NUMBERS AND SYMBOLS

* -property
  of BLP model, 245
  in Chinese Wall model, 282
3gpp (Third Generation Partnership Project), 617–619
4758, IBM
  API attack on, 551–552
  high-end physically secure processors, 486–487
  how to hack, 491–492
5000 series microcontroller, 495–496
9/11 terrorist attacks
  security engineering conclusions, 891
  security engineering framework, 5
  terror, justice and freedom, 769–771

A
A5 algorithm, 613–617
AACS (Advanced Access Content System), 701–703
Abadi, Martin, 180
  absolute limits, 57–59
  abstract networks, 564–565
  access control, 93–96
  Apple’s OS/X, 101–102
  capabilities, 103–104
  environmental creep, 125–126
  further reading, 127–128
  groups and roles, 98
  hardware protection, 113–117
  introduction, 93–96
  lists, 99
  mandatory, 239
  middleware, 107–110

in multilateral security. See multilateral security
  operating system, 96–97
Orange Book evaluation classes, 871
remedies, 124
research problems, 127
sandboxing and proof-carrying code, 110–111
search terms and location data, 782–783
smashing the stack, 118–119
social networking security, 740–741
summary, 126
technical attacks, 119–121
trusted computing, 111–113
Unix OS security, 100–101
user interface failures, 121–122
virtualization, 111
what goes wrong, 117–118
why so many things go wrong, 122–124
Windows added features, 104–107
Windows basic architecture, 102–103
access control lists (ACLs)
  defined, 99
Unix OS security, 100–101
Windows added features, 104–107
access tickets, 202–203
access triples
  in Clark-Wilson, 320
  defined, 97
accessory control
  copyright protection and, 684, 723–725
  defined, 69
account master file, 318
accountability, intelligence, 788–789
accounting systems. See bookkeeping systems
ACID (atomic, consistent, isolated and durable), 190–191
ack wars, 580
ACLs (access control lists)
defined, 99
Unix OS security, 100–101
Windows added features, 104–107
Acorn Rise Machine (ARM) processors, 116
acoustic side channels, 542–543
Acquisti, Alessandro, 233
acting managers, 98
active attacks
defined, 304–305
emission security, 538–542
Active Directory, 105
Adams, John, 820–821, 824
additive stream ciphers, 162
address hijacking, 636–637
address resolution protocol (ARP), 635
addresses
vs. phone numbers, 204
stability of, 208–209
Adleman, Len, 171
Adler, Andy, 480
admissibility of evidence, 806–807
Advanced Access Content System (AACS), 701–703
advanced electronic signature, 807
Advanced Encryption Standard (AES)
defined, 153–155
history of cryptography, 135
adverse selection, 223
adware
defined, 648
Google security, 737
AES (Advanced Encryption Standard)
defined, 153–155
history of cryptography, 135
affect heuristic
defined, 27
psychology of political violence, 772
affective systems vs. cognitive systems, 26–27
AFIS (automatic fingerprint identification systems), 464–466
aggregation
attacks, 297
control, 289
MLS systems problem, 268–269
Agrawal, Rakesh, 543
aimbots, 732–733
Akerlof, George, 223
alarms
attacks on communications, 383–386
feature interactions, 382–383
how not to protect a painting, 379–380
overview, 378–379
sensor defeats, 380–382
Albert, Reka, 675
ALE (annual loss expectancy), 846–847
alert toolbars, 47
algorithms
AES, 613–617
cut-and-rotate, 691–692
DSA, 177
KEA, 175
key scheduling, 167
Pagerank, 737
rendezvous, 200–201
RSA, 171–173
Serpent, 153
alias band structures, 439
alterations, security printing, 441–443
Ames, Aldritch, 278
Ames, Stan, 280
amplifiers, smurf, 639
Amulet, 116
analysis framework, 4
anchoring effect, 25
Anderson, James, 242
Anderson, John, 555
Anderson, Margo, 307
Angola, MiG-in-the-middle attack, 73–74
annual loss expectancy (ALE), 846–847
anomaly detection, 661–662
anonymity
defined, 14
emailing, 747–749
inference control problems in medicine, 293–295
phone calls, 751–753
prepaid phones and, 612–613
privacy technology, 745–746
web browsing, 749–751
anonymous remailers
defined, 573
privacy technology, 748–749
answering machine attacks, 603
anthropometry, 464
anti-evidence seals, 449
antifuse devices, 497–498
anti-gundecking measures, 448–449
antijam techniques, 567–571
anti-piracy trade organizations, 686
anti-radiation missiles (ARMs), 575–576
anti-virus products
backscatter and, 643
malware countermeasures, 651
anycast, 641
API (application programming interface)
attacks, 547–548
further reading, 557
introduction, 547–548
on operating systems, 554–555
research problems, 557
on security modules, 548–554
summary, 555–557
Apple
  online rights-management, 706–707
OS/X access control, 101–102
application programming interface (API) attacks. See API (application programming interface) attacks
application relays, 655–657
applications
  access control levels, 93–94
  redundancy levels, 198
  web security. See web application security
architecture
  defense against network attacks, 657–660
  physical protection, 369
smartcards and microcontrollers, 501
team management, 850–851
argument size, 118–119
arithmetic, fundamental theorem of, 170
ARM (Acorn Rise Machine) processors, 116
ARMs (anti-radiation missiles), 575–576
ARP (address resolution protocol), 635
Arrow, Kenneth, 217
Art of Deception (Mitnick), 19
Asbury, David, 470
Asch, Solomon, 28
Asonov, Dmitri, 543
ASs (Autonomous Systems), 635
assumptions
  changing environment and protocols, 79–80
  in Common Criteria, 875
  cultural and naming, 206–207
  formalizing logic, 87–91
  reflection attacks and trust, 77
assurance. See also system evaluation and assurance
  conclusions, 890
  evolution and security, 868–869
  growth, 866–868
  perverse economic incentives, 858–860
  process, 863–866
  project, 860–863
  security and, 767–768
assurance requirements
  Common Criteria, 875
  defined, 3–4
atomic, consistent, isolated and durable (ACID), 190–191
atomic bomb security. See nuclear command and control
attack in depth, 162
attacks
  active, 304–305
  aggregation, 297
API. See API (application programming interface) attacks
  based on psychology, 18–22
  biometrics, 477–478
  against block ciphers, 145–146
  chosen protocol, 80–82
  on communications, 383–386
  on distributed systems. See distributed systems
  electronic and information warfare. See electronic and information warfare
  emission security, 544–546
  evaluating attackers, 492–493
  on fingerprint verification, 468
  hacking cryptoprocessors, 488–492
  hacking smartcards, 502–512
  home banks and money laundering, 358–361
  man-in-the-middle, 73–76
  master key, 374
  message manipulation, 78–79
  network. See network attack and defense
  online game cheating, 730–732
  password entry, 54–56
  password storage, 56–57
  phishing. See phishing
  phone metering, 596–599
  phone signaling, 599–601
  phone switching and configuration, 601–603
  reflection, 76–78
  replay, 83
  side channel, 542–543
  smashing the stack, 118–119
  social-engineering, 40–42
special purpose primitives, 178–179
  strength of, 181–182
asymmetric information, 223
asymmetric primitives, 138
asymmetry and usability, 17–18
AT&T
  fraud by, 626
  unlawful surveillance, 781–782
ATMs (automatic teller machines)
  in bank example, 6
  basics, 334–337
  fraud, 337–341
  incentives/injustices, 341–343
  overview, 333–334
  password stealing, 42–43
atomic, consistent, isolated and durable (ACID), 190–191
atomic bomb security. See nuclear command and control
attack in depth, 162
attacks
  active, 304–305
aggregation, 297
API. See API (application programming interface) attacks
  based on psychology, 18–22
  biometrics, 477–478
  against block ciphers, 145–146
  chosen protocol, 80–82
  on communications, 383–386
  on distributed systems. See distributed systems
  electronic and information warfare. See electronic and information warfare
  emission security, 544–546
  evaluating attackers, 492–493
  on fingerprint verification, 468
  hacking cryptoprocessors, 488–492
  hacking smartcards, 502–512
  home banks and money laundering, 358–361
  man-in-the-middle, 73–76
  master key, 374
  message manipulation, 78–79
  network. See network attack and defense
  online game cheating, 730–732
  password entry, 54–56
  password storage, 56–57
  phishing. See phishing
  phone metering, 596–599
  phone signaling, 599–601
  phone switching and configuration, 601–603
  reflection, 76–78
  replay, 83
  side channel, 542–543
  smashing the stack, 118–119
  social-engineering, 40–42
special purpose primitives, 178–179
  strength of, 181–182
asymmetric information, 223
asymmetric primitives, 138
asymmetry and usability, 17–18
AT&T
  fraud by, 626
  unlawful surveillance, 781–782
ATMs (automatic teller machines)
  in bank example, 6
  basics, 334–337
  fraud, 337–341
  incentives/injustices, 341–343
  overview, 333–334
  password stealing, 42–43
atomic, consistent, isolated and durable (ACID), 190–191
atomic bomb security. See nuclear command and control
attack in depth, 162
attacks
  active, 304–305
aggregation, 297
API. See API (application programming interface) attacks
  based on psychology, 18–22
  biometrics, 477–478
  against block ciphers, 145–146
  chosen protocol, 80–82
  on communications, 383–386
  on distributed systems. See distributed systems
  electronic and information warfare. See electronic and information warfare
  emission security, 544–546
  evaluating attackers, 492–493
  on fingerprint verification, 468
  hacking cryptoprocessors, 488–492
  hacking smartcards, 502–512
  home banks and money laundering, 358–361
  man-in-the-middle, 73–76
  master key, 374
  message manipulation, 78–79
  network. See network attack and defense
  online game cheating, 730–732
  password entry, 54–56
  password storage, 56–57
  phishing. See phishing
  phone metering, 596–599
  phone signaling, 599–601
  phone switching and configuration, 601–603
  reflection, 76–78
  replay, 83
  side channel, 542–543
  smashing the stack, 118–119
  social-engineering, 40–42
attacks (continued)
SWIFT and, 331–333
on tachographs, 398–402
technical access control attacks, 119–121
terror, justice and freedom. See terror, justice and freedom
tracker, 298
trusted path, 42–43
user interface failures, 121–122
valet, 68
attributes in Windows architecture, 102
attribution errors, fundamental, 27
attribution in BMA model, 289
audio copyrighting, 689–690
audit based control, 300–301
audit trails, 318
auditors
banking crime, 326
control tuning and corporate governance, 839
security project management, 819
authentication
automatic teller machines, 6
with biometrics. See biometrics
CDA, 356–357
DDA, 356
definitions, 12–13
encryption key management protocols, 82–87
GSM security mechanisms, 609–611
SDA, 352–356
seals as, 435
simple protocols, 66–69
two-channel, 49–50
two-factor, 47–48
unconditionally secure, 420–422
authentication vector AV, 618
authenticators, 420
authenticity, 14
authoritarian regimes, 798–800. See also terror, justice and freedom
authority, social psychology and, 28–29
authorization, 419–420
autokeying, 169
automated biometrics. See biometrics
automated face recognition, 462–464
automatic fingerprint identification systems (AFIS), 464–466
automatic fraud detection, 346–347
automatic teller machines (ATMs). See ATMs
automated teller machines (ATMs)
automatic upgrade problems, 268
Autonomous Systems (ASs), 635
availability heuristic, 25
avalanche effect, 153
average solution time of DES, 158
Axelrod, Bob, 226–227
Ayres, Ian, 368
behavioural economics. See also economics
perceptual bias and, 24–26
privacy and, 232–233
Bellare, Mihir, 164
Bell-LaPadula (BLP) security policy model. See
BLP (Bell-LaPadula) security policy model
Bellovin, Steve, 49
beneficiary-encrypted records, 294
Bentford’s law, 662
Benji the Binman, 20
Berlin, Sir Isaiah, 240
Bertillon, Alphonse, 464
Bertillonage, 464
BGP (Border Gateway Protocol), 635–636
Blatto, Benazir, 741
Blatto, Bilawal, 741
Biba, Ken, 250–251
Biba model, 250–252
bigotry and psychology of political violence,
773
Biham, Eli, 540, 615
bilinear pairing, 179
billing mechanisms, 627–630
BIN (bank identification number), 201–202
biometrics, 457–458
Bertillonage, 464
crime scene forensics, 469–472
face recognition, 461–464
fingerprint, 464–466
fingerprint and identity claims, 466–469
further reading, 482
handwritten signatures, 458–461
introduction, 457–458
iris codes, 472–475
other systems, 476–477
research problems, 482
summary, 481
voice recognition, 475–476
what goes wrong, 477–481
birthday theorem
biometrics vulnerabilities, 479
defined, 142–143
birthmarks, software, 682
Biryukov, Alex, 614
Bishop, Matt, 761
bitting, 373
Black Chambers, 776
Blacker, 253
black/red separation, 530–531
Blair, Tony, 290
democratic response to terrorism, 776
electronic elections security, 762
export control, 796
Blaze, Matt
Clipper chips, 793
master key attacks, 374
policy languages, 109
bleeding edge, 727–728
anonymous email, 747–749
anonymous web browsing, 749–751
computer games, 728–734
confidential and anonymous phone calls,
751–753
eBay, 735–736
elections, 759–763
e-mail encryption, 753–754
further reading, 765–766
Google, 736–739
introduction, 727–728
privacy technology, 745–747
putting privacy technology together,
757–759
research problems, 764–765
social networking sites, 739–744
steganography and forensics
countermeasures, 755–757
summary, 764
web applications, 734–735
Bleichenbacher, Daniel, 173
Blind signatures, 178
blind write-up, 268
block ciphers
chaining, 161
defined, 130–132
getting hash functions from, 165–169
history of cryptography, 134–135
in random oracle model, 144–146
SP-networks, 149–153
block size, 150
blockers, 694
blogs, 727–728
Bloom, Paul, 26–27
BLP (Bell-LaPadula) security policy model
alternatives, 248–250
Biba model and Vista, 250–252
classifications and clearances, 243–245
compartmentation and, 277–281
criticisms, 246–248
information flow control, 245–246
overview, 242–243
blue boxes, 600
Bluetooth, 668
Blu-ray, 701–704
BMA (British Medical Association) model
overview, 282–284
pilot implementations, 289–290
privacy issues, 290–293
security policy, 287–289
threat model, 284–287
bodily measurement identification, 464
Boebert, Earl, 249
Boehm, Barry, 828
Bond, Mike
attacks on IBM 4758, 551
Bond, Mike  (continued)
differential protocol attacks, 552
neotactics, 732
PIN mailers, 445
xor-to-null-key attacks, 550
Boneh, Dan
bilinear pairing, 179
differential fault analysis, 540
timing analysis, 531
book copyrighting, 688
bookkeeping systems. See also banking and
bookkeeping
access control, 97
in bank example, 6
double-entry, 316
origins, 315–316
Border Gateway Protocol (BGP), 635–636
Borisov, Nikita, 666
born classified, 429
botnets
DDoS attacks, 640
defined, 199
herders, 634
Storm network, 649
bots, 732–733
bottom pins, 372
Bowen, Debra, 761
Bowes, Walter, 408–409
Bradshaw, Frank, 280
brain
mental processing, 26–27
type S vs. type E, 28
what it does better than computers, 30
what it does worse than computers,
23–24
Brandeis, Louis, 809
Brewer, David, 281
Brin, David, 811
British electronic elections security, 762
British Medical Association (BMA) model. See
BMA (British Medical Association) model
broadcast encryption, 701–703
broken window theory, 369–370
Brooks, Fred, 851, 881
Brown, Gordon, 776
browsers
anonymous web browsing, 749–751
phishing alert toolbars, 47
search terms and location data access,
782–783
security. See web application security
using password database, 44–45
Brumley, David, 531
BSD layer, 101–102
Buchanan, James, 774
bugs
fixing, 836–837
OS access controls, 117–118
patching cycle, 229–230
project assurance, 860–863
why Windows is so insecure, 230–232
bugs, surveillance. See wiretapping
bugtraq, 885–886
Bühler, Hans, 792
builds, regression testing, 829
bulla, 315, 434
bump keys, 373
bumping, 372–376
burglar alarms, 10. See also alarms
Burma, censorship in, 799
burned in, 490
burn-through, 576
Burrows, Abadi and Needham (BAN) logic, 87,
88–89
burst communications, 570–571
burst transmission, 567
bus encryption, 495–496
Bush, President George W., 776
business process re-engineering, 841
businesses and emission security, 545–546
Byzantine failure model, 193–194
C
cache misses, 531
cache poisoning, 643
Caesar, Augustus, 130
Caesar, Julius, 130
Caldicott, Dame Fiona, 294
California, 761–762
call detail record (CDR), 628
call forwarding, 606
callback mechanisms
defined, 188
phone phreaking, 606
call-sell operation
defined, 607
prepaid phones, 613
Camp, Jean, 836
Campbell, Duncan, 528, 803
Canadian Trusted Products Evaluation Criteria
(CTPEC), 872
canaries, 124
CAP (Chip Authentication Program)
challenge-response authentication, 72–73
chosen protocol attacks and, 81–82
defined, 48
capabilities
names as, 202–203
OS access controls, 103–104
Windows feature, 104–107
Capability Maturity Model (CMM), 849,
864–866
capitalist bombs, 584
Capstone chips
defined, 494
medium security processors, 496–499
CAPTCHAs (Completely Automated Public
Turing Tests to Tell Computers and Humans
Apart)
defined, 59–60
what brain does better than computer, 30
capture errors, 23–24
capture-recapture statistics, 142
card verification values (CVVs)
ATM fraud, 339–340
credit card forgery, 345
defined, 203
Cardan grille, 713
Caridi, Carmine, 702
Carroll, Lewis, 15
cars
challenge and response, 70
simple authentication protocols, 68–69
Carter, President Jimmy, 776
Cary, Chris, 697
cascade problem, 262–263
cash, digital
defined, 178
electronic elections and, 759–760
cash machines. See automatic teller machines
(ATMs)
caveats in classifications and clearances, 244
CBC (cipher block chaining), 161
C-C3 (Counter-Command, Control and
Communications) operations, 563
CCM, 164–165
CDA (combined data authentication), 356–357
CDI, constrained data items, 319
CDMA (code division multiple access), 570
CDR (call detail record), 628
cell phones. See mobile phones
cells
in inference control theory, 297
suppression, 299–300
censorship
with application relays, 656
cache poisoning and, 643
social networking security, 742
terror, justice and freedom, 797–803
census data inference control, 296–297
centralization and privacy, 292–293
centrally assigned passwords, 37
certificate revocation lists, 674
certificates
naming, 200
public key, 104
rights erosion and Common Criteria, 880
certification
CMM, 865
defined, 179–181
certification authority (CA), 180
certificational threats, 146, 169
CERTs (Computer Emergency Response
Teams), 118, 753, 885–886
CFB (cipher feedback), 163
chaff, 575
chain of custody, 804
chaining, 161
challenge and response
IFF systems, 580
protocols, 69–73
change permissions attribute, 102
channels, covert
in MLS systems, 263–265
side channel attacks, 542–543
channels, side
attacks, 523
optic, acoustic and thermal, 542–543
chargebacks, 350
Chaum, David, 747–748, 759
cheating
electronic elections security, 760–763
fraud. See fraud
in online games, 730–732
check clearing, 460
check digits, 202
check fraud
identity failure leading to, 205
security printing, 442
checkpoints, 197
checksummers, 650
chief programmer teams, 851
child pornography, 797, 801–803
children and social networking security,
739–740
China, 797–799
Chinese Wall model, 281–282
Chip Authentication Program (CAP)
challenge-response authentication, 72–73
chosen protocol attacks and, 81–82
defined, 48
chipcards, 347–348. See also smartcards
chipping, 397
chirp, 570
chops, 442
chosen ciphertext attacks, 145
chosen distortion attacks, 717
chosen drug attacks, 304
chosen plaintext attacks, 145
chosen plaintext/ciphertext attacks, 145
chosen protocol attacks, 80–82
chosen-key attacks, 167
Christmas virus, 645
Cinderella attacks, 191–192
cipher block chaining (CBC), 161
cipher feedback (CFB), 163
cipher instruction search attack, 496
signals intelligence techniques, 563–565
surveillance. See surveillance
Communications Assistance for Law
Enforcement Act (CALEA), 777
communications intelligence (Comint)
defined, 560
on foreign targets, 785–787
communications security (Comsec), 560
community detection, covert, 564
Comp128 hash function, 610
compartmentation, 277–281
Compartmented Mode Workstations (CMWs)
MLS Unix and, 253–254
policy, 249
compatibility
value of lock-in, 221–223
Vista and, 106
competitive equilibrium, 220
complacency cycle, 820–821
complementary cell suppression, 299–300
Completely Automated Public Turing Tests to
Tell Computers and Humans Apart (CAPTCHAs)
defined, 59–60
what brain does better than computer, 30
complexity
API attacks caused by, 556
as enemy of security, 890–891
composability in MLS systems, 261–262
composite modes of operation, 164–165
compromising emanations
defined, 523
first known use, 525
computational security, 420–422
Computer Emergency Response Teams
(CERTs), 118, 753, 885–886
computer forensics, 803–805
computer systems
bank, 317–319
gaming, 728–734
privacy, 808
what brain does better than, 30
what brain does worse than, 23–24
computing, trusted, 111–113
Confsec (communications security), 560
conclusions, 889–891
concurrency
API attacks on OS, 554–555
distributed systems, 186–192
conditional access mechanisms, 690
conference calls, 606
Confidential clearance, 243–244
confidentiality
defined, 13–14
multilevel, 240
phone call privacy technology, 751–753
configuration attacks, 601–603
configuration management
defined, 242
network security, 652–654
confinement problem, 113–114
conflicts of interest, 819
conflictual hostile review, 882
conforming, social psychology and, 28
confusion as cipher property, 149
confusion pricing, 625
conical scan, 574
conjunction, 211
consent, patient. See patient consent
consistent in naming, 203–204
contactless payment
defined, 357–358
smartcards, 499
Content Protection & Copy Management
(CPCM), 698
content scrambling system (CSS), 698–701
contextual security information, 37–38
contractual hostile review, 882
control, access. See access control
control, accessory
copyright protection and, 684, 723–725
defined, 69
control, inference. See inference control
control, nuclear. See nuclear command and
control
current communications, 562
Control Objectives for Information and related
Technology (CobiT), 838–839
control tuning, 838–839
control words, 691
table, 301–302
convergence, 190
Conway, John, 75
COPAC system, 87–88
copy generation control
defined, 683
watermarks and, 711–712
copyright and DRM, 679–680
accessory control, 723–725
attacks on hybrid scrambling systems, 693–697
audio, 689–690
books, 688
copyright marking scheme applications, 718
copyright marking schemes attacks, 714–718
defined, 680–681
DVB, 697–698
DVDs, 698–701
further reading, 726
general platforms, 704–710
HD-DVD and Blu-ray, 701–704
information hiding, 710–711
information hiding techniques, 712–714
cracking defined, 37 passwords, 57
cramming defined, 611 economics of telecom security, 626
Creative Commons licenses, 722
credit cards automatic fraud detection, 346–347 concurrency problems, 187
cross-border fraud, 348
cross-site scripting (XSS) defined, 734
crowd, social networking security, 743
crowd detection, 524–525
cryptanalysis attacks on communications, 565–566 defined, 130
differential, 152–153 linear, 151
cryptographic keys. See keys, encryption cryptography, 129–130
Advanced Encryption Standard (AES), 153–155
asymmetric crypto primitives, 170
asymmetric crypto primitives, strength of, 181–182
asymmetric primitives, 138
attacks on IBM 4758, 551–552
automatic teller machines, 6
based on discrete logarithms, 173–177
based on factoring, 170–173
certification, 179–181
cover-text, 712
covertness, 571
covans, Steven, 470
Cowburn, Russell, 444
Coyne, James, 820
CPCM (Content Protection & Copy Management), 698
Index — C–D 1007

