, 1062
- telepresence in meeting applications, 695
- temperature
  - data processing facilities, 446
  - HVAC systems, 453–454
- tempered windows, 441
- templates for disaster recovery plans, 1059
- Temporal Key Integrity Protocol (TKIP), 577–578
- Teredo tunneling, 514
- Terminal Access Controller Access Control System (TACACS), 790–793
- terminals in H.323, 689
- termination processes in personnel security, 37–38
- territorial reinforcement in CPTED, 431–432
- tertiary sites in disaster recovery, 1046
- Tesla, Nikola, 559
- test coverage, 837
- test-driven development
  - Extreme Programming, 1102
  - software development, 1089
- testing
  - application security, 1139–1140
  - backups, 863
  - code reviews, 833–834
  - code testing, 834–835
  - compliance checks, 838
  - data loss prevention, 270–271
  - disaster recovery goals, 1054
  - disaster recovery plans, 1061–1065
  - federated identity, 755
  - interface, 837
  - log reviews, 828–831
  - misuse cases, 835–836
  - overview, 817
  - penetration, 822–827
  - red teaming, 827–828
  - SDLC, 1080, 1089–1091
  - Spiral methodology, 1098
  - strategies, 813–816
  - synthetic transactions, 832
  - test coverage, 837
  - vulnerabilities, 817–822
- testing mode in anomaly-based IDS/IPS, 967
- text messages in disaster recovery plans, 1056
- TGSs (ticket granting services) in KDC, 785–786
- Thailand, Personal Data Protection Act in, 144
- The Onion Router (TOR), 307
- The Open Group Architecture Framework (TOGAF), 172, 194–195
- The Silk Road, 665
- thermal relocking function in safes, 222
- third-generation (3G) mobile wireless, 585–586
- Third Generation Partnership Project (3GPP), 586
- third-generation programming languages, 1118–1119
- third parties
  - audits, 843–844
  - business continuity planning, 1068
  - connectivity, 705–706
  - dealing with, 39
  - security provided by, 973–974
  - software escrow, 1143
  - software security, 1147
- third-party sensors in incident detection, 995
- third-party services, federated identity with, 754–756
- threat data sources for security operations
  - centers, 942–943
- Threat Dragon, 1087
- threat hunters, tasks and responsibilities, 886
- threat hunting in security operations
  - centers, 943
- threat intelligence analysts on incident response teams, 1001
- threat intelligence in security operations
  - centers, 941–942
- threat modeling
  - attack trees, 386–387
  - Cyber Kill Chain, 387–389
  - importance, 389–390
  - MITRE ATT&CK framework, 389
  - network security, 598
  - overview, 385
  - site and facility security, 418–419
  - software development design, 1086
  - STRIDE, 387–388
  - third-party connectivity, 705
- threat trees in software development
  - design, 1086
- threat working group (TWG), 92

