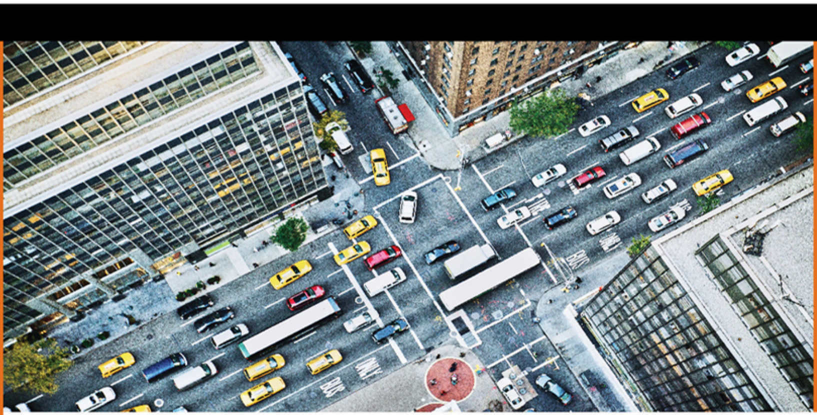
SECURITY



Orchestrating and Automating Security for the Internet of Things

Delivering Advanced Security Capabilities
from Edge to Cloud for IoT

Anthony Sabella, CCIE® No. 5374
Rik Irons-Mclean
Marcelo Yannuzzi

With Foreword by Maciej Kranz
VP, Cisco Strategic Innovation Group, Cisco Strategy Office (CSO)

ciscopress.com

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Orchestrating and Automating Security for the Internet of Things

Anthony Sabella, CCIE No. 5374
Rik Irons-Mclean
Marcelo Yannuzzi

Cisco Press

Orchestrating and Automating Security for the Internet of Things

Anthony Sabella
Rik Irons-Mclean
Marcelo Yannuzzi

Copyright © 2018 Cisco Systems, Inc.

Published by:
Cisco Press

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

01 18

Library of Congress Control Number: 2018938188

ISBN-13: 978-1-58714-503-2

ISBN-10: 1-58714-503-0

Warning and Disclaimer

This book is designed to provide information about Internet of Things Security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Senior Project Editor: Tonya Simpson

Copy Editor: Krista Hansing Editorial Services, Inc.

Technical Editors: Brian Sak, Maik Seewald

Editorial Assistant: Vanessa Evans

Cover Designer: Chuti Prasertsith

Composition: Studio Galou

Indexer: Publishing Works, Inc.

Proofreader: Chuck Hutchinson

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

About the Author(s)

Anthony Sabella, CCIE No. 5374, is the lead cybersecurity architect for the Enterprise Chief Technology Office at Cisco and has worked at Cisco for eight years. Anthony leads innovative work streams on methods to break free from manual tasks by applying the latest virtualization and orchestration techniques to cybersecurity. He combines this with machine learning concepts and the ingestion of intelligence feeds, to design effective solutions that can self-manage and self-heal. Anthony applies these concepts across a variety of use cases, including financial institutions, healthcare, energy, and manufacturing (examples included in this book).

Before joining Cisco, Anthony worked as principal engineer for a global service provider for 13 years, where he created cybersecurity solutions for enterprise customers. Anthony was also the cofounder and CTO for a technology consulting firm responsible for designing cybersecurity solutions for both commercial and enterprise customers. Anthony's expertise has resulted in speaking engagements at major conferences around the world for both Cisco and its major partners. Anthony holds a master's degree in computer science and an active CCIE, and he is a contributing member in the IEEE Cyber Security community.

Rik Irons-Mclean is the Industry Principal for Oil & Gas at Cisco. Rik has worked at Cisco for 11 years and has had lead roles in IoT/IIoT, communications and security for power utilities and process control industries, and energy management and optimization. He has led technical global teams in taking new products to market in all theaters, specializing in driving new technology adoption in both established and emerging markets. Before joining Cisco, he worked for a Cisco service provider partner for eight years, where he focused on converged solutions.

Rik has represented Cisco in a number of industry and standards bodies, including Open Process Automation, IEC 61850 for industrial communications, and IEC 62351 for industrial security. Additionally, he elected the U.K. lead for Cigre SC D2 for communications and security in the power industry. Rik has written for a number of industry publications and authored whitepapers on such topics as industrial cybersecurity, IoT security, distributed industrial control systems, next-generation operational field telecoms, fog computing, and digital IoT fabric architectures.

Rik holds a bachelor of science degree and a master of business administration degree, focused on international leadership. He is currently studying for a doctorate in cybersecurity.

Marcelo Yannuzzi is a principal engineer at the Chief Strategy Office in Cisco. Marcelo leads strategic innovation in the areas of IoT, security, and novel architectures fusing cloud and fog computing. He has led flagship innovations across different industry verticals, some of which are outlined in this book. Marcelo also provides strategic advisory on new business opportunities and technologies for Cisco and start-ups.

Before joining Cisco, Marcelo was the head of the Advanced Network Architectures Lab at the Department of Computer Architecture in a Barcelona university. He was the cofounder and CTO of a start-up for which Cisco was its first customer. Marcelo is the author of more than 100 peer-reviewed publications, including top journals and conferences in the areas of IoT, fog computing, security, NFV, software-defined systems (SDX), multilayer network management and control, sensor networks, and mobility. Marcelo has led several European research projects and contracts in the industry, and his research was funded multiple times by Cisco. He is a frequent speaker and invited panelist at major conferences and forums. He held previous positions as an assistant professor at the physics department in a university's school of engineering.

Marcelo holds a bachelor's degree in electrical engineering and both a master of science degree and a Ph.D. in computer science.

About the Technical Reviewers

Brian Sak, CCIE No. 14441, is a solutions architect at Cisco Systems who focuses on solutions development and enablement for Cisco security products and services. Brian has more than 20 years of experience in information security, spanning such facets as consultative services, assessment services and penetration testing, implementation, architecture, and practice development. Brian holds a master's degree in information security and assurance, holds many technical security and industry certifications, and has contributed to or authored publications from The Center for Internet Security, Packt Publishing, and Cisco Press.

Maik Seewald has nearly 30 years of engineering and security experience. He works as a senior technical leader in the Cisco Enterprise Networking Group, where he focuses on the development of industrial IoT architecture, security, and standards for the Cisco CTAO team.

Before Cisco, Maik was a senior research and development architect and CISSP for Siemens, specializing in systems, software, and security architectures in energy and industrial automation. Earlier, he held project management, architecture, and engineering positions at Infineon, Audi, Siemens COM, and AMD. Maik earned a degree in informational techniques and a qualified engineer degree from Dresden University. His special fields of interest include cybersecurity, system and software architecture of IoT/M2M systems, and distributed intelligence.

Maik is the Cisco representative for communication, security, and automation in IEC TC 57, IEC TC 65, DKE, IEEE, OPC-UA, and UCA. He participates actively in standard development, with a focus on deterministic networking, IEC 61850, IEC 62351, and IEC 62443/ISA99. He has strong domain expertise in power grid and industrial automation, smart grid architecture, and cybersecurity for industrial control systems. Maik is the co-chair of TC CYBER (Security) in ETSI. He is a frequent public speaker and technical writer, with a focus on cybersecurity and IoT. Maik spends as much time as he can with his family and likes literature, pictorial arts, and the great outdoors, especially Alaska.

Dedications

This effort is dedicated to my mother, Carole Sabella, a woman who has given birth to eight children and has endured the swells of life like no other. Her unparalleled strength provides all the inspiration I need. Additionally, I'm quite proud to have been associated with my amazing coauthors and tech editors on this journey.

—*Anthony Sabella*

"Good company in a journey makes the way seem shorter." (Izaak Walton). Another step on my own path completed—fortunately, accompanied by very talented coauthors. More importantly, to Karen, Chloe, and Jake—thank you for your amazing patience and being there for me! Love you always! x

—*Rik Irons-Mclean*

First and foremost, to my family, Chani, Tathiana, Camila, Mateo, and Vilma, for your incredible love and support. You are my source of energy and inspiration; I love you endlessly! Second, to the talented team I have the pleasure to work with at Cisco.

—*Marcelo Yannuzzi*

Acknowledgments

Maciej Kranz: Maciej, as a leading industry expert in IoT and the direction it is taking, thank you for your Foreword and endorsement of this book. It is the perfect way to set the stage for why we need a more comprehensive approach to both secure and deliver on the promise of IoT.

