# INDEX

## A


**access control, 109**
**access control (spam), 136**
  accountability, 136-140
  accreditation, 148-150
  authentication, 140-147
  consequences, 151
**access control as service, SAML, 296-297**
**accessibility, Secure Internet Letterhead, 244-245**
**accountability**
  spam, access control, 136-140
  trust, 238
    *issuer accountability, 241-242*
    *re-establishing, 239-240*
**accountability controls, 108**
  accreditation, 109
  authentication, 108
  consequences, 109
**The Accountable Net, 136**
**accreditation, 139**
  accountability controls, 109
  platform security, 351
  spam, access control, 148-150
**accreditation authority, 148**
**adding**
  devices to networks, 337
  wireless devices to networks, 337-338
**addresses**
  MAC/EUI addresses, 328
  secure names, 312
**Advance Fee, 21**
**advocacy in standardization, 101**
**adware, 28**
**Aladeff, Joe, 267**
**Algol 60, platform security, 344**
**Allow or Deny dialog (Windows Vista), 345**
**AMEY (AOL, Microsoft, EarthLink, and Yahoo), 151**

**ANI (Automatic number identification), 313**
**antihacking statutes (Internet law), 367**
**AOL (America Online), 110**
  e-mail, 142
  spam, 139
**Aravosis, John, 257**
**architecture**
  design for deployment, 109-112
  secure names, 319
    *DNS policy, 320*
    *DNS security, 321*
    *DNS service specification, 319-320*
**arms suppliers, Internet law, 367-368**
**assertions, 297**
**assurance, 245**
  communicating, 247-248
**asymmetric key cryptography, symmetric key cryptography versus, 209**
**attribute only authentication, 308**
**audio format standardization, 92**
**audit requirements, effecting change, 103**
**authentication, 139**
  accountability controls, 108
  e-mail
    *designing for deployment, 263-264*
    *DKIM, 265-267*
  enterprise authentication, secure identity, 301
  identity, 278-279
    *attribute only authentication, 308*
    *biometrics, 287-288*
    *callback schemes, 281-282*
    *first contact, 279-280*
    *hybrid tokens, 286*
    *knowledge-based authentication, 281*
    *machine verification, 282*
    *one-time password tokens, 282-285*
    *passwords/PINs, 280-281*
    *smartcards/smart tokens, 285-286*
  messaging, 251-252
  public key cryptography, 211
  SenderID/SPF, 263
  spam, access control, 140-147
  ubiquitous authentication, default deny, 327-330
**Authenticode, 352**
**Automatic number identification (ANI), 313**

## *B*

**banking, secure online banking, 303-304**
**banks, profiling customers, 282**
**base64 encoding, 262**
**bell-shaped curve, growth of network hypertext programs, 84**

**benefits of trust, 236-237**
**Berlind, David, 135**
**Berners-Lee, Sir Tim, 86, 97, 300**
**BGP, secure networks, 339-341**
**biometrics, identity authentication, 287-288**
**blacklists, 248**
spam, 121-124
**Bletchley Park, 58, 204**
**blogspam, stopping, 301-303**
**Bluetooth keyboards, 286**
**Bonded Sender program, 149**
**bootstrapping, trustworthy computing, 349**
**"botnet", 175**
**Brickley, Dan, 316**
**bridge CA, 224**
**broadcast communications, 332**
**broken windows theory, 379**
**Britton, William, broken windows theory, 379**

## *C*

**CA Browser forum, 240**
**Caesar, Julius, development of cryptography, 199**
**Callas, Jon, 267**
**callback schemes, identity authentication, 281-282**
**Caller-Id for e-mail, 146**
**CallerID, 312**
**CallerID blocking, 312**
**Cameron, Kim, 291**
**canonical form, 269**
**canonicalization, DKIM, 269-270**
**CANSPAM, 127**
**Canter, Laurence, 120**
**Canter and Siegal, 120**
**carding, 8, 13-15, 158, 166-171**
one-time passwords, 283
**CardSpace**
cookies, 304
identity, user experiences, 291-294
**CAs, 239**
insurance, 246-247
**censorship, 122**
**certificate issuer liability, 246-247**
**certificates, 239**
extended validation certificates, 240-241
**certificates (digital), 219**
Kohnfelder model, 219
revocation, 220
**challenge response, 131-132**
**challenge-response, 129-130**
**change, effecting, 101**
audit requirements and, 103
liability and, 102
regulation and, 103-104
with customers, 102
**chickenboners, 357**
**chief information security officer (CISO), 333**
**children, protecting, 305-306**
**chrome, 233-235**

