

INDEX

Numbers

3D visualization, for mapping attacks to physical location and organizational mission, 117–118, 118

A

Abdullah, Kulsoom, 50–51, 220

Abowd, Gregory D. (*Human-Computer Interaction*), 212

abstract data, information visualization and, 2

Address Resolution Protocol (ARP), 102–103

packet length, 86

adjacency matrix, 9, 9

Adobe PDF files, metadata analysis, 205

Advanced Encryption Standard (AES) algorithm, 30, 31, 200

AfterGlow, 129, 145, 221

aggregation, 139

Ahamad, Mustaque, 220

alert threshold analysis, of TreeMap, 158–159

algorithm selection, 193

American Registry for Internet Numbers (ARIN), IP address lookup service, 98

American Standard Code for

Information Interchange (ASCII), 22–24

color for printable bytes in network packets, 79

animation

packets with Nessus, 65–66, 65
in visualization, 122

anomaly detection, 26

antivirus applications, analyzing effectiveness, 108, 110

application layer

attacks on software in, 161
in protocol hierarchy, 36–38
visualization support, 207

ArcSight, Enterprise Security Management (ESM), 119, 119

Argus, 121*n*

ARIN (American Registry for Internet Numbers), IP address lookup service, 98

ARP (Address Resolution Protocol), 102–103

packet length, 86

ASCII (American Standard Code for Information Interchange), 22–24

color for printable bytes in network packets, 79

assembly language, converting program to, 203

Atlas of Cyberspace (Dodge and Kitchin), 225

attackers

identifying, 214–215
network traffic level and detection, 44

attack-resistant systems, 163

- attacks
 - on security visualization systems, 163–175
 - autoscale, 169–170, 170
 - labeling, 164–165, 164, 165
 - occlusion, 166, 166
 - round-off, 170–172
 - tainted data, 174
 - windshield wiper, 167–168, 167, 168
 - trends, 161
- audio CD, Sony rootkit on, 106
- auditory information, 2
- autoscale attacks, 169–170, 170
- Axelsson, Stefan (*Understanding Intrusion Detection Through Visualization*), 225
- axis histogram, 93*n*

B

- backbone providers, 42
- background radiation, Internet, 84
- Bagle mass email virus, 97
- bar charts, 108, 109
- Bartoletti, Tony, 113, 220
- Beale, Russell (*Human-Computer Interaction*), 212
- Bearavolu, Ratna, 220
- Bederson, Benjamin B., 219
- bidirectional links in graphs, 9
- big-picture context, 14
- binary rainfall, 78
 - attack targeting, 173
 - of network packets, 116, 116, 117
- binary visualization
 - of photo in different file formats, 28
 - of Word document, 30
 - with AES algorithm encryption, 31
 - with password protection, 31
- bits, 21
 - converting characters to, 22
- Black Hat, 227
- blocked outbound traffic, steps for generating graph, 140, 141
- blocked state for ports, 57
- BMP file format
 - binary visualization of photo, 28
 - relative size, 27
- Boggs, David, 41
- bottlenecks in performance, 195
- Boutell, Thomas, 23
- Bro intrusion detection system, 172
- brushing, 14, 15, 16–17
- Bugtraq, 177, 212
- building community, 210–212
- byte frequency distribution, of packets, 176
- byte presence visualization, 100–101, 101

C

- cable modems, 84, 103
 - and ARP request for MAC address, 102
- CanSecWest, 227
- Card, Stuart K., 219
- CarnivorePE, 221
- carriage returns and line feeds (CRLFs), 25
- categorical data types, 6–7
- cd command, 75
- chaffing, 166
- Chaos Computer Congress, 227
- charts, for analysis, 96–97
- chmod command, 22
- Christensen, Marvin, 113
- client-server architecture, for Nessus, 60
- closed ports, 57
- collaboration, 211
- color encoding, 17–18, 18
 - bits from text file plotted as image, 24, 24
 - common protocols, 84
 - link graphs, 137–138
 - addresses, 131
 - printable ASCII bytes in network packets, 78, 79
 - on RUMINT plots, 66
 - in smart books, 27
- command line
 - as application interface, 191
 - attacker access to, 74
- Common Vulnerabilities and Exposures (CVE) database, 211–212
- communication graph, and firewall logs, 133
- community building, 210–212

