Index

Symbols
3D polygon 255
3D polygonal meshes 255, 256
18 USC 1030 41, 42
18 USC 1343 34
18 USC, Chapter 63 34
1976 Copyright Act 62

A
Absinthe 102, 103
abstract syntax trees 209, 217
Activity Theory 46, 47, 48, 49, 53, 54, 55, 56, 57
Ad Hoc On Demand Distance Vector (AODV) 125, 131, 132, 133, 134, 136, 139, 143, 144
ad-hoc queries 14
Advanced Finger Print Identification Technology (AFIT) 17
adware 178
Aggregator Nodes (ANs) 146, 147, 151
Aggregators 146
algebraic attacks 220
algebraic degree 221, 222, 223, 225, 228
algebraic immunity 220, 225, 226, 230
algebraic normal form (ANF) 221, 223
American Civil Liberties Union (ACLU) 42, 44
anonymity 60, 89, 97, 98
Anti-Terrorist squad (ATS) 50, 51, 55
Anti-Virus 93
Apparition Virus 182
appending virus 180
application programming interface (API) 88, 89, 94, 96, 97, 169, 170, 176
Application Vulnerability Description Language (AVDL) 90
Architecture for Wireless Attack Resistance (AWARE) 135
Army Special Operations 51
ARPANET 87
artificial intelligence 71
artificial neural network (ANN) 74
asymptotic upper bound 223
Atkinson Footwear v. Hodgskin International Services Ltd. 65
Attacking Region (AR) 130, 131
Attestation Identity Keys (AIKs) 206
attributes 107, 111
Authenticated Routing for Ad hoc Networks (ARAN) 132
Authentication Header (AH) 89
avalanche 220, 224, 225, 226, 227, 228
avalanche criterion 220, 224, 225, 226, 227, 228

B
backbone capable node (BCN) 141
backbone node (BN) 141
Base Stations (BSs) 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 157, 158, 159, 160, 161, 162, 163, 164, 167
Basic Input Output System (BIOS) 179, 184
Belgian Personal Identity Card (BELPIC) 6, 8
Bell’s inequality 231, 232, 236, 237
Bell’s theorem 235, 236, 238, 239
Below Poverty Line (BPL) 14
Berlekamp-Massey algorithm 241
Berlekamp-Massey attack 241
binary code 189, 190, 200
binary instrumentation 205
binary multisequence 240, 242
binary sequence 221, 242, 249
binary vectors 221
Biometric Identification and Personal Detection Ethics (HIDE) 19, 22
Biometric Identification Technology Ethics (BITE) 19, 22
Black Hole attack 138
blackhole node 138, 141, 143
Bohr’s stance 236
Boolean function 220, 221, 222, 224, 225, 226, 227, 228, 229, 230
boot block 179, 180
boot sector infector (BSI) 179
Border Gateway Protocol (BGP) 87
botnets 178
BSQLHacker 102, 103
business process outsourcing (BPO) 24
byte string 170

