

# INDEX

- Adaptable security program management
  - continuous audit cycles, 39
  - continuous improvements, 37
  - risk treatment, 37, 38
- Advanced Encryption Standard (AES), 98
- Apple's iPhone, 61
- Application programming interfaces (APIs), 80
- Artificial intelligence (AI), 15, 69
- Attestation, 195
- Augmented intelligence (AI), 69
- Authenticated encryption with associated data (AEAD), 98
- Authentication/
  - authorization
  - decentralized identity, 133, 139–140
  - identity proofing, 133–134
  - individual credential, 143–144
  - multifactor authentication, 137–139
  - OpenID, 132
  - PAKE, 134–135
  - passwords, 132, 134–135
  - public key pairs, 135–137
  - single credential, 141–143
  - single (reduced) sign-on (SSO), 140–141
  - WebAuthn, 132
- Automated Certificate Management Environment (ACME), 2, 110–113
- Automated system posture assessment
  - Common Information Model (CIM), 168
  - Network Endpoint Assessment (NEA), 166
  - NIST's SCAPv2.0, 166–167, 169

- Software Inventory
  - Message and Attributes (SWIMA), 168
  - standardized protocol, 166
  - system integrity verification, 167
  - Tripwire integrity assessment, 168
- Autonomous system
  - numbers (ASNs), 115
- Biometrics, 138
- Bit Index Explicit Replication (BIER), 116, 118
- Board-level program
  - evaluation/guidance adaptable security program management, 37–39
  - control automation, 46–51
  - data-centric security models, 21
  - governance and risk management, 24–28
  - multiparty compute (MPC), 23
  - outsource applications, 21
  - partner and supply chain vendors, 20
  - posture assessment, 21
  - secure and hardened operating systems, 21
  - security control framework selection, 28–36
  - security program evaluation, 23–24
  - supplements to frameworks, 39–46
  - trends, 19
  - two-factor secure single sign-on technology, 22
- Border Gateway Protocol (BGP), 175
- Center for Internet Security (CIS), 39
- Centralized services, 177
- Chromebooks, 61
- CloudFlare, 92
- Code signing, 63
- Common Information Model (CIM), 168
- Confidentiality, integrity, and availability (CIA), 16
- Containers, end point, 154–156
- Continuous audit cycles, 27, 39
- Control automation
  - Distributed Management Task Force (DMTF), 49
  - management information base (MIB), 48
- Simple Network Management

- Protocol (SNMP), 48
- Tripwire, 50
- Web-Based Enterprise Management (WBEM), 49
- zero trust model, 46
- Crypto Forum Research Group (CFRG), 135
- Cryptographic algorithms, 98–99
- Data-centric security
  - models, 11–12, 55, 75–76
  - data leakage patterns, 57
  - fine-grained controls, 57–58
- Data management, 78
- Data protection, 76–83
- Decentralized identity, 133, 139–140
- Defense-in-depth, 12
- DELL Unified Workspace, 55
- Demilitarized zone (DMZ) model, 184
- Deployment, encryption, 128
- Destination Options (DO), 121–122
- Distributed Denial of Service (DDoS), 175–176
- Distributed Management Task Force (DMTF), 49
- Domain Name Service (DNS), 87–88
  - DNS over HTTPS (DOH), 90–93
  - DNS over TLS (DOT), 89–90
  - filtering, 116–117
- Domain Name System Security Extensions (DNSSEC), 86–87
- Ecosystem, 196
- Encryption, 99–100
  - application and deployment, 74
  - data-centric security, 75–76
  - data protection, 76–83
  - edge termination to data center, 6
  - end-to-end encryption protocol, 5
  - meta-data, 4
  - pervasive monitoring, 83–85
  - session signaling information, 4
  - shift to ubiquitous, 74
  - transport layer protocols, 5
  - user control data, 76–83
- End point
  - apps, 154–156
  - automated system posture assessment. *See* Automated system posture assessment