Wei Zou: Thank you for your contribution and guidance on Chapter 16, "The Connected Car." Your insight and expertise helped bring the chapter to life with a practical feel.

Arik Elberse: Your reviews, support, and recommendations really helped shape Chapter 14, "Smart Cities." Our thanks.

Hugo Latapie: Hugo, thank you for your guidance and ability to translate complex subject matter into something digestible in the areas of Artificial Intelligence and machine learning.

Roque Gagliano: Thanks, indeed, for your expert help and insights on NFV and SDX, and the invaluable discussions we had around orchestration.

David Carrera, Barcelona Supercomputing Center: Huge thanks to you and your team for helping us drive and accelerate our innovations on fog and IoT, including the development of cutting-edge technologies and some of the use cases covered in this book. David, you rock!

James Honeybourne and Atilla Fazekas: Huge thanks to you both for your direction and thought leadership in the oil and gas industry. It is great to be continually challenged by your innovation and ideas. May your IoT/IIoT projects bring you the success they deserve!

Xavier Ramón, Federal Signal VAMA: Xavier, our thanks for not only your practical work in successfully deploying the technologies highlighted in this book, but also for your continued direction regarding the needs of the emergency fleet industry. And an extra thanks for allowing us to use images from your vehicle in Chapter 16, "The Connected Car."

Josep Martî, NearbySensor: Josep, thank you for the joint innovation we delivered in Barcelona that started this journey, as well as your expertise in the smart city vertical. Additional thanks for allowing us to use photos of your proven implementations in Chapter 14, "Smart Cities."

Barry Einsig and Tao Zhang: Thanks to you both for your suggested direction and ideas in Chapter 16, "The Connected Car."

Jason Greengrass: Thanks for your continual sanity checking (particularly in Chapter 8) on the technologies used throughout the book, and for translating the designs and architectures into deployable working solutions.

Eleanor Bru: Thanks for your patience, guidance, direction, and drive to get us through each step of this process. We wouldn't have made it without you!

Mary Beth Ray: Thank you for lending us your expertise to overcome some difficult challenges along the journey. Your advice has made a significant impact on our result.

Contents at a Glance

Foreword xxvii

Introduction xxix

Part I Introduction to the Internet of Things (IoT) and IoT Security

Chapter 1 Evolution of the Internet of Things (IoT) 1

Chapter 2 Planning for IoT Security 11

Chapter 3 IoT Security Fundamentals 31

Chapter 4 IoT and Security Standards and Best Practices 49

Chapter 5 Current IoT Architecture Design and Challenges 83

Part II Leveraging Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for IoT

Chapter 6 Evolution and Benefits of SDX and NFV Technologies and Their Impact on IoT 185

Chapter 7 Securing SDN and NFV Environments 251

Chapter 8 The Advanced IoT Platform and MANO 287

Part III Security Services: For the Platform, by the Platform

Chapter 9 Identity, Authentication, Authorization, and Accounting 323

Chapter 10 Threat Defense 417

Chapter 11 Data Protection in IoT 499

Chapter 12 Remote Access and Virtual Private Networks (VPN) 575

Chapter 13 Securing the Platform Itself 625

Part IV Use Cases and Emerging Standards and Technologies

Chapter 14 Smart Cities 669

Chapter 15 Industrial Environments: Oil and Gas 729

Chapter 16 The Connected Car 797

Chapter 17 Evolving Concepts That Will Shape the Security Service Future 873

Index 903

Contents

Foreword xxvii

Introduction xxix

Part I Introduction to the Internet of Things (IoT) and IoT Security

Chapter 1 Evolution of the Internet of Things (IoT) 1

Defining the Internet of Things 2

Making Technology and Architectural Decisions 5

Is the Internet of Things Really So Vulnerable? 8

Summary 9

References 10

Chapter 2 Planning for IoT Security 11

The Attack Continuum 11

The IoT System and Security Development Lifecycle 13

Phase 1: Initiation 15

Phase 2: Acquisition and Development 15

Phase 3: Implementation 16

Phase 4: Operations and Maintenance 17

Phase 5: Disposition 17

The End-to-End Considerations 17

Segmentation, Risk, and How to Use Both in Planning the Consumer/Provider Communications Matrix 21

Segmentation 21

New Approach 25

Summary 30

References 30

Chapter 3 IoT Security Fundamentals 31

The Building Blocks of IoT 31

The IoT Hierarchy 35

Primary Attack Targets 37

Layered Security Tiers 43

Summary 46

References 47

Chapter 4 IoT and Security Standards and Best Practices 49

Today's Standard Is No Standard 49

Defining Standards 53

The Challenge with Standardization 56

IoT "Standards" and "Guidance" Landscape 58

Architectural or Reference Standards 59

Industrial/Market Focused 61

Standards for NFV, SDN, and Data Modeling for Services 63

Data Modeling and Services 67

Communication Protocols for IoT 70

Physical and MAC Layers 73

Network Layer 73

Transport Layer 74

Application Layer 74

Specific Security Standards and Guidelines 75

Summary 79

References 80

Chapter 5 Current IoT Architecture Design and Challenges 83

What, Why, and Where? A Summary 85

Approaches to IoT Architecture Design 88

An X-Centric Approach 91

The People-/User-Centric IoT Approach (Internet of People and Social IoT) 98

The Information-Centric IoT Approach 100

The Data-Centric IoT Approach 104

System Viewpoint: A Cloudy Perspective 106

Cloud Computing 106

Fog/Edge Computing 112

Middleware 118

Lambda Architecture 119

Full IoT Stack/Universal 120

General Approaches 120

Internet of Things Architecture Reference Architecture (IoT-A RA) 120

ITU-T Y.2060 125

IoT World Forum (IoTWF) Reference Model 126

oneM2M Reference Architecture 129

IEEE P2413 IoT Architecture 132
The OpenFog Consortium Reference Architecture 133
Alliance for the Internet of Things Innovation (AIOTI) 138
Cloud Customer Architecture for IoT 140
Open Connectivity Foundation and IoTivity 142
Industrial/Market Focused 144
The Industrial Internet Consortium (IIC) 144
Industry 4.0 148
OPC Unified Architecture (OPC UA) 150
Cisco and Rockwell Automation Converged Plantwide Ethernet 153
Cisco Smart Grid Reference Model: GridBlocks 153
NFV- and SDN-Based Architectures for IoT 154
Approaches to IoT Security Architecture 156
Purdue Model of Control Hierarchy Reference Model 157
Industrial Internet Security Framework (IISF) IIC Reference Architecture 160
Cloud Security Alliance Security Guidance for IoT 165
Open Web Application Security Project (OWASP) 168
Cisco IoT Security Framework 168
The IoT Platform Design of Today 172
Security for IoT Platforms and Solutions 178
Challenges with Today’s Designs: The Future for IoT Platforms 179
Summary 183
References 183

Part II Leveraging Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for IoT

Chapter 6 Evolution and Benefits of SDX and NFV Technologies and Their Impact on IoT 185

A Bit of History on SDX and NFV and Their Interplay 185
Software-Defined Networking 188
OpenFlow 192
Open Virtual Switch 195
Vector Packet Processing 198
Programming Protocol-Independent Packet Processors (P4) 201
OpenDaylight 203
Extending the Concept of Software-Defined Networks 212

Network Functions Virtualization 217
Virtual Network Functions and Forwarding Graphs 221
ETSI NFV Management and Orchestration (MANO) 225
The Impact of SDX and NFV in IoT and Fog Computing 235
Summary 248
References 249

Chapter 7 Securing SDN and NFV Environments 251

Security Considerations for the SDN Landscape 251
1: Securing the Controller 252
Securing the Controller Application 252
Securing the Underlying Operating System 253
Securing the Controller East-West Communications 254
2: Securing Controller Southbound Communications 256
Authentication and Encryption 258
Leveraging Inherent Protocol Security Options 259
Revocation 259
Checks and Balances 260
3: Securing the Infrastructure Planes 260
Operations 261
Management Plane 261
Control Plane 262
Data Plane 262
4: Securing Controller Northbound Communications 263
API/REST Authentication 264
Authorization 267
Nonrepudiation 267
5: Securing Management and Orchestration 268
6: Securing Applications and Services 270
Security Considerations for the NFV Landscape 272
NFV Threat Landscape 273
Secure Boot 274
Secure Crash 275
Private Keys Within Cloned Images 276
Performance Isolation 278
Tenant/User Authentication, Authorization, and Accounting (AAA) 279
Authenticated Time Service 281