**cipher machines, 206**
**ciphers, cryptography development**
cipherstreams, 201-202
stream ciphers, 201-202
substitution ciphers, 200-201
**cipherstreams, cryptography, development of, 201-202**
**CISO (chief information security officer), 333**
**civil law**
Judge Hands formula, 371
liabilities, eliminating, 371-372
responsibility, 368-371
risk evaluation formula, 371
**clarification, Internet law, 365**
**co-browser, 28**
**collateral damage, 122**
**communicating**
assurance, 247-248
perimeter security, 275
**CompuServe GIFformat standardization, 92**
**confidentiality**
e-mail, designing for deployment, 264-265
messaging, 254-255, 273-274
*communicating with perimeter security, 275*
*mail receipt policy, 274*
**consequences, 139**
accountability controls, 109
spam, access control, 151
**consistency, standardization and, 96-97**
**contact, gatekeepers, 314**
**cookies, 303**
**core, Internet, 111**
**cost of trust, 236-237**
**credit cards, 220**
**crime (Internet)**
civil law
*eliminating liabilities, 371-372*
*Judge Hands formula, 371*
*responsibility, 368-371*
*risk evaluation formula, 371*
Hill, Zachary Keith, 360
international law, 360-361
Jaynes, Jeremy, 359
law, 355
*lawsuits, 356-357*
*prison sentences, 357-358*
*probation, 358*
legislation, 361
*antihacking statutes, 367*
*arms suppliers, 367-368*
*clarification, 365*
*deemed losses, 363*
*jurisdictions, 362-363*
*loopholes, 365*
*spam affiliate programs (agencies), 365*
*spyware, 366*
*tripwire offenses, 365*
*U.S. CAN-SPAM act, 365*

Levin, Valdimir, 359
prosecution, 372
*money trails, 373*
**critical mass, Secure Internet Letterhead, 253-254**
**CRM, 335**
**cryptography, 199, 213**
asymmetric key cryptography, symmetric key cryptography versus, 209
Caesar's cipher, 199
cipherstreams, 201-202
digital signatures, 210-211
historical use of, 199
machine encryption, 204
*cipher machines, 206*
*Enigma machine, 204-206*
network security versus, 199
no-secret encryption, 207
one-time pads, 201-203, 206
PKI, 216-218
*bridge CA, 224*
*digital certificates, 219-220*
*OCSP, 220*
*SCVP, 225*
*Web of Trust, 221-224*
*XKMS, 225-226*
public key cryptography, 207-208, 215-216
*authentication, 211*
*message digest function, 211*
session keys, 209-210
smartcards, 211-212
stream ciphers, 201-202
substitution ciphers, 200-201
symmetric key cryptography, asymmetric key cryptography versus, 209
VENORAdecrypts, 203
**curtained memory, 350**
**customers**
effecting change, 102
profiling, 282

## D

**damaged messages, 261-263**
**Danish, Hadmut, 146**
**data-level security, default deny (secure networks), 333-335**
**de facto standards, 93**
**de jure standards, 93**
**deemed losses (Internet law), 363**
**default deny, 324**
secure networks, 326-327
*data-level security, 333-335*
*ubiquitous authentication, 327-330*
*ubiquitous policy enforcement, 331-332*

**default deny infrastructure, 324**
**default permit, 324**
**dependency, standardization and, 97-101**
**deperimeterization, 113, 323**
**deploying**
DKIM, 275-276
Sender-ID/SPF, 153-154
**design for deployment, 107, 115-116**
architecture, 109-112
e-mail, 259
*authentication, 263-264*
*confidentiality, 264-265*
*damaged e-mail, 261-263*
*user-level keying, 265*
objectives of, 108-109
persuading early adopters, 116-117
strategy, 112-115
**design plans (security), 378**
**designing for deployment, secure networks, 324-325**
IPv6, 325-326
**device drivers, platform security, 347**
**devices**
adding to networks, 337
ubiquitous authentication, default deny, 329-330
**DHCP, 338**
**Diffie, Whitfield, public key cryptography, 207-208**
**digital certificates, 219**
Kohnfelder model, 219
revocation, 220
**digital rights management (DRM), 335**
**digital signatures, 210-211, 262, 266-267**
DKIM, 266
Secure Internet letterhead, 271-272
Yahoo!, 267
**DKIM (Domain Keys Identified Mail), 99-101, 265-267**
canonicalization, 269-270
deploying, 275-276
key distribution by DNS, 270-271
signing e-mail, 267-268
**DNS (Domain Name System), 142**
key distribution, 270-271
mail sending policies, 272-273
**DNS infrastructure, DKIM and, 99-101**
**DNS policy, secure names, 320**
**DNS security, secure names, 321**
**DNS server deployment, dependency on e-mail server deployment, 99-101**
**DNS Service (SRV) record, 320**