Computer Intrusion Detection and Network Monitoring (Marchette), 225

Computer Networking (Kurose and Ross), 36

context, visualization techniques with, 49

Conti, Gregory, 220

controls, interacting with, 16–20

Copeland, John A., 220

co-processors, 199

Core Security Technologies, CORE IMPACT, 60*n*

Cranor, Lorrie Faith (*Security and Usability*), 226

critical machines, using color to identify in link graph, 137

CRLFs (carriage returns and line feeds), 25

cryptanalysis, visual, 200–202

Cube of Potential Doom, 172, 222
wire diagram, 172

CVE (Common Vulnerabilities and Exposures) database, 211–212

D

dark address space, IP addresses in, 137

data
files, identifying, 21–22
sources, questions for reviewing, 187
storage, RAM buffer for, 189–190
types, 4–9

Data Encryption Standard (DES), 200
initial and final permutations, 201

data link layer, in protocol hierarchy, 41–44

database security, 206

dataflow design, 189–190

datasets
attacker insertion of malicious data into, 162
fields in, 4
parsing, 189
records in, 193
structure of typical, 5

datastream review, 185–187

DCOM (Distributed Component Object Model) services, port 135
for, 69

Deadhat worm, 97

DEFCON, 227

density histogram, 93*n*

derived information, 185

DES (Data Encryption Standard), 200
initial and final permutations, 201

The Design of Everyday Things (Norman), 225

Designing Web Usability (Nielsen), 225

destination
addresses, visualizing connections between source and, 129–130, 130

ports
filtering traffic based on, 66–67, 67, 68
for TCP, 54
socket, for Metasploit, 76–77

Destination Unreachable packets, 102

destination-centric analysis, of
TreeMap, 157–158, 158

detail, visualization techniques with, 49

DF control flag, 88

Digg, 210

dir command, 75

direct manipulation of objects and controls, 16

directed graphs, 9

directional graph, for link graph, 129, 129, 130

disassembling files, 203

disciplines, evaluating others for trends, 215–216

display resolution, constraints on visualization systems, 167

distractors, 4

distributed attacks, 158

Distributed Component Object Model (DCOM) services, port 135
for, 69

distributed sensors, for monitoring widespread network attacks, 111–112

Dix, Alan (*Human-Computer Interaction*), 212

DNS (Domain Name System), 41

.doc file extension, 22

documentation, 195, 211

Dodge, Martin (*Atlas of Cyberspace*), 225

Domain Name System (DNS), 41
Doomjuice worm, 97
dynamic queries, 19–20, 19

E

echo requests, 144
edges
 in graph data, 9
 in link graphs, 128
eEye, Retina, 60*n*
egress filters, 140
Eick, Stephen, 32–33, 219
ELF (Executable and Linking File)
 format, 202
 viewing structure of, 203
email attachments, attacks with,
 161–162
encryption, lack of proof of secure, 202
end users
 analysis of, 184–185
 feedback from, 194
 role in visualization system
 development, 184
 training on attack detection, 177
 visualization for, 208
enterprise network, monitoring intrusion
 detection alerts on,
 124, 125
Enterprise Security Management
 (ESM), 119, 119
Erbacher, Robert, 122, 220
EtherApe, 222
Ethernet, 41
 information in home ISP connection
 dataset, 87–88
 largest permissible packet, 62
Ehertype, 87
evaluating visualization systems,
 194–195, 212
event node, in link graph, 131, 132
Ewing, Larry, 200
.exe file extension, 22
Executable and Linking File (ELF)
 format, 202
 viewing structure of, 203
executable files, identifying, 21–22
exploit command (Metasploit), 75
exploits, 72
eye candy, avoiding visualizations as, 20

F

failure, studying to achieve success, 163
false negatives, 150
 in anomaly detection, 26
false positives, 150
 in anomaly detection, 26
 determining, 157
 reducing, 153
fe3d, 57
 graphical presentation from, 58
feedback
 for slow response time, 13
 from users, 194
Fekete, Jean-Daniel, 225
field-programmable gate arrays
 (FPGAs), 199
fields in datasets, 4
file
 permissions, in Linux/Unix, 22
 types
 identifying data vs. executable,
 21–22
 relative size of graphic formats, 27
 using color to display, 18
file extensions, 21–22
File Monitor (Sysinternals), 209
filesystem browser, SequoiaView, 14,
 17–18, 18
filtering, 190, 192–193
 based on destination ports, 66–67,
 67, 68
 iterative, 138–139
 noise, 214
 responses from port scanning, 48
filters
 egress, 140
 threshold, 158–159
fingerprints, of security tools, attacks,
 and protocols, 211
Fink, Glenn, 112–113, 220
Finlay, Janet (*Human-Computer
Interaction*), 212
firewall logs, 127
 entry contents, 128
 extracting IP addresses from, 130
 file configurations, 136
 graph interpretation, 142–144, 143
 hypothesis-based analysis, 145–148
 link graphs to analyze, 128–132, 129

