Index

a
access control systems 328
access threats 314
admission control approach
brutal admission control 413–415
customer’s satisfaction 401
demand-side management 402
fair priority-based admission control 417–419
GridLAB-D and GridMat simulation tools 400, 403
load admission control 403–404
load shedding mechanisms 400, 404–410
load-size-based admission control 413–416
normal operation 411–413
PHEV charging 402
priority-based admission control 416–418
priority-based load protection and control scheme 402
proposed approach 400
simulation scenarios 410–411
utility-side load management 402
wide area information (WAI)-based control scheme 402
wide area measurement (WAM) 402
Advanced Encryption Standard (AES) 184, 248, 309
advanced metering infrastructure (AMI) 264, 285
Alarm-Net 311
anomaly detection 346–347
anonymity 188–189
anonymized authentication 199
arranger robot 197
artificial neural network (ANN) 290
assistant robots 197
attack strategies 288–289
attribute-based access control (ABAC) model 164
attribute-based encryption (ABE) 196, 207–208
authentication 189–190, 207
automatic repeat request 227

b
biometric solutions 315–316
BLE. Bluetooth 309
block chain 187
Bluetooth 309
body area network (BAN) 266
body area network authentication (BANA) scheme 317
bolus-enabled temperature sensing 381
boothstrapping 212–213
Building Automation and Control Networks (BACnet) 335–336
building automation systems (BAS) 330
Byzantine attack 230

C
CapBAC model 164
certificate revocation lists (CRLs) 197
certification authority (CA) 274
ciphertext 184
ciphertext (encrypted) character 183
ciphertext-policy attribute-based encryption scheme 208–209

Edited by Houbing Song, Glenn A. Fink and Sabina Jeschke.
© 2018 John Wiley & Sons Ltd. Published 2018 by John Wiley & Sons Ltd.
city-based cloud  277
cloud-based robotic networks
  ad hoc network  218
  attribute-based encryption  196
  communication security  207–212
  as a community  200–201
  doctrine  201–207
  law governed interaction  218
  Persona  219
  policy-based establishment  201
  security management  212–217
  security requirements  200
  security threats and challenges  199
Terminodes  218
Cloud computing and IoT
Arduino YUN security
  extensions  149
  hardware  140–141
  legacy protocols  137
OpenStack  141
reference scenario and motivation  142
remote attestation  152
SAaaS vision  137
secure registration  151–152
security and privacy  139–140
security keys, cryptographic algorithms,
  and hidden IDs  148–149
sensing resource virtualization and
  management  139
Stack4Things architecture  138
board-side architecture  144–145
board-side security extension  149–150
cloud-side security extension  150
control and actuation  145–146
security services  150
sensing data collection  146
Trusted Computing  147–148
web connectivity  141
WebSocket technology  138
Cloud services  26
CodeBlue  310
collaborative last mile logistics  361
collar-mounted accelerometers  383
communication security
  attribute-based encryption  207–208
ciphertext-policy attribute-based
  encryption scheme  208–209
CP-ABE key revocation  209–210
integration of CP-ABE and robot
  community architecture  210–212
preliminaries  208
Shamir’s secret sharing  209
computationally hard/information theoretic
  technique  183
confidentiality  182–186
  data confidentiality  313, 391–392
lightweight cryptography (LWC)  250
security and privacy  2
constraints specification  205–206
Cow Manager  380
CP-ABE key revocation  209–210
CRYPE  317
cryptographic hash function  187
cryptographic solutions  316–318
cryptography  274–276
cyber-network-defense
  (CND)  180–181
cyber-physical hacking  389
cyber-physical systems (CPS)
  air traffic control  245
  applications  243
  cybercriminals  117
  definition  243
  embedded system  4
infrastructureal CPSs  5
key management
  accountability  122
  centralized vs. distributed scheme  128–129
  challenges and open research issues  132–133
  communications  118–119
  deterministic vs. probabilistic scheme  129–130
  dynamic vs. static management  124–125
  embedded processors  118
  freshness  122
  heterogeneity  122
  interoperability  123
  key distribution and key revocation  131
Index
429