**DNS service specification, secure names, 319-320**
**DNSSEC (DNS Security), 321**
**Domain Keys Identified Mail (DKIM), 99-101, 265-267**
canonicalization, 269-270
deploying, 275-276
key distribution by DNS, 270-271
signing e-mail, 267-268
**domain names, 141**
**domain-validated encryption, 238**
**drivers, secure drivers (platform security), 351-352**
**DRM (digital rights management), 335**
**Dunbar, Robin, 97**
**DVD specification, 91**

## *E*

**e-mail server deployment, dependency on DNS server deployment, 99-101**
**ease of use, messaging, 255-257**
**edge, Internet, 111**
**Edison, Thomas, 88**
**Ellis, James, no-secret encryption, 207**
**Ellison, Larry, 140**
**e-mail, 143. *See also* messaging**
accountability, 136-138
accrediting, 148-150
authenticating, 145-147
authentication, 144
*DKIM, 265-267*
confidentiality, 140
consequences for spammers, 151
designing for deployment, 259
*authentication, 263-264*
*confidentiality, 264-265*
*damaged e-mail, 261-263*
*user-level keying, 265*
DKIM, signing, 267-268
mailing lists, 143
security requirements for, 258
*authentication, 251-252*
*confidentiality, 254-255*
*ease of use, 255, 257*
sending policies, 272-273
spam. *See* spam
SSL and, 260
**encryption**
domain-validated encryption, 238
no-secret encryption, 207
**encryption (machine), 204**
cipher machines, 206
Enigma machine, 204-206

**end, Internet, 111**
**end-to-end principle, 64-66**
**Enigma machine, 58, 204-206**
**enterprise authentication, secure identity, 301**
**enterprises, Secure Internet letterhead (critical mass), 253-254**
**Extended Validation, 242-243**
opinion letters, 244
**extended validation certificates, 240-241**
**eXtensible Access Control Markup Language (XACML), 299**

## *F*

**factors, 279**
**FDIC (Federal Deposit Insurance Corporation), 246**
**features, spam, 126**
**feedback (positive), 381**
**filtering spam, 381**
**filters, spam, 125-126**
**first contact, identity authentication, 279-280**
**five-point security design plan, 378**
**FOAF (Friend of a Friend), 316-318**
**419 fraud, 21**
**FTC (Federal Trade Commission) Internet law, 363**

## *G*

**gatekeepers, secure names, 313-314**
introductions, 315
levels of contact, 314
**gateways, 86**
**GCHQ, no-secret encryption, 207**
**GIF format standardization, 92**
**Google, blogspam, 302**
**government regulation.** ***See*** **regulation**
**green card spam, 120-121**
**group size limits, 97**
**growth of Web, 81-85**
**growth phase (in S-curve), 82**

## *H*

**hacker, 3, 7, 10, 13, 38-41, 175-176, 180, 187-189, 192-194, 197, 367**
"MIT usage," 38
**Hellman, Martin, public key cryptography, 207-208**
**HEPNET, 86, 110**
**Hill, Zachary Keith, Internet crime, 360**
**honeypot e-mail addresses, 123**

**HTTP cookies, 303**
**hybrid tokens, identity authentication, 286**

## *I*

**identity**
attribute only authentication, 308
authentication, 278-279
*biometrics, 287-288*
*callback schemes, 281-282*
*first contact, 279-280*
*hybrid tokens, 286*
*knowledge-based authentication, 281*
*machine verification, 282*
*one-time password tokens, 282-285*
*passwords/PINs, 280-281*
*smartcards/smart tokens, 285-286*
blogspam, 301-303
enterprise autentication, 301
Identity 2.0. *See* Identity 2.0
protecting children, 305-306
secure online banking, 303-304
secure transactions, 304-305
ubiquitous customization, 305
unlinkable identifiers, 308-309
user experiences, 288-289
*CardSpace, 291-294*
*log in, 290*
*OpenID, 294-295*
*registration, 290*
*roaming, 291*
*ubiquity, 290*
*user centric, 289*
**Identity 2.0, 295-296**
SAML
*access control as service, 296-297*
*identity assertions, 298-299*
*problems with, 300*
*Semantic Web, 299-300*
**Identity 3.0, 306-307**
deferred registration, 307-308
**identity assertions, SAML, 298-299**
**identity infrastructure, 278, 288-289**
**identity providers, 295**
**IETF, 93**
**impersonation, 108**
**implementing spam reduction strategies, 151-153**
**inclusiveness, technical inclusiveness, 95-96**
**information, sending to gatekeepers, 315**