- containers, 154–156
  - definition, 145
  - managing security, 169–172
  - micro-services, 154–156
  - organizations, 147–148, 163–165
  - secure operating systems. *See* Secure operating systems
  - supply chain attestation. *See* Supply chain attestation
- End-to-end encryption
  - protocol, 5, 54, 94–95
  - application, 96–97
  - transport encryption, 102
- Entity Attestation Tokens (EAT), 161
- European Union with the
  - General Data Protection Regulation (EUGDPR), 44
- Exceptional access, 14
- Extended Validation (EV), 3
- Federal Information Security Management Act of 2002 (FISMA), 32
- Firewalls, 184–187
- Flow Identifier, 120
- Generic Network Virtualization
  - Encapsulation (GENEVE), 115–116
- Google’s BeyondCorp model, 16
- Governance, Risk, and Compliance (GRC), 45
- Homomorphic encryption, 99, 100
- Hop-by-hop extension header, 122
- Identity proofing, 133–134
- Incident detection/prevention
  - attestation, 192–193
  - behavioral analysis, 193
  - data encryption, 193
  - Distributed Denial of Service (DDoS), 175–176
  - firewalls, 184–187
  - hardware-based attacks, 189–190
  - intrusion detection, 184–187
  - patterns, 177
  - posture assessment, 192
  - responses, 182–184
  - sharing groups, 193
  - social engineering, 188–189
  - supply chain, 189–190
  - trust models. *See* Trust models
- Indicators of Behavior (IoB), 182

- Individual credential, 143–144
- Inevitable shift, market demands, 67–69
- Information security
  - professional deficit, 15–17
- Interception, 85
- Interconnected trends, 1
  - data-centric security models, 11–12
  - deployment of
    - encryption, 2–4
    - information security professional deficit, 15–17
    - strong encryption, 4–7
  - transport protocol stack evolution, 7–11
  - user control of data, 13–15
- Internet Assigned Numbers Authority (IANA), 98
- Internet Engineering Task Force (IETF), 2
- Internet Key Exchange Protocol v 2, 124
- Internet Protocol Security (IPSEC), 124–125
  - definition, 124
  - encryption management, 125
- Internet Protocol Version 6 (IPv6)
  - definition, 119–120
  - Destination Options (DO), 121–122
  - factors, 120
- Flow Identifier, 120
- Metadata, 121
- network address
  - translation (NAT), 121
- privacy techniques, 122–124
- protocol stack evolution, 127–129
- routing overlay protocols, 121
- Internet Research Task Force (IRTF), 123, 135
- Internet Society, 120
- Intrinsically secure systems, 177
- Intrusion detection, 184–187
- JSON Object Signing and Encryption (JOSE), 162
- Key Management
  - Interoperability Protocol (KMIP), 110–113
- Lawful interception, 14, 81
- Lightweight Directory Access Protocol (LDAP), 141
- Machine learning (ML), 15, 69
- Mail delivery agent (MDA), 117

- Mail transport agents (MTAs), 117
- Management information base (MIB), 48
- Manufacturer Usage Description (MUD), 59
- MAP research group (MAPRG), 123
- Metadata, 121
- Micro-services, 154–156
- Mobile Device Management (MDM), 55
- Mobility, 13, 80
- Mozilla, 92
- Multi-cloud data, 102
- Multifactor authentication, 137–139
- Multiparty computation (MPC), 23, 77
- Multiprotocol label switching (MPLS), 116
- Network address translation (NAT), 120–121, 121
- Network End point Assessment (NEA), 94, 161, 166
- Network monitoring, 126
- Network Service Headers (NSH), 118
- NIST’s SCAPv2.0, 166–167, 169
- One-time passwords (OTP), 138
- Online certificate status protocol (OCSP), 136
- OpenID, 132, 144
- Open Virtual Network (OVN), 118
- OpenvSwitch (OVS), 118
- Open Web Application Security Project (OWASP), 40
- Opportunistic security, 2, 3
- Organizing Transparent Governance, 38
- Outsourcing, 70–71
- Packet header metadata, 74
- PAKE, 134–135
- Passwords, 132, 134–135
- Path Layer UDP Substrates (PLUS), 10
- Patterns that scale, 58
  - Apple’s iPhone, 61
  - architectural patterns, 65
  - authorized applications, 62
  - automated updates and mitigation controls, 60
- Chromebooks, 61
- code signing, 63
- incident response
  - analysis distribution, 66
- Manufacturer Usage Description (MUD), 59
- SafeBrowsing, 65
- supply chain, 63