- outbound traffic analysis with, 140–145
- visualizing connections between source and destination addresses, 129–130, 130
- firewalls, 127–128
 - and IDSs, 149
- fish-eye view, 12, 13
- flags in TCP, 38
- Focus + Context, 12, 12
- FPGAs (field-programmable gate arrays), 199
- fragmented packets, 88–89, 89
- Freeciv, 16–17, 17
- Frincke, Deborah, 122, 220
- Fyodor, 43, 227

G

- game-programming community, 199
 - security concerns, 206
- Garber, Menashe, 122
- Garfinkel, Simson (*Security and Usability*), 226
- GIF file format
 - binary visualization of photo, 28
 - relative size, 27
- gnuplot, 120
- Goodall, John R., 220, 224
- GPUs (graphics processing units), 199
 - The Grammar of Graphics* (Wilkinson), 218
- graph data, 4, 9
- graphical
 - layout techniques, 9–12
 - Focus + Context, 12, 12
 - small multiples, 11, 11
 - starplots, 10–11, 10
 - reports, 212–213
 - user interfaces, 191
- graphics draw (GD) library, 23*n*
- graphics processing units (GPUs), 199
- graphing tools, open source, 120
- GraphViz library, 131
- GUI Bloopers* (Johnson), 225
- GUI widgets, 19

H

- Hack Proofing Your Network* (Russell), 79
- hacker conferences, 227

- Hacker Disassembling Uncovered* (Kaspersky), 79
- Hack.lu, 227
- header fields, assessing, 51, 52–53, 54–55
- Healey, Christopher, 4*n*
- hexadecimal packet, dissecting, 43
- hierarchical
 - data, 4, 7, 8
 - layout, for link graphs, 129
 - relationships, TreeMaps for, 152
- high-volume activity, focusing on, 97
- Hinden, Robert, 198
- histograms, for antivirus software analysis, 108, 110
- holes, Nessus count of, 61
- Hollan, James D., 219
- home ISP connection dataset, 83. *See also* ISP connection dataset
- Homepage Usability* (Nielsen), 225
- Honeynet Project, 227
 - extended timelines to observe trends, 120–121, 121
- horizontal port scans, 120
- Howard, Michael (*Writing Secure Code*), 177
- HTML (HyperText Markup Language), 38
- HTTP (HyperText Transfer Protocol), 37–38
- human analysts, 208
- human processing
 - and computer interaction, 225–226
 - vs. machine processing, 25–26
- human-centered design, 184
 - Human-Computer Interaction* (Dix, Finlay, Abowd, and Beale), 212
- HyperText Markup Language (HTML), 38
- HyperText Transfer Protocol (HTTP), 37–38
- hypothesis-based analysis, of firewall logs, 145–148

I

- IANA (Internet Assigned Number Authority) port assignment list, 39, 100

- ICMP. *See* Internet Control Message Protocol (ICMP)
 - IDA Pro disassembler, 202
 - IDSs. *See* intrusion detection systems (IDSs)
 - IEEE Symposium on Information Visualization, 219
 - images
 - bits from text file plotted as, 23
 - color to enhance, 24, 24
 - metadata analysis, 205
 - inbound traffic, separating from outbound traffic in Metasploit, 79
 - incoming packets to home computer, capturing, 84
 - information visualization
 - advantages of, 2–4
 - goal of, 1
 - InfoVis Toolkit, 225
 - Inselberg, Alfred, 45, 219
 - installation of software, ease of, 193
 - integrity of data, protecting, 176
 - interaction techniques, 12–20
 - interactive line chart, 3
 - interface, application, 191–192
 - International Organization for Standardization (ISO), 36
 - Internet
 - background radiation, 84
 - protocol hierarchy, 36–44
 - Internet Assigned Number Authority (IANA) port assignment list, 39, 100
 - Internet Control Message Protocol (ICMP), 90, 102–103
 - echo requests, 103
 - packet length, 86
 - Internet Protocol (IP), 40
 - addresses, 40, 91–92, 91
 - in dark address space, 137
 - extracting from firewall log, 130
 - lookup service, 98
 - checksum, 90
 - differential services field, 88
 - flags, 88
 - fragmentation, in ISP connection dataset, 88–89, 89
 - identification field, 88
 - spoofing, 175
 - transport protocol field, 90
 - Internet Protocol version 6 (IPv6), 40*n*
 - packet header, 198
 - and security visualization research challenges, 198
 - Internet service provider (ISP) connection dataset, 83–103
 - big-picture analysis, 84–92, 85
 - Ethernet and IP versioning information, 87–88, 87
 - IP addresses, ports, and sequence numbers, 91–92, 91
 - IP fragmentation, 88–89, 89
 - packet length, 86–87, 86
 - TTL, transport protocols, and checksums, 89, 90–91
 - traffic slices, analyzing and removing, 92–103
 - ARP and ICMP, 102–103
 - TCP, 92–97, 93, 94, 95
 - UDP, 98–103, 99
 - interval data types, 6–7
 - Interz0ne, 227
 - intrusion detection logs, 127
 - intrusion detection systems (IDSs), 111, 149
 - features and capabilities for signature analysis, 156
 - on large-scale networks, 122, 123
 - monitoring alerts on enterprise networks, 124, 125
 - and signature-matching, 208
 - and TreeMaps
 - analyzing, 153–159
 - constructing, 152–153, 152, 153
 - signature tuning with, 150–151
 - IP. *See* Internet Protocol (IP)
 - ISO (International Organization for Standardization), 36
 - ISP. *See* Internet service provider (ISP) connection dataset
- ## J
- Johnson, Brian, 219
 - Johnson, Jeff (*GUI Bloopers*), 225
 - JPEG file format
 - binary visualization of photo, 28
 - relative size, 27
 - jumbo frames, 37*n*, 62