**Initiative for Open AuTHentication (OATH), 284**
**insurance, CAs, 246-247**
**intelligence, ubiquitous policy enforcement (secure networks), 332**
**international law, Internet crime, 360-361**
**Internet crime**
civil law
*eliminating liabilities, 371-372*
*Judge Hands formula, 371*
*responsibility, 368-371*
*risk evaluation formula, 371*
Hill, Zachary Keith, 360
international law, 360-361
Jaynes, Jeremy, 359
law, 355
*lawsuits, 356-357*
*prison sentences, 357-358*
*probation, 358*
legislation, 361
*antihacking statutes, 367*
*arms suppliers, 367-368*
*clarification, 365*
*deemed losses, 363*
*jurisdictions, 362-363*
*loopholes, 365*
*spam affiliate programs (agencies), 365*
*spyware, 366*
*tripwire offenses, 365*
*U.S. CAN-SPAM act, 365*
Levin, Valdimir, 359
prosecution, 372
*money trails, 373*
security controls, 84-85
**Internet service provider (ISP), 138**
**internetworks, 109-110**
securing, 339
*BGP security, 339-341*
**IP addresses, 141**
**IPv6, secure networks, 325-326**
**IronPort, Bonded Sender program, 149**
**ISP (Internet service provider), 138**
**issuer accountability, 241-242**

## *J*

**JANET, 86**
**Jaynes, Jeremy, Internet crime, 359**
**Judge Hands formula (civil law), 371**
**jurisdictions (Internet law), 362-363**

## *K*

**key distribution, DNS, 270-271**
**killer applications, Web as, 85-86**
**knowledge-based authentication, identity authentication, 281**
**Kohnfelder digital certificate model, 219**

## *L*

**Lampson, Butler, reference monitor concept (privilege control), 346**
**law**
civil law
*eliminating liabilities, 371-372*
*Judge Hands formula, 371*
*responsibility, 368-371*
*risk evaluation formula, 371*
international law, 360-361
legislation, 361
*antihacking statutes, 367*
*arms suppliers, 367-368*
*clarification, 365*
*deemed losses, 363*
*jurisdictions, 362-363*
*loopholes, 365*
*spam affiliate programs (agencies), 365*
*spyware, 366*
*tripwire offenses, 365*
*U.S. CAN-SPAM act, 365*
prosecution, 372
*Hill, Zachary Keith, 360*
*Jaynes, Jeremy, 359*
*lawsuits, 356-357*
*Levin, Vladimir, 359*
*Mitnick, Kevin, 358*
*money trails, 373*
*prison sentences, 357-358*
*probation, 358*
**least privilege principle, 345**
**Lee, Adelyn, 140**
**legislation (Internet crime), 361**
antihacking statutes, 367
arms suppliers, 367-368
clarification, 365
deemed losses, 363
jurisdictions, 362-363
loopholes, 365
spam affiliate programs (agencies), 365
spyware, 366
tripwire offenses, 365
U.S. CAN-SPAMact, 365
**levels of contact, gatekeepers, 314**
**Levin, Vladimir, Internet crime, 359**

**liability, effecting change, 102**
**light bulbs, standardization, 87-89**
**LinkedIn, 316**
**linkspam, 302**
**loopholes, Internet law, 365**
**luxury, messaging, 255-257**

## *M*

**MAC/EUI addresses, 328**
**machine encryption, 204**
cipher machines, 206
Enigma machine, 204-206
**machine verification, identity authentication, 282**
**Madrid Protocol, 243**
**mail receipt policy, 274**
**mail sending policies, 272-273**
**mailing lists, 143**
**Malthus, Thomas, 101**
**MAPS blacklist, 121-123**
**mashups, 114**
**maturity phase (in S-curve), 82**
**meetings, scheduling, 318-319**
**memory, curtained memory, 350**
**message digest function (public key cryptography), 211**
**messaging. *See also* e-mail**
authentication, 251-252
confidentiality, 254-255, 273-274
*communicating perimeter security, 275*
designing for deployment, 259
*authentication, 263-264*
*confidentiality, 264-265*
*damaged e-mail, 261-263*
*user-level keying, 265*
luxury, 255-257
mail receipt policy, confidentiality, 274
**Microsoft**
patents, 147
SPF/Sender-ID, 152
**Microsoft CardSpace, 291-294**
**Miller, Jim, 146**
**Miller, Libby, 316**
**Mitnick, Kevin, Internet law, 358**
**money (Internet crime), 373**
**Mythbusters, 287**