public key vs. symmetric key 125–128
real-time availability 122–123
resilience to attacks 123
SCADA systems 131–132
scalability 121
security goals 120–121
standard vs. proprietary scheme 130
survivability 123–124
threats and attacks 119–120
personal CPS technologies 5–6
security and privacy 245–246
security services 117
specific computational and physical processes 244
system workflow 244–245
wireless technologies 117
cyber-physical vulnerabilities
damage to the lives 273–274
damage to the properties 273
definition 270
interactions and threats 271
possible attacks 271–272
privacy infiltration 274
service interruption 272–273

d
Data Encryption Standard (DES) 248
data integrity attacks 283
data-loss liability 192
data ownership and usage policies 191
data retention and destruction policies 192
data security controls 191–192
DeLaval farm-monitoring camera system 378–379
denial-of-service (DOS) attack 246, 314
DESL 251–252
DESXL 251–252
detection 4, 289
deterrence 3–4
disclosure threat 314
discrete logarithm problem 183
distributed cybersecurity monitoring (DSM) 180–181
distributed security monitoring system anonymity 188–189
authentication 189–190
confidentiality 182–186
data-loss liability 192
data ownership and usage policies 191
data retention and destruction policies 192
data security controls 191–192
information security 179–181
integrity 186–188
minimality 188
privacy policies and consent 192
trading security for cost 182
transparency 190–191
documentation
abstract community description 202
attribute types and user-attribute assignment policies 203
authentication 207
authorization and obligation policies 203–205
constraints specification 205–206
definition 201
information model 202–203
preferences specification 206
service access control 207
trusted key specification 206
Dossia 319

e
EASiER 219
eavesdropping attack 231–232
secure data storage 234–237
secure data transmission 234–236
eCare Companion 319–320
ECC-based public key scheme 316
E-Government Act of 2002 355
electric power 5
electric vehicles (EVs) 265
elliptic curve cryptography (ECC) 254–255
Elliptic Curve Primitive 248
encryption 182
endorser robot 197
End-User License Agreement (EULA) 12
energy-based cyber-physical system 283
enhanced mail and parcel services
feedback loop 362
new services 362
operational cost reduction of missed
delivery 362
security and convenience for recipients
smart mailbox 363–364
visibility 361
EnOcean Radio Protocol 338
EnOcean Serial Protocol 338
estrus monitoring 379–380
f
facility management systems 329–330
“farm-to-fork” animal tracking 377
feature data 287
Federal Aviation
Administration 109–111
Federal Communications Commission 105–106
Federal Trade Commission (FTC)
consumer focus 104
deceptive trade practices 102–104
unfair trade practices 102
fire alarm systems 328
firewalls 345
Food and Drug Administration 108–109
“French IoT” initiative 357
g
game theoretic deployment 277
garbled circuit computation 185
Google Health 319
GridLAB-D simulation tool 282
GrowSafe system 381
guide robots 195
h
hashtag 187
Health 320
Google Health 319
rumen health 380–382
HealthVault 319
Heatime 380
heating, ventilation, and air conditioning
(HVAC) systems 328
HIGHT 252
housekeeping robots 195
i
identity threat 314
IEEE 802.15.6 310
IEEE 802.15.4 standard 309
individual mailbox/parcelbox model 364
industrial robots 195
information security 2, 179–181, 191
integrity 186–188
intelligent sensor network
(ISN) 269–270
intelligent transport system applications
intelligent sensor network 269–270
roadside unit 268–269
vehicular sensor network 269
Intel™ processor architecture 184
Internet Engineering Task Force (IETF) 112
Internet of postal things (IoPT)
competing on price to competing on
overall value 357
critical brand attribute 355–356
customer demand for information 356
development stages 367–368
energy costs 364
enhanced mail and parcel services
361–364
implementation challenges 368–370
from industries to ecosystems 357
neighborhood services 365–367
operational experience in data collection
and analytics 356
smarter post office 365
“smart” products and services 357
successful platform strategy 371
transportation and logistics 358–361
vast infrastructure 354–355
from workforce replacement to
human-centered automation
357–358
Internet of Things (IoT) 25, 77, 179
access control adaptation
context-aware security policies 165
enforcement issues 167–168
personal sensor network 165
semantic context-aware policies 166–167
access control models
attribute-based access control (ABAC) model 164
CapBAC model 164
location and context information 161
node mobility 162
novel policy languages 161
policy-based approaches 161
policy decision point (PDP) 162
policy enforcement/deployment 162
role-based access control (RBAC) model 163
runtime innovative models 161
in agriculture 384–385
cyber-physical system vulnerabilities 385–386
data confidentiality 391–392
data integrity 393
data leakage via leased equipment and software 388–389
misuse of provenance data 387–388
misuse of research data 387
misuse of video data 386–387
political action and terrorism 389–390
system availability 393
system safety 393–395
and Cloud computing (see Cloud computing and IoT)
heterogeneity and resource constraints 158–159
IoT-enhanced PA 383
legal considerations (see legal issues, for CPS and IoT)
Proteus model 168–174
size and dynamicity 160
intersection attacks 188
intrusion detection system (IDS) 276

