

Index

A

- access control 170
- access rights 60
- address filtering 319
- anomaly detection 40
- anonymity 61, 144
- asymmetric key systems 6
- authentication 1, 60, 174, 325
- authentication authority 59
- authentication authorization accounting (AAA) 316
- authentication infrastructure 58
- authentication methods 61
- authenticity 144, 170
- authorization 1, 325

B

- bandwidth 169, 224
- biometric information 63
- Bluetooth 8

C

- certificate 115
- certificate exchange 121
- certification authority (CA) 285

- client 111
- collaborative investigation team 166
- common mode failure 287
- community context 25
- compliance checker 119
- confidentiality 1, 144, 170, 171
- content download 12
- content on device 12
- context awareness 22
- context manager (CM) 90
- context-aware access control 85
- context-aware service provisioning 84
- convenience 205, 237
- credential 115
- credential authorities (CAs) 112
- credential language 115
- credential types 115
- credit reference 59
- cryptographic algorithm 325
- cryptography 173
- customer module 243
- cycle-stealing 172

D

- data confidentiality 5
- data integrity 5

data integrity 245
 data sets 116
 declaration 115
 decryption 37
 denial-of-service (DoS) 172
 digital cash 150
 digital credentials 110
 digital signature 219
 digital signature scheme 290
 digital signing key security 286
 digital wallet 195
 disabling of service 172
 disclosure policies 112
 disclosure policies language 117
 dishonest feedback 22
 DoS attack 21

E

eavesdropping 46, 171
 El Gamal public key cryptosystem 271
 electronic commerce (e-commerce)
 2, 19, 57, 58, 110, 141, 264
 electronic payment systems 217
 embedded operating system 243
 encrypted information 244
 enhanced messaging services (EMS)
 11
 entity authentication 245
 extensible authentication protocol
 (EAP) 141

F

feedback system 26
 flooding attack 46
 foreign agents (FA) 285
 fraud 219
 fraud management systems 205
 frequency hopping 173

G

global secure mobile payment service
 236
 GSM security 10

H

handheld device 142
 hash chain 219
 hash collisions 221
 hash sequences 221
 home agents (HA) 285
 home directory 67
 home location registry (HLR) 168
 home-base key 292
 host-based vulnerability scanner 42

I

impersonation 46
 in-band method 14
 in-band purchase 247
 integrity 1, 144, 170
 Internet 141, 165, 214
 Internet payment 251
 Internet service provider (ISP) 58
 interoperability 15, 170
 intrusion detection 36, 39
 intrusion detection system 41
 iPIN 199
 IPV6 319

J

Jalda 203
 Java 2 micro edition 243
 Java card 315

K

Kerberos 65
 key management 175
 key splitting 271
 KTH airlines 113

L

latency 169
 limited-liability keys 278
 local security association 321
 location awareness 22
 low security guarantee 317

M

- m-commerce fraud management 192
- m-Pay 201, 238
- m-payment 193
- m-payment lifecycle 194
- m-payment solution 192
- m-payment value chain 193
- malicious SMS messages 20
- man-in-the-middle 46, 171
- master agent 269
- MCKE 292
- memory card 315
- merchant module 244
- message authentication code (MAC) 223
- metadata manager (MM) 93
- micro-payment scheme 214
- micro-payment system 215
- microprocessor card 315
- middleware proxies 87
- millicent scheme 223
- misuse detection 39
- mobile agent (MA) 88, 263, 285
- mobile agent technology 142
- mobile auction 165
- mobile authentication protocol 323
- mobile commerce (m-commerce) 19, 57, 111, 140, 141, 164, 192, 214, 263
- mobile commerce platform 36
- mobile commerce security 1
- mobile communication system 224
- mobile content 246
- mobile cryptography 267
- mobile hose 312
- mobile network fraud 206
- mobile network operator (MNO) 238
- mobile networking 286
- mobile payment 1, 236
- mobile payment solutions 238
- mobile payment systems 197
- mobile phone fraud 205
- mobile stock trading 97
- mobile-IP network attack 289
- mobile-OP protocol 288
- multi-agent model 268

- multi-party micro-payment 216
- multicast routing 175
- multilevel security 170
- multimedia messaging services (MMS) 11
- multiple cryptography 270
- multisignatures 270

N

- negotiation tree 123
- NetPay scheme 222
- network access provider 59
- network hijack 45
- network infrastructure 7
- network layer security 319
- network-based scanner (NIDS) 41
- network-based vulnerability system 42
- Nokia 203
- non-repudiation 144

O

- online business model 143
- online e-business 149
- operating systems (OS) 242
- out-of-band model 14

P

- P2P payment 248
- Paybox 198
- payment credentials 60
- payment instruction 143
- payment lifecycle 15
- PayWord evaluation 222
- PayWord scheme 222
- PIN 241
- PKI 241
- point of sale 12
- point of sale (POS) payment 249
- policy language 113
- portable middleware facilities 94
- privacy 61, 171
- private key 245, 292
- private key-evolving scheme 291
- private keys refresh algorithm 299
- private keys update algorithm 298

proactive schemes 287
 proximity payment 14
 public key certificates 278
 public key infrastructure (PKI) 63
 public key system 6
 public keys 62
 public-key cryptosystem 263
 purchase order 143

R

R-term 117
 radio access network (RAN) 9
 random Oracle model 303
 refresh 293
 reliability 169
 remote digital signing 263, 276
 reputation data dissemination 22
 reputation system 19
 resource description framework (RDF)
 93

S

scanning tools 42
 secure authentication infrastructure 56
 secure electronic transaction (SET)
 145
 secure mobile commerce 167
 secure sockets layer (SSL) 65
 secure trust data transmission 23
 security 110, 140, 205, 244, 288, 324
 security assertion markup language
 (SAML) 66
 security associations 324
 security attack 171
 security requirements 60
 SeMoPS 236
 service provider 59, 82
 session hijacking 172
 shared secret 62
 signature generation 271
 signer key 292
 signing algorithm 300
 SIM card 66
 SIM toolkit (STK) 242
 smart card 66, 195, 312

sniffing 45
 spoofing 45
 symmetric key systems 6
 system state characterization 43

T

third parties 59
 threshold cryptography 270
 traffic analysis 171
 transaction context 25
 transaction specific risks 20
 tree manager 119
 trust 19
 trust model 23
 trust negotiation 109
 trust parameters 23
 trust relationships 57
 trust sequence 121
 trust-X 109, 119
 trust-X negotiations 120
 trust-X policies 117
 trusted third party (TTP) 245

U

UMTS security 10
 unauthorized access 45
 user 59
 user authentication 13, 57
 user registration protocol 321

V

verifiable signatures 61
 verifying algorithm 300
 virus attack 21
 Vodafone 200
 vulnerability analysis 36, 42
 vulnerability index evaluation 43
 vulnerability metrics 43

W

Wi-Fi security 8
 WICoCo 83
 wireless application protocol (WAP) 37,
 196

- wireless coverage area 168
- wireless identity module (WIM) 37, 196
- wireless Internet 81
- wireless local area networks (WLAN) 4
- wireless networking 286
- wireless security issues 167

X

- X-profile 116, 121