## *N*

**names, 311. *See also* secure names**
**network administration, secure networks, 335**
adding devices to networks, 337

adding wireless devices to networks, 337-338
starting networks, 336-337
WiFi, 338
**network effect, 83**
**network security, cryptography versus, 199**
**networks, 109, 138**
secure networks. *See* secure networks
**Nigeria, Internet crime, 360**
**Nigerian letters, 21**
**no-secret encryption, 207**

## O

**Oasis, 93**
**OATH (Initiative for Open AuTHentication), 284**
**objectives, design for deployment, 108-109**
**OCSP(Online Certificate Status Protocol), 220**
**one-time pads**
cipher machines, 206
stream ciphers, 201-203
substitution ciphers, 202
**one-time password tokens, identity authentication, 282-285**
**one-way functions. *See* message digest function**
**online banking, 303-304**
**OpenID, 300**
Identity, user experiences, 294-295
**opinion letters, Extended Validation, 244**
**opportunity, strategies for change, 114**
**OS (Operating Systems), trustworthy computing, 349-350**
**OTP tokens (one-time passwords), 284**
**ownership, secure names, 313**
**ownership of patents, effect on standardization, 90-93**

## P

**package reshipping, 15**
**padlock icon, 289**
SSL, 231
**pads (one-time)**
cipher machines, 206
stream ciphers, 201-203
substitution ciphers, 202
**pain, 113**
**Panera, WiFi, 338**
**passwords, 277**
identity authentication, 280-281
one-time password tokens, identity authentication, 282-285

**patents, 147**
effect on standardization, 90-93
**path validation, SenderID/SPF, 265**
**perimeter security, 323**
communicating, 275
**persuading early adopters, 116-117**
**PGP**
authentication, 263
confidentialilty, 264
damaged goods, 262
**phishing, 10-14, 46-47, 56-57, 74, 155-170, 185, 212-213, 283, 364, 368**
Hill, Zachary Keith, 360
one-time passwords, 283
prosecution, following the money, 373
**phreak, 39**
**pink contracts, 121**
**PINs, identity authentication, 280-281**
**pixels, standardization, 90**
**PKI (Public Key Infrastructure), 216-218**
bridge CA, 224
digital certificates, 219
*Kohnfelder model, 219*
*revocation, 220*
digital signatures, 266
OCSP, 220
problems with, 286
SCVP, 225
Web of Trust, 221-224
XKMS, 225-226
**platform security, 343**
Algol 60, 344
privileges, controlling
*least privilege principle, 345*
*reference monitor concept, 346*
*TCB, 346*
secure code
*accreditation, 351*
*privilege revocation, 352*
*secure drivers, 351-352*
*signed code, 350-352*
trustworthy computing, 347-348
*bootstrapping, 349*
*OS, 349-350*
*TPM, 349-350*
**platform security, device drivers, 347**
**policies**
mail receipt policy, 274
mail sending policies, 272-273
ubiquitous authentication, default deny, 330
ubiquitous policy enforcement, default deny, 331-332
**positive feedback, 381**

**Postal Inspection Sevice (U.S.): Internet law, 363**
**power supplies, standardization, 87**
**pretexting, 253**
**prison sentences (Internet crime), 357-358**
**privileges**
platform security
*least privilege principle, 345*
*reference monitor concept, 346*
*TCB, 346*
revocation, 352
**probation (Internet crime), 358**
**problems**
with SAML 1.0, 300
with SSL, 231-233
**profiling customers, 282**
**programming languages, Algol 60, 344**
**promiscuous security, 237**
**prosecution (Internet crime), 372**
money, 373
**protecting children, 305-306**
**pseudonymity, 108**
**public key cryptography, 207-208, 215-216**
authentication, 211
message digest function, 211

## Q

**QWERTY keyboards, standardization, 89**

## R

**Ranum, Marcus, 324**
**RDF (Resource Description Framework), 302**
**re-establishing accountability, 239-240**
**re-vic fraud, 24**
**receiving stolen goods, 15**
**reference monitor concept (privilege control), 346**
**Referer field, standardization, 89**
**registration**
identity, user experiences, 290
Identity 3.0, 307-308
**regulation, effecting change, 103-104**
**reputation**
blacklists, 248
trusted agents, 249-250
**reputation authority, 148**
**Request For Proposals (RFP), 297**
**requirements for e-mail security, 258**
authentication, 251-252
confidentiality, 254-255
ease of use, 255-257

**Resource Description Framework (RDF), 302**
**revocation, digital certificates, 220**
**revocation (privileges), platform security, 352**
**RFP (Request For Proposals), 297**
**risk evaluation formula (civil law), 371**
**roaming identity, user experiences, 291**