K

Kaminsky, Dan, 106, 107
Kaspersky, Kris (*Hacker Disassembling Uncovered*), 79
Kershaw, Mike, 222
Kirhenshtein, Victor, 60
Kitchin, Rob (*Atlas of Cyberspace*), 225
known vulnerabilities, 59
Koike, Hideki, 111, 220
Koizumi, Kanba, 111, 220
Komlodi, Anita, 220
Krasser, Sven, 50, 66
Krystosk, Paul, 113
Kurose, James (*Computer Networking*), 36

L

labeling
 attacks, 164–165, 164, 165
 mechanics of, 50
 occlusion from, 49
Lakaraju, Kiran, 220
large documents, multiple columns to display, 32, 33
Lau, Stephen, 172, 220
LeBlanc, David C. (*Writing Secure Code*), 177
Lee, Chris, 220
library of security data, 210–211
lifespan of worms, viewing, 121
line chart, interactive, 3
line feeds, to see semantic structure of files, 25
link graphs
 for analyzing firewall logs, 128–132, 129
 and directional graphs, 129, 129, 130
 generation process, 132–140
 color mapping, 137–138
 data fields identification, 133
 iterative aggregation, 139–140
 iterative filtering, 138–139
 mapping data to graph nodes, 133–137, 134, 135
 objective definition of, 132–133
 hierarchical layout for, 129
 for showing relationships, 128
linking, 16–17
Linux
 file types, 22
 high port numbers as indicator, 47

listening ports, port scan probes for, 61
listening program, 87
log files, and Splunk analysis tool, 212, 213
low-and-slow scan, 44
 detecting, 121
low-volume activity, 97
ls command (Unix), 202
 binary view of, 203
Lutters, Wayne G., 220

M

Ma, Kwan-Liu, 113, 220
machine processing, 208–211
 correlating network traffic to, 112, 113
 and human interaction, 225–226
 vs. human processing, 25–26
Mac operating systems
 CRLFs in, 25*n*
 Dock in, 12
magic lens, 12
malicious visualization, 199
malware, 108
 collection, 87*n*
manipulation of objects and controls, 16
Many Eyes, 211
mapping, 7
 packet data to visualizations, 44
Marchette, David J. (*Computer Intrusion Detection and Network Monitoring*), 225
Marty, Raffy, 211, 221
MaxMind, 106*n*
McPherson, Jonathan, 113
metadata analysis, 205
Metasploit, 59, 72–81
 analyzing exploitations, 78–79
 choosing exploits, 73
 choosing payloads, 74–75
 commands
 exploit, 75
 set LHOST, 75
 set PAYLOAD, 74
 show exploits, 73
 show options, 73, 74
 show payloads, 74–75
 type, 75