C
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) 128, 130, 131, 145
central processing units (CPU) 91
certificate authority (CA) 106, 109, 110
Certification Revocation Lists (CRL) 9, 110
Certification Service Providers (CSP) 8
challenges 1, 2, 7, 9, 11, 12, 13, 16, 17
characterization vectors (CV) 191
Cheating 146, 159
Checkstyle 101, 103
Checkup Reply (CREP) 140
Checkup Request (CREQ) 140
Child Internet Protection Act (CIPA) 41, 42
Child On-Line Protection Act (COPA) 41, 42
circuit-switch 169
Circuit switching 169, 177
C++ language 101
clone detection 209, 210, 218
Cloud Computing 115, 116, 117, 118, 119, 120, 123
Cluster Heads (CHs) 147, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161
code clone detection 209, 218
colluding adversaries attack (CAA) 130, 131
Communication Decency Act (CDA) 41, 42
complexity measures 220, 221, 228
computational algorithms 231
computing platform 204, 205
confidentiality, integrity, availability, authentication, authorization, accounting, and anonymity (CI5A) 89, 95, 98
constant values in field variables (CVFV) 211
Control flow graphs (CFG) 185, 193, 195, 196, 200
copyright piracy 60, 66
copyrights 59, 60, 61, 62, 63, 64, 65, 66, 67
Copyright Treaty (WCT) 65
correlation attacks 220, 222, 228
correlation immunity 220, 228
cover data 250
cppcheck 101, 103
cryptogram 232, 233
cryptographic community 220
cryptographic framework 223
cryptographic techniques 250
cryptography 231, 232, 233, 234, 235, 236, 237
cryptology 231, 232, 233, 237, 238, 240
cryptosystems 220, 223, 228
culture 1, 17
cyber attacks 71
cyber crime 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45
cyber infrastructures 25
cyber laws 39
cyber piracy 66
cyber security 24
cyberspace 59, 60, 64, 66
cyber terrorism 36
Cyber wing 21

D
DARPA Agent Markup Language (DAML) 73, 76, 86
data collection 147, 148
Data Routing Information (DRI) 139
data tagging 207
Dempster Shafer Theory 190
Index

Denial-of-Message Attacks on Sensor Network Broadcasts” (DDMA) 150, 151
Denial of Service (DoS) 124, 125, 126, 128, 129, 130, 131, 133, 135, 140, 143
Description Logic reasoner 76, 78, 81
destination sends the route reply (RREP) 131, 132, 134, 135, 138, 139, 141
detection techniques 178, 179, 199
Developers 120, 122
diamond characteristic value (DCV) 253, 254
differential attacks 220
differential cryptanalysis 223, 224, 225
DigiDoc 9
digital identities 106, 107, 110
Digital Millennium Copyright Act, 1998 62
Digital Signature Act (DSA) 8, 9
digit block 254
discrete cosine transform (DCT) 254, 255, 256, 257, 258
discrete log (DL) 121
Disposition Reporting Improvements (DRI) 17
Distributed Coordination Function (DCF) 128
Distributed Coordination Function Inter frame Space (DIFS) 129, 130
Dynamic Dependence Graph (DDG) 211
Dynamic Source Routing (DSR) 125, 131, 132, 133, 134, 136, 143

E

economic times 24, 27, 29, 31, 32
ECRYPT Stream Cipher Project 220, 221, 229
e-Governance 13
e-Government 6, 7, 8, 22
Einstein-Podolsky-Rosen (EPR) 231, 232, 235, 236, 237
electronic Identity (eID) 6, 7, 8, 12, 22
elementary algorithm 221
elliptic curve discrete logarithm problem (ECDLP) 121
embedding algorithm 252
embedding scheme 250
Emergency-as-Activity 49
emergency response 46, 47, 48, 49, 50, 51, 52, 53, 56
empathy 26, 28, 29
Encapsulating Security Payload (ESP) 89
End Users 119, 121
Energy Efficiency Ratio (EERs) 135
engine friendliness 192
EPR paradox 235
error multisequence 240, 242, 244, 245
error sequence 242
eSTREAM Project 220, 221
ethics 1, 5
Euclidean distance 189, 191, 193
exit strategy 31
Extended Inter frame Space (EIFS) 129, 130
Extended Stamp Martin Algorithm 240, 242, 248
Extensible Record Format (ERF) 170
extrication 26, 29

F

factorization algorithm 231
federated 110
feedback polynomial 241
FG-Injector Framework 102
file infector 180
finger-printing algorithm 210
first in first out (FIFO) 134
Flawfinder 101, 103
Forward Error Correction (FEC) 127
Forwarding Rejection Attacks 133, 136
frequency domain 251

G

garbage code 186
generic algorithm 252
generic embedding 250
generic extracting 250
generic extracting scheme 250
genuine nano 213, 215
global avalanche characteristics (GAC) 224, 225
Global Information Infrastructure (GII) 91, 103
global overview 61
global positioning systems (GPS) 49, 53
Gray Hole attack 140
Grid Computing 115, 118
Grokster case 63, 67
guidance 31
Index