defined, 2
in designing internal controls, 322–323
digital signatures, 147–149
eyearly block cipher, 134–135
eyearly stream cipher, 131–132
elliptic curve, 179
Feistel ciphers, 155–160
further reading, 183–184
hash functions, 165–169
historical background, 130–131
introduction, 129–130
mobile phone security failures, 621
modes of operation, 160–165
one-time pad, 132–134
one-way functions, 136–138
physical tamper resistance. See physical tamper resistance
public key certificates, 104
public key encryption and trapdoor one-way permutations, 146–147
random functions, 140–143
random generators, 143–144
random oracle model, 138–140
random permutations, 144–146
research problems, 183
simple authentication, 66–69
special purpose primitives, 178–179
summary, 182
symmetric crypto primitives, 149–153
cryptology, 130
cryptomathematics, 427
cryptoprocessors
defined, 507
how to hack, 488–492
CSS (content scrambling system), 698–701
CTPEC (Canadian Trusted Products Evaluation Criteria), 872
ctrl-alt-del, 42–43
Cuba
MIG-in-the-middle attack, 73–74
nuclear command and control evolution, 418–419
cultural assumptions in naming, 206–207
culture
medical privacy distinctions, 308
psychology of political violence, 772–773
currency in virtual world economy, 733
curtained memory, 115
Curtis, Bill, 842–843
customers
education as phishing countermeasure, 45–46
social psychology and, 29–31
cut and choose protocols, 426
cut-and-rotate algorithm, 691–692
CVVs (card verification values)
ATM fraud, 339–340
credit card forgery, 345
defined, 203
D
Daemon, Joan, 153
Dallas 5000 series, 495–496
Danezis, George, 465
Darwin, Charles, 465
DAT (digital audio tape), 689
data concurrency problems, 186–187
data detective work, 303
Data Encryption Standard (DES) crypto research and, 792–793
defined, 155–160
history of cryptography, 135
data matching, 783
data mining
redlining and, 663
terror, justice and freedom, 783–784
data protection laws
defined, 284
terror, justice and freedom, 808–812
data subjects
defined, 284
privacy and data protection, 808
database access controls, 107–108
Daugman, John, 377, 473
DDA (dynamic data authentication), 356
DDoS (distributed denial-of-service) attacks
defined, 199
network attack and defense, 640–642
DDT (delayed data transfer), 78
deadlock, 189–190
Debreu, Gérard, 217
defense in depth
lessons from electronic warfare, 590–591
smartcard security, 513
Defensible Space, 369
defensive programming, 541
de-identified information
defined, 294
inference control and, 302–303
delayed data transfer (DDT), 78
degulation, 211
delete attribute, 102
demilitarized zone (DMZ), 657–658
DeMillo, Richard, 540
democracy
electronic elections security, 760–763
response to terrorism, 775–776
deniability, 745
denial of service attacks. See service denial attacks
Denning, Dorothy
cryptography, 180
information warfare, 588
lattice model, 280
dependability, economics of, 228–234
deperimeterization
defense against network attacks, 659–660
defined, 638
VPNs and, 670
DES (Data Encryption Standard)
crypto research and, 792–793
defined, 155–160
history of cryptography, 135
dES keys, 551–552
descriptors in classifications and clearances, 244
design
iterative, 827–829
top-down, 826–827
design, environmental
physical protection, 369
prepayment meter protection, 395
design errors
ATM fraud, 340
passwords, 37–39
detection
designing internal controls, 322–323
intrusion, 652
network problems with, 664–665
network security and, 660–663
deter–detect–alarm–delay–respond, 366
deterministic signature schemes, 147–148
deterrence
of fingerprint verification, 468–469
physical protection, 368–370