- Metasploit, *continued*
 - determining source and destination sockets, 76–77
 - executing attacks, 75–76
 - port socket for, 76–77
 - separating inbound from outbound traffic in, 79
 - stepping through attacks, 79–81
 - Metcalfe, Robert, 41*n*
 - MF control flag, 88
 - Microsoft Remote Procedure Call (RPC) DCOM service, 72
 - Microsoft Security Bulletin, 72*n*
 - Microsoft Word documents
 - binary visualization of, 30
 - with AES algorithm encryption, 31
 - with password protection, 31
 - dissecting security behavior of, 29–32
 - metadata analysis of, 205
 - mobile device security, 206
 - modify password, in Microsoft Word, 29–30
 - monitors, constraints on visualization systems, 167
 - mouseover element, for labeling information, 50
 - Muelder, Chris, 220
 - Muessig, Paul, 220
 - multiples, small, 11
 - multivariate visualizations, 10–11, 10
 - Mydoom virus, 97
- N**
- National Center for Advanced Secure Systems Research (NCASSR), 223
 - National Oceanic and Atmospheric Administration (NOAA) Satellite and Information Service, 216
 - neato, 131
 - Nessus, 59, 60–72, 205
 - adding plug-ins for, 60, 60
 - analyzing vulnerabilities reported, 71
 - animating packets, 65–66, 65
 - dissecting vulnerability assessments, 61–62
 - exploring remaining activity, 66–67
 - filtering traffic based on destination port, 66–67, 67, 68
 - finding and removing port scans, 63–64, 63
 - identifying ports, 68–72
 - viewing packet length visualizations, 62–63, 63
 - NessusWX, 60
 - network
 - attacks, using distributed sensors to monitor widespread, 111–112
 - data, 4, 9
 - flows, 43, 120
 - capturing, 121*n*
 - management, security visualization and, 210
 - operations center, 204
 - protocols, 36–44
 - application layer, 36–38
 - data link layer, 41–44
 - network layer, 40–41
 - transport layer, 38–40
 - reconnaissance, 35
 - scanning output, visualizing, 56–57
 - topology information, for signature tuning, 151
 - traffic, correlation to machine process, 112, 113
 - network layer, in protocol hierarchy, 40–41
 - Nielsen, Jakob
 - Designing Web Usability*, 225
 - Homepage Usability*, 225
 - Nmap, 43, 46, 72, 205
 - comparing visual fingerprints of Unicornscan and, 55–56
 - NOAA (National Oceanic and Atmospheric Administration) Satellite and Information Service, 216
 - nodes, 41
 - configuration, 136
 - in link graphs, 128
 - noise
 - inserted into security data, 166
 - filtering out, 214
 - nominal data types, 6–7
 - NOP (no operation) instruction, hex 90 (0x90) for, 116*n*
 - Norman, Donald (*The Design of Everyday Things*), 225
 - North, Chris, 220

North, Stephen, 220
NVisionIP, 223

O

objects, interacting with, 16–20
occlusion
 attacks, 166, 166
 with windshield wiper effect,
 167–168, 167, 168
 overcoming through zooming, 46–51
 in parallel coordinate plots, 46
Ohno, Kazuhiro, 111, 220
OllyDbg debugger, 202
open password, in Microsoft Word,
 29–30
open ports, 57
open source movement, 210
 security visualization applications,
 221, 225
Open Systems Interconnection (OSI)
 reference model, 36
optical illusions, 173*n*
ordinal data types, 6–7
organizational mission, 3D visualiza-
 tion for mapping attacks to,
 117–118, 118
OSI (Open Systems Interconnection)
 reference model, 36
outbound traffic
 analyzing with firewall logs, 140–145
 monitoring, 207
 separating from inbound traffic in
 Metasploit, 79

P

p0f, 48
packet
 byte structure, 114, 115, 116
 encapsulation, 37, 37
 headers, viewing data in, 44–45
 length visualization, 78, 78
 for home ISP connection dataset,
 86–87, 86
 with Nessus, 62–63, 63
 sniffers, 46
packets, 37
 animating with Nessus, 65–66, 65
 byte frequency distribution of, 176
 capturing incoming, 84
 color for printable ASCII bytes in, 79

 dissecting hexadecimal, 43
 fragmented, 88–89, 89
 length of, 88
 occlusion attacks using, 166
 RAM buffers for storing data,
 189–190
Packit, 164
PacSec, 227
parallel coordinate plot visualization
 attacks on labeling, 164–165,
 164, 165
 for big-picture analysis, 84
 confirming port scan, 64
 drawbacks of, 93
 ICMP responses to UDP packet,
 102–103
 occlusion in, 46
 for viewing packet header data,
 44–45
parsing
 datasets, 189
 log files, 160
password protection, in Microsoft
 Word, 29–30
 binary visualization of, 31
payload, 72
 tricking programs into sending, 87
 in UDP packets, 98
 visual analysis of malicious, 79
penetration testers, 205
performance bottlenecks, 195
pf2csv.pl, 130
phishing emails, 162
physical location, using 3D visualiza-
 tion for mapping attacks to,
 117–118, 118
Piccolo toolkit, 225
pie graphs, 108, 109
ping command, 144
ping of death, 88
Plaisant, Catherine, 219
plug-ins, for Nessus, 60, 60
policy for firewall, 127
port numbers, 39
 53 (DNS traffic), 144
 135 (DCOM services), 69
 445 (Windows file sharing), 69
 512 (syslog), 144
 1025 (Microsoft RPC service), 97
 1434 (SQL Server), 98