H
Hamming distance 222
Hamming weight 222, 224
havoc 59
Hidden Markov Model (HMM) 194, 195
hidden message 250, 252
Home Location Register (HLR) 90
Home Subscriber Server (HSS) 90

I
identifier 107
identity management 106, 107, 110, 111, 112, 113
identity provider 110, 111, 112, 113
ID theft 4
IEEE 802.11 125, 126, 127, 128, 129, 130, 143, 144, 145
ILOVEYOU virus 33, 34, 40
Import Address Table (IAT) 182, 188
Incident Command System (ICS) 54
Indian Copyright Law 62
infected nano 213, 215
infection mechanisms 178, 179
information and communications technology (ICT) 6, 39
Information Security Monitoring System (ISMS) 75
information system (IS) 72, 73
information technology (IT) 24, 32
Infrastructure as a Service (IaaS) 91, 115, 116, 121
infrastructure for ad hoc migration scheme (IAMS) 128
inheritance structure (IS) 211
integrity measurements 205, 207
Intelligence Bureau (IB) 52
Interface Message Processor (IMP) 87
Intermediate Node (IN) 139
intermediate nodes 147
International Business Machines (IBM) 116
International Conference on Computer Communication (ICCC) 87
Internet Host Providers (IHPs) 62, 63
Internet Protocol (IP) 87, 88, 89, 90
Internet Service Providers (ISPs) 61, 62, 63,
67, 68
Interrupt Vector Table (IVT) 184
Interstate Photo System Enhancements (IPS) 17
Intrusion Detection (ID) 123, 134, 135, 137, 139
Intrusion Detection System (IDS) 90, 93, 102
Intrusion Prevention System (IPS) 90, 93, 102
IP Multimedia Subsystem (IMS) 90
IP Security (IPsec) 88, 89
ISP liability 62
issues 1, 2, 5, 9, 12, 15, 18, 19, 21
Itar-Tass Russian News Agency v. Russian Kurier, Inc 65

J
jamming 126, 127, 128, 130, 131, 145
JBroFuzz 102, 104
JellyFish (JF) 136
joint linear complexity 240, 241, 242, 244, 245, 246, 248
jump instructions 185, 186, 196
jurisdiction 59, 60, 64, 65

K
k-error 240, 241, 242, 246, 248
k-error joint linear complexity 240, 241, 242, 246, 248
key distribution (KD) 231, 232, 234, 237
keystream 220, 221, 240, 241
keystream generator 241
keystream sequence 240, 241
knowledge transfer 26, 28

L
least significant bits (LSB) 252, 253, 257
legal 1, 2, 8, 10, 11, 12, 13, 20
Legal Reforms 13
lex loci delicti 64
LFSR sequences 220
liability 59, 60, 61, 62, 63, 64, 67
Liberty Alliance 110
linear complexity 240, 241, 242, 244, 245, 246, 248, 249
linear, differential attacks 220
Index

Linear (non-linear) Feedback Shift Registers (LFSRs) 220, 221
linear structure 223
linear subspace 223, 227
Local Area Network (LAN) 92
London School of Economics (LSE) 5, 6, 23
Longest Common Subsequence (LCS) 178, 195, 196, 197, 198, 199, 200