depleted uranium, 350
detonator command and control, 424–425
development of secure systems management. See managing development of secure systems
DHCP (Dynamic Host Configuration Protocol), 635
diagrams, 135
dial tone stealing, 598
dial-through fraud, 603–604
dictionaries
attacks, 57
communications intelligence on foreign targets, 787
defined, 565
differential cryptanalysis, 152–153
differential fault analysis, 540
differential power analysis
defined, 509, 533–534
differential protocol analysis, 552–553
differential trace, 533
Diffie, Whitfield, 174–175, 759
Diffie-Hellman protocol, 174–175
diffusion, 149
Digimarc, 715–716
digital audio tape (DAT), 689
digital cash
defined, 178
electronic elections and, 759–760
digital copyright marks, 439
digital elections, 759–763
Digital Millennium Copyright Act (DMCA)
copyright policy, 718–719
defined, 620–621
digital radio frequency memory (DRFM), 576
digital rights management (DRM). See DRM (digital rights management)
Digital Signature Algorithm (DSA), 177
digital signatures
admissibility of evidence, 807
defined, 130, 147–149
digital tachographs and, 405
ElGamal, 176–177
history of cryptography, 138
postage meters, 409–410
digital tachographs, 403–408
digital technology and GSM security mechanisms, 608–617
digital versatile disks (DVDs)
copyright, 698–701
HD-DVD and Blu-ray, 701–704
digital video broadcasting (DVB), 697–698
dining cryptographers’ problem, 747–748
dining philosophers’ problem, 189–190
direct inward system access (DISA), 603
direct sequence spread spectrum (DSSES), 567, 569–570
directed energy weapons, 584–586
direction finding, 562
directional transmission links, 567
directory-enquiry services, 605
Direct-recording electronic (DRE) voting systems, 761
DISA (direct inward system access), 603
discrete logarithms, 173–177
discretionary access control
defined, 246
Orange Book evaluation classes, 871
discriminating monopolist, 218
discrimination and redlining, 663
displacement activity, 822–823
distortions in copyright marking, 716–717
distributed denial-of-service (DDoS) attacks
defined, 199
network attack and defense, 640–642
distributed systems, 552
distributed systems, 185–186
concurrency, 186–192
defined, 2
distributed systems view of naming, 200–204
fault tolerance and failure recovery, 192–199
further reading, 213
introduction, 185–186
name types, 211
naming, 200
naming vulnerabilities, 204–211
research problems, 212–213
summary, 211–212
distribution, trusted, 270
diversification, key. See key diversification
DMCA (Digital Millennium Copyright Act)copyright policy, 718–719
defined, 620–621
DMZ (demilitarized zone), 657–658
DNS (Domain Name System) security
defined, 635–636
networks and, 643
Domain Name System (DNS) cache poisoning
censorship with, 799
defined, 643
DNS (Domain Name System) security
defined, 635–636
networks and, 643
Domain and Type Enforcement, 249–250
Domain Name System (DNS) cache poisoning
censorship with, 799
defined, 643
Domain Name System (DNS) security
defined, 635–636
networks and, 643
domains
Orange Book evaluation classes, 871
partitioning in Windows architecture, 102–103
in type enforcement model, 249
dominant strategies, 224
dominant strategy equilibrium
defined, 224
the prisoner’s dilemma, 225–226
dongles, 683
doppler radar, 574
double-entry bookkeeping, 316
Downey, Peter, 279
DRE (Direct-recording electronic) voting
systems, 761
DRFM (digital radio frequency memory), 576
Drive-By Pharming, 636
driver pins, 372
Drivers’ Privacy Protection Act, 810
DRM (digital rights management)
copyright and. See copyright and DRM
economics of, 233–234
in mobile phones, 620
with Trusted Computing, 111–113
Dror, Itiel, 470
DSA (Digital Signature Algorithm), 177
DSSS (direct sequence spread spectrum), 567, 569–570
dual control
defined, 316
in designing internal controls, 321–324
dual-use goods, 796
due diligence
Common Criteria limitations, 880
risk management, 848
Dunn, Patricia, 19
durability in non-convergent state, 191
DVB (digital video broadcasting), 697–698
DVDs (digital versatile disks)
copyright, 698–701
HD-DVD and Blu-ray, 701–704
dynamic data authentication (DDA), 356
Dynamic Host Configuration Protocol (DHCP), 635
E
EAL (evaluation assurance level), 874–876
eavesdropping
electromagnetic, 524
password entry, 55
protocols and risks, 65–66
TLS network security, 672
eBay, 735–736
ECB (electronic code book), 160–161
Echelon
communications intelligence on foreign
targets, 786–787
defined, 565
ECMs (entitlement control messages), 691
e-commerce history, 316–317
economics, 215–216
antiterrorism, 770
classical, 216–220
Common Criteria limitations, 880
credit card fraud, 347–348
DDoS attacks, 641
further reading, 235–236
game theory, 223–228
history of government wiretapping, 778–779
incentives. See incentives
information, 220–223
intelligence strengths and weaknesses, 787–789
introduction, 215–216
perceptual bias and behavioural, 24–26
phone company fraud, 625–627
PKI limitations, 674–675
political violence causes, 772
public-choice, 774–775
research problems, 235
security, 2
of security and dependability, 228–234
Economics (continued)
security engineering conclusions, 891
summary, 234–235
tale of three supermarkets, 816–818
telecom billing mechanisms, 627–630
telecom system security, 624–625
of telecom system security, 624–625
in virtual worlds, 733–734
Edelman, Ben, 51
EDI (electronic data interchange), 318
education, 886
EEPROM, 503
EES (Escrowed Encryption Standard)
crypto wars, 789
defined, 496
EFF (Electronic Frontier Foundation), 158
efficiency
MLS systems practical problems, 269
wholesale payment systems, 329
efficient, Pareto, 218
egress filtering
defense against network attacks, 657
defined, 642
Eisenhower, Dwight D., 770
election security, 759–763
electricity
alarms/barriers, 382–383
metering, 392–393
electromagnetic analysis, 534
electromagnetic compatibility (EMC), 524
electromagnetic eavesdropping attacks, 324
electromagnetic pulse (EMP), 584–586
electronic and information warfare, 559–560
electronic attack, 560
international use interaction, 572–573
communication systems, 561–563
communication systems attacks, 565–566
communication systems protection, 567–572
directed energy weapons, 584–586
further reading, 593
IEDs, 582–584
IFF systems, 579–582
information warfare, 586–592
introduction, 559–560
in military base example, 7
research problems, 592
signals intelligence techniques, 563–565
summary, 592
surveillance and target acquisition, 574–579
electronic attacks, 560
first known use, 525
electronic banking. See also banking and bookkeeping
automatic fraud detection, 347
history of e-commerce, 316–317
home banks and money laundering, 358–361
electronic code book (ECB), 160–161
electronic data interchange (EDI), 318
electronic election security, 759–763
Electronic Frontier Foundation (EFF), 158
electronic intelligence (Elint), 560
electronic keysearch machines, 158–159
electronic locks, 376–378
electronic patient record (EPR), 287–288
electronic protection, 560
Electronic Signature Directive, 807
Electronic Signatures in Global and National Commerce (‘ESIGN’) Act, 807
electronic support, 560
electronic voting, 759–763
elementary sets, 297
elevation prompt, 105
ElGamal digital signature scheme, 176–177
Elint (electronic intelligence), 560
elliptic curves
cryptography, 179
defined, 173
email
anonymous, 747–749
data mining, 784
cryptography, 753–754
malware in attachments, 651
TLS network security, 672
emanations, compromising
defined, 523
electronic attacks, 560
electronic banking. See also banking and bookkeeping
automatic fraud detection, 347
history of e-commerce, 316–317
home banks and money laundering, 358–361
electronic code book (ECB), 160–161
electronic data interchange (EDI), 318
electronic election security, 759–763
Electronic Frontier Foundation (EFF), 158
electronic intelligence (Elint), 560
electronic keysearch machines, 158–159
electronic locks, 376–378
electronic patient record (EPR), 287–288
electronic protection, 560
Electronic Signature Directive, 807
Electronic Signatures in Global and National Commerce (‘ESIGN’) Act, 807
electronic support, 560
electronic voting, 759–763
elementary sets, 297
elevation prompt, 105
ElGamal digital signature scheme, 176–177
Elint (electronic intelligence), 560
elliptic curves
cryptography, 179
defined, 173
email
anonymous, 747–749
data mining, 784
cryptography, 753–754
malware in attachments, 651
TLS network security, 672
emanations, compromising
defined, 523
electronic attacks, 560
embedded systems
API attacks, 548
multilevel security, 261
embedded text, 712–714
active attacks, 538–542
attacks, 544–546
further reading, 546
history, 524–526
introduction, 523–524
leakage through RF signals, 534–538
optic, acoustic and thermal side channels, 542–543
research problems, 546
summary, 546
technical surveillance and countermeasures, 526–529
EMV standards
API attacks, 553–554
defined, 351–357
EMV standards
API attacks, 553–554
defined, 351–357

Index

evaluation. See also system evaluation and assurance
Common Criteria, 873–876
Common Criteria shortcomings, 876–880
overview, 869–870
by relying party, 870–873
evaluation assurance level (EAL), 874–876
evaluation certificates, 516
evergreening, 721
everyone in Windows architecture, 103
evidence, rules of, 803–807
evolutionary development, 828–829
evolutionary games, 226–228
e-war, 591–592. See also electronic and information warfare
exchange control fraud, 332–333
execute attribute, 102
exploits, online games, 730–732
export controls, 796–797
export licensing, 793–794

F
face recognition, 461–464
Facebook, 739–744
facial thermograms, 477
facial thermograms, trusted, 369
failure
defined, 193
model, 834
recovery, 192–199
fall-stop processors, 170–173
false alarms
information warfare, 590
intrusion detection limitations, 663
sensor defeats, 380–381
false terminals, 341
Fanning, Shawn, 707
Farley, Mark, 282
farming, 733
fast-flux, 634
Faulds, Henry, 465
fault analysis, differential, 540
fault induction attacks, 506
fault injection, 862
fault masking, 833
fault tolerance, 192–199
fault tree analysis, 831
faults, 193
fearmongering
democratic response to terrorism, 775–776
psychology of political violence, 773
security engineering conclusions, 891
FEC (Federal Election Commission), 761
Federal Election Commission (FEC), 761
Federal Rules of Evidence, 806
feedback
complacency cycle and risk thermostat, 821
project assurance, 863
feedforward mode, 165
Feistel ciphers, 155–160
Fellwock, Perry, 786
Feltan, Ed, 721
Fenton, Jeffrey, 279
Ferraiolo, David, 250
Fiat, Amos, 701
FIB (Focused Ion Beam Workstation), 507–509
files
in access triples, 97
integrity levels, 106
file-sharing, peer-to-peer
censorship and, 801–803
copyright and DRM, 707–709
fill gun, 485
filtering
censorship, 797–803
defined, 652
network security, 654–660
financial fraud. See fraud
financial intrusion detection, automatic, 346–347
finger command, 118–119
fingerprints
biometrics, 464–466
crime scene forensics, 469–472
identity claims and, 466–469
information hiding, 710
finished messages, 670–671
FIPS certification scheme, 493
firewalls, 654–660
fist, 476
fixed-point attacks, 167
flares, 578
Flask security architecture, 258–259
Flickr, 742
flooding, SYN, 638–639
floor limits
credit card fraud, 344
defined, 187
Florida elections, 760–763
Fluhrer, Scott, 666
FMEA (failure modes and effects analysis), 831
Focused Ion Beam Workstation (FIB), 507–509
FOIA, 244
follower jamming
countermeasures, 576–577
defined, 568
For Official Use Only (FOUO), 244
foreign target communications intelligence, 785–787
forensic phonology, 475–476
forensics
crime scene, 469–472
crime, 737
handwritten signatures, 458–461
security packaging and seals. See security
printing and seals
formal methods of project assurance, 862
formal verification protocol, 87–91
format string vulnerability, 120
fortified password protocols, 49
forward security
defined, 169
key establishment, 175–176
FOUO (For Official Use Only), 244
foxes vs. hedgehogs, 240
FPGA security, 496–499
fragile watermarks, 711
framing, 25
France
chip cards, 347–348
smartcards, 350–351
Franklin, Matt, 179
fraud
ATM, 337–341
automatic credit card fraud detection, 346–347
banking and bookkeeping, 325–326
click, 737
credit card, 344–345
on eBay, 735–736
economics, 347–348
mobile phone cloning, 607–608
mobile phone security, success or failure?, 621–622
online credit card fraud, 348–350
phone company, 625–627
rates, 460
SWIFT vulnerabilities, 331–333
free market economy, 216–217
free software, 882–884
free speech, 742. See also censorship
FreeBSD
Apple’s OS/X, 101–102
defined, 100
freedom, terror and justice. See terror, justice
and freedom
freedom and privacy protection, 745–747
freedom-of-information law, 811–812
frequency hoppers, 567–568
freshness in biometrics, 478
Friedman, William, 476, 792
friendship trees, 564
Friendster, 741–742
functional separation, 321–322
functionality and evaluation, 859–860
functions
one-way, 136–138
random, 140–143
fundamental attribution errors, 27
fundamental theorem of arithmetic, 170
fundamental theorem of natural selection, 867
funded organizations as attackers, 493
Furby toys, 529
fuzzers, 850

G
Galois Counter Mode (GCM), 164–165
Galton, Francis, 462, 465
game theory, 223–228
games, computer, 728–734
Garfinkel, Simson, 308
Gates, Bill, 682, 686
GCHQ (Government Communications Headquarters), 786
GCM (Galois Counter Mode), 164–165
gender, usability and psychology, 27–28
general trackers, 298
Generalized Noninterference, 249
generators, random, 143–144
Generic Software Wrapper Toolkit (GSWTK), 554–555
ghosting
defined, 400
digital tachographs and, 403
Gilbert, Daniel, 25
glitch attacks, 540
glitches, emission security, 526
global names, 202
Global Positioning System (GPS), 572–573
Global System for Mobile Communications (GSM)
mobile phone security, 608–617
success or failure?, 621–622
glue, secure packaging, 444–445
glue logic, 510–511
goats, 461
Goguen, Joseph, 248
Goldberg, Ian, 666
Goldilocks pricing, 347
Goldwasser, Shafi, 172
Gollman, Dieter, 84–85
Gong, Li, 701
Gonggrijp, Rop, 373
Google
hacking, 634, 736
privacy and data protection, 812
web application security, 736–739
Gore, Al, 796
Göttrup, Henry, 350
Government Communications Headquarters (GCHQ), 786
governments
emission security and, 544–545
open-source software, 883–884
perverse economic incentives and assurance, 860
phone security and, 615–617
risk management, 820
terror, justice and freedom. See terror, justice and freedom
GPS (Global Positioning System), 572–573
grabbers, 65–66
Gramm-Leach-Bliley Act, 320–321
granularity of middleware, 108–109
Grapp, Fred, 34
Greenberg, Jeff, 772–773
Grew, Nathaniel, 465
groups
defined, 12
name types, 211
operating system access controls, 98
in RBAC, 250
Windows added features, 104–105
GSM (Global System for Mobile Communications)
mobile phone security, 608–617
success or failure?, 621–622
GSWTK (Generic Software Wrapper Toolkit), 554–555
Guanella, Gustav, 569
guard band receivers
defined, 575
information warfare, 590
guessability and passwords, 52
gundecking, 449
Gutmann, Peter, 231
Guy, Mike, 56–57

