Table of Contents

Preface **ix**

Chapter 1: A Brave New World **1**

Defining the IoT **3**

Cybersecurity versus IoT security and cyber-physical systems 5

Why cross-industry collaboration is vital **7**

IoT uses today **10**

Energy industry and smart grid 11

Connected vehicles and transportation 11

Manufacturing 11

Wearables 12

Implantables and medical devices 12

The IoT in the enterprise **13**

The things in the IoT 17

The IoT device lifecycle 17

The hardware 19

Operating systems 20

IoT communications 21

Messaging protocols 23

Transport protocols 27

Network protocols 28

Data link and physical protocols 28

IoT data collection, storage, and analytics 30

IoT integration platforms and solutions 30

The IoT of the future and the need to secure **31**

The future – cognitive systems and the IoT 31

Summary **32**

Chapter 2: Vulnerabilities, Attacks, and Countermeasures 33
Primer on threats, vulnerability, and risks (TVR) 34
The classic pillars of information assurance 34
Threats 36
Vulnerability 36
Risks 38
Primer on attacks and countermeasures 39
Common IoT attack types 39
Attack trees 41
Building an attack tree 42
Fault (failure) trees and CPS 46
Fault tree and attack tree differences 47
Merging fault and attack tree analysis 47
Example anatomy of a deadly cyber-physical attack 49
Today's IoT attacks 52
Attacks 53
Wireless reconnaissance and mapping 53
Security protocol attacks 54
Physical security attacks 54
Application security attacks 54
Lessons learned and systematic approaches 55
Threat modeling an IoT system 56
Step 1 – identify the assets 58
Step 2 – create a system/architecture overview 59
Step 3 – decompose the IoT system 62
Step 4 – identify threats 65
Step 5 – document the threats 68
Step 6 – rate the threats 69
Summary 70
Chapter 3: Security Engineering for IoT Development 71
Building security in to design and development 72
Security in agile developments 73
Focusing on the IoT device in operation 76
Secure design 78
Safety and security design 79
Threat modeling 79
Privacy impact assessment 79
Safety impact assessment 80
Compliance 81
Security system integration 84
Processes and agreements 88
Secure acquisition process 88
Secure update process 88
Establish SLAs 88

Establish privacy agreements 89
Consider new liabilities and guard against risk exposure 90
Establish an IoT physical security plan 91
Technology selection – security products and services 92
IoT device hardware 92
Selecting an MCU 92
Selecting a real-time operating system (RTOS) 93
IoT relationship platforms 94
Cryptographic security APIs 95
Authentication/authorization 97
Edge 98
Security monitoring 99
Summary **102**
Chapter 4: The IoT Security Lifecycle **103**
The secure IoT system implementation lifecycle **104**
Implementation and integration 105
IoT security CONOPS document 105
Network and security integration 107
System security verification and validation (V&V) 111
Security training 112
Secure configurations 113
Operations and maintenance 116
Managing identities, roles, and attributes 116
Security monitoring 120
Penetration testing 122
Compliance monitoring 126
Asset and configuration management 126
Incident management 128
Forensics 128
Dispose 128
Secure device disposal and zeroization 129
Data purging 129
Inventory control 129
Data archiving and records management 129
Summary **130**
Chapter 5: Cryptographic Fundamentals for IoT Security Engineering **131**
Cryptography and its role in securing the IoT **132**
Types and uses of cryptographic primitives in the IoT 133
Encryption and decryption 134
Symmetric encryption 136
Asymmetric encryption 138
Hashes 139
Digital signatures 141
Symmetric (MACs) 143

Random number generation 144
Ciphersuites 146
Cryptographic module principles 147
Cryptographic key management fundamentals 153
Key generation 155
Key establishment 155
Key derivation 156
Key storage 158
Key escrow 158
Key lifetime 158
Key zeroization 159
Accounting and management 160
Summary of key management recommendations 161
Examining cryptographic controls for IoT protocols 162
Cryptographic controls built into IoT communication protocols 162
ZigBee 163
Bluetooth-LE 165
Near field communication (NFC) 167
Cryptographic controls built into IoT messaging protocols 167
MQTT 167
CoAP 167
DDS 168
REST 168
Future directions of the IoT and cryptography 169
Summary 171
Chapter 6: Identity and Access Management Solutions for the IoT 173
An introduction to identity and access management for the IoT 174
The identity lifecycle 176
Establish naming conventions and uniqueness requirements 177
Naming a device 178
Secure bootstrap 179
Credential and attribute provisioning 181
Local access 183
Account monitoring and control 183
Account updates 183
Account suspension 184
Account/credential deactivation/deletion 184
Authentication credentials 184
Passwords 184
Symmetric keys 185
Certificates 186