k
KATAN 253
key distribution center (KDC) 274
key management
accountability 122
centralized vs. distributed scheme 128–129
challenges and open research issues 132–133
communications 118–119
deterministic vs. probabilistic scheme 129–130
dynamic vs. static management 124–125
embedded processors 118
freshness 122
heterogeneity 122
interoperability 123
key distribution and key revocation 131
public key vs. symmetric key 125–128
real-time availability 122–123
resilience to attacks 123
SCADA systems 131–132
scalability 121
security goals 120–121
standard vs. proprietary scheme 130
survivability 123–124
threats and attacks 119–120
key predistribution-based tag encoding scheme 233
KLEIN 252
KNX/EIB 333–335
KTAN-hardware-oriented cipher 258
KTANTAN 253

I
LAURA 311–312
law governed interaction (LGI) 218
LED 253
legacy systems 19–20
legal issues, for CPS and IoT
anti-Paparazzi law 99
Computer Fraud and Abuse Act 99
contractual and tort liability, personal injuries 99
digital music file sharing 97
federal and state laws 96
Fifth Amendment 96
government and nongovernment intrusion 98
Griswold v. Connecticut 98
HIPAA Act 99
legal issues, for CPS and IoT (contd.)  

laissé faire approach 97  
regulatory legal issues  
executive branch agencies 101  
Federal Aviation Administration 109–111  
Federal Communications Commission 105–106  
Federal Trade Commission 101–104  
Food and Drug Administration 108–109  
National Highway and Traffic Safety Administration 106–108  
standards of care 101  
Riley v. California 98  
Roe v. Wade 98  
statutory and regulatory protection 99  
U.S. v. Quartavious Davis 98  
LifeGuard 310–311  
lighting control systems 328  
lightweight cryptography  
(LWC) 243–244  
authentication 250  
clever outside attacker 249  
confidentiality 250  
data communication 250  
data encryption standard 247  
design constrains 247  
design goals 247  
embedded systems 249  
funded organizations 249  
hardware implementations of asymmetric ciphers 254–255  
hardware implementations of symmetric ciphers 251–253  
information security services 249  
invasive attacks 249  
knowledgeable inside attacker 249  
lightweight symmetric ciphers 250  
limited-resources systems 249  
low computation cryptographic algorithms 247  
opportunities and challenges 257–258  
passive attacks 249  
secure hash algorithms 256–257  
security services 247  
smart object networks 249  
software implementations of asymmetric ciphers 255  
software implementations of symmetric ciphers 253–254  
symmetric and asymmetric cryptography 248  
lightweight encryption scheme 236  
linear network coding 226  
linear secret sharing 185  
link loss rate inference 228–229  
load-altering attack 288  
localized encryption and authentication protocol (LEAP) 275  
LonTalk protocol 339  
LWC. see lightweight cryptography (LWC)  
m  
machine learning-based detection 282, 290–291  
man-in-the-middle attacks 189  
masquerade attack threat 314  
mathematical metrics  
derivation of mutual information 72–74  
information theoretic foundations 62–63  
k-anonymity, concept of 65–68  
proof of corollary 74  
Smart City scenario 58  
smart home scenario 58  
surprise and specific information 63–64  
medical cyber-physical systems  
access threats 314  
authentication 313  
authorization 313  
biometric solutions 315–316  
challenges with LPWNs in WBANs 308  
cryptographic solutions 316–318  
data confidentiality 313  
data freshness 313  
data integrity 313  
data security and privacy threats and attacks 314  