H
hacking
cryptoprocessors, 488–492
Google, 634, 736
home banks and money laundering, 358–359
information warfare, 587–588
smartcards, 502–512
wall hacks, 732
Hagar, Nicky, 565, 786
Hagelin, Boris, 792
Halifax Share Dealing Services, 42
Hall, Chris, 531
Hamming weight, 532
hand-geometry readers, 464
handwritten signatures, 458–461
hard kills, 561
hardware protection access control, 93–94, 113–117
Harrison-Ruzzo-Ullman model, 249
hash functions
Comp128, 610
defined, 130, 165–169
in random oracle model, 140–143
universal, 164
watermarks and copy generation management, 711
hash values, 136
hate speech and censorship, 801–803
hawk-dove game, 227
hazard elimination, 830–831
HCI (human-computer interaction)
defined, 23
gender and, 27–28
HD-DVD copyrighting, 701–704
HE (home environment), 618
head vs. heart in mental processing, 26–27
Health Insurance Portability and Accountability Act (HIPAA)
defined, 282–283
hospital example, 10
privacy and data protection, 810
healthcare BMA model. See BMA (British Medical Association) model
healthcare example, 9–10
heart vs. head in mental processing, 26–27
hedgehogs vs. foxes, 240
Heintze, Nevin, 409
Hellman, Martin, 174–175
Henry, Sir Edward, 465–466
herders, botnet, 634
HERF (high-energy RF) devices, 585
Herodotus, 712
Herschel, William, 465
heuristic, affect
defined, 27
psychology of political violence, 772
heuristic, availability, 25
hiding information. See information hiding
high water mark principle, 247
high-end physically secure processors, 486–492
high-energy RF (HERF) devices, 585
high-tech attacks, 402
Hijack attacks
address, 636–637
defined, 530
Hill, Sir Rowland, 408
hill-climbing attacks, 480
HIPAA (Health Insurance Portability and Accountability Act)
defined, 282–283
hospital example, 10
privacy and data protection, 810
hippus, 474
Hiroshima, 417–418
Hirshleifer, Jack, 229, 232
history of bookkeeping, 315–316
history of command and control, 417–420
history of cryptography
asymmetric primitives, 138
early block cipher, 134–135
early stream cipher, 131–132
one-time pad, 132–134
one-way functions, 136–138
overview, 130–131
history of e-commerce, 316–317
history of emission security, 524–526
history of government wiretapping, 776–779
history of malicious code, 644–645
history of malware, 647–650
history of MLS systems, 252–257
history of physical tamper resistance, 485–486
history of security printing and seals, 434–435
history of smartcards and microcontrollers, 500–501
HLR (home location register), 609
HMAC (hash MAC) function, 168
Hobbes, Thomas, 228
Hoeffler, Anne, 772
Holland, 79–80
Hollywood, 680
holograms, 438
home banking and money laundering,
358–361
home environment (HE), 618
home location register (HLR), 609
home security engineering example, 10–11
HomePlug, 668–669
homomorphism, 172
honey traps
defined, 287
intrusion detection, 662
hospital security engineering example, 9–10
hostile reviews, 882
hot credit cards
defined, 187
hot card lists, 344
Howard, Michael, 119, 850
HTTP Digest Authentication, 70
Huang, Bunnie, 721
Human Error (Reason), 832
human intelligence, 787–788. See also brain
human motivations, 270–271
human-computer interaction (HCI)
defined, 23
gender and, 27–28
human-rights workers, 752–753
Hupp, Jon, 644
hybrid scrambling techniques, 697–698
Hyman, Bruce, 758
IBM 4758
- API attack on, 551–552
  - high-end physically secure processors, 486–487
- how to hack, 491–492
IBM AS/400 series systems, 104
iButton, 494–495
ICMP (Internet control message protocol), 639
ID (identification)
  - cards, 206–207
  - face recognition, 461–464
  - naming, 200
  - through biometrics. See biometrics through voice recognition, 475–476
identify-friend-or-foe (IFF)
  - electronic and information warfare, 579–582
  - protocols, 73–76
  - reflection attacks and, 76–78
identity
  - defined, 13
  - escrow, 759
  - fingerprints and, 466–469
  - management, 178
  - naming and, 204–206
  - theft, 32
  - identity-based cryptosystems, 179
  - identity-based signature schemes, 179
  - ideology of phone phreaking, 600
IDO markings, 244
IEDs (improvised explosive devices), 582–584
IFF (identify-friend-or-foe)
  - electronic and information warfare, 579–582
  - protocols, 73–76
  - reflection attacks and, 76–78
IKE (Internet Key Exchange) protocol, 669
imperfect protection value, 305–306
impersonation in nuclear command and control, 420–421
implementations
  - of BMA model, 289–290
  - perverse economic incentives and assurance, 859
implied queries control, 300
impossible cryptanalysis, 152
impression spam, 737
improvement, Pareto, 218
improved explosive devices (IEDs), 582–584
IMSI (international mobile subscriber identification), 609
IMSI (international mobile subscriber identification)-catchers, 613
IMSI-catchers, 613
in-band signaling, 599–600
incentives
  - ATM, 341–343
  - defense against network attacks, 660
  - economics of security. See economics
intelligence strengths and weaknesses, 787–789
moral hazards, 823–824
online credit card fraud, 349
perverse economic and assurance, 858–860
phone billing mechanisms, 628
security engineering framework, 5
SPDC protection, 703–704
tamper-resistant devices and, 517
incidental complexity, 826
incompetent security managers, 823
inconsistent updates, 188
incremental development, 849
Independent Verification and Validation (IV&V), 872, 882
indirect names, 205
individual trackers, 298
indoctrination, 278
induction attacks, fault, 506
inertia in Common Criteria, 878–880
inexperienced security managers, 823
infallibility and fingerprint analysis, 471–472
inference control
  - defined, 277
  - generic approach limitations, 302–305
in medicine, 293–296
other applications of, 296–297
social networking security, 741–742
theory, 297–302
value of imperfect protection, 305–306
infinite units, 503
information economics, 220–223. See also economics
information flow control
  - in BLP security policy model, 245–246
  - lateral. See multilateral security
  - MLS systems practical problems, 268–269
  - restrictions, 8
information hiding
  - copyright marking scheme applications, 718
  - copyright marking schemes attacks, 714–718
  - defined, 710–711
  - techniques, 712–714
  - watermarks and copy generation
    - management, 711–712
Information Rules (Shapiro and Varian), 216
information security conclusions, 889–891
information superiority, 588
Information Technology Security Evaluation Criteria (ITSEC), 872
information warfare. See electronic and information warfare
infrared sensors, 380–381
infrared tokens, 66–69
Ingenico i3300, 353–354
ingress filtering, 657
inidicia, 148
initialization vectors, 161
injection, fault, 862
injustices, ATM, 341–343
inks, security printing, 438
insecure end systems, 603–605
insider fraud, 339. See also internal controls
inspections, security printing
costs and nature, 451–453
threat model, 437
instrument tampering, 401–402
insult rates, 460
insurance and risk management, 847
intaglio, 437
integer manipulation attacks, 120
integrity
in Biba model, 250–252
defined, 14
protection with SELinux, 258–259
Vista file integrity levels, 106
Intel processors and Trusted Computing, 114–116
intellectual property (IP) copyright policy, 718–722
intelligence agencies
communications intelligence on foreign targets, 785–787
multilevel security and, 270–271
signals intelligence techniques, 563–565
strengths and weaknesses, 787–789
surveillance tactics. See surveillance
intent in nuclear command and control evolution, 419–420
interface attacks, application programming. See API (application programming interface) attacks
interface design
password entry, 54
user interface failures, 121–122
interference cancellation, 572
internal controls
banking and bookkeeping, 320–324
reliability interaction, 821
risk management, 818–819
Internal Revenue Service (IRS) pretexting, 19–20
international mobile subscriber identification (IMSI), 609
international mobile subscriber identification (IMSI)-catchers, 613
International Telegraph Union (ITU), 777
International Traffic in Arms Regulations (ITAR), 796
Internet
censorship, 797–803
web application security. See web application security
worm, 645–646
Internet control message protocol (ICMP), 639
Internet Key Exchange (IKE) protocol, 669
Internet protocol (IP) addresses, 635
Internet protocol (IP) networks. See IP (Internet protocol) networks
Internet relay chat (IRC), 639
Internet Service Provider (ISP) surveillance
defined, 784–785
network neutrality and, 800–801
intrusion detection
network problems with, 664–665
network security, 660–663
invasive attacks, 509
inverse gain amplitude modulation, 576
inverse gain jamming, 576
Ioannidis, John, 667
IP (intellectual property) copyright policy, 718–722
IP (Internet protocol) addresses, 635
IP (Internet protocol) networks
DDoS attacks, 640–642
DNS security and pharming, 643
smurfing, 639–640
spam, 642–643
SYN flooding attacks, 638–639
voice over, 623–624
IPsec (IPsecurity), 669–670
IRC (Internet relay chat), 639
iris codes, 472–475
IRS (Internal Revenue Service) pretexting, 19–20
Iscoe, Neil, 842–843
ISO 9001 standard, 865
ITAR (International Trafficking in Arms Regulations), 796
iterative design, 827–829
ITSEC (Information Technology Security Evaluation Criteria), 872
ITU (International Telegraph Union), 777
iTunes rights-management, 706–707
IV&V (Independent Verification and Validation), 872, 882
i-war, 591–592. See also electronic and information warfare
jammers, 535
jamming
antijam techniques, 567–571
attacks on communications, 566
electronic attacks, 560–561
GPS, 572–573
lessons from electronic warfare, 590–591
multisensor issues, 578–579
surveillance and target acquisition, 575–577
jamming margin, 568
Java sandboxing, 110–111
Java Virtual Machine (JVM), 110–111
Jeffery, Ray, 369
Jeong, Hawoong, 675
Jevons, Stanely, 217, 220
jihadist websites and censorship, 801–802
jitterbugs
defined, 528
using against active attacks, 541
Jobs, Steve, 706
Johansen, Jon Lech, 699
Joint Tactical Information Distribution System (JTIDS), 571
Joint Tactical Radio System (JTRS), 581
Jonas, Jeff, 784
Jones, R. V., 789
journals
bank computer systems, 318
redundancy levels, 197
JTIDS (Joint Tactical Information Distribution System), 571
JTRS (Joint Tactical Radio System), 581
Judd, Dorothy, 341
jurisdiction rule, 89
justice, terror and freedom. See terror, justice and freedom
JVM (Java Virtual Machine), 110–111

K
Kaashoek, Frans, 646, 749
Kahn, David, 776, 786
Kahneman, Daniel, 24–25
Kain, Dick, 249
Karger, Paul, 248
Kasiski, Fredrich, 132
Kasumi, 617
Katz vs. United States, 777
KEA (key exchange algorithm), 175
Keller, Nathan, 615
Kelling, George, 369
Kelsey, John, 531
Kennedy memorandum, 418–419
Kerberos, 82–87
Kerckhoffs, Auguste, 884
kernel bloat, 123
key differs, 372–373
key diversification
defined, 67
formal verification limitations, 90–91
prepayment meters, 394
key escrow
crypto wars, 789–794
crypto wars significance, 794–796
protocols, 618
key establishment, 175–176
key exchange algorithm (KEA), 175
key exchange messages, 670–671
key fingerprints, 753
key log attacks
defined, 78
home banks and money laundering, 358–359
key memory, 487
key pins, 372
key recovery
attacks, 145
Clipper chips and, 793
key scheduling algorithm, 167
key updating, 169
keyloggers, 652
keys, encryption. See also cryptography
chosen protocol attacks and, 81–82
hacking cryptoprocessors, 488–492
management, 82–87, 407–408
public key certificates, 104
xor-to-null-key attacks, 549–551
keysearch machines, 158–159
keystream
generators, 143–144
hybrid scrambling attacks, 693–694
in OFB, 162
keyword filtering, 799
kiddieporn censorship, 802–803
Kilian, Joe, 164
kinegrams, 438
Klein, Daniel, 34
Kluksdahl, Normal, 820
knowledgeable insiders as attackers, 493
known plaintext attack, 145
Knudsen, Lars, 477
Kocher, Paul
cryptography, 130
smartcard hacking, 509
timing analysis, 531
Kohfelder, Loren, 180
Kömmerling, Oliver, 506
Krasner, Herb, 842–843
Kügler, Denis, 668
Kuhn, Markus
emission security, 526, 536
physical tamper resistance, 496
side channel attacks, 542
video scrambling, 692
Kuhn, Richard, 250
Kumar, Sandeep, 158

L
labeling
BLP model classifications and clearances, 243–245
in lattice model, 278–281
lag sequences, 576
Lamport, Leslie, 193
Lamport time, 192
Lampson, Butler, 665
LAN (local area network) security, 636–638
landing pads, 118
Landwehr, Carl, 117
laptop microphone bugs, 529
laser microphones
countermeasures, 528
defined, 527
Laser Surface Authentication, 444
lateral information flow. See multilateral security
lattice model
definition, 277–281
maximum order control and, 300
Law Enforcement Access Field (LEAF), 496–499
laws
admissibility of evidence, 806–807
copyright and DRM. See copyright and DRM
export control, 796–797
mobile phone locking, 620–621
privacy and data protection, 808–812
regulations. See regulations
LCD display eavesdropping, 535
leading edge trackers, 576–577
LEAF (Law Enforcement Access Field), 496–499
leakage
hybrid scrambling attacks, 694
through power and signal cables, 530–534
through RF signals, 534–538
LeBlanc, David, 119, 850
ledgers in bank computer systems, 318–319
Leeson, Nick, 325
legal claims and password design errors, 38
legal regulations. See regulations
legitimate relationships, 290
Lessig, Larry, 719
letterpress, 438
letters of guarantee, 332
levels
access control, 93
middleware and, 108–109
where redundancy is, 197–198
Levitt, Steven, 368
Lewis, Owen, 563
liability
ATM incentives/injustices, 341–343
Common Criteria limitations, 880
dumping, 360–361
handwritten signatures, 458
tamper-resistant devices and, 517–518
trusted interface problem and, 514
volume crime, 323–326
libraries, 850–851
license servers
MLS systems practical problems, 267–268
software copyright protection, 686
licensing
export control, 797
software copyright protection, 681–688
Windows media rights management, 705–706
Life on the Mississippi (Twain), 465
limited data sets, 294
Linden Labs, 204–205, 733
linear cryptanalysis, 151
linearization attacks, memory, 506
Linux
DVD protection, 700
multilevel security, 258–259
OS security, 100–101
vulnerabilities, 117–118
Lipton, Richard, 540
lists, access control. See ACLs (access control lists)
literary analysis, 476
LITS (Logistics Information Technology System), 255–256
lobbyists, IP, 720–722
local area network (LAN) security, 636–638
location
data access, 782–783
privacy, 616–617
theft deterrence, 368–369
lock-ins
pervasive economic incentives and assurance, 860
value of, 221–223
locks
electronic, 376–378
mechanical, 372–376
in mobile phones, 620–621
to prevent inconsistent updates, 188
Loewenstein, George, 233
logarithms, discrete, 173–177
logic of belief, 87
Logistics Information Technology System (LITS), 255–256
logistics systems, 255–256
London and changing environment protocols, 79
Longley, 548
look-down shoot-down systems, 577
loops in fingerprint analysis, 465
losses, risk management, 846–848
Loughry, Joe, 543
Love Bug virus, 646
low clock frequency, 503
low water mark principle, 251
low-probability-of-intercept (LPI) techniques. See LPI (low-probability-of-intercept) techniques
Index

L–M 1019

low-probability-of-position-fix (LPPF) techniques, 567
LPI (low-probability-of-intercept) techniques bugs, 528
defined, 567
history, 525
radio links, 8
LPPF (low-probability-of-position-fix) techniques, 567
Luby, Mike, 157
Luby-Rackoff theorem, 157
lunchtime attackers, 146