- YANG modules, 60
- Payment Card Industry
  - Data Security Standard (PCI DSS), 44
- Personally identifiable information (PII), 42
- Pervasive monitoring, 83–85
- Pretty Good Privacy (PGP) model, 139
- Privacy, 14, 81, 122–124
- Protocol stack refresher, 104–106
- Public key infrastructure (PKI), 132, 135–138, 141–143
- Public key pairs, 135–137
- QUIC protocol, 7, 9, 85–86, 114–115, 127
- Remote Integrity Verification (RIV), 159
- Root of trust, 158–159
- Routing overlay protocols
  - autonomous system numbers (ASNs), 115
- Bit Index Explicit Replication (BIER), 116, 118
  - definition, 115
- DNS filtering, 116–117
- Generic Network Virtualization Encapsulation (GENEVE), 115–116
- mail delivery agent (MDA), 117
- mail transport agents (MTAs), 117
- virtual local area networks (VLANs), 115, 117
- SafeBrowsing, 65
- Secure operating systems
  - ChromeOS, 149
  - Container OSes, 149
  - Linux, 149–150, 152
  - Microsoft, 150–151
  - MINIX, 150
  - operating systems, 148
  - UNIX, 149–150, 152
- Security architecture
  - patterns, 197–198
- Security Assertion Markup Language (SAML), 142
- Security control framework
  - selection
    - business partners/customers, 31
    - cost, 31
    - ISO 27002, 34, 35
    - ISO/IEC JTC 1/SC 27, 33
    - NISTSP800-30, 32
    - NISTSP800-37, 31
    - NISTSP800-53, 32
    - NISTSP800-137, 32
    - program maturity, 31

- regional applicability of
  - business, 30
- regulatory requirements, 30
- risk tolerance, 31
- security level agreements (SLAs), 33
- Security controls
  - pass-phrase, 29
  - password policy, 29
  - policy guidance, 30
- Security Function Chaining (SFC), 117
- Security level agreements (SLAs), 21, 33
- Security program
  - evaluation, 23–24
- Server Name Indicator (SNI), 85
- Service Function Chaining (SFC), 186–187
- Service function path (SFP), 118
- Service level agreements (SLAs), 70
- Simple Network
  - Management Protocol (SNMP), 48
- Single credential, 141–143
- Single (reduced) sign-on (SSO), 140–141
- Social engineering, 188–189
- Software-Defined
  - Networking (SDN)-based IPsec Flow Protection, 125
- Software Identification (SWID), 160–161
- Software Inventory
  - Message and Attributes (SWIMA), 168
- Supply chain attestation
  - code signing, 157, 161–162
- JSON Object Signing and Encryption (JOSE), 162
- Remote Integrity Verification (RIV), 159
- root of trust, 158–159
- Software Identification (SWID), 160–161
- system measurements, 157
- Trusted Computing Group (TCG), 158
- Trusted Platform Module (TPM), 157–159
- System Assessment and Continuous Monitoring (SACM), 94
- System integrity verification, 167
- System measurements, 157
- TCPcrypt, 113
- Transport layer encryption, 106–107

- Transport Layer Security (TLS), 85–86, 107–110
- Transport protocol stack evolution
  - Automated Certificate Management Environment (ACME), 110–113
  - Cloud data, 102
  - data center architectures, 102
  - end-to-end transport encryption, 102
  - Internet Protocol Security (IPSEC), 124–125
  - Internet Protocol Version 6 (IPV6). *See* Internet Protocol Version 6 (IPV6)
  - Key Management Interoperability Protocol (KMIP), 110–113
  - measurement aids
    - administrators, 103
  - network and traffic management, 103
  - Path Layer UDP Substrates (PLUS), 10
  - protocol stack refresher, 104–106
  - QUIC, 7, 9, 114–115
  - routing overlay protocols. *See* Routing overlay protocols, 11
- TCPcrypt, 113
- transport layer encryption, 106–107
- transport layer security, 107–110
- Tripwire, 50, 168
- Trusted Computing Group (TCG), 158
- Trusted execution environment (TEE), 158
- Trusted Platform Module (TPM), 157–159
- Trust models
  - automated control management, 180
  - Forum For Incident Response and Security Teams (FIRST), 179
  - information sharing groups, 178
  - technologies, 180–181
- User control data
  - business drivers, 80
  - exceptional access, 14
  - lawful interception, 14
  - mobility, 13
  - privacy, 14
- Virtualized environments, 126
- Virtual local area networks (VLANs), 115, 117
- VMware, 68

- WebAuthn, 132
- Web-Based Enterprise Management (WBEM), 49
- Workload mobility, 81
- YANG modules, 60, 125
- Zero Trust Model, 12, 55–58
- Zero Trust Networks, 16, 75