disclosure threat 314  
Dossia 319  
eCare Companion 319–320  
extisting WBAN-based health monitoring systems 310–312
feedback control in WBANs 308–309
fundamental security requirements 312
Google Health 319
Health 320
HealthVault 319
identity threat 314
interference in WBANs 308
network topology 307–308
patient’s prescription leakage 314
privacy 313
radio technologies 309–310
Redwood MedNet 319
solutions on implantable medical devices 318–319
WBANs 306–307
wireless sensor networks 306
MEDiSN 311
message authentication code (MAC) 276
minimality 188
MobiCare 311
Mobile Delivery Devices (MDD) 356
Modbus 339
MooMonitor 380
mopper robots 197
multichannel authentication 189
multifactor authentication 189
mutual authentication and access control scheme based on elliptic curve cryptography (MAACE) 317
n
nanotechnology 94
National Institute of Science and Technology CPSs 244
National Institute of Standards and Technology (NIST) 2
national livestock identification system (NLIS) 377
national security concerns
CIA Triad 79
companies and consumers 79
data breaches 79
data’s confidentiality 79
denial-of-service attacks 79
file’s integrity 79
future attacks 82
German SteelMill 81–82
international law-of-war principles
jus ad bellum and jus in bello 83
Tallinn Manual 83
Stuxnet 80–81
use of military force
armed attack 87–89
Article 2(4) of United Nations Charter 84
Article 51 of United Nations Charter 84
Nicaragua v. United States 84
physical system 86
United Nations Draft Articles on Responsibility of States for Internationally Wrongful Acts 86
warfare law 84
NATO Cooperative Cyber Defence Centre of Excellence 78
neighborhood services, IoPT
carriers as neighborhood logistics managers 366–367
dollar value of IoPT applications 367
smart cities need local partners 365–366
network coding
background and preliminaries 225–226
Byzantine attack 230
classification of security attacks
Byzantine and pollution attacks 233–234
defense against Byzantine and pollution attacks 233–234
defense against traffic analysis 234
eavesdropping attack 231–232,
234–237
max-flow min-cut theorem 223
network tomography 228–229
pollution attack 230
protocol simplification 228
random linear network coding 223
robustness enhancement 227–228
secret key exchange 237–238
security 229
state-aware network coding protocols 229–230
network coding (contd.)
  stateless network coding protocols 229
  throughput/capacity enhancement 226–227
  traffic analysis 230–231
  in wired networks 223–224
  in wireless networks 223–224
  network model 285–286
network security and privacy
  client-server model 26
  Cloud-interconnected CPSs
    data handling requirements 46
    data storage 42–44
    model-driven privacy 46
    security mechanisms 44–45
Cloud services 26
CPS reference model
  All-IP vision 30
  Big Data 30
  cloud level 28
  Cloud platforms 29
  control/enterprise level 27
  device level 27
  future evolution 28
  RFID technology 29
  smartphones 29
  threats and challenges 30–31
  wireless sensor networks (WSNs) 29
Internet of Things 25
internet-wide secure communication
  Cloud services 36
  end-to-end security protocols 37–39
  RAM and ROM 38
  resource heterogeneity 39–41
  transport layer security (TLS) 37
local communication, security of
  Internet Protocol (IP) 35
  6LoWPAN fragments 35
  medium access control 34–35
  network layer 35
  physical layer 34
secure device bootstrapping
  device life cycle 33–34
  initial key exchange 33
network tomography 228–229
nice but curious nodes 231