M
MAC (mandatory access control). See also MLS (multilevel security)
in BLP model, 246
defined, 239
Orange Book evaluation classes, 871
machinima, 733
MACs (message authentication codes) chosen protocol attacks and, 81
computing with hash functions, 168
defined, 163–164
history of cryptography, 136
in postage meters, 411–412
TLS network security, 670–671
Made for Adsense (MFA), 737
Mafia in malware history, 648–649
Mafia-in-the-middle attacks, 81–82
MagicGate, 512
Maguire, Steve, 849
maiden names in passwords, 37
mail guards, 252
mail order and telephone order (MOTO) transactions, 344
mail theft, 338–339
mailers, PIN, 445–446
maintenance, firewall, 638
malicious code history, 644–645
malicious exit node, 750
Malone, Gerry, 286–287
Malpighi, Marcello, 465
malware defined, 644–645
history, 647–650
mobile phone problems, 619
management designing internal controls, 320–324
encryption keys, 82–87
malware countermeasures, 651
roles, 98
security and, 767–768
trusted facility, 270
management, rights. See rights-management
managing development of secure systems, 815–855
further reading, 854–855
introduction, 815–816
iterative design, 827–829
lessons from safety critical systems, 829–834
methodology, 824–825
organizational issues, 819–824
parallelizing, 844–846
project requirements, 842–844
project risk management, 818–819
requirements evolution, 835–842
research problems, 853–854
risk management, 846–848
security projects, 816
security requirements engineering, 834–835
summary, 852–853
tale of three supermarkets, 816–818
team management, 848–852
top-down design, 826–827
Manber, Udi, 605
mandatory access control (MAC). See MAC (mandatory access control)
manglers, password, 43–44
man-in-the-middle attacks, 73–76
manipulation of Common Criteria, 878–880
Mantin, Itzhak, 666
Mark XII system, 580
marked text, 712
market dominance and Windows insecurity, 230–232
market failures
asymmetric information, 223
classical economics, 217–220
marking key, 712
marking schemes
applications, 718
attacks, 714–718
Marks, Leo, 132
masking, fault, 833
master key attacks
defined, 374–375
safety critical systems, 832–833
master keys
leakage, 694
management, 86–87
Mastercard, 351–357
master-secret keys, 671
materials control in security printing, 450–451
mathematics of cryptography. See cryptography
matrices, access control capabilities, 103–104
introduction, 96–97
matrix, payoff, 224
Matsui, Mitsuru, 617
Matsumoto, Tsutomu, 468
maximum order control, 300
Maybury, Rick, 96
Mayfield, Brandon, 470
Mazières, David, 646, 749
McGraw, Gary, 120, 850
McKie, Shirley, 469–471
McLean, John, 246–247
MD4, 167–168
MD5, 167–168
mean-time-before-failure (MTBF), 193
mean-time-to-repair (MTTR), 193
mechanical locks, 372–376
Media Key Block, 701–702
media’s role in anti-terror security, 775
medical inference control, 293–296
medical privacy in BMA model. See BMA
(British Medical Association) model
medium range ballistic missile (MRBM) treaty, 428
medium security processors, 494–499
meet-in-the-middle attacks, 551–552
memory
MLS systems practical problems, 269
overwriting attacks, 118–119
password design errors, 37
password difficulties, 33
smartcard architecture, 501
memory, curtained, 115
memory linearization attacks, 506
memory remanence, 490
men, gender usability and psychology, 27–28
Menger, Carl, 217, 220
mental processing, 26–27. See also brain
merchant discounts, 343
Mercuri, Rebecca, 761
Merritt, Michael, 49
Meseguer, Jose, 248
meshes
cryptoprocessor hacking, 491
smartcard hacking, 507–508
message authentication codes (MACs). See MACs (message authentication codes)
message content confidentiality, 14
message digests, 140
message meaning rule, 89
message source confidentiality, 14
messaging systems
in bank example, 7
manipulation, 78–79
recovery, 148
metadata, 113
meteor burst transmission, 570–571
metering attacks, 596–599. See also monitoring and metering
methodology, management
iterative design, 827–829
lessons from safety critical systems, 829–834
overview, 824–825
top-down design, 826–827
methods, formal in project assurance, 862
MFA (Made for Adsense), 737
Micali, Silvio, 172
microcontrollers
architecture, 501
history, 500–501
overview, 499
security evolution, 501–512
micropayment mechanisms, 629
microphone bugs, 526–529
microprinting, 438
Microsoft Passport, 46–47
microwave links, 611
middleperson attacks, 73–76
middleware
access control levels, 93–94
defined, 107–110
MIG-in-the-middle attacks, 73–76
Milgram, Stanley, 28–29
military
vs. civil uses in electronic and information warfare, 572–573
electronic and information warfare. See electronic and information warfare
nuclear command and control. See nuclear command and control
security engineering example, 7–9
millenium bug, 843
Miller, George, 23
Mills, Harlan, 828, 851
minutiae in fingerprints, 465
misidentification through fingerprint analysis, 469–472
mission creep, 305–306
misuse detection, 661
Mitnick, Kevin
phone phreaking, 602
pretexting, 19
mixes, 747–749
Mixmaster, 748–749
MLS (multilevel security), 239–240
Bell-LaPadula alternatives, 248–250
Bell-LaPadula criticisms, 246–248
Bell-LaPadula security policy model, 242–243
Biba model and Vista, 250–252
cascade problem, 262–263
classifications and clearances, 243–245
composability, 261–262
covet channels, 263–265
further reading, 272–273
future MLS systems, 257–261
historical examples of MLS systems, 252–257
information flow control, 245–246
introduction, 239–240
MLS implications, 269–271
polyinstantiation, 266–267
practical problems, 267–269
research problems, 272
security policy model, 240–242
summary, 272
virus threats, 265–266
mnemonic phrases for passwords, 36–37
mobile phones
3gpp, 617–619
cloning, 607–608
GSM security mechanisms, 608–617
platform security, 619–621
security success or failure?, 621–622
smartcard history, 500
telemeter system security, 606–607
VOIP, 623–624
modes of operation in cryptography, 160–165
Moreno, Khalid Shaikh, 787
money laundering and home banking, 358–361
money printing. See security printing and seals
monitoring and metering, 389–390
digital tachographs, 403–408
further reading, 414
introduction, 389–390
meter system, 393–395
postage meters, 408–412
prepayment meters, 390–392
research problems, 413–414
summary, 412–413
tachographs, 398–402
taxi meters, tachographs and truck speed
limiters, 397–398
utility metering, 392–393
what goes wrong, 395–397
monitors, reference, 114, 243
monopulse radars, 577–578
moral hazards
defined, 223
security project management, 823–824
Moreno, Roland, 350
Morris, Robert, 34, 645
Morse, Samuel, 317, 877
mortality salience, 773
mother’s maiden name in passwords, 37
motion detector defenses, 380–381
MOTO (mail order and telephone order)
transactions, 344
movement sensor defeats, 380–381
Moynihan, 270–271
MP3stego, 755
MRBM (medium range ballistic missile) treaty,
428
MTBF (mean-time-before-failure), 193
MTTR (mean-time-to-repair), 193
Mueller, John, 273, 775
mules, 360
Multics
multilevel security, 248
SCOMP, 252–253
multifunction smartcards, 80–82
multilateral security, 275–277
BMA model, 282–284
BMA pilot implementations, 289–290
BMA privacy issues, 290–293
BMA security policy, 287–289
BMA threat model, 284–287
Chinese Wall model, 281–282
compartmentation, 277–281
further reading, 310–311
generic approach limitations, 302–305
inference control in medicine, 293–296
inference control theory, 297–302
introduction, 275–277
other applications of inference control,
296–297
research problems, 310
residual problem, 306–309
summary, 309–310
value of imperfect protection, 305–306
multilevel security (MLS). See MLS (multilevel
security)
multiparty computation, 552–553
multiplicative homomorphism, 172
multisensor data fusion, 578–579
Munden, John, 342
Murdoch, Steve
application relays, 656
emission security, 526
security printing, 445
side channel attacks, 543
music industry
copyright and DRM, 689–690
DRM beneficiaries, 722–723
peer-to-peer file sharing censorship, 801
Musica, Philip, 327–328
mutable states and ACLs, 101
mutual authentication, 76–78
MySpace, 739–744
The Mythical Man Month (Brooks), 880
N
Nacchio, Joe, 781
Nagaraja, Shishir, 676
naive access control matrix, 96
Namibia MIG-in-the-middle attack, 73–74
naming
distributed systems view of, 200–204
overview, 200
types of, 211
vulnerabilities, 204–211
Naor, Moni, 701
Napster, 707–708
Narayanan, Arvind, 295
narrow pipes, 610
Nash, John, 225
Nash, Michael, 281
Nash equilibrium, 225
National Security Agency (NSA)
communications intelligence on foreign targets, 785–786
unlawful surveillance, 781–782
natural selection, fundamental theorem of, 867
Naval Research Laboratory (NRL), 254–255
NCP (Nexus Control Program), 113
near-field communications (NFC), 358
Needham, Roger
access control introduction, 96
on certification, 180
naming, 201
network protection with encryption, 665
steganography, 755
usability and psychology, 56–57
Needham-Schroeder protocol, 84–85
neotactics, 732
net neutrality, 797
Netherlands electronic elections security, 762
network attack and defense, 633–634
Bluetooth, 668
configuration management and operational security, 652–654
DDoS attacks, 640–642
detection problems, 664–665
DNS security and pharming, 643
filtering, 654–660
further reading, 678
HomePlug, 668–669
how worms and viruses work, 646–647
Internet worm, 645–646
introduction, 633–634
intrusion detection, 660–663
IPsec, 669–670
LANs, 636–638
malicious code history, 644–645
malware history, 647–650
peer-to-peer file sharing, 707–709
PKI, 672–675
protocol vulnerabilities, 635–636
research problems, 677–678
smurfing, 639–640
social networking security, 739–744
spam, 642–643
SSH, 665–666
summary, 676–677
SYN flooding attacks, 638–639
TLS, 670–672
topology, 675–676
Trojans, viruses, worms and rootkit countermeasures, 650–652
Trojans, viruses, worms and rootkits, 644
WiFi, 666–668
network externalities, 221
Network File System (NFS), 637
network neutrality, 800–801
network time protocol (NTP), 192
neutrality, net, 797
neutrality, network, 800–801
neutron bombs, 584
Newman, Mark, 564
Newman, Oscar, 369
news, role in anti-terror security, 775
Newsham, Peg, 786
Nexus Control Program (NCP), 113
NFC (near-field communications), 358
NFS (Network File System), 637
no read up (NRU) property, 245
no write down (NWD) property, 245
noise jamming, 573
nonces
defined, 67
key management with, 84
nonce-verification rule, 89
non-convergent state, 190–191
nondeducibility, 248–249
noninterference, 248–249
noninvasive attacks, 509–510
nonlinear junction detectors, 528
nonmonotonic, 255
nonproliferation controls, 791
non-repudiation, 343
Nonstop, 539
non-technical losses, 394
no-operation (NOP) commands, 118
NOP (no-operation) commands, 118
NRL (Naval Research Laboratory), 254–255
NRU (no read up) property, 245
NSA (National Security Agency)
communications intelligence on foreign targets, 785–786
unlawful surveillance, 781–782
NTP (network time protocol), 192
nuclear command and control, 415–417
evolution of, 417–420
further reading, 430–431
introduction, 415–417
military base example, 8
research problems, 430
secrecy or openness, 429–430
shared control systems, 422–424
summary, 430
tamper resistance and PALs, 424–426
treaty verification, 426
unconditionally secure authentication, 420–422
what goes wrong, 427–428
nuclear energy, 584
NWD (no write down) property, 245
nymservers, 748–749

OAEP (optimal asymmetric encryption padding), 172
Oberholzer, Felix, 234
object request brokers (ORBs), 109–110
O'Dell, Walden, 760
Odlyzko, Andrew, 232, 625
OFB (output feedback), 161–162
offender-rehabilitation laws, 812
Ogborn, Louise, 29
Ogden, Walter, 280
OGELs (Open General Export Licenses), 797
old data concurrency problems, 186–187
Olmstead vs. United States, 777
OMA (Open Mobile Alliance), 707
omertá, 226
one-time authentication codes, 420
one-time pads, 132–134
one-way encryption, 56–57
one-way functions
  defined, 136–138
  hash, 140–143
one-way homomorphism, 174
The Onion Router (Tor), 749–751
Onion Routing, 749–751
online activism and DDoS, 642
online businesses
  concurrency, 186
  credit card security, 346–347
  rights-management, 706–707
  online credit card fraud, 348–350
  online games security, 728–734
  online registration and copyrighting, 686–687
Open General Export Licenses (OGELs), 797
Open Mobile Alliance (OMA), 707
open PKI, 672
openness and nuclear command and control, 429–430
OpenNet Initiative, 763
open-source software, 229–230, 882–884
operating system access controls
  access control levels, 93–94
Apple’s OS/X, 101–102
  capabilities, 103–104
  groups and roles, 98
  lists, 99
  middleware, 107–110
  overview, 96–97
  sandboxing and proof-carrying code, 110–111
  trusted computing, 111–113
Unix OS security, 100–101
virtualization, 111
Windows added features, 104–107
Windows basic architecture, 102–103
operating system API attacks, 554–555
operational security
  in BMA model, 285
  defined, 20–21
network attack and defense, 652–654
password issues, 39
optic side channels, 542–543
optical probing
  defenses against, 542
smartcard hacking, 510
optical scanning, 761
optimal asymmetric encryption padding (OAEP), 172
Orange Book
  defined, 253
  evaluations by relying party, 871–873
ORBs (object request brokers), 109–110
organizational issues
  changes and naming, 202
  Common Criteria policies, 875
  managing change, 841–842
  managing development of secure systems, 819–824
  security projects, 819–824
organized crime
  Mafia-in-the-middle attacks, 81–82
  in malware history, 648–649
OS/X
  Apple’s, 101–102
  defined, 100
output feedback (OFB), 161–162
overflow vulnerabilities, 119–121
Ozment, Andy, 230
P
packaging
  security printing, 443–446
  video copyrighting and, 690
packet filtering, 654–655
Paganini, 689
Pagerank algorithm, 737
PALs (permissive action links), 424–426
PALs (prescribed action links), 424–426
PAN (primary account number), 334
Pancho, Susan, 84–85
paper money printing. See security printing and seals
PAPS (prescribed action protective system), 424
parallelizing security requirements engineering, 844–846
Pareto, Vilfredo, 218
Pareto efficient
  defined, 218
  the prisoner’s dilemma, 226
### Pareto improvement, 218

- Parsons, Captain Deak, 417–418
- partial band jamming, 568, 571
- partitioning
  - as active attack countermeasure, 304
  - virtualization, 111
- Passfaces, 59
- passivation layers, 504
- passive attacks, 530–534
- passive coherent location, 578
- passive eavesdropping, 672
- passwords
  - absolute limits and, 57–59
  - design errors, 37–39
  - difficulties remembering, 33
  - entry attacks, 54–56
  - entry reliability difficulties, 32–33
  - generators, 71–73
  - manglers, 43–44
  - naive choices, 34–35
  - operational issues, 39
  - phishing countermeasures, 43–50
  - phishing future, 50–52
  - protocols and eavesdropping risks, 65–66
  - sniffing attacks, 636
  - social-engineering attacks, 40–42
  - storage attacks, 56–57
  - trusted path, 42–43
  - usability and psychology, 31–32
  - user abilities and training, 35–37
- Pastor, José, 409
- patches
  - bug fixing, 836–837
  - defense against network attacks, 652–653
  - managing cycle, 229–230
  - penetrates-and-patch, 885–886
- patents, 721
- patient consent
  - active attacks and, 305
  - in BMA model, 288–289
  - current privacy issues, 291
  - patient record systems, 9
- Patriot Act, 779
- patriotism and psychology of political violence, 773
- paying to propagate state, 186–187
- payloads, 646–647
- payment, contactless
  - defined, 357–358
  - smartcards, 499
- Payment Card Industry Data Security Standard (PCI DSS)
  - defined, 349
  - WiFi network protection, 668
- payment protocols, 89–90
- payoff matrix, 224
- PayPal, 735–736
- pay-TV
  - copyright and, 690–691
  - DDT attacks, 78
  - hybrid scrambling attacks, 693–697
- PBXes (private branch exchange) systems, 603–604
- PCI DSS (Payment Card Industry Data Security Standard)
  - defined, 349
  - WiFi network protection, 668
- Pease, Marshall, 193
- peer-to-peer file sharing
  - censorship and, 801–803
  - copyright and DRM, 707–709
  - pen registers, 780
  - penetrates-and-patch, 885–886
  - peoples’ differences, 27–28
  - perceptual bias, 24–26
  - permissions, access control. See access control
  - permissive action links (PALs), 424–426
- permutations
  - random, 144–146
  - trapdoor one-way, 146–147
  - persistence in BMA model, 289
  - personal area networks, 668
  - persons, 12
  - perturbation, 301
  - Petitcolas, Fabien, 755
  - PETs (Privacy Enhancing Technologies), 293–295
- PGP (Pretty Good Privacy), 753–754
- phantom withdrawals
  - ATM fraud, 338–339
  - changing environment and protocols, 79–80
- pharming, 643
- phenotypic, 473
- phishing
  - in bank example, 6
  - countermeasures, 43–50
  - defined, 17, 21–22
  - eBay, 735–736
  - future, 50–52
  - home banks and money laundering, 359–361
  - social networking security, 743
  - social-engineering attacks and, 40–42
  - phone calls, anonymous and confidential, 751–753
- phone companies
  - fraud by, 625–627
  - network neutrality, 800
- phone numbers vs. computer addresses, 204
- phone phreaking
  - feature interactions, 605–606
  - insecure end systems, 603–605
  - metering attacks, 596–599
  - signaling attacks, 599–601
Index

switching and configuration attacks, 601–603

telecom system security, 596

photo ID recognition, 461–464

physical destruction
attacks on communications, 566
electronic attacks, 561

physical protection, 365–366

alarm feature interactions, 382–383
alarms, 378–379
attacks on communications, 383–386
defence, 368–370
electronic locks, 376–378
further reading, 388
how not to protect a painting, 379–380
introduction, 365–366
lessons learned, 386–387
mechanical locks, 372–376
research problems, 388
summary, 387–388
threat model, 367–368
threats and barriers, 366–367
walls and barriers, 370–372

physical tamper resistance, 483–485
evaluation, 492–494
further reading, 520–521
high-end physically secure processors, 486–492
history, 485–486
introduction, 483–485
medium security processors, 494–499
research problems, 520
smartcard and microcontroller architecture, 501
smartcard and microcontroller history, 500–501
smartcard and microcontroller security
evolution, 501–512
smartcards and microcontrollers, 499
state of the art, 512–514
summary, 520
what goes wrong, 514–518
what to protect, 518–519
picking locks, 372–373