- port scanning, 35, 120
 - filtering responses from, 48
 - finding and removing with Nessus, 63–64
 - network traffic level and attack detection, 44
 - Nmap for, 43
 - visualizing, 44–58
 - assessing header fields, 51, 52–53, 54–55
 - comparing visual fingerprints of Nmap and Unicornscan, 55–56
 - mapping packet data, 44
 - network scanning output, 56–57
 - overcoming occlusion through zooming, 46–51
 - viewing header data with parallel coordinate plot, 44–45, 47
 - Portall system, 112
 - ports
 - blocked state for, 57
 - closed, 57
 - listening, port scan probes for, 61
 - PortVis system, 114
 - Pouvesle, Nicolas, 60
 - PowerArchiver, 30
 - preattentive processing, 4, 5
 - predicate node, in link graph, 131, 132
 - process-to-process communication, analysis, 112–113
 - progress bar, 13
 - protocol analysis tool. *See* Wireshark
 - protocol hierarchy
 - application layer, 36
 - data link layer, 41–44
 - network layer, 40–41
 - transport layer, 38–40
 - protocols, 36
 - prototypes, 192
- R**
- R Graph Gallery, 108*n*
 - R Project, 108*n*
 - Radical Software Group, 221
 - RAM
 - buffer, 189
 - for visualization and analysis, 207
 - ranking items, hierarchical data structure for, 7
 - Rao, Ramana, 219
 - ratios, 4*n*
 - RECON, 227
 - records, in dataset, 193
 - relationships, link graphs for showing, 128
 - reliability, TCP header for, 38
 - Request For Comments (RFC), 39
 - 791 (Internet Protocol), 40
 - resolution, constraints on visualization system displays, 167
 - resources, visualization system need for, 198–199
 - Retina, 60*n*
 - reverse engineering of software, 202–204
 - RFC (Request For Comments), 39
 - 791 (Internet Protocol), 40
 - Rheingans, Penny, 220
 - Robertson, George, 219
 - rootkits, 106
 - Ross, Keith (*Computer Networking*), 36
 - round-off attacks, 170–172
 - routers, 42
 - RUMINT, 224
 - dynamic exploration with, 61–62
 - for home ISP connection dataset analysis, 83
 - interface, 62, 192
 - markers on side panes, 66
 - packet slider bar, 87, 87
 - RAM buffer for storing packet data, 189–190
 - and sensor logs, 104
 - with Wireshark, 98
 - Russell, Ryan (*Hack Proofing Your Network*), 79
- S**
- Sandalski, Stou, 57
 - Sands, David (*Understanding Intrusion Detection Through Visualization*), 225
 - sanitized data analysis, 113–114
 - Sasser worm, 111
 - scientific visualization, 2
 - scripts, 191
 - secure coding practices, 177, 193
 - Secure Sockets Layer (SSL), 38

- SecureScope visualization
 - framework, 117
- security
 - data
 - library of, 210–211
 - unifying streams, 214
 - logs, for Honeynet data, 120
 - researchers, goal of, 14
 - resources on, 226–227
 - and system design, 176–177
 - tools, 227
- Security and Usability* (Cranor and Garfinkel), 226
- Security Incident Fusion Tools (SIFT)
 - research project, 223
- security research needs
 - application layer visualization
 - support, 207
 - attacker identity, 214–215
 - collaboration, 211
 - creating library of security data, 210
 - creating library of visualization systems, 211
 - cross-disciplinary, 215–216
 - database security, 206
 - filtering improvements, 214
 - game platform security, 206
 - memory visualization and analysis, 207
 - metadata analysis, 205
 - mobile device security, 206
 - network operations center, 204
 - new challenges, 197–199
 - computer resource requirements, 198–199
 - IPv6, 198
 - malicious visualization, 199
 - offensive tools, 204–205
 - outbound data flow monitoring, 207
 - reverse engineering of software, 202–204
 - security visualization in
 - classroom, 204
 - spam analysis, 205
 - visual cryptanalysis, 200–202
 - visualization for end users, 208
 - VoIP, 205
 - webserver security, 206
 - wireless security visualization, 205
- security visualization
 - 3D visualization to map attacks to
 - physical location and organizational mission, 117–118, 118
 - antivirus applications effectiveness, 108, 110
 - dissecting behavior of Microsoft Word document, 29–32
 - extended timelines to observe
 - Honeynet trends, 120–121, 121
 - human attention in, 26
 - monitoring widespread network attacks with distributed sensors, 111–112, 111
 - multiple views, 119, 119
 - packet byte structure, 114, 115, 116
 - process-to-process communication analysis, 112–113, 113
 - sanitized data analysis, 113–114
 - and Sony rootkit, global spread of, 106, 107
- security visualization systems
 - attacks, 161, 163–175
 - autoscale, 169–170, 170
 - labeling, 164–165, 164, 165
 - occlusion, 166, 166
 - round-off, 170–172
 - tainted data, 174
 - windshield wiper, 167–168, 167, 168
 - building, 193
 - in classroom, 204
 - creation process, 183
 - dataflow design, 189–190
 - datastream review, 185–187
 - interaction design, 191–193
 - process overview, 184
 - technology assessment, 187–188
 - user analysis, 184–185
 - visualization design, 190–191
 - defending, 175–179
 - diversity of windows, 175–176
 - with filtering, 177, 178, 179
 - integrity protection, 176
 - secure coding practices, 177
 - user training on attack detection, 177
 - documentation for, 195
 - testing and evaluating, 194–195
- security-in-depth approach, 127