- ul style="list-style-type: none;">
- threats
  - cybercriminals, 60
  - defined, 8
  - duress, 931–932
  - hacktivists, 61
  - identifying, 62–63
  - internal actors, 61–62
  - nation-state actors, 60–61
  - nature, 62
  - overview, 58
  - site planning, 423
- three-factor authentication, 719
- three-way-handshake process
  - SIP, 689
  - TCP, 949–951
- throughput in cabling, 654–655
- thunking, 296
- ticket granting services (TGSs) in KDC, 785–786
- tickets in KDC, 785–788
- Tier 1 (organization view) in risk management, 55
- Tier 2 (mission/business process view) in risk management, 55
- tiers
  - Cybersecurity Framework, 182
  - risk management, 55
- tight coupling software, 1131–1132
- time division multiple access (TDMA)
  - GTS, 570
  - mobile communications, 584
- time-division multiplexing (TDM), 541–542
- time-limited trials for third-party software, 1147
- time-of-check to time-of-use (TOC/TOU)
  - in atomic execution, 410
- time to first byte (TTFB) in latency, 654
- Time to Live (TTL) values in packets, 512
- TIME-WAIT state in TCP connections, 951
- timely characteristic in threat intelligence, 941
- timeouts in session termination, 741
- timing attacks in cryptography, 371–372
- timing smart cards, 735
- TKIP (Temporal Key Integrity Protocol), 577–578
- TLS. *See* Transport Layer Security (TLS)
- TOC/TOU (time-of-check to time-of-use)
  - in atomic execution, 410
- TOGAF (The Open Group Architecture Framework), 172, 194–195
- token passing, 491–492
- Token Ring, 495–496, 499
- tokens
  - electronic access control, 925
  - one-time passwords, 730
- toll fraud
  - IP telephony, 692
  - PBX systems, 666
- tool sets for secure software, 1138
- top-down approach in security programs, 199
- top-level domains in DNS, 527
- top secret classification level, 216–218
- topologies for local area networks, 487–490
- Tor network, 665
- TOR (The Onion Router), 307
- tort law system, 127–129
- Total Access Communication System (TACS), 584
- total risk vs. residual risk, 81
- TPC (Transmit Power Control), 574
- TPMs (Trusted Platform Modules), 404–406
- TPs (transformation procedures)
  - in Clark-Wilson model, 400
- Traceroute tool, 520–522
- tracking
  - digital asset management, 261–262
  - hardware, 224
  - software, 224–227
- trade secrets, 148–149
- trademarks, 150
- traffic direction in packet-filtering firewalls, 948
- traffic-flow security, 601
- traffic shaping in QoS, 551
- trailer hot sites, 1049
- training, 40
  - artificial intelligence tools, 977–978
  - content reviews, 43
  - degrees and certifications, 40–41
  - disaster recovery communications, 1057
  - disaster recovery plans, 1060–1061, 1064–1065
  - evaluating, 43–44
  - incident response, 993
  - measuring security, 863–867
  - methods and techniques, 41–43
  - personnel, 930–931

- training mode in anomaly-based IDS/IPS, 967
  - transactions, synthetic, 832
  - transborder data flow (TDF), 146–147
  - transfer risk strategy
    - ISO/IEC 27005, 178
    - overview, 79
  - transfers in personnel security, 37–38
  - transformation procedures (TPs)
    - in Clark-Wilson model, 400
  - Transmission Control Protocol (TCP)
    - connection-oriented protocol, 479
    - data structures, 509
    - handshakes, 508, 949–951
    - transport layer, 479, 503
    - vs. UDP, 503–506
  - Transmission Control Protocol/Internet Protocol (TCP/IP) suite, 471, 502–503
  - transmission media
    - cabling, 648–655
    - overview, 643–644
    - types, 644–648
  - transmission methods for local area networks, 499–500
  - Transmit Power Control (TPC), 574
  - transparent bridging, 656–657
  - transponders, 925
  - transport adjacency in IPSec, 609
  - transport layer
    - functions and protocols, 484
    - OSI model, 479–480
  - Transport Layer Security (TLS)
    - data in motion, 255–256
    - malware using, 604–605
    - network security, 602–605
    - suites, 603–604
    - types, 610–611
  - transport supplies in forensics field kits, 1015
  - transposition ciphers, 318
  - travel safety, 930
  - tree topology, 488
  - trials for third-party software, 1147
  - trialware, 153
  - TrickBot Trojan, 604, 969
  - Trojans in TLS, 604
  - trust but verify principle
    - network security, 599
    - secure architectures, 392
    - site and facility security, 420
    - third-party connectivity, 706
    - web services, 612
  - Trust Centers for mobile communications, 572
  - trust in federated identity, 755
  - Trusted Computing Group (TCG), 404
  - trusted execution environments (TEEs), 408–411
  - Trusted Platform Modules (TPMs), 404–406
  - TTFB (time to first byte) in latency, 654
  - TTL (Time to Live) values in packets, 512
  - TTXs (tabletop exercises) in disaster recovery plans, 1063–1064
  - tumbler locks, 918
  - tuning data loss prevention, 270–271
  - tunnels
    - DNS, 619
    - ICMP, 520
    - IPv6, 514–515
    - TLS, 610
  - turnstiles, 441
  - Tuzman, Kaleil Isaza, 20
  - TWG (threat working group), 92
  - twisted-pair cabling, 649–650
  - two-factor authentication (2FA), 719
  - type 1 hypervisors in virtual machines, 297
  - type 2 hypervisors in virtual machines, 297
  - Type I errors in biometric authentication, 724–725
  - Type II errors in biometric authentication, 724–725
  - types in incidents classification, 1002
- ## U
- U.S. Patent and Trademark Office (USPTO), 150
  - UAC (User Agent Client) in SIP, 689
  - UAS (User Agent Server) in SIP, 689
  - ubiquitous computing, 305
  - UBR (unspecified bit rate) in ATM, 551
  - UC (unified communications), 695–696
  - UCDs (use case diagrams) in software development, 1083
  - UDIs (unconstrained data items) in Clark-Wilson model, 400
  - UDP. *See* User Datagram Protocol (UDP)
  - UEBA (user and entity behavior analytics), 981