Back Doors with Test and Monitor Functions 281

Multi-administrator Isolation 282

Single Root I/O Virtualization (SRIOV) 283

SRIOV Security Concerns 285

Summary 285

References 285

Chapter 8 The Advanced IoT Platform and MANO 287

Next-Generation IoT Platforms: What the Research Says 287

Next-Generation IoT Platform Overview 291

Platform Architecture 294

Platform Building Blocks 295

Platform Intended Outcomes: Delivering Capabilities as an Autonomous End-to-End Service 303

Model-Driven and Service-Centric 304

Service Chaining 306

Contextual Automation 307

Example Use Case Walkthrough 308

Event-Based Video and Security Use Case 309

Preparatory Work 315

Deploying the Use Case 316

The Use Case in Action 319

Summary 321

References 321

Part III Security Services: For the Platform, by the Platform

Chapter 9 Identity, Authentication, Authorization, and Accounting 323

Introduction to Identity and Access Management for the IoT 324

Device Provisioning and Access Control Building Blocks 326

Naming Conventions to Establish "Uniqueness" 327

Secure Bootstrap 328

Immutable Identity 328

Bootstrapping Remote Secure Key Infrastructures 329

Device Registration and Profile Provisioning 330

Provisioning Example Using AWS IoT 331

Provisioning Example Using Cisco Systems Identity Services Engine 334

Access Control 336

Identifying Devices 336

Endpoint Profiling 337

Profiling Using ISE 337

Device Sensor 340

Methods to Gain Identity from Constrained Devices 345

Energy Limitations 346

Strategy for Using Power for Communication 347

Leveraging Standard IoT Protocols to Identify Constrained Devices 348

CoAP 349

MQTT 350

Authentication Methods 351

Certificates 351

X.509 352

IEEE 1609.2 353

Private Key Infrastructure 353

Trust Stores 355

Revocation Support 356

CRL 356

OCSP 357

SSL Pinning 357

Passwords 357

Limitations for Constrained Devices 358

Biometrics 359

TouchID 359

Face ID 359

Risk Factor 360

AAA and RADIUS 361

A/V Pairs 362

802.1X 363

MAC Address Bypass 365

Flexible Authentication 366

Dynamic Authorization Privileges 367

Cisco Identity Services Engine and TrustSec 368

RADIUS Change of Authorization 368

CoA Requests 368

CoA Request/Response Code 369

Session Identification 369

CoA Request Commands 370

VLAN 371

Access Control Lists 374

TrustSec and Security Group Tags 376

The Security Group Tag 377

Software Defined 378

Dynamic Segmentation Based on RBAC 378

TrustSec Enablement 379

Classification 380

Propagation 381

Inline Tagging Mediums (Ethernet and L3 Crypto) 383

Enforcement 384

SGACL 384

Consumer/Provider Matrix 384

SGACL for North–South and East–West 386

Automation of SGACLs and Dynamic Segmentation 388

Manufacturer Usage Description 390

Finding a Policy 390

Policy Types 390

The MUD Model 392

AWS Policy-based Authorization with IAM 394

Amazon Cognito 395

AWS Use of IAM 395

Policy-based Authorization 395

Accounting 397

How Does Accounting Relate to Security? 398

Using a Guideline to Create an Accounting Framework 398

Meeting User Accounting Requirements 400

Scaling IoT Identity and Access Management with Federation Approaches 402

IoT IAM Requirements 403

OAuth 2.0 and OpenID Connect 1.0 404

OAuth 2.0 404

OpenID Connect 1.0 405

OAuth2.0 and OpenID Connect Example for IoT 405

Cloud to Cloud 406

Native Applications to the Cloud 408

Device to Device 409

Evolving Concepts: Need for Identity Relationship Management 411

Summary 414

References 415

Chapter 10 Threat Defense 417

Centralized and Distributed Deployment Options for Security Services 418

Centralized 418

Components 419

Distributed 420

Hybrid 422

Fundamental Network Firewall Technologies 422

ASAv 423

NGFWv 423

Network Address Translation 424

Dynamic NAT 424

Static NAT 424

Overlapping 425

Overloading or Port Address Translation 425

Packet Filtering 426

Industrial Protocols and the Need for Deeper Packet Inspection 428

Common Industrial Protocol 428

Lack of Security 429

Potential Solutions: Not Good Enough 430

Alternative Solution: Deep Packet Inspection 430

Sanity Check 431

User Definable 432

Applying the Filter 432

Application Visibility and Control 433

Industrial Communication Protocol Example 435

MODBUS Application Filter Example 436

Intrusion Detection System and Intrusion Prevention System 437

IPS 438

Pattern Matching 438

Protocol Analysis 439

IDS/IPS Weakness 439

Advanced Persistent Threats and Behavioral Analysis 440

Behavior Analysis Solutions 441

Protocols Used to Gain Additional Visibility 442

NetFlow 442

Flexible NetFlow 444

Network-Based Application Recognition 444

Network Security Event Logging 444

Network as a Sensor 444

Algorithms for Security Events 445

Pairing with Contextual Information and Adaptive Network Control 446

Cisco TrustSec Fields in Flexible NetFlow 447

Anomaly Detection Example 447

Encrypted Traffic Analytics 450

Detecting Threats Using Encrypted Traffic Analytics 451

Crypto Compliance 454

WannaCry Example 454

Malware Protection and Global Threat Intelligence 455

Cisco Advanced Malware Protection and TALOS 456

Point-in-Time Detection, Retrospective Security, and Sandboxing 456

Example of How the Firewall Uses the Malware Feature 459

File Policy 461

DNS-Based Security 462

Umbrella (DNS Security + Intelligent Proxy) 463

Intelligent Proxy 464

Umbrella + AMP Threat Grid 465

Using Umbrella to Help Protect Healthcare 465

Centralized Security Services Deployment Example Using NSO, ESC, and OpenStack 466

ETSI MANO Components in the Use Case 468

VMs (Services) Being Instantiated in the Use Case 469

Use Case Explanation 469

Activation Sequence Basics and NSO Service Creation (VNFD, NSD, and NSR) 470

Activation Sequence Example 472

Fulfillment and Assurance Sequences Basics 474

Monitoring and KPI 475

Prerequisites for Monitoring 475

Metrics and Actions and Dynamic Mapping 475

Dynamic Mapping in the Data Model 478

Monitoring Methods 479

Fulfillment and Assurance Sequence Examples 479

KPI 480

Rules 483

Distributed Security Services Deployment Example Using Cisco Network Function Virtualization Infrastructure Software (NFVIS) 486

Solution Components 487

NFVIS 488

Hardware 488

Supported VMs 490

Orchestration 490

vBranch Function Pack 490

Service Chaining and Traffic Flow 494

Summary 495

References 495

Chapter 11 Data Protection in IoT 499

Data Lifecycle in IoT 507

Data at Rest 518

Data Warehouses 521

Data Lakes 522

Data in Use 524

Data on the Move 527

Protecting Data in IoT 531

Data Plane Protection in IoT 531

Message Queuing Telemetry Transport Protocol 532

Authentication in MQTT 533

Authorization in MQTT 535

Confidentiality in MQTT 539

Integrity in MQTT 540

Availability in MQTT 542

Nonrepudiation in MQTT *543*

RabbitMQ *544*

Authentication in RabbitMQ *547*

Authorization in RabbitMQ *548*

Confidentiality in RabbitMQ *549*

Integrity in RabbitMQ *549*

Availability in RabbitMQ *550*

Other Considerations Related to Data Availability in RabbitMQ *550*

Nonrepudiation in RabbitMQ *552*

Example: Orchestrated Security on RabbitMQ at the Fog Node Level *552*

Cisco Edge and Fog Processing Module (EFM) *560*

Data Virtualization: Enabling Single Query Models in IoT *564*

Protecting Management Plane Data in IoT 565

Protecting Control Plane Data 566

Considerations When Planning for Data Protection 567

Summary 573

References 574

Chapter 12 Remote Access and Virtual Private Networks (VPN) 575

Virtual Private Network Primer 575

Focus for This Chapter 576

Site-to-Site IPsec VPN 576

IPsec Overview 577

Authentication Header (AH) *578*

Encapsulating Security Payload (ESP) *578*

Internet Key Exchange (IKE) Overview *578*

IKEv1 Phase 1 579

Authentication Method *579*

Diffie-Hellman (D-H) Groups *580*

Encryption Algorithms *580*

Hashing Algorithms *580*

IKE Modes (Main and Aggressive) *580*

Aggressive Mode *582*

IKEv1 Phase 2 582

NAT-Traversal (NAT-T) *583*

Perfect Forward Secrecy (PFS) 584

Internet Key Exchange Protocol Version 2 584

IKEv2 Exchange 584

Benefits of IKEv2 over IKEv1 586

Software-Defined Networking-Based IPsec Flow Protection IETF Draft 588

IPsec Databases 589

Use Case: IKE/IPsec Within the NSF 589

Interface Requirements 590

Multiple Security Controllers 591

Applying SDN-Based IPsec to IoT 592

Leveraging SDN for Dynamic Decryption (Using IKE for Control Channels and IPsec for Data Channels) 592