- Seesoft system, 32, 33
- semantic
 - information, 185
 - scaling technique, 50
 - structure of document, carriage
 - returns and line feeds to
 - see, 25
- Sendmail log, 212–213
- sensors, distributed, for monitoring
 - widespread network attacks, 111–112
- SequoiaView filesystem browser, 14
 - color encoding in, 17–18, 18
- server, misconfiguration of, 144
- set LHOST command (Metasploit), 75
- set PAYLOAD command (Metasploit), 74
- shellcode, 79
- ShmooCon, 227
- Shneiderman, Ben, 152, 219
 - information visualization mantra, 14–15, 15, 191
 - TreeMaps, 160
- show exploits command (Metasploit), 73
- show options command (Metasploit), 73, 74
- show payloads command (Metasploit), 74–75
- SIFT (Security Incident Fusion Tools)
 - research project, 223
- signature
 - matching, 25–26
 - and intrusion detection systems, 208
 - tuning
 - process, 154–156
 - with TreeMaps, 150–151, 153
- signature-based IDSs, 150
- signatures, 26
- Silence on the Wire* (Zalewski), 48
- situational awareness, 14
- Slagell, Adam, 220
- Slashdot, 210
- small multiples, 11, 11
- smart books, 26–29
- SmartMoney, Map of the Market, 7*n*
- Snort, 150
- social networks, 9
- software
 - ease of installation, 193
 - reverse engineering of, 202–204
- Solid Mux Server, 100
- Sony rootkit, visualizing global
 - impact of, 106, 107
- source
 - addresses, visualizing connections
 - between destination addresses and, 129–130, 130
 - IP address, 92
 - node, in link graph, 131, 132
 - ports
 - on attacker’s machine, 47
 - for TCP, 54
 - socket, for Metasploit, 76–77
- source-based analysis, of TreeMap, 156–157, 156
- spam, 162
 - analysis of, 205
- SPAN (Switched Port ANalyzer)
 - port, 121*n*
- spear phishing emails, 162
- Spinning Cube of Potential Doom, 172
 - wire diagram, 172
- Spitzner, Lance, 120
- Splunk, 212, 213
- Spotfire, 19*n*
- spring model, 128, 129
- SQL
 - injection, 206
 - slammer worm, 100
- SSH server, attacker scan for, 146, 147
- SSL (Secure Sockets Layer), 38
- Starfield Technologies, Traffic Facts, 3*n*, 170
- starplots, 10–11, 10
 - small multiples with, 11
- Stasko, John T., 219, 220
- status bar, brushing to display information in, 16–17, 17
- Steffen, Joseph, 32
- subgraphs, 146
- Sumner, Eric, 32
- Switched Port ANalyzer (SPAN)
 - port, 121*n*
- Swivel, 211
- Symposium on Usable Privacy and Security, 226
- Sysinternals, 208
 - File Monitor, 209
- syslog, 144

- system
 - files, 21
 - response, to user interaction, 12–13

T

- tables of data
 - analyzing, 2–3, 96–97
- tainted data attack, 174
- target
 - machines, vulnerability to attack, 155
 - node, in link graph, 131, 132
- TCP. *See* Transmission Control Protocol (TCP)
- tcpdump, 44
- technology assessment, 187–188
- testing, visualization system, 194–195
- text files
 - binary visualization of, 29
 - multiple columns to display large documents, 32, 33
 - structure of, 22–32
- text rainfall, 70, 71
 - for UDP packet, 101, 101
- 3D visualization, to map attacks to physical location and organizational mission, 117–118, 118
- threshold filter, 158–159
- TIFF file format
 - binary visualization of photo, 28
 - relative size, 27
- Time-based Network Traffic Visualizer (TNV), 224
- Time-to-Live (TTL) field, 54, 90
 - attacker constraint on, 175
- Toledo, Juan, 222
- tooltips, for labeling information, 50
- ToorCon, 227
- TOS (Type of Service) field, 88
- traceroute command (Unix), 41
- tracert command (Windows), 41
- Transmission Control Protocol (TCP), 38, 90
 - analysis, 92–97, 93, 94, 95
 - header format, 39
 - packet length, 86
 - ports, 91, 91
 - behavior of, 54
 - sequence numbers, 91, 91
 - session, 38