'picture-in-picture' websites, 47
pin stacks, 372

PNs
ATM basics, 334–337
eavesdropping risks, 65–66
mailers, 445–446
retying, 55
translation, 335
pin-tumbler locks, 372–373
piracy
audio, 689–690
DVB, 697–698
hybrid scrambling attacks, 693–697
software, 682–688

Pitney, Arthur, 408–409

PKI (public key infrastructure), 672–675

plaintext
attacks, 145
defined, 130

platform security
copyright and DRM, 704–710
DRM beneficiaries, 722–723
LAN vulnerabilities, 637
mobile phone security, 619–621
phone billing mechanisms, 628
plausible deniability, 745
Playfair block cipher, 134–135
points in fingerprinting, 469
Poisson distribution, 866–867

policies
in BLP security policy model. See BLP
(Bell-LaPadula) security policy model
Common Criteria, 875
copyright and DRM, 718–723
crypto wars, 790–792
defined, 15
lessons from electronic warfare, 589–591
pervasive economic incentives and assurance, 858–859
security engineering conclusions, 889–891
security engineering framework, 4–5
security requirements engineering, 834
social networking security, 740–741
tamper-resistant devices and, 517–518
terror, justice and freedom. See terror, justice and freedom
Windows added features, 104–105
policing
malware countermeasures, 652
steganography and forensics
countermeasures, 756–757
surveillance tactics. See surveillance
policy languages, 109–110
political violence, 771–776
politics
institutional role in anti-terror security,
774–775
security and, 767–768
solving the wrong problem, 822–823
terror, justice and freedom. See terror, justice and freedom
polyinstantiation, 266–267
polymorphic code, 590
polymorphism, 650
Popek, Gerald, 279
Posner, Richard, 232
postage meters, 408–412
post-completion errors, 24
post-cut-through dialed digits, 783
potting, 489
Poulson, Kevin, 601
power analysis
attacks on AES, 155
differential. See differential power analysis
emission security, 523
power cable leakage, 530–534
prank calling, 606
pre-authorization, 188
precise protection, 297
pre-issue fraud, 205, 345
premium rate phone services
dial-through fraud, 604
fraud by phone companies, 627
telecom system security, 599
prepaid phones, 612–613
prepayment meters
defined, 390–392
how they work, 393–395
utility, 392–393
what goes wrong, 395–397
prescribed action links (PALS), 424–426
prescribed action protective system (PAPS), 424
press
managing bug fixes, 837
role in anti-terror security, 775
pretexting
attacks based on psychology, 19–21
defined, 18
phishing and, 40
Pretty Good Privacy (PGP), 753–754
prevent-detect-recover model, 322–323
prevention through internal controls, 322–323
PRF (pulse repetition frequency), 574
Price, George, 226
price discrimination, 625
price setters, 218
price takers, 218
primary account number (PAN), 334
primary inspection, 437
prime numbers, 170
primitive roots, 173
primitives
asymmetric crypto. See asymmetric crypto
primitives
special purpose, 178–179
symmetric crypto, 149–153
principal in role, 211
principals
defined, 12–13
in Windows architecture, 102–103
principle of least privilege, 124
principles for distributed naming, 201–204
principles of BMA security policy, 288–289
printer cartridges and accessory control, 723–724
printing, security. See security printing and seals
prisoner’s dilemma, 225–226
prisons and social psychology, 29
privacy
biometrics and, 479–480
in BMA model. See BMA (British Medical
Association) model
copyright policy and, 719–720
defined, 13–14
economics of, 232–233
Google security, 738–742
in hospital example, 9
multilateral security and, 275–277
phone security and, 616–617
pretexting and, 19
terror, justice and freedom, 808–812
Privacy Enhancing Technologies (PETs), 293–295
Privacy Rule, 283
privacy technology
anonymous email, 747–749
anonymous web browsing, 749–751
bleeding edge, 745–747
confidential and anonymous phone calls, 751–753
e-mail encryption, 753–754
putting privacy technology together, 757–759
steganography and forensics
countermeasures, 755–757
private branch exchange (PBXes) systems, 603–604
private keys, 138
Proactive Security, 196
probabilistic encryption, 172
probing attacks, 510
probing stations, 504–505
process assurance, 863–866
process gains, 568
process group redundancy, 197
processing errors in ATM fraud, 338
Processing Key, 701–702
processors
ARM processor access controls, 116
high-end physically secure, 486–492
medium security, 494–499
Trusted Computing and Intel, 114–116
product assurance, 866
product packaging
security printing, 443–446
techniques, 441
production attacks, 565–566
profiling, 663
programming errors in ATM fraud, 340
project assurance, 860–863
project risk management, 818–819. See also risk
management
projects, security. See security projects
proof-carrying code, 110–111
propaganda, 588
propagating state, 186–187
properties
of BLP model, 245
of Chinese Wall model, 281–282
of hash functions, 141
tranquility, 247
prospect theory, 25
protection
communication systems, 567–572
defined, 15
physical. See physical protection
precise, 297
value of imperfect, 305–306
protection domain, 97
protection problem, 113
protection profiles
Common Criteria, 873–876
defined, 15
in security policy models, 241–242
protection requirements. See security
requirements engineering
protective detonation, 424–425
protesters and DDoS attacks, 642
protocol analysis, differential, 552–553
protocol robustness, 91
protocols, 63–65
3gpp, 618–619
challenge and response, 69–73
chosen protocol attacks, 80–82
EMV standards, 352–357
encryption key management, 82–87
environment changes, 79–80
fortified password, 49
further reading, 92
getting formal, 87–91
GSM authentication, 609–611
introduction, 63–65
message manipulation, 78–79
MIG-in-the-middle attacks, 73–76
password eavesdropping risks, 65–66
reflection attacks, 76–78
research problems, 92
simple authentication, 66–69
summary, 91
protocols, network
DDoS attacks, 640–642
DNS security and pharming, 643
LAN vulnerabilities, 636–638
smurfing, 639–640
spam, 642–643
SYN flooding attacks, 638–639
vulnerabilities, 635–636
prototyping, 827
Provenzano, Bernardo, 130
pseudorandom crypto primitives, 138–139
psychology
in bank example, 7
Crime Prevention Through Environmental
Design, 369
of face recognition, 461–462
fingerprint analysis and, 470
of political violence, 772–773
software copyright protection and, 683–684
usability and. See usability and psychology
public goods, 219–220
public key certificates
defined, 104
naming, 200
Windows added features, 105
public key encryption
based on discrete logarithms, 174–175
history, 138
special purpose primitives, 178–179
trapdoor one-way permutations and, 146–147
public key infrastructure (PKI), 672–675
public keyrings, 753
public-access records, 294
public-choice economics, 774
public-key block ciphers, 130
publish-register-notify model, 188
Pudd’nheadWilson (Twain), 465
pulse compression, 577
pulse repetition frequency (PRF), 574
Pulsed Doppler, 577
pumps
defined, 246
NRL, 254–255
purchase profiling, 346
Putin, Vladimir, 763
Putnam, Robert, 744
Pyshkin, Andrei, 667
Pyszczynski, Tom, 772–773
Q
quality enforcement on passwords, 34
quantum computers, 182
query overlap control, 300–301
query sets
in inference control theory, 297
size control, 298
sophisticated controls, 298–299
quis custodiet ipsos custodes, 862–863
Quisquater, Jean-Jacques, 534
R
R vs. Gold and Schüfreen, 39
race conditions
access control vulnerabilities, 120
concurrency problems, 186–187
defined, 46
Rackoff, Charlie, 157
radar
  countermeasures, 577–578
  jamming techniques, 575–577
  surveillance and target acquisition, 574
radar cross-section (RCS), 575
Radio Direction Finding (RDF), 563
radio frequency interference (RFI), 524
radio microphones, 527
radio signals
  communication protection techniques, 567–572
  IEDs, 582–584
RAIDs (redundant arrays of inexpensive disks), 197
rail noise analysis, 532
Rainbow Series, 270
rainbowing, 438
RAM (Random Access Memory) remanence, 490
Rampart, 195–196
Randall, Brian, 825
Random Access Memory (RAM) remanence, 490
random failure effect, 449–450
random oracle model
  defined, 87
  overview, 138–140
  random functions, 140–143
  random generators, 143–144
  random permutations, 144–146
random passwords, 44–45
random sample queries, 302
randomization, 301–302
randomized response, 302
randomized signature schemes, 147–148
range gate pull-off (RGPO), 576
range gates, 574
rational components vs. emotional components, 26–27
rationale in Common Criteria, 875
Raymond, Eric, 883
RBAC (role-based access control)
  in banking security policy, 323
  defined, 98, 290
RCS (radar cross-section), 575
RDF (Radio Direction Finding), 563
read attribute, 102
Reagan, Ronald, 776
real time gross settlements, 189
Reason, James, 832
Receiver Operating Characteristic (ROC)
  defined, 460, 660
  watermarks and copy generation management, 712
records
  in BMA model, 288
  inference control, 293–295
Red Hat, 288–299
red thread, 791
red/black separation, 530–531
redlining, 663
redundancy
  fault tolerance, 194–195
  levels where it is, 197–198
redundant arrays of inexpensive disks (RAIDs), 197
Reedy, Thomas, 803
reference monitors, 114, 243
refiling calls, 603
reflection attacks, 76–78
region coding
  defined, 698–699
printer cartridges, 723
Regional General Processor (RGP), 330–331
registration, online and copyright protection, 686–687
Registry, 103
regression testing, 829
Regulation E, 631
Regulation of Investigatory Powers (RIP) Act, 781, 790
regulations
  designing internal controls, 320–321
  future of phishing, 51
  handwritten signatures, 459
  history of government wiretapping, 777–779
  mobile phone locking, 620–621
  on name use, 210–211
  privacy and data protection, 808–812
  resulting from crypto wars, 794–796
  tamper-resistant devices and, 517–518
  unlawful surveillance, 781
  VOIP security, 623–624
reinstallation as defense against network attacks, 653
related-key attacks, 146
relay attacks, 357
relays, application, 655–657
reliability
  evolution and security assurance, 868–869
  growth models, 863
  password entry difficulties, 32–33
  process assurance, 866–868
  security project management, 821
religion and psychology of political violence, 773
relying party evaluations, 870–873
remailers, anonymous
  defined, 573
  privacy technology, 748–749
remanence, memory, 490
remedies for access control failures, 124
remote attestation, 112
remote programmability, 355
rendezvous algorithm, 200–201
renewability, security, 196
repeater jamming, 576
replay attacks
concurrency problems, 186–187
key management and, 83
replication mechanisms
malware countermeasures, 650–651
in viruses and worms, 646
reply blocks, 748–749
reputation services, 736
requirements engineering, security. See security
requirements engineering
Rescorla, Eric, 230
resilience
defined, 194
what it is for, 195–196
responsibility in managing patching cycle, 229–230
Restricted, 244
restrictiveness in multilevel security, 249
resurrecting duckling security policy model, 407–408
revocation
AACS, 702
electronic locks and, 376–377
hybrid scrambling attacks, 695–696
process assurance, 866
Revolution in Military Affairs (RMA), 582
RF fingerprinting
defined, 563
mobile phone cloning, 608
RF signal leakage, 534–538
RFI (radio frequency interference), 524
RFID
signals intelligence techniques, 563
tale of three supermarkets, 817
RFID credit cards, 357–358
RGP (Regional General Processor), 330–331
RGPO (range gate pull-off), 576
Ricardo, David, 217
Rifkin, Stanley, 333
rights management languages, 705
rights-management
certificates and, 880
digital with Trusted Computing, 111–113
economics of, 233–234
policy languages, 109–110
Rijmen, Vincent, 153
ringback, 606
rings of protection
defined, 114
in Intel processors, 114–115
RIP (Regulation of Investigatory Powers) Act, 781, 790
risk dumping, 516
risk management
designing internal controls, 321
misperception, 25–26
overview, 846–848
security projects, 818–819
security requirements engineering and, 835
risk thermostat, 820–821
Rivest, Ron, 171
Rivest Shamir Adleman (RSA) algorithm, 171–173
RMA (Revolution in Military Affairs), 582
Robust Security Network (RSN), 667
robustness
phone number, 204
protocol, 91
ROC (Receiver Operating Characteristic)
defined, 460, 660
watermarks and copy generation
management, 712
Rogaway, Philip, 164
rogue access points, 638
role-based access control (RBAC)
in banking security policy, 323
defined, 98, 250
roles
defined, 12
name types, 211
operating system access controls, 98
root filehandles, 637
rootkits
countermeasures, 650–652
defined, 118
malware countermeasures, 651
network attack and defense, 644
roots, primitive, 173
rotor machines, 136
round functions
common hash functions, 167–168
in DES, 157–158
in Feistel cipher, 155–157
rounds, 150
Rounds, William, 280
routing, source, 639–640
rows and capabilities, 103–104
Royal Holloway protocol, 619
Royce, Win, 826
RSA (Rivest Shamir Adleman) algorithm, 171–173
RSN (Robust Security Network), 667
rubber hose cryptanalysis, 754
rubber stamps, 438
Rubin, Avi, 667, 760
rules
attacks and following, 24
BAN logic, 89
exploiting in online games, 730
rules of evidence, 803–807
runaways and social networking security, 740
running keys, 132
runtime security with capabilities, 103–104
Russia and information warfare, 586–587
Rutkowska, Joanna, 258