Software-Based Extranet Using Orchestration and NFV 594

Traditional Approach 594

Automating Extranet Using Orchestration Techniques and NFV 595

Software-Based Extranet Use Case 597

Remote Access VPN 598

SSL-Based Remote Access VPN 598

SSL VPN for Multiple Solutions 599

Reverse Proxy 599

Clientless and Thin Client VPN 599

Tunnel Groups and Group Policies 600

Clientless Components 602

Clientless Portal 602

Application Access (Bookmarks, Port Forwarding, Smart Tunnels) 604

Dynamic Access Policy 609

Clientless Example for IoT: Oil and Gas 610

Client Based: Cisco AnyConnect Secure Mobility Client 611

Cisco AnyConnect 611

Deployment 611

Configuration Choices 612

Modules 612

VPN Module 612

Network Access Manager Module 614

Endpoint Compliance Module 614

Roaming Protection Module 614

Network Visibility Module 615

Threat Protection Module 616

Using AnyConnect in Manufacturing: Use Case Example 617

Use Case 617

Working Components 618

Summary 622

References 622

Chapter 13 Securing the Platform Itself 625

(A) Visualization Dashboards and Multitenancy 627

(B) Back-End Platform 631

Scenario 1: A New Endpoint Needs to Be Connected to the Network 639

Scenario 2: A User Wants to Deploy a New Service Across the Fog, Network, and Data Center Infrastructure 639

Scenario 3: Creating New Data Topics and Enabling Data Sharing Across Tenants 641

Docker Security 653

Kubernetes Security and Best Practices 656

(C) Communications and Networking 658

(D) Fog Nodes 660

(E) End Devices or “Things” 666

Summary 667

References 667

Part IV Use Cases and Emerging Standards and Technologies

Chapter 14 Smart Cities 669

Use Cases Introduction 669

The Evolving Technology Landscape for IoT 670

The Next-Generation IoT Platform for Delivering Use Cases Across Verticals: A Summary 672

Smart Cities 676

Smart Cities Overview 678

The IoT and Secure Orchestration Opportunity in Cities 688

Security in Smart Cities 693

Smart Cities Example Use Cases 696

Use Case Automation Overview and High-Level Architecture 701

Power Monitoring and Control Use Case: Secure Lifecycle Management of Applications in the Fog Nodes 702

Access Control and Sensor Telemetry of City Cabinets: Simple and Complex Sensor Onboarding 705

Sensor Access Control 708

Event-Based Video: Secure Data Pipeline and Information Exchange 709

Public Service Connectivity on Demand: Secure User Access and Behavioral Analysis 714

Emergency Fleet Integration 718

Automated Deployment of the Use Cases 721

Summary 725

References 727

Chapter 15 Industrial Environments: Oil and Gas 729

Industry Overview 733

The IoT and Secure Automation Opportunity in Oil and Gas 735

The Upstream Environment 738

Overview, Technologies, and Architectures 739

Digitization and New Business Needs 742

Challenges 743

The Midstream Environment 744

Overview, Technologies, and Architectures 744

Digitization and New Business Needs 747

Challenges 748

The Downstream and Processing Environments 749

Overview, Technologies, and Architectures 749

Digitization and New Business Needs 752

Challenges 753

Security in Oil and Gas 754

Oil and Gas Security and Automation Use Cases: Equipment Health Monitoring and Engineering Access 763

Use Case Overview 763

Use Case Description 765

Deploying the Use Case 767

Preconfiguration Checklist 773

Automated Deployment of the Use Cases 777

Securing the Use Case 778

Security Use Case #1: Identifying, Authenticating, and Authorizing the Sensor for Network Use 778

Security Use Case #2: Detecting Anomalous Traffic with Actionable Response 780

Power of SGT as a CoA 781

Auto-Quarantine Versus Manual Quarantine 782

Security Use Case #3: Ensuring That Contractors and Employees Adhere to Company Policy (Command Validation) 782

Leveraging Orchestrated Service Assurance to Monitor KPIs 783

Security Use Case #4: Securing the Data Pipeline 786

Evolving Architectures to Meet New Use Case Requirements 788

Summary 792

References 794

Chapter 16 The Connected Car 797

Connected Car Overview 800

The IoT and Secure Automation Opportunity for Connected Cars 809

The Evolving Car Architecture 824

Security for Connected Cars 830

Connected Car Vulnerabilities and Security Considerations 838

Connected Car Security and Automation Use Case 849

Use Case Overview 852

Use Case Automation Overview 854

Secure Access/Secure Platform: Boundary Firewall for OTA Secure Updates 855

Secure Network: Segmentation, Zones, and Interzone Communication 857

Secure Content: Intrusion Detection and Prevention 858

Secure Intelligence: Secure Internet Access from the Vehicle 861

The Future: Personalized Experience Based on Identity 862

Federal Sigma VAMA: Emergency Fleet Solution 863

Automated Deployment of the Use Case 867

Summary 871

References 871

Chapter 17 Evolving Concepts That Will Shape the Security Service Future 873

A Smarter, Coordinated Approach to IoT Security 876

Blockchain Overview 880

Blockchain for IoT Security 888

Machine Learning and Artificial Intelligence Overview 890

Machine Learning 893

Deep Learning 894

Natural Language Processing and Understanding 895
Neural Networks 896
Computer Vision 898
Affective Computing 898
Cognitive Computing 898
Contextual Awareness 899
Machine Learning and Artificial Intelligence for IoT Security 899
Summary 900
References 901

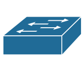
Index 903

Reader Services

Register your copy at www.ciscopress.com/title/9781587145032 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587145032 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Icons Used in This Book

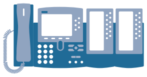

Switch

Phone

Fog Node

Server

Lock


IP Phone

Router

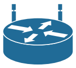
Firewall

vASA

Router with Firewall

File Server

Cloud


Wireless Router

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the Cisco IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Foreword: The Challenge and Opportunity of IoT Security

The Internet of Things (IoT) presents a unique security challenge—and opportunity.

The challenge is that IoT is more distributed, more heterogeneous, and more dynamic than anything we've seen before in traditional IT security environments. It introduces complex scenarios and elements that an IT manager never would have thought about back in the days when networks just connected computers. Consider networks of connected cars or sensor swarms[md]or the plethora of now-connected consumer-class devices that have become the weak link in IoT security.

It's no wonder that concerns about security have become the single biggest barrier to IoT adoption.

But the opportunity is, when you address these challenges with a comprehensive, risk-based architectural approach, you open the door to billions—some say trillions—of dollars in business value.

Much has been said about the exponentially growing number of devices connected to the Internet, which is forecast to reach as many as 75 billion by 2025.[1] However, the number of devices is far less important than what we can do with those connections: delivering better public services in smart cities, driving more safely in connected cars, transforming energy production and distribution, changing businesses with powerful new connected capabilities. The Internet of Things has the potential to reinvent entire industries. But only if we get IoT security right.

This book comes at a pivotal moment. We see the possibility of industry-wide transformation and unprecedented value. And at the same time, we face continually evolving security threats at an unprecedented scale.

Over the years, I have worked with countless companies and government organizations as they have taken their first steps on the IoT journey. And, of course, security concerns have popped up early and often along the way. Back in the day when industrial enterprises ran self-contained, proprietary systems, "security by obscurity" was standard practice[md]if you're not connected to anything, no one can break in. That approach no longer applies in today's connected IoT environment (if it ever did), so businesses must rely on a policy-based architectural approach and ask their chief information security officers (CISOs) to own security strategy for the entire enterprise.