- UEM (unified endpoint management) systems, 226
  - UML (Unified Modeling Language)
    - software development, 1083
    - use case diagrams, 835–836
  - uncertainty in risk assessment, 74
  - unclassified classification level, 216–218
  - unconstrained data items (UDIs)
    - in Clark-Wilson model, 400
  - undercover investigations in digital forensics, 1020
  - understanding factor in outsourced security services, 974
  - unicast transmission method, 499
  - unified communications (UC), 695–696
  - unified endpoint management (UEM) systems, 226
  - Unified Modeling Language (UML)
    - software development, 1083
    - use case diagrams, 835–836
  - uniform resource identifiers (URIs) for web services, 613–614
  - uniform resource locators (URLs) in DNS, 524, 531
  - uninterruptible power supplies (UPSs)
    - data processing facilities, 446
    - online, 452–453
    - standby, 453
  - unit testing in software development, 1089, 1091
  - United States laws for data breaches, 141–142
  - unmanaged patching, 904–905
  - unshielded twisted pair (UTP) cable, 649–650
  - unspecified bit rate (UBR) in ATM, 551
  - updates
    - Internet of Things, 307
    - profiles, 740
  - UPS Brown color, 150
  - UPSs (uninterruptible power supplies)
    - data processing facilities, 446
    - online, 452–453
    - standby, 453
  - upstream suppliers in risk management, 98
  - uptime in high availability, 1050
  - urgency in incidents classification, 1002
  - URIs (uniform resource identifiers) for web services, 613–614
  - URLs (uniform resource locators) in DNS, 524, 531
  - usage in TCP vs. UDP, 506
  - use case diagrams (UCDs) in software development, 1083
  - use cases
    - data loss prevention, 271
    - misuse case testing, 835–836
  - Use Limitation Principle in OECD, 142
  - user access review for identity and access, 797
  - user-activated readers, 925
  - User Agent Client (UAC) in SIP, 689
  - User Agent Server (UAS) in SIP, 689
  - user and entity behavior analytics (UEBA), 981
  - user data file backups, 861
  - User Datagram Protocol (UDP)
    - connectionless protocol, 479
    - connections, 951–952
    - vs. TCP, 503–506
    - transport layer, 479
  - user-level event audits, 743
  - user managers, 24
  - user stories in Agile methodologies, 1101
  - users
    - Clark-Wilson model, 400
    - description, 25
    - provisioning, 739
  - USPTO (U.S. Patent and Trademark Office), 150
  - utilities
    - electric power, 448–453
    - HVAC, 453–454
    - water and wastewater, 448–450
  - utility tunnels in physical security, 439
  - UTP (unshielded twisted pair) cable, 649–650
- ## V
- vacations, mandatory, 35, 890
  - Valasek, Chris, 627
  - validation
    - assessments, 815–816
    - parameters, 1132
    - risk controls, 90
    - software development, 1090
  - Validation practice in Good Practice Guidelines, 106
  - valuation of assets, 65–66
  - variable bit rate (VBR) in ATM, 551
  - vaulting for backups, 1038–1039
  - vaults, protecting, 222