S
SAAF (South African Air Force), 73–74
Sacco, Giovanni, 180
safe harbor agreement, 808
SafePass, 49
safety case, 830–834
safety critical systems, 829–834
salted list, 686
same origin policy, 734
Samuelson, Pamela, 719
Samyde, David, 534
sandboxing, 96, 110–111
Sarbanes-Oxley Act, 320–321
Sarkozy, Nicholas, 722
Sasse, Angela, 31
satellite TV smartcard security, 502
satisficing, 26
S-boxes
choices of, 151
defined, 149
scanners, 650
scents, 477
Schaeffer, Rebecca, 810
Schechter, Stuart, 230
Schell, Robert, 248
Schell, Roger, 279
Schneier, Bruce
on face recognition, 463
perceptual biases, 25–26
on security theatre, 5
social-engineering attacks, 18
tamper-resistant devices, 515
timing analysis, 531
Schumpeter, Joseph, 865
science, decision, 24–26
SCMS (serial copy management system), 689
SCOMP (secure communications processor), 252–253
scrambling techniques
attacks on hybrid, 693–697
video, 691–693
screen traps, 439
SDA (static data authentication), 352–356
seals, security printing. See security printing and seals
search term access, 782–783
Second Life, 733
secondary inspection, 437
secrecy
defined, 13–14
multilevel security and, 270–271
nuclear command and control, 429–430
Secret classification, 243–244
secret sharing, 422
secure attention sequences, 42–43
secure communications processor (SCOMP), 252–253
secure distributed systems, 1. See also distributed systems
secure shell (SSH) encryption, 665–666
secure systems, managing development of. See managing development of secure systems
secure time, 191–192
SecurID, 72
security, economics of, 228–234. See also economics
security, multilateral. See multilateral security
security, multilevel. See MLS (multilevel security)
security associations, 669
security assurance, 868–869
security categories, 244
security engineering, 3–15
bank example, 6–7
conclusions, 889–891
definitions, 11–15
framework, 4–6
home example, 10–11
hospital example, 9–10
introduction, 3–4
military base example, 7–9
overview, 1–2
summary, 15
security failures, 15
security modules
API attacks on, 548–554
ATM basics, 334
in high-end physically secure processors, 487
security policies
Bell-LaPadula. See BLP (Bell-LaPadula)
security policy model
BMA model, 287–289
Clark-Wilson, 319–320
defined, 15
multilateral security. See multilateral security
multilevel security, 240–242
resurrecting duckling, 407–408
security requirements engineering, 834
security printing and seals, 433–434
anti-gundecking measures, 448–449
evaluation methodology, 453–454
further reading, 455
history, 434–435
inspection costs and nature, 451–453
introduction, 433–434
materials control, 450–451
not protecting right things, 451
overview, 435–436
packaging and seals, 443–446
random failure effect, 449–450
research problems, 454–455
summary, 454
systemic vulnerabilities, 446–447
techniques, 437–443
threat model, 436–437
threat model peculiarities, 447–448
security processors, 116–117
security projects
managing development of secure systems, 816
organizational issues, 819–824
requirements, 842–844
risk management, 818–819
tale of three supermarkets, 816–818
security protocols. See protocols
security questions, 37–38
security renewability, 196
security requirements engineering
overview, 834–835
parallelizing, 844–846
project requirements, 842–844
requirements evolution, 835–842
Security Support Provider Interface (SSPI), 105
security targets
in Common Criteria, 874
defined, 15
in security policy models, 241
security requirements engineering, 834
security testing, 861
security theatre
face recognition as, 463
Schneier on, 5
security-by-obscenity
copyright marking, 718
tamper-resistant devices, 517
security-industrial complex, 891
see-through register, 438
segment addressing, 114
selective availability, 572
selective service denial attacks, 198
Self-Protecting Digital Content (SPDC), 703–704
self-service scanning, 817–818
self-timed logic
ARM processor access controls, 116
using against active attacks, 542
SELinux, 258–259
Seltzer, William, 307
semantic contents naming, 207
semantic security, 172
semi-conductor rights-management, 709–710
semi-open design, 884–885
senescence, 866
Sengoopta, Chandak, 465
sensitive statistics, 297
sensor defeats, 380–382
sensor meshes
cryptoprocessor hacking, 491
smartcard hacking, 507–508
sensors
electronic attacks, 561
how not to protect a painting, 379–380
surveillance and target acquisition, 574–579
separation, red/black, 530–531
separation of duty
defined, 281
internal controls, 321
September 11, 2001
security engineering conclusions, 891
security engineering framework, 5
terror, justice and freedom, 769–771
sequence key cells, 703
serial copy management system (SCMS), 689
serial numbers
in Intel processors, 115
mobile phone cloning, 607–608
Serpent algorithm, 153
server certificates, 44
server hello, 670
service denial attacks
access control vulnerabilities, 121
DDoS, 640–642
digital tachographs, 405–406
in electronic and information warfare, 559–560
fault tolerance and, 198–199
Internet worm, 645–646
network topology, 675
physical protection, 366
prepayment meters, 395–396
system issues, 53
usability and psychology, 53
Session Initiation Protocol (SIP), 623
set-top boxes, 691
set-user-id (suid) file attribute, 101
sex crimes, 739–740
SHA, common hash functions, 168
Shachmurove, Yochanan, 374
shadow passwords, 58
Shaked, Yaniv, 668
Shamir, Adi
A5 algorithm vulnerabilities, 614
asymmetric crypto primitives, 171
cryptography, 179
differential fault analysis, 540
side channel attacks, 543
smartcard hacking, 506
steganography, 755
WiFi network protection, 666
Shannon, Claude, 133, 149
Shapiro, Carl
copyright history, 688
distributed systems, 216
Goldilocks pricing, 347
shared control systems
defined, 322
hacking cryptoprocessors, 488
shared control systems (continued)
  nuclear command and control, 422–424
shared-key block ciphers, 130
sharing and naming, 201
shear lines, 372
Shmatikov, Vitaly, 295
Shoch, John, 644
Shor, Peter, 182
short termination, 627
shortcut attacks, 159
Shostack, Adam, 515
Shostak, Robert, 193
shoulder surfing
  ATM fraud, 339–340
  defined, 54
  shuffle, 154
Shumway, David, 280
side channels, optic acoustic and thermal, 542–543
side-channel attacks, 509, 523
sidelobes, 576
signal cable leakage, 530–534
signaling attacks, 599–601
signals intelligence (Signit)
  defined, 560
  overview, 563–565
  strengths and weaknesses, 788–789
signatures
  deterministic, 147–148
  digital. See digital signatures
  handwritten, 458–461
  intrusion detection, 661
  signature verification keys, 138
  Signit (signals intelligence)
  defined, 560
  overview, 563–565
  strengths and weaknesses, 788–789
Simmons, Gus, 287, 710
Simon, Herb, 842
simple security property, 245, 281
SIMs (subscriber identity modules)
  defined, 500
  GSM security mechanisms, 609
Simultan presses, 438
Singh, Simon, 170
single user Multics, 124
SIP (Session Initiation Protocol), 623
situation awareness, 370
skimmers
  credit card forgery, 345–346
  defined, 43
  Skipjack block cipher, 496–497
Sklyarov, Dmitri, 720
Skorobogatov, Sergei
  combination attacks, 541
  emission security, 534
  physical tamper resistance, 510
Skype
  confidential and anonymous phone calls, 752–753
  VOIP security, 623–624
Skyrms, Brian, 227
slamming, 626
Slovic, Paul, 27
smartcard-based banking
  EMV standards, 351–357
  overview, 350–351
  RFID, 357–358
smartcards
  architecture, 501
  banking protocol, 87–88
Common Criteria limitations, 878–879
history, 500–501
hybrid scrambling attacks, 693–697
overview, 499
power analysis, 533–534
security evolution, 501–512
security processors, 116–117
service denial attacks, 199
video copyrighting and, 691
smashing stacks, 118–119
Smith, Adam, 216–217
Smith, John Maynard, 226
smooth integers, 181
smurf amplifiers, 639
smurfing, 639–640
snowball searches, 564
Snyder, Window, 843
social context of naming, 209–210
social defenses, 799
social engineering attacks
  CDA vulnerabilities, 357
  phone phreaking, 602
  telecom system security, 598–599
social networks
  peer-to-peer file sharing, 707–709
  topology, 675–676
  web application security, 739–744
social psychology
  managing patching cycle, 229–230
  research insights, 28–30
Social Security Numbers (SSNs), 210
social-engineering attacks
  defined, 18
  passwords and, 40–42
Society for Worldwide International Financial
  Telecommunications (SWIFT), 329–331
socio-technical attacks, 743
soft keyboards, 45
soft kills
  defined, 561
  lessons from electronic warfare, 591
Soft Tempest, 536–537
software
  API attacks, 548
  bug fixing, 836–837
  copyright and DRM, 681–688
  free and open-source, 882–884
  sandboxing, 110–111
software birthmarks, 682
software crisis, 824–825
software engineering, 826
software radios, 545
Software Security — Building Security In
  (McGraw), 850
Software Security (McGraw), 120
software-as-a-service, 687–688
Solomon, Sheldon, 772–773
solution time of DES, 158
Song, Dawn, 543
source routing, 639–640
South African Air Force (SAAF), 73–74
spam
  filtering, 655–657
  impression, 737
  network protocol vulnerabilities, 642–643
SPDC (Self-Protecting Digital Content), 703–704
speaker recognition, 475–476
spear phishing, 52
special purpose primitives, 178–179
spiral model, 828
split responsibility, 316
SP-networks, 149–153
spoofing
  as censorship, 643
  DDoS attacks, 640–641
defined, 384
IFF systems, 580
spread spectrum encoding, 713–714
spreading in DSSS, 569
spyware, 648
SQL injection attacks, 120
squidging oscillators, 575
SSH (secure shell) encryption, 665–666
SSL certificates, 105–107
SSNs (Social Security Numbers), 210
SSPI (Security Support Provider Interface), 105
STU-III smartcard, 505
stability of names and addresses, 208–209
stack overflows, 119–120
stack smashing, 118–119
Stanford Prisoner Experiment, 29
Starlight, 255
state
  maintaining in Clark-Wilson, 320
middleware and, 108–109
non-convergent, 190–191
using old data vs. paying to propagate, 186–187
static analysis tools, 850
static data authentication (SDA), 352–356
statistical security
  biometrics vulnerabilities, 479
defined, 143–144
inference control. See inference control
stealth
  defined, 575
  intrusion detection limitations, 665
  malware countermeasures, 650
  with rootkits, 644
steganography
  defined, 710
privacy technology countermeasures,
  755–757
stego-key, 712
stego-text, 712
Stirmark, 716–717
stock, printing, 439
Stone, Andrew, 337
stop loss, 513–514
storage, password, 56–57
storage channels, 264
Storm network, 649
strategy evolution, 226–228
stream ciphers
  additive, 162
defined, 130–132
history of cryptography, 131–132
one-time pads, 132–134
in random oracle model, 143–144
structured protection, 871
Strumpf, Koleman, 234
Stubblefield, Adam, 667
Stubbs, Paul, 324
STU-III secure telephone certification, 181
style and team building, 852
subjects, 12
subliminal channels, 427–428
subscriber authentication keys, 609
subscriber identity modules (SIMs)
defined, 500
GSM security mechanisms, 609
substitution, 420–421
substrates, 443–446
uuid (set-user-id) file attribute, 101
sum-of-efforts vs. weakest-link, 229
Sun, 110–111
supply tampering, 400
suppression, cell, 299–300
surplus, 218
surveillance
  communications intelligence on foreign
targets, 785–787
countermeasures and technical, 526–529
crypto wars, 789–794
crypto wars significance, 794–796
surveillance (continued)

data mining, 783–784
export control, 796–797
intelligence strengths and weaknesses, 787–789
ISP, 784–785
receivers, 528
search terms and location data access, 782–783
target acquisition and, 574–579
traffic analysis, 779–781
unlawful, 781–782
wiretapping, 776–779
Sutherland, David, 248
Sweeney, Latanya, 303
swept-frequency jamming, 571
Swiderski, Frank, 843
SWIFT (Society for Worldwide International
Financial Telecommunications), 329–331
Swire, Peter, 233, 884
switching attacks, 601–603
Sybard Suite, 256
Sybil attacks, 731
symbolic links, 205
symmetric crypto primitives, 149–153
SYN flooding attacks
defined, 121
network protocol vulnerabilities, 638–639
synchronization
DSSS and, 570
simple authentication protocols, 68–69
syncookies, 121, 638
system administrators
internal controls, 323–324
middleware and, 109
Unix OS security, 100–101
user interface failures, 122
system call wrappers
API attacks on OS, 554–555
defined, 121
system evaluation and assurance, 857–858
assurance growth, 866–868
Common Criteria, 873–876
Common Criteria shortcomings, 876–880
education, 886
evaluation, 869–870
evolution and security assurance, 868–869
free and open-source software, 882–884
further reading, 887
hostile review, 882
introduction, 857–858
penetrate-and-patch, CERTs and bugtraq, 885–886
perverse economic incentives, 858–860
process assurance, 863–866
project assurance, 860–863
by relying party, 870–873
research problems, 887

semi-open design, 884–885
summary, 887
ways forward, 881
System Z, 246–247
systematizers vs. empathizers, 28
systemic risks, 189
systems
defined, 11–12
usability and psychology, 52–53

T

tables, decimalization, 553
tabular adjustment, controlled, 301–302
tachographs
defined, 397–398
monitoring and metering, 398–402
tactical communications security, 562
tactical shooting games, 731–732
tags
defined, 420
product packaging, 443–444
take ownership attribute, 102
tale of three supermarkets, 816–818
tamper evident devices, 485
tamper resistance
DVD protection, 700
nuclear command and control, 424–426
physical. See physical tamper resistance
tampering
clip-on fraud, 597–598
cost and nature of inspection, 451–452
evidence, 434
tachograph instrument, 401–402
tachograph supply, 400
target acquisition, 574–579
target of evaluation (TOE), 874–875
targeted attacks, 644
tattle-tale containers, 485
taxi meters, 397–398
TCB (Trusted Computing Base), 243
TCB bloat, 269
TCP (transmission control protocol), 635
TCP-level filtering, 655
TDOA (time difference of arrival), 563
team management
overview, 848–852
process assurance, 864–866
Teapot, 539
technical attacks, 119–121
technical defeats, 55–56
technical eavesdropping, 65–66
technical lock-in, 221–223
technical surveillance, 526–529
technology, privacy. See privacy technology
telecom system security, 595–596
3gpp, 617–619
Index