But IoT security isn't just the CISO job; it's everybody's job throughout the value chain, from manufacturers to end users.

It starts with device vendors. Too often, device connectivity (especially for consumer-class devices) is an add-on feature with little consideration for enterprise-level requirements,

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

including investment in security. Consumer device makers often view the extra cost, complexity, and time to market as extra burdens with unclear payoff. Thus, it's no wonder that we still find rudimentary vulnerabilities such as default names and passwords hard-coded into these devices. And hackers are more than happy to exploit them.

Security vendors are responding just as they did 15 years ago when Wi-Fi took off and consumer-class Wi-Fi clients started proliferating across enterprises. The industry got together to work on standards, interoperability, and certifications, and we're doing the same thing for IoT today. I'm glad to say that following last year's IoT Distributed Denial of Service (DDoS) attacks, pretty much all major security vendors have finally started to invest appropriately in IoT security.

Standards are evolving in horizontal and vertical standards bodies and in consortia. For example, the Internet Engineering Task Force is working on developing standards governing the ways manufacturers should disclose how their devices are expected to function, so that networks can detect and block anomalous device behaviors. Other organizations, such as the Industrial Internet Consortium's (IIC) security working group and IEEE, have also been very active in developing IoT security frameworks, standards, and methodologies to help ensure cybersecurity across interconnected IoT systems. In vertical standards bodies such as ODVA or ISA the IT and operational technology (OT) teams evolve industry-specific best practices and combine them with horizontal approaches.

Governments have a role in overcoming these security challenges as well. In the United States, the Federal Trade Commission has recently released new guidelines for how manufacturers should inform customers about device security, including whether and how the device can receive security updates, and the anticipated timeline for the end of security support. As governments work closely with the industry to establish consensus around a core set of requirements, IT professionals will have the tools to effectively manage security in the face of rapid proliferation of Internet-connected technologies.

No matter what your role in the IoT ecosystem is, security begins with you. And that is why you have this book in your hand right now. Use it as a guide to creating the comprehensive architectural approach needed for today's complex and dynamic IoT environments. It will enable you to design platform-level security into your IoT installation, with automation features that let you keep up with ever-changing threats.

Providing reliable and flexible IoT security is indeed a challenge. But you do not need to be daunted by the task. For a little inspiration about the opportunities you can unlock, skip to the transformational use cases in Chapters 14 through 17, then start at the beginning and implement IoT as an ongoing process, like the IoT journey itself.

—Maciej Kranz

Introduction

Adoption of Internet of Things (IoT) technologies is accelerating in the enterprise and industrial environments, but IoT presents complex new security challenges. Fortunately, advanced technologies are starting to pave the way for IoT standards and standardized architectures that will make it possible to systematically harden IoT environments. The information in this book introduces a new approach to leveraging orchestration and automation to safeguard IoT systems by delivering security through the application of network function virtualization (NFV), software-defined networking (SDN), software-defined automation (SDA), and fog architectures.

NFV, SDN/SDA, and fog computing are proven technologies used to deploy, operate, and retire use cases at scale. Combining these technologies into a platform approach delivers the capability to address heterogeneous elements of the full IoT stack. This means that efficient service insertion, including security, can be deployed effectively and efficiently in an automated manner throughout a deployed IoT system.

This book uses a four-part approach for understanding and delivering security capabilities via automation. Part I, "Introduction to the Internet of Things (IoT) and IoT Security," begins by reviewing existing IoT and security architectures and standards, identifying key security risks associated with early deployments, and showing how early adopters have attempted to respond. Part II, "Leveraging Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for IoT," introduces standards-based offerings that leverage NFV, SDN, and fog, and it explains why these architectures lend themselves well to IoT and IoT security. Part III, "Security Services: For the Platform, by the Platform," explores advanced security concepts and how they can be leveraged for IoT deployments. Finally, Part IV, "Use Cases and Emerging Standards and Technologies," presents real-world use case examples and previews emerging technologies and security concepts that will shape IoT security in the future.

The reader will

- Learn fundamental standards, architectures, and security for IoT
- Understand how to leverage SDN, NFV, fog, and cloud computing concepts to deliver security capabilities for IoT environments
- Gain knowledge on the book's core concepts and best-practice methodologies through real-world use cases
- Master advanced IoT security concepts and how they can be overlaid onto current IoT deployments, as well as provide the architectural foundation for new ones
- Understand the future direction of IoT technologies and security

Who Should Read This Book?

With the number of IoT implementations in both enterprise and industrial environments continuing to increase, it is essential to provide technical professionals who are looking at automation and virtualization technologies with a resource to deliver security solutions more effectively

Research from Gartner, McKinsey, Forbes, Accenture, and Ovuum all predicts the emergence of services-based automation platforms for IoT and security embedded as a service. Thus, this book content is especially beneficial to anyone looking at the next-generation design for a scalable and interoperable IoT platform.

Anyone working on enterprise or service provider projects with a focus on security or risk management will benefit from understanding the content of this book.

The concepts require a foundational understanding of IoT and security. This book ultimately is aimed at technical IoT professionals, technical security professionals, and business security and risk managers. The content is applicable across a wide range of verticals and market segments, and also is relevant to those working in IT or the operational environment.

How This Book Is Organized

Chapter 1, Evolution of the Internet of Things (IoT)

This chapter introduces IoT, illustrates the rapidly expanding scale of IoT and associated security threats, and outlines why automation is the only solution that can address security at the required scale.

Chapter 2, Planning for IoT Security

Securing the Internet of Things will pose new challenges to organizations. As with any system that needs to be secured, a number of practical steps can be leveraged. This chapter outlines some key considerations to explore as part of a security strategy for IoT.

Chapter 3, IoT Security Fundamentals

This chapter provides an overview of the building blocks of IoT and supplies an introduction to the required architectures in IoT deployments. It also covers the primary attack targets for IoT and the layered security tiers needed to mitigate them.

Chapter 4, IoT and Security Standards and Best Practices

To develop a robust and secure IoT system, openness and standards are required. The aim of this chapter is not to detail or recommend specific standards and guidelines, but to raise awareness of what should be considered when planning to secure an IoT system. It highlights some of the more robust standards and best practices that can help.

Chapter 5, Current IoT Architecture Design and Challenges

This chapter provides an overview of the main architectural approaches to building out IoT systems with security at the foundation. This includes benefits and drawbacks that existing architectures and platforms still need to address. This chapter aims to highlight what has already been proposed, to set the context and foundations for what needs to be done, as highlighted in subsequent chapters.

Chapter 6, Evolution and Benefits of SDX and NFV Technologies and Their Impact on IoT

This chapter gives an overview of the evolution and strengths of SDX and NFV technologies, both in isolation and combined. It examines their roles as technology enablers for IoT, 5G, and it looks at the expected interplay between fog and cloud computing. The chapter also covers several aspects of service automation in NFV/SDX scenarios, including the application of one of the most promising orchestration architectures in the industry for IoT.

Chapter 7, Securing SDN and NFV Environments

The focus of this chapter is how to secure both SDN and NFV environments. It organizes the various elements of SDN and breaks the infrastructure into categories, each of which can be examined for potential vulnerability and associated options to bolster. The same is done for NFV; the chapter examines the NFV threat landscape as defined by the ETSI Industry Specification Group (ISG) and discusses both the issues and associated methods in each category.

Chapter 8, The Advanced IoT Platform and MANO

This chapter covers the latest industry thought leadership related to architecting IoT platforms and the technology building blocks needed to deliver a next-generation solution. It then focuses on how advanced services (particularly security) can be created and delivered in an automated way before finally providing solution architectures that describe how this might look in a real-world deployment.

Chapter 9, Identity, Authentication, Authorization, and Accounting

Key topics in this chapter include the technology available to gain identity when an endpoint attempts to access the network, methods to authenticate the endpoint, and, ultimately, automated solutions that can couple identity and authentication information and then leverage that information to provide dynamic access privileges based on identity. It explores both legacy protocols and newer methods leveraging OAuth 2.0 and OpenID Connect that are helping to scale identity and authorization within IoT environments. Finally, the chapter looks at the evolution from IAM techniques to identity relationship management (IRM) and explores its potential applicability.