## *S*

**S-curve, growth of Web, 81-85**
**S/MIME, 252**
authentication, 264
**SAML (Security Assertion Markup Language), 295-296**
Identity 2.0
*access control as service, 296-297*
*identity assertions, 298-299*
*problems with, 300*
*Semantic Web, 299-300*
**scheduling meetings, 318-319**
**scratch-off cards, 283**
**screen scraping, 114**
**script kiddie, 41**
**SCVP (Simple Certificate Validation Protocol), 225**
**secure chrome, establishing, 244**
**secure drivers, platform security, 351-352**
**secure identity**
attribute only authentication, 308
authentication, 278-279
*biometrics, 287-288*
*callback schemes, 281-282*
*first contact, 279-280*
*hybrid tokens, 286*
*knowledge-based authentication, 281*
*machine verification, 282*
*one-time password tokens, 282-285*
*passwords/PINs, 280-281*
*smartcards/smart tokens, 285-286*
blogspam, 301-303
enterprise autentication, 301
Identity 2.0. *See* Identity 2.0
protecting children, 305-306
secure online banking, 303-304
secure transactions, 304-305

ubiquitous
customization, 305
unlinkable identifiers, 308-309
user experiences, 288-289
*CardSpace, 291-294*
*log in, 290*
*OpenID, 294-295*
*registration, 290*
*roaming, 291*
*ubiquity, 290*
*user centric, 289*
**Secure Internet Letterhead, 243-244**
accessibility, 244-245
critical mass, 253-254
signatures, 271-272
**secure names, 311**
addresses, 312
architecture, 319
*DNS policy, 320*
*DNS security, 321*
*DNS service specification, 319-320*
gatekeepers, 313-314
*introductions, 315*
*levels of contact, 314*
ownership, 313
rights, 312-313
**secure names, social networking, 315-316**
FOAF, 316-318
scheduling meetings, 318-319
**secure networks**
default deny, 326-327
*data-level security, 333-335*
*ubiquitous authentication, 327-330*
*ubiquitous policy enforcement, 331-332*
designing for deployment, 324-325
*IPv6, 325-326*
internetworks, 339
*BGP security, 339-341*
network administration, 335
*adding devices to networks, 337*
*adding wireless devices to networks, 337-338*
*starting networks, 336-337*
*WiFi, 338*
**secure online banking, 303-304**
**Secure Sockets Layer.** ***See*** **SSL**
**secure transactions, 304-305**
**security**
five-point design plan, 378
network security, cryptography versus, 199
platforms, 343
*Algol 60, 344*
*privilege control, 345-346*

*secure code, 350-352*
*trustworthy computing, 347-350*
trust, definition of, 217
**Security Assertion Markup Language (SAML), 295-296**
Identity 2.0
*access control as service, 296-297*
*identity assertions, 298-299*
*problems with, 300*
*Semantic Web, 299-300*
**security audits, 103**
**security controls, 84-85**
**semantic markup, 303**
**Semantic Web, 97-98, 299-300**
**Sender-ID, 152**
deploying, 153-154
**SenderID/SPF**
authentication, 263
path validation, 265
**sending e-mail, policies for, 272-273**
**services, ubiquitous authentication (default deny), 330**
**session keys, 209-210**
**SGML, 113**
**Shovell, Admiral Sir Clowdisley, 128**
**Siegal, Martha, 120**
**signatures. *See* digital signatures**
**signed code**
Authenticode, 352
platform security, 350
**signing e-mail, DKIM, 267-268**
**Single Sign On systems, 296**
**Sir Winston Churchill, 58**
**smart tokens, identity authentication, 285-286**
**smartcards, 211-212, 277**
identity authentication, 285-286
**Smith, Adam, 91**
**social networking, secure names, 315-316**
FOAF, 316-318
scheduling meetings, 318-319
**spam, 119, 380**
access control, 136
*accountability, 136-140*
*accreditation, 148-150*
*authentication, 140-147*
*consequences, 151*
affiliate programs (agencies), 365
arms suppliers, 367-368
blacklists, 121-124
blogspam, stopping, 301-303
CANSPAM, 127
chickenboners, 357
filtering, 381
filters, 125-126
green card spam, 120-121