- VBR (variable bit rate) in ATM, 551
- VDI (virtual desktop infrastructure), 700–701
- VDSL (very high-data-rate DSL), 684
- vendors, 39
- ventilation ducts in physical security, 439
- Veracode report, 1133
- verifiable property for reference monitors, 766
- verification
  - backups, 860–862
  - message integrity, 354–358
  - risk controls, 90
  - software development, 1090
  - supply chain risk management, 100
- verification 1:1, 718
- Verification function in SAMM, 1109
- Vernam, Gilbert, 325
- Vernam cipher, 325–328
- versatile memory in Trusted Platform Modules, 406
- versioning software, 1142–1144
- vertical enactment for privacy, 147
- very high-data-rate DSL (VDSL), 684
- very high-level programming languages, 1119–1120
- very small aperture terminals (VSATs), 589–590
- vibration detectors, 927
- VIDs (VLAN identifiers), 631
- views in enterprise architecture frameworks, 190, 192
- Vigenère, Blaise de, 319
- Vigenère cipher, 319
- violence, threats of, 931–932
- virtual circuits in WANs, 548–549
- virtual desktop infrastructure (VDI), 700–701
- virtual directories, 750
- Virtual eXtensible Local Area Networks (VxLANs), 632
- virtual firewalls, 964
- virtual local area networks (VLANs)
  - latency, 654
  - overview, 630–632
- virtual machines (VMs), 296, 704–705
  - antimalware, 969–970
  - benefits, 297–298
  - hypervisors, 297
  - third-party connectivity, 705
- Virtual Network Computing (VNC), 700
- virtual NICs (vNICs), 704–705
- virtual passwords, 723
- virtual private clouds (VPCs), 301
- virtual private networks (VPNs)
  - authentication protocols, 697–699
  - data in motion, 256
  - IPSec, 607–609
  - L2TP, 606–607
  - overview, 605, 697
  - PPTP, 606
  - TLS, 610
- Virtual Router Redundancy Protocol (VRRP), 536
- virtual teams in incident response, 991
- virtual tunnel end points (VTEPs), 632
- virtualization
  - backups, 861
  - desktop, 699–701
- virtualized systems
  - containerization, 298–299
  - networks, 704–705
  - overview, 296
  - serverless, 299–301
  - virtual machines, 296–298
- visual recording devices, 913–916
- VLAN identifiers (VIDs), 631
- VLANs (virtual local area networks)
  - latency, 654
  - overview, 630–632
- VMs. *See* virtual machines (VMs)
- VNC (Virtual Network Computing), 700
- vNICs (virtual NICs), 704–705
- voice communications, 682
  - cable modems, 686–687
  - DSL, 683–685
  - IP telephony, 687–692
  - ISDN, 685–686
  - PSTN, 682–683
- voice gateways, 688
- voice over IP (VoIP) networks
  - business continuity planning, 1069
  - vs. IP telephony, 688
  - overview, 687–688
  - security, 693
- voice prints, 728
- voicemail systems, 688
- voices in information access control, 801



- voltage in electrical power, 670
- voltage regulators for electric power, 451
- volumetric IDSs, 926
- VPCs (virtual private clouds), 301
- VPNs. *See* virtual private networks (VPNs)
- VRRP (Virtual Router Redundancy Protocol), 536
- VSATs (very small aperture terminals), 589–590
- VTEPs (virtual tunnel end points), 632
- vulnerabilities
  - defined, 8
  - emergency situations, 869
  - exception handling, 871
  - human, 902–903
  - identifying, 62–63
  - information, 59
  - managing, 900–903
  - overview, 58
  - people, 60
  - processes, 59–60, 902
  - remediation, 871
  - software, 901, 1133–1134
  - testing, 817–822
- vulnerability mapping step in penetration testing, 824
- vulnerability testing vs. penetration tests, 827
- VxLANs (Virtual eXtensible Local Area Networks), 632