- targeted ports, 96
- three-way handshake
 - requirement, 86
- transport layer, in protocol hierarchy, 38–40
- tree data, 4, 7
- TreeMaps, 7, 8
 - analysis, 153–159
 - alert threshold, 158–159
 - destination-centric, 157–158, 158
 - source-based, 156–157, 156
 - constructing, 152–153, 152, 153
 - disadvantage for log analysis, 160
 - for SequoiaView, 14
 - signature tuning with, 150–151
 - for Snort alert log, 154
- trends, evaluating other disciplines for, 215–216
- triple, 152
- trojan ports, 144*n*
- trust, phishing attack success and, 162
- TTL (Time-to-Live) field, 54, 90
 - attacker constraint on, 175
- Tufte, Edward, 218
 - The Visual Display of Quantitative Information*, 11
- tuple, 5
- .txt file extension, 22
- type command (Metasploit), 75
- Type of Service (TOS) field, 88

U

- UDP. *See* User Datagram Protocol (UDP)
- Understanding Intrusion Detection Through Visualization* (Axelsson and Sands), 225
- undirected graphs, 9
- Unicornscan, 51
 - comparing visual fingerprints of Nmap and, 55–56
- University of Maryland, 225
- Unix
 - CRLFs in, 25*n*
 - file types, 22
- unsolicited network traffic, analysis, 84
- User Datagram Protocol (UDP), 38, 90
 - analysis, 98–103, 99
 - header format, 39

- User Datagram Protocol (UDP),
 - continued*
 - packet length, 86, 86
 - ports, 91, 91
 - text rainfall, 101, 101
 - users
 - analysis of, 184–185
 - feedback from, 194
 - interaction with interface, 16–20, 191–192
 - role in visualization system development, 184
 - training on attack detection, 177
 - visualization for, 208
- V**
- vertical port scan, 120
 - vertices, in graph data, 9
 - video game platforms, security concerns, 206
 - Viégas, Fernanda B., 219
 - Virtual Network Computing (VNC) server, 74
 - VisFlowConnect, 223
 - visual cryptanalysis, 200–202
 - The Visual Display of Quantitative Information* (Tufte), 11
 - visualization systems
 - evaluating, 194–195, 212
 - information resources, 218–219
 - classic research, 219
 - on security visualization, 220–225
 - VizSEC (Visualization for Computer Security), proceedings of Workshop on, 220
 - VNC (Virtual Network Computing) server, 74
 - Voice over IP (VoIP), 205
 - von Braun, Joakim, 144*n*
 - vulnerability assessment tools, 59
- W**
- Walker, Kenneth, 122, 220
 - web
 - browsers, 37
 - resources, Request for Comments (RFC) process history, 39
 - webservers, 37
 - and security, 206
 - website usage statistics, visualization vs. table of data, 2–3
 - Welchia worm, 97, 111
 - well-known port range, 120
 - Wget, 170
 - What the Hack, 227
 - white noise, 31
 - Wikipedia, 36
 - Wilkinson, Leland (*The Grammar of Graphics*), 218
 - Windows Distributed Component Object Model (DCOM) services, port 135 for, 69
 - Windows Explorer, directory hierarchy, 8
 - Windows file sharing, port 445 for, 69
 - Windows file types, 21–22
 - Windows Reverse Shell, 74
 - windshield wiper attacks, 167–168, 167, 168
 - wireless security visualization, 205
 - Wireshark, 44, 83, 97
 - filtering in, 192–193
 - protocol parsers, 190
 - RUMINT with, 98
 - to view network packets, 54, 54
 - Workshop on Visualization for Computer Security (VizSEC), proceedings of, 220
 - worms
 - Deadhat, 97
 - Doomjuice, 97
 - lifespan of worms, viewing, 121
 - Sasser, 111
 - SQL slammer, 100
 - Welchia, 97, 111
 - Writing Secure Code* (Howard and LeBlanc), 177
- Y**
- Yurcik, William, 220
- Z**
- Zalewski, Michal (*Silence on the Wire*), 48
 - ZoneAlarm, 209
 - zooming
 - to overcome occlusion, 46–51
 - in on TCP destination ports, 50
 - and visualization applications, 12