M
machine readable data (MRD) 17
Malicious 146
malicious aggregators 147, 150
malicious code 178, 182, 183, 190, 195, 199, 202
malware 178, 179, 180, 182, 183, 184, 185, 186, 189, 190, 191, 192, 193, 194, 195, 199, 200, 201, 202, 204, 205, 207, 208, 211, 217
malware detection 178, 179, 189, 190, 191, 193, 199, 201
malware infection 207
malware threats 178, 184
malware types 178
manifestations of tampering 204
Marine Commandos (MARCOS) 51, 55
measurement kernel 205, 206
metamorphic engine 184, 185, 186, 192
metamorphic malware 178, 179, 182, 185, 186, 189, 192, 193, 194, 195, 200, 201, 202
metamorphic malware detection 178, 179, 193
metamorphic variants 192
metamorphic viruses 178, 179, 189, 192, 193, 195
metamorphism 178, 186, 187, 188
m-fold 240, 242, 243, 244, 248
micro-level manners 74
Microsoft Corporation v. Kiran 62
Ministry of Home Affairs (MHA) 12
misaggregated 147
mobile ad hoc network (MANET) 124, 125, 126, 130, 131, 133, 145
Modified Games Chan algorithm 240, 244
Modified Multi Level Embed Procedure (MM-LEP) 255
Monopolizing Attack 127
Multiple Messages Embedding (MME) 256
Mumbai terror attacks of November 2008 46, 47

N
nano 213, 214, 215, 216
nano program 213, 214
Napster 63
national ID 7, 8, 9
national identity 1, 2, 5
national identity register 5, 23
National Identity Registry (NIR) 5
National Palm Print System (NPPS) 17
National Vulnerability Database (NVD) 89
Nessus 102, 104
Nessus Attack Scripting Language (NASL) 102
Network Allocation Vector (NAV) 128, 129
network analysis 176
network architecture 31
network interface card (NIC) 169, 170, 171
network intrusion detection system 168
Network monitors (NMs) 137
Network Stumbler 102
network traffic 168, 175, 176, 177
Next Generation Internet (NGI) 87, 88
Next Generation Secure Computing Base (NG-SCB) 206
Next Hop Node (NHN) 139
Nexus 206, 207, 219
NGI 87, 88, 89, 90, 91, 94, 101, 105
nonlinear Boolean function 220
nonlinearity 220, 221, 222, 223, 225, 226, 227, 228, 229, 230
nonlinearity value 225
normalization 178, 189, 192, 193, 201
N-tier architecture 13
numerical normal form (NNF) 221

O
obfuscation 178, 179, 186, 188, 189
Oligomophic virus 181
omnipresent authority 108
Online Certificate Status Protocol (OCSP) 9
Online Transaction Processing database (OLTP) 14
ontology  70, 71, 72, 73, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86
Ontology Inference Layer (OIL)  73, 76, 86
open-box semantics  206
OpenID  110, 112, 113
Open Shortest Path First (OSPF)  87
OpenXAdes  10
organizational infrastructure  5
Original Entry Point (OEP)  190
OutGuess  254, 255
outsourced  24, 25

P
packed-code 178
packet capture  168, 169, 170, 177
packet delivery ratio (PDR) 128
packet drop avoidance (PDA) 174
packet headers  169
packet loss  169, 174
Packet switching  169, 177
Passive monitoring  169
pathrater algorithm  140
Patriot Act of 2001  34
Peer to Peer File Sharing (P2P File Sharing)  63
Performance  26, 28, 29
Performances and Recordings Treaty (WPPT)  65
periodic multisequence  240, 241, 242, 243, 245, 248
periodic sequence  241, 244, 245, 247, 249
Physical Layer Convergence Procedure (PLCP)  126, 127
pixel value differencing (PVD)  253
plagiarism detection  210
Platform as a Service (PaaS)  91, 115, 116, 121
Platform Configuration Registers (PCR)  206
Playboy v Frena  62
Pluggable Authentication Module (PAM)  214
Policy Reforms  13
polymorphic viruses  181
polymorphism  178
polynomial algorithm  232
Portable Executable (PE)  182, 183, 188, 190, 191, 200
power on self test  179
Preamble Attack  127
prepending viruses  180
primary boot  179
Primitive Root Modulo  242
Private Cloud  115
program dependence graphs (PDGs)  210, 218
protocols  87, 88, 96, 97, 101, 107, 119, 120
Proxy Reports  146, 148
ProxyStrike  102, 104
Public Cloud  115
public key cryptography (PKC)  233, 234, 235, 237
public-key infrastructure (PKI)  106, 110
Public key Steganography  251
public-key systems  121, 232, 233, 234, 237, 250, 251
Pure Steganography  251