Chapter 10, Threat Defense

This chapter focuses on securing the "during phase" of an endpoint's network connectivity. More specifically, it covers instituting virtualized technology to both detect and mitigate threats while, in parallel, ensuring that the endpoint adheres to company policy. It examines various threat defense methods such as packet filtering techniques, IDS/IPS, behavior analysis, and malware protection. It then examines deploying the VNFs in both distributed form (pushing out toward the edge) and centralized form, and it shows examples of the VM lifecycle management, orchestration, and service chaining processes within.

Chapter 11, Data Protection in IoT

The main aspects of data protection in IoT are the focus of this chapter. It starts with the lifecycle of data and its management and then focuses on protecting data at rest, on the move, and in use. The chapter is fundamentally centered on the confidentiality, integrity, and availability (CIA) triad, and the analysis is complemented with specific examples involving orchestration and automation to protect data exchanges across data centers, networks, and fog. Additionally, the chapter outlines other relevant aspects, such as the General Data Protection Regulation (GDPR), enforced in Europe in May 2018, and the immense potential of novel technologies such as blockchain to become game changers in the space.

Chapter 12, Remote Access and Virtual Private Networks (VPN)

This chapter discusses remote access and virtual private network (VPN) technologies for IoT use cases. In parallel, it highlights methods for leveraging automation and SDN techniques within the remote access scenarios. This includes methods to separate the control and data channels of IPsec and apply them to IoT use cases for better scalability. This chapter also includes remote access scenarios leveraging TLS using both client and clientless versions, and how to create a software-based extranet using IPsec with orchestration and NFV.

Chapter 13, Securing the Platform Itself

This chapter examines the security of the platform itself. It starts with the description of a modular architecture that offers a representative model of a comprehensive IoT platform. The focus is on an NFV-centric architecture, powered by ETSI MANO and SDN capabilities extended to fog computing. The architecture is sliced into five segments and a total of 20 elements, or modules. The security of each is examined throughout the chapter, and the analysis is linked to related contents covered in other parts of the book.

Chapter 14, Smart Cities

Smart cities are the focus of this chapter, which looks at the changes digitization through IoT will bring to cities and highlights how an appropriate security posture can be realized through advanced technologies and automation. The chapter describes a number of use cases that are deployed in smart cities and shows how they can be uniformly and securely delivered through a common platform.

Chapter 15, Industrial Environments: Oil and Gas

This chapter explores the industrial setting, using the oil and gas industry as an example. It discusses how IoT and digitization are driving changes in use cases and how this impacts architectural approaches and security. The chapter then describes a number of use cases and shows how they can be uniformly and securely achieved through a common platform.

Chapter 16, The Connected Car

This chapter covers the rapidly evolving automotive industry, looking at connected cars and the changes digitization through IoT will bring. It highlights how an appropriate security approach can be realized through advanced technologies and the automation needed for technology to be responsive to business needs. The chapter concludes with use case scenarios that guide the reader through a practical deployment to better illustrate the concepts.

Chapter 17, Evolving Concepts That Will Shape the Security Service Future

The final chapter introduces some of the developing technologies that are used for security and, in some cases, that will pose new security threats. Blockchain, machine learning, and Artificial Intelligence are introduced, and the chapter illustrates they can be incorporated into IoT and security for IoT. The chapter discusses how these can also be integrated into an orchestration platform to help automate IoT security at scale.

This page intentionally left blank

Chapter 4

IoT and Security Standards and Best Practices

Topics covered in this chapter include

- Today's Standard Is No Standard
- Defining Standards
- The Challenge with Standardization
- IoT Standards and Guidance Landscape
- Standards for NFV, SDN, and Data Modeling for Services
- Communication Protocols for IoT
- Specific Security Standards and Guidelines

Today's Standard Is No Standard

IoT can be complex and quite broad in what it attempts to address and deliver. IoT can also look and feel very different between each implementation or use case. Yet consistently, for IoT to deliver on the promised business value through connecting things and leveraging produced data for business insight, it must enable devices, networks, and applications to seamlessly work and interoperate together to produce "smart" outcomes. It must also do this in a secure way. If we are unable to deliver on this promise, then we might as well revert back to proprietary or single-vendor solutions and give up on the potential value IoT brings. The question is, will this ever happen? And will we see a time when only a few open IoT standards exist to easily enable the implementation of solutions in a consistent, secure, and manageable way?

In 2015, a McKinsey and Company report concluded that incompatibility is the number one problem facing IoT growth. The authors argued that interoperability among IoT systems is critical. Of the total potential economic value IoT enables, interoperability is required for 40 percent on average and for nearly 60 percent in some settings. With the estimated value of IoT reaching between $4 trillion and $11 trillion in revenue by 2025, the opportunity is huge. McKinsey and Company concluded, "The true potential of the market will be determined by the ability of policymakers and businesses to drive technology and innovation that is interoperable, secure, protective of privacy and property rights, with established business models that better facilitate and enable data sharing." Clearly, to realize the benefit and value IoT can create, interoperability and standards are a must. This includes standards for interoperability and for securing the IoT.

As outlined in Chapter 1, "Evolution of the Internet of Things (IoT)," IoT has existed for many years. Various forms of standardization now being leveraged for IoT also have existed for years. Remember, we are using *IoT* here as an umbrella term that also includes industrial IoT and market- or sector-specific initiatives. Clearly, there are differences in terms of use cases and requirements; however, from a technology perspective, there are also many similarities. Even before the term *IoT* was widely adopted, elements of IoT, such as standardized communication protocols, were being explored. Standards for IoT started to really grow around 2013, with several maturing enough through 2014 to offer limited certification programs. Some of these earlier standards have even started to come to fruition and deliver against use cases. We have also seen some early harmonization of standards efforts for IoT. One example is the Open Connectivity Foundation (OCF), formed when the AllSeen Alliance and the OCF came together under the OCF umbrella, with the aim of providing the interoperability element of an IoT solution at all levels, including silicon, software, platform, and finished goods. The OCF message is clear and accurate: Interoperability standards are the starting point, but standards must progress to include security as a foundation and must address requirements for consumers, business, and industry to deliver value.

The reality, though, is that this is a nice success story in a sea of disparity and competing standards. Despite industry analysts cautiously predicting that 2017 would be the year when standards started to really align, this was not the case. The only agreed-upon conclusion is that we are still a long way from a universal IoT standard—or even two or three IoT standards. Today's perspective from both analysts and researchers is that this disparity is likely to continue over the next few years at the very least.

So why is alignment difficult? After all, IoT is now accepted as a phenomenon, and consumers, vendors, businesses, and industries want it to succeed and provide the value it promises. If only it were that simple. In practice, a wealth of considerations have an impact on the creation and shaping of standards for IoT:

- There is still no single, agreed-upon definition of IoT. Without a universally accepted definition, how do you standardize for it?
- Many different forces continue to shape the IoT landscape, and these forces themselves are evolving. These forces can be broadly grouped into market and social trends, business digitization and transformation, the evolving workforce, and next-generation mobility for people and devices.
- As we discussed in Chapter 3, "IoT Security Fundamentals," we need to standardize many different areas of IoT. An IoT system might contain communications,

management, architecture, data normalization, services, security, hardware, applications, analytics, and so on. Even if one part were standardized, we might encounter interoperability issues with the other parts. Defining what and how things should be standardized is another challenge with no current answer.

- Different verticals and industries often have their own requirements and perspectives, thus driving different standards based on their needs. This could mean differences such as IT and OT standards within the same organization, or specific industry vertical initiatives such as smart cities, digital manufacturing, or smart energy that have different regulations or guiding principles.

- New use cases continue to arise, often driven by the advent of new technology. How can we constantly ensure that standards apply? Creating security by design is difficult if the use case is ahead of technology and security for that requirement. New use cases often leverage proprietary measures with the aim of them becoming standardized at some stage, but this usually results in limited security response capabilities (and even more standardization efforts).

- New technologies and technology architectures are still being developed. If we consider advancements in areas such as NFV, SDN, cloud, fog, software-defined automation (SDA), and autonomic networking, and couple this with new technology areas such as deterministic networking, NB-IoT and LoRa in the RF space, and 5G, and then throw in aspects of Big Data, analytics, machine learning (ML), and AI, we can see that the potential arena is huge. The Gartner Hype Cycle for the Internet of Things (2016) in Figure 4-1 highlights this landscape and shows the emergence of IoT areas; all of these need to be secured and, if possible, standardized.