O
  one-time pad cryptosystem 183
Online Social Network (OSN) 219
OpenStack 141
operating system hardening 343–344

P
  Pacific Northwest National Laboratory (PNNL) 403
  patching 344
  P-coding 236
  PEACE framework 199
  Persona 219
  personal CPS technologies 5–6
  personally identifiable information (PII) 2
  physiological values scheme (PVS) 315
  pollution attack 230
  precision agriculture (PA) 375. see also precision livestock farming (PLF)
  precision livestock farming (PLF)
    estrus monitoring 379–380
    feedback control loops 375–376
    food quality and provenance 377–378
    impact on the environment 382
    IoT solutions 383–384
    IoT technology 376
    labor and workforce effects 377
    rumen health 380–382
    single biochemical process 375–376
    transparency and remote management 378–379
PRESENT 252
PRINCE 253
Privacy Act of 1974, 355
privacy and technology, history of
  cellular phones 94
  Federal regulatory control 95
  Internet connections 95
  oral and written communications 95
  “pen register,” 95
  telegraph 95
  Twitter and Facebook 96
privacy policies and consent 192
programmable logic controller (PLC) 8
Proteus model
  access control policies 169
  access zone element 171
Index 435

active contexts 169
authentication element 171
communication element 171
identity element 171
IoT 172–174
policy conflicts and inconsistencies 170
policy specifications 168
protection context modeling 169
requestor context 169, 171
protocol simplification 228
public key cryptography 125–126
public-key cryptosystems 184
public key-infrastructure (PKI) 275

q
Quality of Context (QoC) 175–176

r
Radio-Frequency Identification (RFID) tags 356
random linear network coding 226
Redwood MedNet 319
reidentification 188
resource heterogeneity
denial-of-service protection 40–41
retransmission mechanisms 39–40
responsibility matrix 345
Resurrecting Duckling Protocol 218
roadside unit 268–269
robot-supported product management system 197–198
role-based access control (RBAC) model 163
routing threats 314
RSA 125, 189, 255
rumen health 380–382