lawsuits, 356-357
linkspam, 302
searching for solutions to, 128-132
suing and jailing spammers, 126-128
U.S. CAN-SPAM act, 365
vigilante justice, 132-133
**Spam Prevention Early Warning System (SPEWS), 124**
**spam reduction strategies, implementing, 151-153**
**SPEWS (Spam Prevention Early Warning System), 124**
**SPF, 146**
deploying, 153-154
**spyware, 28-29, 73, 155, 165-166, 188-190, 366**
Internet law, 366
**SRV, 320**
**SSL (Secure Sockets Layer), 227**
chrome, 233-235
e-mail and, 260
overview of, 227-230
problems with, 231-233
Web servers, 230-231
**standardization**
advocacy in, 101
consistency and, 96-97
dependency and, 97-101
effect of patents on, 90-93
hazards of quick decisions, 89-90
importance of, 87-89
standards organizations, 93-94
**standards, 116**
**standards organizations, 93-94**
**starting networks, secure networks, 336-337**
**startup phase (in S-curve), 82**
**stopping blogspam, 301-303**
**strategic measures (security controls), 84-85**
**strategies, design for deployment, 112-115**
**stream ciphers, development of cryptography, 201-202**
**Strowger, Almon, 313**
**substitution ciphers, development of cryptography, 200-201**
**suing spammers, 126-128**
**Swan, Alfred, 88**
**Swan, Joseph, 88**
**symmetric key cryptography, asymmetric key cryptography versus, 209**

## *T*

**tactical measures (security controls), 84-85**
**tax-havens, international law, 360**

**TCB (Trusted Computing Base), privilege control, 346**
**TCG (Trusted Computing Group), 349**
**technical inclusiveness, 95-96**
**TLS (Transport Layer Security), 227**
**toll-free calls, 313**
**TPM (Trusted Platform Modules), 349-350**
**transactions, secure, 304-305**
**Transport Layer Security (TLS), 227**
**tripwire offenses (Internet law), 365**
**trust, 235-236**
accountability, 238
*issuer accountability, 241-242*
*re-establishing, 239-240*
costs and benefits of, 236-237
definition of, 217
domain-validated encryption, 238
extended validation, 240-241
problems with, 226
promiscuous security, 237
Web of Trust, 221-224
**trusted agents, 249-250**
**Trusted Third Parties (TTPs), 235**
**trustworthy computing**
OS, 349-350
platform security, 347
*bootstrapping, 349*
*TPM, 349-350*
**"trustworthy computing," platform security, 348**
**trustworthy hardware, 249**
**TTPs (Trusted Third Parties), 235**

## *U*

**U.S. CAN-SPAM act, 365**
**ubiquitous authentication, default deny (secure networks), 327-330**
**ubiquitous policy enforcement, default deny (secure networks), 331-332**
**ubiquity**
customization, 305
identity, user experiences, 290
**unlinkable identifiers, 308-309**
**user centric, 289**
**user experience, 54-57**
identity, 288-289
*CardSpace, 291-294*
*log in, 290*
*OpenID, 294-295*
*registration, 290*
*roaming, 291*

*ubiquity, 290*
*user centric, 289*
**user interface, 54**
**user-level keying, e-mail (designing for deployment), 265**
**USPS (United States Postal Service): Internet law, 363**

## V

**validation authorities, 149**
**VDL (Verified Domains List), 150**
**VENORAdecrypts, 203**
**Verifone terminalks, credit cards, 220**
**VeriSign, 150**
**accountability, 239**
**VeriSign SiteSeal, 247**
**vigilante justice, spam, 132-133**
**viral marketing, 83**
**Vista (Windows), Allow or Deny dialog, 345**
**Vixie, Paul, 121, 146**

## W

**W3C (World Wide Web Consortium), 39, 93, 97**
**Wallace, Stanford, 120**
**warranties, certificates, 246-247**
**Web**
as killer application, 85-86
growth of, 81-85
**Web of Trust, 221-224**
**Web servers, SSL, 230-231**
**Web Services, 378, 382**
objective of, 377
**WiFi, 338**
**Windows Vista, Allow or Deny dialog, 345**
**wireless devices, adding to networks, 337-338**
**Wong, Meng Weng, 146**
**World Wide Web Consortium, 39, 93, 97**