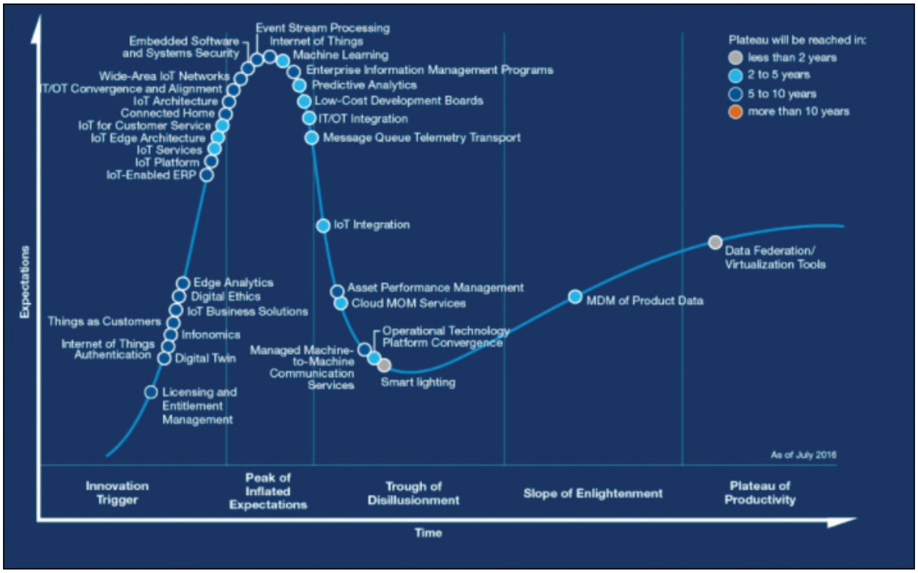


Figure 4-1 *The Gartner Hype Cycle for the Internet of Things (2016)*

- Not all IoT solutions will be deployed in greenfield environments. In fact, a good percentage of environments exist today and are evolving. This means that legacy and proprietary technologies need to be integrated, further muddying the standardization opportunity.
- IoT is more complex than either IT or OT on their own. This might seem pretty obvious because often a combination of IT and operational technologies and systems is needed to deliver against a use case. However, IoT is often approached in the same way organizations address new technology as part of their core IT or OT business. By its very nature, IoT usually generates more data, is more geographically dispersed, contains new devices, involves new technologies, and produces a mixed IT/OT deployment environment.
- IPv6 is an enabler for IoT. IoT6.eu believes that many arguments and features (including scalability, a solution to the NAT barrier problem, multi-stakeholder support, and features such as multicast, anycast, mobility support, autoconfiguration, and address scope) demonstrate that it will be a key communication enabler for IoT in the future. IPv6 also supports tiny operating systems, provides increased hardware support, and supplies new protocols focused on interoperability among different layers of the IoT stack.
- Legislation and regulations are starting to arise. Early examples include NERC-CIP, for power utilities in North America, and ENISA, which focuses on delivering a governance framework to coordinate cybersecurity standardization within Europe.
- A major challenge is that standards groups, alliances, and consortia often consist of large vendors who are unlikely to want to give up their market share. We are starting to see potential shifts here, with customers demanding interoperable efforts. One example is the Open Group Open Process Automation standard, driven by Exxon Mobil requirements for its next-generation processing environments.
- The speed of standards development is usually slow. This contrasts with development within the communications industry, where technology moves at pace to address customer business needs. This pace can result in proprietary efforts because of business demand, not necessarily vendor choice.
- Security itself is not a simple phenomenon. It must be addressed across the board and built in from scratch, not just piecemeal. Security can often be a driver for change, but usually it is playing catchup to try to secure a lack of interoperability.

As a result, we are still waiting for the IoT market to develop an approach that would allow for a fully end-to-end, consistent security strategy. We also need to realize that many standards, guidelines, and consortia have existed before IoT (technology has been around for some time) and must still adapt to IoT. These other standards should not necessarily be discarded; they have already shown value.

Looking at these challenges, IoT remains something of a puzzle. The use cases and business scenarios require interoperability and simplification of technology to work, with enabling technologies rationalized around robust and secure standards that also include legacy environments. However, these use cases and business scenarios are still evolving, with new endpoints and technologies being frequently introduced into a landscape without appropriate standardization. This makes the idea of standards an even more complex and challenging task. We will look at this more closely in this chapter as we explore the following topics:

- How standards are defined
- Why we need standards
- An overview of the IoT standards landscape
- Standards for NFV and SDN
- Security standards for IoT and NFV/SDN

The aim of the chapter is not to detail or recommend standards and guidelines, but to raise awareness of what should be considered when planning to secure an IoT system. We also highlight some of the more robust standards and best practices today that can help.

Defining Standards

So far, we have discussed only the notion of standards for IoT because standards are often the basis for determining how systems are deployed. However, standards are not the only piece to consider. Other tools and techniques can help with implementing IoT systems in as secure a way as possible.

- **Regulations:** Directives that safeguard information technology and computer systems, with the purpose of forcing companies and organizations to protect their systems and information from cyber attacks. Examples include NERC-CIP for power utilities in North America and the Directive on Security of Network and Information Systems (NIS Directive) in Europe. Organizations must adhere to regulations.
- **Standards:** Details on how specific methods must be applied in a consistent manner. Techniques are generally documented in published materials, in an attempt to protect the cyber environment of a user or organization. The principal objective is to reduce risk, including to prevent or mitigate attacks. Conformance to adopted standards is usually compulsory and measured against to ensure an acceptable level of quality or attainment. Examples include IEC-62443 for industrial control system security.
- **Guidelines:** Additional details on ways to secure an environment or system. These are similar to standards but are considered merely recommendations. An example is the NIST NISTIR 7628 guidelines for smart grid cybersecurity.
- **Policies:** A written strategy to meet the security needs of an organization, providing a statement of intent by an organization’s management. Compliance is mandatory. Policies provide top-down requirements for the organization to protect assets and information, as well as to meet any regulations or legal requirements.

- **Procedures:** Step-by-step actions that must be taken to implement policies and standards. These might include a series of detailed steps and instructions to accomplish an end goal. Procedures are mandatory. An example is the maximum duration for user account passwords and the point when new ones need to be created.

It is important to remember that standards are neither essential nor mandatory when designing and implementing IoT systems and platforms. However, they typically make the process easier and should extend the system lifecycle length by increasing the capability to introduce new technologies and upgrades that interoperate with what is already there.

So why is this important? What will standards help deliver in IoT to make them worth pursuing? ETSI outlines these key areas, which are clearly applicable to IoT:

- **Safety and reliability:** In IoT, key focus areas must be delivered against. These include data privacy and security, as well as safety and environmental care in industrial environments. Standards help ensure that these areas can be met, which then improves user confidence and fosters the adoption of new technologies.
- **Interoperability:** A fundamental requirement of IoT is the capability of devices to work together. This is supported by products, technologies, and services that adhere to standards.
- **Scalability:** Scalability is critical in addressing the dynamic technical and business needs for IoT. All architectures and solutions must be capable of deployment for medium-sized instances and then must seamlessly scale up or down, as needed. This includes network, storage, analytics, and security, as required.
- **Support of government policies and legislation:** Standards are frequently referenced or leveraged by those who create legislation to protect user and business interest and to support government policies. In highly regulated industries that leverage IoT, this is essential.
- **Business benefits:** Organizations need a solid foundation to develop new technologies and enhance existing practices. Standards provide this foundation and help customers reduce both capital and operational costs. This could be through opening or establishing new markets for IoT, encouraging innovation, and increasing awareness of IoT initiatives and opportunities.
- **Choice:** Standards provide the foundation for new features and options, enhancing both daily lives at work or in personal areas.
- **Security:** We need to leverage standards and best practices to minimize the attack surface, get better visibility of security incidents, and leverage consistent tools to defend, detect, remediate, and report in the security environment. Before we design and implement the future IoT, we must first ensure that it is secure.

Without standards, there is a much greater chance that technologies and solutions will not work as expected, will have shorter lifespans, will be incompatible with other solutions and thus be siloed, and will confine consumers of IoT technologies to a single vendor with its own proprietary standard. These last two points have often been seen in IoT during the last few years.

This all sounds good in principle, but is it the same in practice? Can we just adopt open standards for IoT and see that everything will turn out okay? Naturally, other areas must be considered.