s
SaaS vision 137
SATIRE 311
secret key exchange 237–238
secure coding 343
secure hash algorithms (SHA) 256–257
Securing User Access to Medical Sensing Information (SecMed) 316
security and privacy
authentication 3
barriers and identifiers 8
blending information 12–14
computerized skid detectors 5
cryptographic confidentiality 2
cyber-physical terrorism 8–9
defense-in-breadth, principle of 16–17
defense-in-depth, principle of 16
definition 2
digital signatures and secure hashes 3
distributed systems 21
end-to-end security 17–18
identity and authentication management 20
least privilege 14–15
legacy systems 19–20
motivating sharing 12
need-to-know, principle of 15
network-connected appliances 12
nonrepudiation 3
pattern obfuscation 17
physical protection 3–4, 8
politicians and industry leaders 2
port attack 10
privacy regulations 18–19
programmable logic controller (PLC) 8
security attack points, in CPSs 6
security surveys 8
segmentation 15–16
smart car hacking 9–10
tamper detection/security 18
user-configurable data collection/logging 17
wearable devices 11–12
security breaches 77
security management, cloud-based robotic networks
bootstrapping 212–213
joining the community 214–215
leaving a community 215–216
service access control 216–217
segmentation 15–16
self-defense 78
sensor spoof prevention 187
sensor substitution and modification of data in transit 187
sequential hypothesis testing-based
detection 282, 291–292
service access control 207, 216–217
SERVICE BROADCAST message 196
service level agreements (SLAs) 200
SERVICE REQUEST message 196
Shamir’s secret sharing 209
shared parcel box model 363–364
signature scheme 233
Silent Herdsman 380
smart appliances 6
smart buildings
  access control systems 328–329
  anomaly detection 346–347
  attacks 340–342
  BACnet 335–336
  BAS communication protocols 332
  building automation systems 330
  definition 327–328
  EnOcean 338–339
  facility management systems 329–330
  fire alarm systems 328–329
  firewalls 345
  fuzzing approaches 347
  HVAC systems 328–329
  interoperability and interconnectivity 339–340
  known cases of attacks 331–332
  KNX/EIB 333–335
  lighting control systems 328–329
  LonTalk protocol 339
  Modbus 339
  monitoring and intrusion detection systems 345
  operating system hardening 343–344
  patching 344
  physical access control 343
  raising security awareness and develop security know-how 342–343
  responsibility matrix 345
  secure coding 343
  separation of networks 345
  smart cities 330–331
  traffic normalization 346
  video surveillance systems 328–329
  visualization 346
  ZigBee 336–338
smart cities
  bluetooth detector 59
  Bluetooth ID 61
  bluetooth receiver 60
  concept and components 263–265
cryptography 274–276
cyber-physical vulnerabilities 271–274
game theoretic deployment 277
intelligent sensor network 269–270
intrusion detection system 276
localization 60
managed security 277–278
physical security measures 278
privacy-preserving system 60
real-time monitoring and safety alert 270
roadside unit 268–269
smart homes 265–267
substation monitoring 267–268
system perspective
  anonymization, of Bluetooth ID 71
  attack with anonymization, of ZIP 70–71
  attack without anonymization 68–70
  traffic efficiency 59
  vehicular sensor network 269
  watchdog system 277
smarter post office 365
smart grid 264, 267–268
admission control approach (see admission control approach)
data integrity 281
demand response process 399
distribution 403
evaluation results 294–297
evaluation setup 292–294
excess load 403
extension 297–298
GridLAB-D simulation tool 282
literature review 283–284
load management 400
machine learning-based detection 282, 290–291
network model 285–286
overview 287–289
physical domain and cyber domain 399
power generator 399
power grid simulation model 403
sequential hypothesis testing-based detection 282, 291–292
statistical anomaly-based detection 282, 289–290
substation 403
threat model 286–287
Smart Grid Program 244
smart homes 265–267
smart mailbox 363–364
Stack4Things 138
  board-side architecture 144–145
  board-side security extension 149–150
  cloud-side security extension 150
  control and actuation 145–146
  security services 150
  sensing data collection 146
state-aware network coding protocols 229–230
stateless network coding protocols 229
statistical anomaly-based detection 282, 289–290
Stuxnet 80–81
substation cluster head gateway 268
supervisory control and data acquisition (SCADA) 286
transparency 190–191
transportation and logistics 358–359
  collaborative last mile logistics 361
  driverless vehicles 360
  fuel management 359–360
  load optimization 360
  predictive maintenance 359
  real-time dynamic routing 360–361
  usage-based insurance 360
Transport Layer Security (TLS) 184
transposition substitution folding shifting encryption algorithm (TSFS) 248
trusted key specification 206
trusted third party (TTP) 274
TWINE 253
two-stage attacking scheme 284
U
UbiMon 310
ultra-wideband (UWB) standard 310
V
vehicle-to-infrastructure (V2I) communication 265
vehicle-to-vehicle (V2V) communication 265
vehicular sensor network (VSN) 269
video surveillance systems 328–329
virtual hardware security module (HSM) 185
voiceprints 12
W
watchdog system 277
weakly secure system 236
Web Application Messaging Protocol (WAMP) 138
WebSocket technology 138
wireless body area networks (WBANs) 305
wireless sensor networks (WSNs) 29
  intelligent sensor network 269–270
  real-time monitoring and safety alert 270
  roadside unit 268–269
  smart homes 265–267
  substation monitoring 267–268
  vehicular sensor network 269
wiretapping nodes 231
X
XTEA 253
Z
ZigBee 309, 336–338