## X

**XACML (eXtensible Access Control Markup Language), 299**
**XKMS (XMLKey Management Specification), 225-226**

## Y

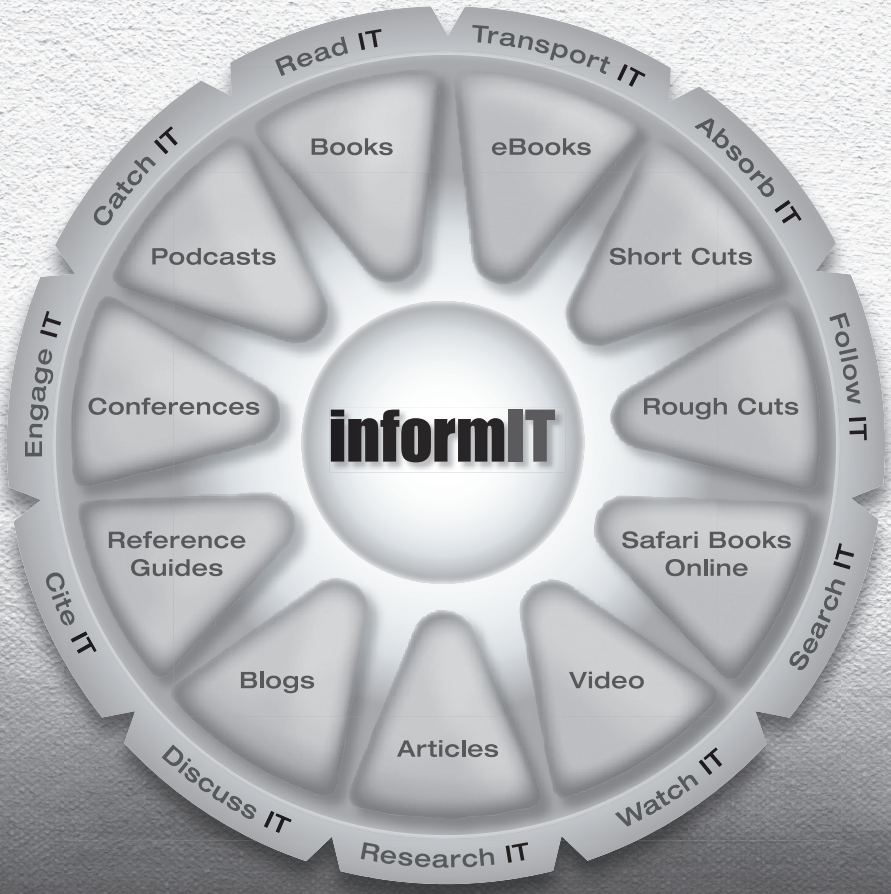
**Yahoo!, digital signatures, 267**

## Z

**zombie, 3**

# LearnIT at InformIT

## Go Beyond the Book




**11 WAYS TO LEARN IT** at **www.informIT.com/learn**

The online portal of the information technology publishing imprints of Pearson Education


# THIS BOOK IS SAFARI ENABLED

## INCLUDES FREE 45-DAY ACCESS TO THE ONLINE EDITION

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

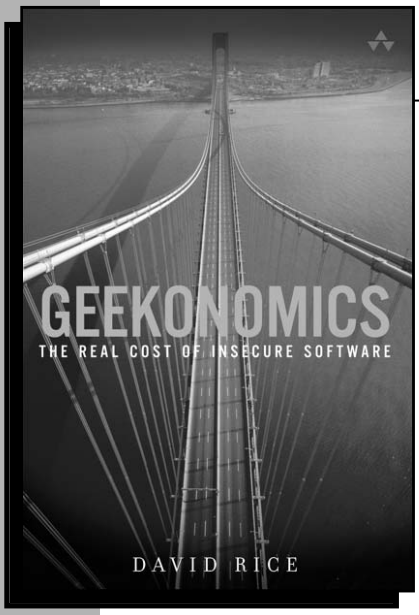
**TO GAIN 45-DAY SAFARI ENABLED ACCESS TO THIS BOOK:**

- Go to **http://www.awprofessional.com/safarienabled**
- Complete the brief registration form
- Enter the coupon code found in the front of this book on the "Copyright" page

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

# The Terrifying Cost of Insecure, Badly Written Software...

## and How to Finally Fix the Problem, Once and for All!




David Rice
ISBN 978-0-32-147789-7

Software has become crucial to the very survival of civilization. But badly written, insecure software is hurting people—and costing businesses and individuals billions of dollars every year. This must change. In *Geekonomics*, David Rice shows how we can change it.

Rice reveals why the software industry is rewarded for carelessness, and how we can revamp the industry's incentives to get the reliability and security we desperately need and deserve. You'll discover why the software industry still has shockingly little accountability—and what we must do to fix that.

Brilliantly written, utterly compelling, and backed by real-world data, *Geekonomics* is a long-overdue call to arms. Whether you're a software user, decision maker, developer, or manager, this book will change your life...or even the entire industry.

David Rice is an internationally recognized information security professional and an accomplished educator and visionary. For a decade he has advised, counseled, and defended global IT networks for government and private industry. David has been awarded by the U.S. Department of Defense for "significant contributions" advancing security of critical national infrastructure and global networks. Additionally, David has authored numerous IT security courses and publications, teaches for the prestigious SANS Institute, and has served as adjunct faculty at James Madison University. He is a frequent speaker at information security conferences and currently Director of The Monterey Group.