X.509 186
IEEE 1609.2 187
Biometrics 187
New work in authorization for the IoT 188
IoT IAM infrastructure 188
802.1x 189
PKI for the IoT 189
PKI primer 190
Trust stores 192
PKI architecture for privacy 193
Revocation support 194
Authorization and access control 195
OAuth 2.0 195
Authorization and access controls within publish/subscribe protocols 197
Access controls within communication protocols 198
Summary 198
Chapter 7: Mitigating IoT Privacy Concerns 199
Privacy challenges introduced by the IoT 200
A complex sharing environment 201
Wearables 202
Smart homes 202
Metadata can leak private information also 202
New privacy approaches for credentials 203
Privacy impacts on IoT security systems 204
New methods of surveillance 205
Guide to performing an IoT PIA 206
Overview 206
Authorities 208
Characterizing collected information 208
Uses of collected information 212
Security 212
Notice 213
Data retention 214
Information sharing 214
Redress 215
Auditing and accountability 216
PbD principles 216
Privacy embedded into design 216
Positive-sum, not zero-sum 217
End-to-end security 217
Visibility and transparency 218
Respect for user privacy 218

Privacy engineering recommendations 219
Privacy throughout the organization 220
Privacy engineering professionals 221
Privacy engineering activities 222
Summary 223
Chapter 8: Setting Up a Compliance Monitoring Program for the IoT 225
IoT compliance 226
Implementing IoT systems in a compliant manner 227
An IoT compliance program 229
Executive oversight 229
Policies, procedures, and documentation 230
Training and education 231
Testing 234
Internal compliance monitoring 234
Periodic risk assessments 239
A complex compliance environment 244
Challenges associated with IoT compliance 244
Examining existing compliance standards support for the IoT 245
Underwriters Laboratory IoT certification 245
NIST CPS efforts 246
NERC CIP 247
HIPAA/HITECH 248
PCI DSS 248
NIST Risk Management Framework (RMF) 250
Summary 251
Chapter 9: Cloud Security for the IoT 253
Cloud services and the IoT 254
Asset/inventory management 254
Service provisioning, billing, and entitlement management 255
Real-time monitoring 255
Sensor coordination 255
Customer intelligence and marketing 256
Information sharing 256
Message transport/broadcast 257
Examining IoT threats from a cloud perspective 257
Exploring cloud service provider IoT offerings 259
AWS IoT 259
Microsoft Azure IoT suite 264
Cisco Fog Computing 265
IBM Watson IoT platform 267
MQTT and REST interfaces 267

Cloud IoT security controls **268**
Authentication (and authorization) 268
Amazon AWS IAM 268
Azure authentication 269
Software/firmware updates 269
End-to-end security recommendations 270
Maintain data integrity 271
Secure bootstrap and enrollment of IoT devices 272
Security monitoring 272
Tailoring an enterprise IoT cloud security architecture **273**
New directions in cloud-enabled IOT computing **275**
IoT-enablers of the cloud 275
Software defined networking (SDN) 275
Data services 276
Container support for secure development environments 276
Containers for deployment support 277
Microservices 277
The move to 5G connectivity 278
Cloud-enabled directions 278
On-demand computing and the IoT (dynamic compute resources) 278
New distributed trust models for the cloud 279
Cognitive IoT 280
Summary **280**
Chapter 10: IoT Incident Response **281**
Threats both to safety and security **282**
Planning and executing an IoT incident response **285**
Incident response planning 287
IoT system categorization 287
IoT incident response procedures 289
The cloud provider's role 290
IoT incident response team composition 291
Communication planning 292
Exercises and operationalizing an IRP in your organization 292
Detection and analysis 293
Analyzing the compromised system 295
Analyzing the IoT devices involved 298
Escalate and monitor 299
Containment, eradication, and recovery 300
Post-incident activities 301
Summary **302**
Index **303**