Q
quadratic bound  225, 226
quadratic functions  225
Quality Check Automation (QCA)  17
Quality of Service (QoS)  26, 28, 29
Quantization Index Modulation (QIM)  255
quantum computing  232
quantum communication  231, 232, 238, 239
quantum cryptography  231, 232, 234, 235, 236
quantum cryptography  231, 232, 234, 235, 237, 238
Quantum Currency  238
Quantum Dense Coding  232, 238
Quantum Key Distribution (QKD)  231, 235
quantum mechanics  232, 235, 236, 237
quantum particle  235
quantum polynomial  232
quantum polynomial algorithm  232
quantum retro-crypto analysis  232
quantum states  234, 236
quantum systems  234, 235, 236
Quantum Teleportation  232, 238
quantum theory  236

R
random access memory (RAM)  91
random assessment delay (RAD)  134
RDF Schema (RDFS)  76
Reactive Attack  127
Reed-Muller code  223, 229, 230
Ref. Switching  169
RegSwap virus  188
regular node (RN)  141
regulations  31
remote procedure calls (RPC)  15
Report Dropping  146, 147
Report Tampering  146
Representation Rearrangement Procedure (RRP)  255
Reputation Table (RT)  132
Request to Send/Clear to Send (RTS/CTS)  128, 129
Resource Deprivation Attacks  133
Resource Description Framework (RDF)  76
Resource Unlimited Attack (RUA)  127
retroactive decryption  232
risk  24, 25, 26, 27, 29, 30, 31, 32, 115
rootkits  178, 191
route discovery by broadcasting a route request (RREQ)  131, 132, 133, 134, 135, 136, 137, 138, 139
Route Disruption Attacks  133
route error (RRER)  135
rushing attack  142

S

Scalable Protocol for Robust Information Dissemination (SPROID)  150
scientific revolution  231
secret information  250, 251
secret key  220, 250, 251, 255
Secret key steganography  251
secret message  250, 251, 254
Secure Aggregation Tree (SAT)  149
secure cloud environment  119
Secured Network Programming (SNP)  90, 105
Secured Socket Layer (SSL)  90, 101
Secure identity across borders linked (STORK)  6
Secure Information Aggregation (SIA)  148, 149, 150, 151, 156, 158, 166
secure internet protocol (IPsec)  120
Secure Position Aided Ad hoc Routing (SPAAR)  132
secure socket layer (SSL)  120
secure wireless LAN architecture (SWAN)  142, 145
Security Aware Ad-Hoc Routing (SAR)  132
security-aware software development life cycle (SaSDLC)  93, 102, 105
security forensics  176
security ontology (SO)  73
self replicating virus  180
semantic relationships  70, 71, 73, 75, 77, 79
Semantic Web Rule Language (SWRL)  76, 80, 83, 84
Sensor Networks  146
sequence of method calls (SMC)  211
service oriented architecture (SOA)  91, 93
SFD Attack  127
shared environments  26, 28
shared-key  251
Shor algorithm  231
Shor quantum algorithm  231
Short Inter frame Space (SIFS)  127, 129
single adversary attack (SAA)  130
snort  168, 169
social networking  36
Social Security Administration (SSA)  2, 3
Social Security Number (SSN)  2, 3, 4, 10, 11, 18, 23
software as a service (SaaS)  91
Software as a Service (SaaS)  115, 116, 121
software attestation  204
SoftWare based ATTestation (SWATT)  207, 208, 217
software birthmark  204, 209, 210, 211
Software Develop Life Cycle (SDLC)  93, 94, 102
software piracy  210
software similarity  204
software tampering  204, 205, 209, 210
software watermark  204, 210, 217
spatial domain  250, 251, 252, 253, 255
Index