## W

- wafer tumbler locks, 919
- waiting room feature for meeting applications, 694
- walkthrough tests in disaster recovery plans, 1063
- walls
  - considerations, 437
  - data processing facilities, 446
- WANs. *See* wide area networks (WANs)
- WAPs (wireless access points), 564–565
- warded locks, 918
- warez sites, 149–150
- warm sites, 1045–1047
- Wassenaar Arrangement, 145–146
- water and wastewater, 448–450
- water detectors, 445
- water lines, 438
- water sprinklers, 459–460
- Waterfall software development, 1095–1096
- watts
  - electrical power, 670–672
  - radio signals, 560
- wave-division multiplexing (WDM), 544
- wave-pattern motion detectors, 927
- WBSs (work breakdown structures) in project management, 1081
- WDM (wave-division multiplexing), 544
- weaponization in Cyber Kill Chain model, 387, 994
- web application security risks, 1134
- web of trust, 367
- web portal functions in FIM systems, 753–754
- web proxies, 665
- web services
  - HTTP, 613–614
  - overview, 611–612
  - REST, 615–616
  - SOAP, 614–615
- Web Services Security (WS-Security or WSS) specification, 615
- well-formed transactions in Clark-Wilson model, 400
- well-known ports, 507
- WEP (Wired Equivalent Privacy), 575–576
- wet chemical fire extinguishers, 459
- wet pipe water sprinkler systems, 460
- whaling, 865
- White, Joe, 20
- white box testing, 826
- whitelisting
  - applications, 225
  - intrusion detection and prevention systems, 968–969
- whole-disk encryption, 255
- Wi-Fi Protected Access 2 (WPA2), 576–578
- wide-angle lenses in CCTV systems, 915
- wide area networks (WANs)
  - ATM, 550–552
  - CSU/DSU, 543–545
  - dedicated links, 541–543
  - frame relay, 547–548
  - HSSI, 552
  - overview, 540
  - switching, 545–547
  - virtual circuits, 548–549
  - X.25, 549–550

- WIDSs (wireless intrusion detection systems), 967
  - WiMAX standard, 569, 587
  - windows
    - considerations, 437
    - types, 441
  - WIPO (World Intellectual Property Organization), 150
  - Wired Equivalent Privacy (WEP), 575–576
  - wired windows, 441
  - wireless access points (WAPs), 564–565
  - wireless intrusion detection systems (WIDSs), 967
  - wireless LANs (WLANs)
    - best practices, 582
    - components, 564–565
    - security, 575–582
    - standards, 565–574
  - wireless networking
    - chapter questions, 592–595
    - chapter review, 590–592
    - communication techniques overview, 559–561
    - mobile communications, 582–588
    - OFDM, 563–564
    - overview, 559
    - satellites, 589–590
    - spread spectrum, 561–563
    - WLAN components, 564–565
    - WLAN security, 575–582
    - WLAN standards, 565–574
  - wireless personal area networks (WPANs), 570
  - wiring closets, 446
  - WLANs. *See* wireless LANs (WLANs)
  - Woods, John F., 1079
  - work area security, 441–443
  - work area separation, 803
  - work breakdown structures (WBSs)
    - in project management, 1081
  - work factor
    - cryptosystems, 325
    - electrical power, 671
  - work factor in RSA, 342
  - work recovery time (WRT) in disaster recovery, 1031–1032
  - working images for evidence, 1012
  - World Intellectual Property Organization (WIPO), 150
  - World Wide Web (WWW), 777
  - WPA Enterprise, 577
  - WPA2 (Wi-Fi Protected Access 2), 576–578
  - WPA3, 578–579
  - WPANs (wireless personal area networks), 570
  - write-once media for logs, 745, 831
  - wrongs against a person category
    - in civil law, 127
  - wrongs against property category
    - in civil law, 127
  - WRT (work recovery time) in disaster recovery, 1031–1032
  - WS-Security specification, 615
  - WSS (Web Services Security) specification, 615
  - WWW (World Wide Web), 777
- ## X
- X.25 protocol, 549–550, 552
  - X.509 certificates, 359
  - XaaS (Everything as a Service), 304–305
  - XACML (Extensible Access Control Markup Language), 781
  - XDR (extended detection and response)
    - platforms, 968
  - XML (Extensible Markup Language), 615, 777
  - XOR operation
    - one-time pads, 326–327
    - stream ciphers, 333
  - XTACACS (Extended TACACS), 790–791
  - YAML Ain't Markup Language (YAML), 615
- ## Y
- Ying, Jun, 20
- ## Z
- Zachman, John, 172, 192
  - Zachman Framework, 172, 192–194
  - zero-day attacks, 971
  - zero knowledge in penetration testing, 825
  - zero trust principle
    - network security, 599
    - secure design, 392
    - site and facility security, 419–420
    - third-party connectivity, 706
    - web services, 612
  - ZigBee standard, 571–572
  - Zimmermann, Phil, 367
  - zombies, 965

zone transfers in DNS, 525

zones

access control, 803

CPTED, 429–430

DNS, 525

lighting, 911

Zoom-bombing, 694

zoom in CCTV systems, 914–915