billing mechanisms, 627–630
complacency cycle and risk thermostat, 820–821
economics of, 624–625
feature interactions, 605–607
further reading, 632
GSM security mechanisms, 608–617
insecure end systems, 603–605
introduction, 595–596
metering attacks, 596–599
mobile phone cloning, 607–608
mobile phone security, success or failure?, 621–622
mobile phones, 606–607
phone company fraud, 625–627
phone phreaking, 596
platform security, 619–621
research problems, 631–632
signaling attacks, 599–601
summary, 630–631
switching and configuration attacks, 601–603
VOIP, 623–624
telegraphs
history of e-commerce, 316–317
history of government wiretapping, 776–777
telemetry communications security, 562
telephones
communication attacks, 384–385
history of government wiretapping, 776–779
risks of, 529
temperature and hacking cryptoprocessors, 490
Tempest attacks
defined, 530
electronic elections security, 762
precautions against, 536
virus, 538–539
Tempest defenses, 523
temporary mobile subscriber identification (TMSI), 613
tents in fingerprint analysis, 465
terminal draft capture, 345
Terminal Master Keys, 335, 549
terror, justice and freedom, 769–771
censorship, 797–803
communications intelligence on foreign targets, 785–787
crypto wars, 789–794
crypto wars significance, 794–796
data mining, 783–784
export control, 796–797
forensics and rules of evidence, 803–807
further reading, 813–814
intelligence strengths and weaknesses, 787–789
introduction, 769–771
ISP surveillance, 784–785
privacy and data protection, 808–812
research problems, 813
search terms and location data access, 782–783
summary, 812–813
terrorism, 771–776
traffic analysis, 779–781
unlawful surveillance, 781–782
wiretapping, 776–779
terrorism, 771–776
electronic and information warfare. See electronic and information warfare
security engineering conclusions, 891
tertiary inspection, 437
test keys
defined, 136–137
history of e-commerce, 317
wholesale payment systems, 328–329
testing
process assurance, 866–868
project assurance, 861
regression, 829
Tews, Erik, 667
The Mythical Man-Month (Brooks), 851
theft
ATM fraud, 338–339
banking and bookkeeping, 324–328
physical protection. See physical protection
reputation, 736
theorem of arithmetic, fundamental, 170
theorem of natural selection, fundamental, 867
theory, inference control, 297–302
thermal side channels, 542–543
Third Generation Partnership Project (3gpp), 617–619
Thompson, Ken, 248, 644–645
threat models
alarms, 379–380
BMA model, 284–287
physical protection, 367–368
postage meters, 409–412
requirements and, 842–844
in security policy models, 240
security printing, 436–437
security project management, 816
security requirements engineering, 834
threat trees, 831
threats
in Common Criteria, 875
defined, 15
physical protection, 366–367
three supermarkets, tale of, 816–818
threshold crypto, 178
Thurmond, Strom, 786
Tian, XuQing, 543
tick payments, 629
ticketing vs. prepayment meters, 397
time, secure, 191–192
time bombs, 682
time difference of arrival (TDOA), 563
time phased force deployment data (TPFDD) system, 252–253
time-hop, 570
time-of-check-to-time-of-use (TOCTTOU) API attacks on OS, 555
attacks, 187
vulnerability, 46
timestamps
hash functions, 140
Kerberos, 85
key management with, 83
timing analysis
attacks on AES, 155
passive emission attacks, 531
timing attacks, 55
timing channels, 264
Titanic Effect, 379
tit-for-tat, 226
TLS encryption, 670–672
TMSI (temporary mobile subscriber identification), 613
TOCTTOU (time-of-check-to-time-of-use) API attacks on OS, 555
attacks, 187
vulnerability, 46
TOE (target of evaluation), 874–875
tokens
simple authentication protocols, 66–69
utility metering, 392–393
Windows added access control features, 105–106
tolerance, fault, 192–199
toll data surveillance, 781
tone pulses, 599–600
toolbar phishing, 47
tools
team management, 850–851
vulnerability remedies, 124
top pins, 372
Top Secret classification, 243–244
Top Secret Special Compartmented Intelligence (TS/SCI), 244
top-down design, 826–827
topology of the network
attack and defense, 675–676
defined, 634
Tor (The Onion Router), 749–751
total exhaust time
defined, 58
of DES, 138
total lock-in value, 221–223
TPFDD (time phased force deployment data) system, 252–253
TPM (Trusted Platform Module)
Intel processors and, 115
Trusted Computing, 112–113
TPM chips
defined, 500
phishing countermeasures, 48
TPs (transformation procedures), 319
trace, differential, 533
traceability, 758
traceback, 641
tracking, traitor, 701–703
trackers
attacks, 298
defined, 297
traffic analysis
anonymous web browsing, 750–751
defined, 563–565
terror, justice and freedom, 779–781
traffic selection, 305
tragedy of the commons, 839–841
training users, 35–37
traitor tracing
defined, 424
HD-DVD and Blu-ray copyright protection, 701–703
tranquility property
defined, 247
in designing internal controls, 323
transaction processing systems, 314
transformation procedures (TPs), 319
transmission control protocol (TCP), 635
transmission links, directional, 567
transponders, 576
transpositions, 524
trap-and-trace devices, 780
trapdoor one-way permutations, 146–147
trapdoors
crypto research and DES, 793
malware history, 645
treaty verification, 426
Treyfer block cipher, 166–167
triple-DES, 159
triples, access
in Clark-Wilson, 320
defined, 97
triplets, GSM, 609
Trojan Horse attacks
countermeasures, 650–652
network attack and defense, 644
user interface failures, 121–122
Tromer, Eran, 543
truck drivers
digital tachographs, 403–408
tachographs, 398–402
truck speed limiters, 397–398
TrueCrypt, 756
Trujillo, Sonia, 452
Index

trust, 13
trust assumptions, 77
Trusted Computing
API attacks, 548
in BMA model, 289
defined, 96, 111–113
economics of DRM, 234
initiative, 48
Intel processors and, 114–116
Trusted Computing Base (TCB), 243
trusted configuration management, 242
trusted distribution
multilevel security, 270
security printing, 433
trusted facility management, 270
trusted interface problem, 514–515
trusted path
defined, 42–43
multilevel security, 270
Trusted Platform Module (TPM)
Intel processors and, 115
Trusted Computing, 112–113
trusted subjects, 246
Trusted Third Parties (TTP)
defined, 793
encryption key management, 83
trustworthiness
defined, 13
tamper-resistant device protection, 519
TS/SCI (Top Secret Special Compartmented Intelligence), 244
TTP (Trusted Third Parties)
defined, 793
encryption key management, 83
tumblers, 607
tuning, control, 838–839
tuples, 124
Turing, Alan, 59–60
Tversky, Amos, 24–25
TV-pay. See pay-TV
Twain, Mark, 465
two-channel authentication, 49–50
two-factor authentication
challenge and response, 71–72
phishing countermeasures, 47–48
two-key triple-DES, 159
two-sided markets, 221
Tygar, Doug
emission security, 526
monitoring and metering, 409
PGP, 754
side channel attacks, 543
type 1 errors, 460
type 2 errors, 460
type A brains, 28
type enforcement model, 249–250
type S brains, 28
types in enforcement model, 249–250
typing, biometrics, 476–477

U
UAC (User Account Control), 105
UCNI (unclassified controlled nuclear information), 429
UDIs (unconstrained data items), 319
Ugon, Michel, 350
Ultra security, 277–278
Umphress, David, 543
UMTS (Universal Mobile Telecommunications System), 617–618
UMTS SIM (USIM), 618
unauthorized copying protection. See copyright and DRM
unauthorized software, 732–733
Unclassified, 243–244
Unclassified but Sensitive, 244
unclassified controlled nuclear information (UCNI), 429
unconditional anonymity, 748
unconditional security, 143–144
unconditionally secure authentication, 420–422
unconstrained data items (UDIs), 319
uniqueness
naming and, 207–208
software, 682–683
UNITA, MIG-in-the-middle attack, 73–74
United States, privacy and data protection, 810–812
universal hash function, 164
Universal Mobile Telecommunications System (UMTS), 617–618
Unix
environmental creep, 124–125
multilevel security, 253–254
operating system access controls, 100–101
security, 34
vulnerabilities, 117–118
unlawful surveillance, 781–782
unlocking mobile phones, 620–621
unspeading in DSSS, 569
updates
locking to prevent inconsistent, 188
non-convergent state, 190–191
order of, 188–189
upgrades
FPGA vulnerabilities, 499
MLS systems practical problems, 268
US Secure Hash Standard, 167
usability
evaluation and, 859
man-in-the-middle attack protocols, 74–76
PKI limitations, 672–673
usability (continued)

    social networking security, 742
    Vista and, 107

usability and psychology, 17–18

    absolute limits, 57–59
    attacks based on psychology, 18–22
    CAPTCHAs, 59–60
    further reading, 61–62
    introduction, 17–18
    mental processing, 26–27
    password choice naivete, 34–35
    password entry attacks, 54–56
    password entry reliability difficulties, 32–33
    password memory difficulties, 33
    password storage attacks, 56–57
    passwords, 31–32
    passwords and design errors, 37–39
    passwords and operational issues, 39
    peoples’ differences, 27–28
    perceptual bias and behavioural economics, 24–26

phishing countermeasures, 43–50

phishing future, 50–52

research insights, 22

research problems, 61

service denial, 53

social psychology, 28–30

social-engineering attacks, 40–42

summary, 60–61

system issues, 52–53

trusted path, 42–43

user abilities and training, 35–37

user protection, 53–54

what brain does better than computer, 30

what brain does worse than computer, 23–24

User Account Control (UAC), 105

user compliance, 37

user interface failures

    defined, 121–122

    trusted interface problem, 514–515

userids, 100–101

users

    in access triples, 97

    passwords, abilities and training, 35–37

    privacy technology. See privacy technology
    profiles, 739–744

    protection, 53–54

    Unix OS security and, 101

    USIM (UMTS SIM), 618

utility metering

    defined, 392–393

    smartcards in, 501

validation in top-down design, 826

van Eck, Wim, 525

Vance, Cyrus, 776

Varian, Hal

    on accessory control, 724–725

    copyright history, 688

    distributed systems, 216

    on DRM, 722

    economics of DRM, 233–234

    Goldilocks pricing, 347

    on privacy, 232

    security economics, 229

    VDU eavesdropping, 535

    vehicles

        digital tachographs, 403–408

        monitoring and metering, 397–398

        tachographs, 398–402

    velocity gate pull-off (VGPO), 576

    velocity gates, 574

    vending machines, 394–395

    verification

        formal, 87–91

        Orange Book evaluation classes, 871

        top-down design, 826

    treaty, 426

    Verified by VISA program, 344

    Vernam, Gilbert, 132

    VGPO (velocity gate pull-off), 576

    Vialink read only memory (VROM), 497

    vibration detectors, 380–381

    video

        attacks on hybrid scrambling systems,
        693–697

        DVB, 697–698

        pay-TV and, 690–691

        scrambling techniques, 691–693

    video camera defeats, 380

    Video Privacy Protection Act, 810

    video signal eavesdropping, 535

    Vigenère, Blaise de, 131–132

    violence, political. See terror, justice and
    freedom

    virtual private networks (VPNs)

        defined, 655

        IPsec and, 670

    virtual world security, 733–734

    virtualization

        defined, 96, 111

        multilevel security, 260–261

        Windows added access control features,
        106

    viruses. See also malware

        countermeasures, 650–652

        early history of, 644–645

        how they work, 646–647

        information warfare, 587–588

        in MLS systems, 265–266

Val di Fassa, 79

valet attacks, 68
network attack and defense, 644
software copyright protection and, 685
VISA, EMV standards, 351–357
visitor location register (VLR), 609
Vista
access control introduction, 96
added access control features, 105–107
basic Windows architecture, 102
Biba model and, 250–252
multilevel security, 257–258
why Windows is so insecure, 230–232
VLR (visitor location register), 609
voice over IP (VOIP), See VOIP (voice over IP)
voice recognition, 475–476
VOIP (voice over IP)
confidential and anonymous phone calls, 751–753
defined, 325
Volume Unique Key (VUK), 702
vulnerabilities
banking and bookkeeping, 324–328
biometrics, 477–481
bug fixing, 836–837
composability of MLS systems, 261–262
covet channels, 263–265
DDA, 356
defined, 15
hacking cryptoprocessors, 488–492
MLS polyninstantion, 266–267
MLS systems cascade problem, 262–263
MLS systems practical problems, 267–269
naming, 204–211
online game cheating, 730–732
of operating system access controls, 117–118
overwriting attacks, 118–119
phone insecure end systems, 603–605
remedies, 124
SDA, 352–353
security printing, 446–447
SWIFT, 331–333
tamper-resistant devices, 514–518
technical attacks, 119–121
virus threats to MLS, 265–266
why there are so many, 122–124
why Windows is so insecure, 230–232
W
Wagner, David
electronic elections security, 761
side channel attacks, 543
timing analysis, 531
WiFi network protection, 666
wall hacks, 732
walls, 370–372
Walras, Léon, 217
Walsh report, 794–795
Walter, Kenneth, 280
Waltz, Edward, 588
Wang, Xiaoyun, 168
Ware, Willis, 525
warfare, electronic and information. See electronic and information warfare
warrantless wiretapping, 779
waste processing, nuclear command and control, 427
waterfall model, 826–827
watermarks
copy generation management, 711–712
defined, 438
information hiding, 710
magnetics, 443
Watson, Robert
defined, 121
API attacks, 554
application relays, 656
Weber, James, 389
weakest-link vs. sum-of-efforts, 229
The Wealth of Nations (Smith), 216
weapons security
directed energy weapons, 584–586
nuclear command and control. See nuclear command and control
with resurrecting duckling, 408
web application security
eBay, 735–736
Google, 736–739
overview, 734–735
social networking sites, 739–744
web browsing, anonymous, 749–751
web of trust, 753
web-based technologies, 9
websites
in bank example, 6
online credit card fraud, 348–350
Weinmann, Ralf-Philipp, 667
Wels, Barry, 373
WEP (wireless equivalent privacy), 666–667
Wheatstone, Sir Charles, 134
Wheeler, David, 701
White, David, 803
white-box testing, 861
Whitehouse, Ollie, 587, 668
whitelists, 564
Index

whitening, 159–160
Whitten, Alma, 754
who shall watch the watchmen, 862–863
wholesale payment systems, 328–333
whorls in fingerprint analysis, 465
Wiesner, Jerome, 418
WiFi
network attack and defense, 666–668
rogue access points, 638
Wi-Fi Protected Access (WPA), 667–668
Wilson, Dave, 319
window threads, 436
Windows
access control and added features, 104–107
basic architecture, 102–103
Biba model and Vista, 250–252
user interface failures, 122
vulnerabilities, 117–118
why it’s so insecure, 230–232
Windows Media Player (WMP), 705–706
Windows Media Rights Management (WMRM), 705–706
Winterbotham, Frederick, 786
wired equivalent privacy (WEP), 666–667
wiretapping
avoiding with VOIP, 751–753
classifications/clearances and, 244–245
ISP, 784–785
multilevel security applications, 256–257
switching and configuration attacks, 601
terror, justice and freedom, 776–779
Wittneben, Bettina, 676
WMP (Windows Media Player), 705–706
WMRM (Windows Media Rights Management), 705–706
Wolf, Hans-Georg, 536
Wolfram, Catherine, 836
women, gender usability and psychology, 27–28
Wood, Elizabeth, 369
Woodward, John, 249
Wool, Avishai, 668
words, control, 691
World War II reflection attacks, 77–78
World Wide Military Command and Control System (WWMCCS), 279
worms. See also malware
countermeasures, 650–652
eyearly history of, 644–645
how they work, 646–647
Internet, 645–646
network attack and defense, 644
WPA (Wi-Fi Protected Access), 667–668
wrappers, system call
API attacks on OS, 554–555
defined, 121
write attribute, 102
Writing Secure Code (Howard and LeBlanc), 119, 850
wrongful convictions and fingerprint analysis, 469–472
WWMCCS (World Wide Military Command and Control System), 279
Wycliffe, John, 798
X
XACML, 109
xor-to-null-key attacks, 549–551
XrML, 109
XSS (cross-site scripting)
defined, 734
social networking security, 743
Y
Yale, Linus, 372
Yale locks, 372–373
Yee, Bennett, 409
yescards, 354
Ylön, Tatu, 665–666
Z
zero-day exploits, 117
zero-sum game, 224
Zhou, Feng, 526, 543
Zhuang, Li, 526, 543
Zielinski, Peter, 552
Zimbardo, Philip, 29
Zimmerman, Phil, 790
zone system, 536
Zuckerberg, Mark, 742