SpikeProxy 102
spyware 178
ssh program 214, 216
Start Frame Delimiter (SFD) 126, 127, 171
static analysis 178, 189, 190, 191, 192
Static Analyzer for Vicious Executable (SAVE) 189, 202
static executable code 211
static source code 211
Statistical Analysis of Multipath (SAM) 137
steganalysis 250, 252, 253, 254, 255, 257
steganalysis algorithms 254
steganographic capacity 256
steganographic embedding 250, 254, 258
steganographic embedding schemes 250
steganographic methods 251, 254, 255
steganographic technique 253
steganography 250, 251, 252, 254, 255, 256, 257
steganography scheme 250, 252, 254, 257
StegHide 254, 255
stego coding method 254
stego data 250
stego image 252, 253
stego keys 252
stego object 250
stream cipher 220, 221, 222, 223, 224, 229, 230, 240, 241
stream cipher cryptography 220
strict avalanche criterion (SAC) 224
Subafilms Ltd. v. MGM-Pathe Communications Co 64
subroutine inlining 189
Symbol Attack 127
Symmetric Multi Threading (SMT) 208, 209
System Architects 120, 121
System Call Dependence Graph (SCDG) 211, 212
System Network Architecture (SNA) 87

T

technical 1, 7, 10, 11
Technology Act of 2002 42
Telecom network 89
The Copyright, Designs and Patents Act 1988 62
Third Party Auditors 120, 123
Time Machine (TM) 168, 171, 172, 173, 174, 175, 176
Time Stamp Providers (TSP) 8
Time Travel 175, 176, 177
transform domain 250
transport layer security (TLS) 90, 103, 120
tri-way differencing scheme 253, 254
tri-way pixel value differencing (TPVD) 253
Trojans 178
trust 26, 28, 29, 108, 110, 113
trusted computing 204, 205, 206, 217, 219
Trusted Computing Base (TCB) 207, 219
Trusted Computing Group (TCG) 205, 206, 207
Trusted Computing Platform (TCP) 204, 205, 206
Trusted Platform Module (TPM) 205, 206
Trusted Virtual Machine Monitor (TVMM) 206, 207

U

UID cards 20
UID framework 20
UID system 1, 11, 12, 13, 14, 15, 16, 20
Unified Modeling Language (UML) 94, 95, 97
Unique Identification Authority of India (UIDAI) 1, 2, 12, 21
Unique Identification Numbers (UID) 1, 2, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21
Unique Identification (UID) 1
unique identity 1
United States Code (USC) 34, 41, 42
upper bound 223, 224, 225, 226, 228, 229, 230
used classes (UC) 211
User Profile Server Function (UPSF) 90
Utility Computing 118

V

vector space 221
Virtual Firewall System (VFS) 122
virtualization 115, 118, 119
Virtual Machine (VM) 191, 206
virus code 179, 180, 181, 189, 196
viruses 178, 179, 180, 181, 182, 185, 186, 189, 192, 193, 194, 195, 198, 200, 201, 202
Index

VM traffic 121
voice-over-Internet protocol (VoIP) 49, 53
Voice over IP (VoIP) 88

W
watchdog algorithm 140
Watchdog (WD) 132
Web 1.0 90
Web 2.0 36, 88, 90
Web 3.0 88, 90, 91, 105
Web Hosting 61, 62
Web Ontology Language (OWL) 76, 78, 80, 81, 82, 83, 84, 85, 86
whole program path (WPP) 211, 218

WiFiHopper 102, 105
Wireless Sensor Networks (WSN) 146, 147, 148, 149, 150, 153, 164
Wireless Sensor Networks (WSNs) 147
World Intellectual Property Organization (WIPO) 65
World Wide Web (WWW) 60, 61, 64, 65, 66
wormhole attack 136, 137, 145
worms 178, 190
WS-Trust 110

Y
Yet Another Steganographic scheme (YASS) 255, 257