What do we mean by *open standard*? As with the definition of IoT, no single, agreed-upon definition exists for what constitutes an open standard. The ITU provides a good perspective, describing open standards as those available to the general public that are developed (or approved) and maintained via a collaborative and consensus-driven process to facilitate interoperability and data exchange among different products or services, for widespread adoption. In "What are open standards?" (2008) Stephen Walli further clarifies this and argues that technology interoperability standards are specifications that define the boundaries between two objects that have been put through a recognized consensus process. That consensus process could be a legal process supported by national standards organizations, by industry or trade organizations with a broad interest, or by a consortia or alliance with a narrower focus. Unfortunately, Walli admits that the standards process does not always seek to find the best technical solution; instead, it looks for the best consensus-driven solution for all participants.

This leads us to another nuance in the standards world. *Open* does not mean *interoperable*, although the two words are often used interchangeably. *Open* means that a system has been designed so that interoperability with it is possible. However, the other technology will have to work with a specific part or parts of a standard, and today there are many such standards. IoT entails multiple and diverse technologies, and these must communicate and interwork on all levels—communications and connectivity, software and applications, platforms to bring things together, and business and industry models. Only when all these areas have common standards will we have true interoperability.

This is a daunting challenge because we need to address architecture, system, hardware, data and file formats, languages and models, and communications protocols. Just because we use a particular protocol between devices and they can communicate with syntactic interoperability does not mean the devices can automatically interpret the information exchanged meaningfully and accurately to produce useful results (demonstrating semantic interoperability). Having an "open" architecture does not mean interoperable or open communications are included. So as we plan, design, and build our IoT systems and platforms, we need to be careful with our use of terms: *Open* does not necessarily mean *open*, and *interoperable* does not necessarily mean *interoperable*, despite what the standard states.

On the positive side, we do have examples today of open interoperable standards in technology, such as TCP/IP or UNIX, and we also have examples of an open, interoperable system, with the Internet. We now need to see the same methodology, principles, and practices emerge for IoT standards to meet the requirements of an open and interoperable IoT system. This will bring out the capability to provide services to and accept services from other systems, and to use the services exchanged to operate effectively together. Both the devices and users would benefit greatly. This is where standards should play the part, facilitating interoperability between products in heterogeneous multivendor, multinetwork, and multiservice and -application environments. Linked to this, standards groups should focus on working with other standards groups, consortia and alliances, and regulators to try to achieve interoperability.

In practical terms, we need standards to help deliver, in a consistent way, a heterogeneous architecture and communication approach for IoT platforms that are open and interoperable. For this to happen, we need to improve connectivity and communications protocols, leverage common processing and programming interfaces and languages, and provide orchestration and automation platforms that remove the barriers among diverse computing platforms, devices, and operating systems. This heterogenous design requirement flows neatly into the NFV and SDN domains, which focus on the outcomes of the system and the system resources instead of on specific physical boxes confined to specific tasks and not being interoperable with other vendors' tasks or systems. We also need to change the approach from the traditional system, in which data is created, captured, and used by humans, to one in which potentially millions or tens of millions of devices are interconnected and interoperate by capturing and using data created by other devices. Only at this stage will we have a chance at true interoperability and open standards for IoT.

The Challenge with Standardization

So what does this mean in terms of choosing the right IoT standards to focus on? First, we need to understand who is involved in standardization or guidance efforts:

- **Alliances:** An alliance is an agreement between two or more parties to pool resources to make a more powerful impact. It usually is not a legal partnership entity, agency, or corporate affiliation.
- **Consortia:** A consortium agreement is a private agreement between two or more parties that outlines rights and obligations among themselves. The objective is to pool resources to achieve a common goal. However, the members are responsible only to the group in regard to the obligations in the consortium contract. Each member remains independent in normal business operations, with no say over other members' work that is not related to the consortium.
- **Standards bodies:** Known as standards organizations, standards bodies, standards-developing organizations (SDO), or standards-setting organizations (SSO), their primary activities are developing, coordinating, revising, and producing technical standards to address the needs of a group. Standards bodies can be international, regional, or national.
- **Regulatory bodies:** These bodies set mandatory or legal requirements, often drawing from standards to leverage existing best practices developed by expert committees using a consensus-based and transparent process.

If we attempted to research and outline every standard and set of guidelines that applies to IoT, we would need to write volumes, as you will see from the compiled list of 109 different bodies later in this chapter (see Figure 4-2)—and this is not an exhaustive list. Furthermore, some of the groups have multiple standards or guidelines that apply to IoT. One example is the IEEE, which outlines 80 of its own IEEE standards as applicable to IoT (see http://standards.ieee.org/innovate/iot/stds.html) and has an additional 45 standards in development for this space. Working through this minefield, we also need to understand that standards are often driven by consortia and alliances, which naturally push for their own interests. Beyond that, standards are usually merely a best fit, not the best technical solution. So why do we bother?

The answer is simple: Without standards, we will not see the potential returns and benefits promised by IoT. At a bare minimum, we need communication standards for interoperability. Without interoperability, different devices and systems from different vendors will not work with one another, and this will return us to the silos of yesterday. Yet we must go beyond just connectivity to realize the benefits.

As the industry evolves, we have an increasing need for a standard model and process, not just to allow devices to communicate, but also to perform common IoT back-end tasks such as security, automation, analytics, and business insight. As end users continue to drive this need, we will see different IoT solutions interoperating with common back-end services, guaranteeing levels of interoperability, portability, serviceability, and manageability that are impossible to achieve with current IoT solutions. A 2015 Gartner study argues that this next-generation IoT system will be delivered as a service (aaS), aligning with our approach for the SDN- and NFV-focused platform we discuss in detail in Chapter 8, “The Advanced IoT Platform and MANO.” This means that the scope of standards we need to address is not limited to the traditional IoT ones, but should be expanded to include SDN and NFV. We also need standardized ways to deliver the necessary IoT capabilities as a service and we need security-specific standards that might not have been developed with IoT in mind.

As we look to architect, design, and build our IoT systems, we need to carefully consider what standards are out there today and which standards are developing. We need to choose wisely. We currently have a broad collection of standards, alliances, consortia, and also regulatory bodies to help, and we outline these in the next section. From a security perspective, standards will help our cause. We need standards to minimize the attack surface, gain better visibility of security incidents, and provide consistent and usable tools to defend, detect, remediate, and report security incidents.

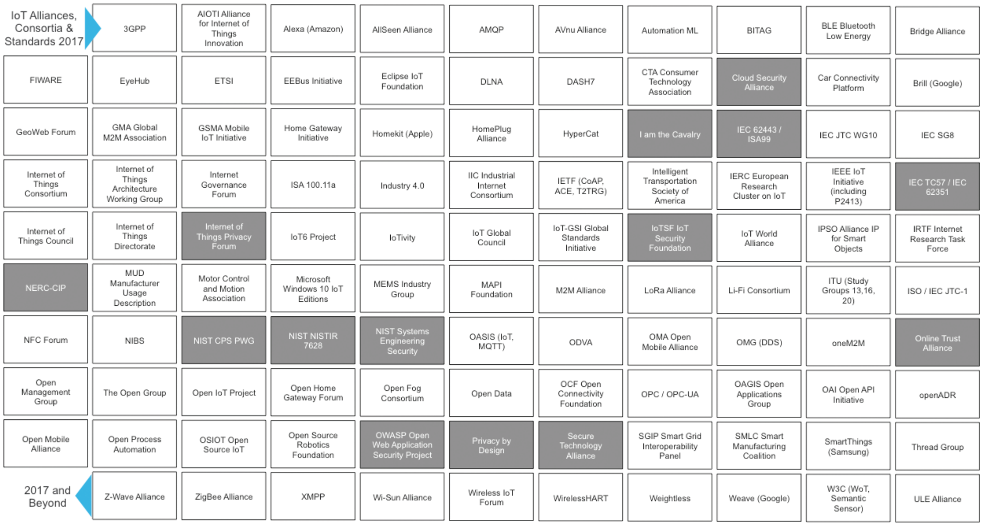
The following are some practical considerations:

- Do not create something that already exists. The U.S. Department of Homeland Security recommends building on recognized architectural and security practices as part of a strategy to secure IoT. Many tested practices used in traditional IT and network security can be applied to IoT. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices and systems.

- Start with basic, consistent architecture and cybersecurity standards and best practices, and apply them to not only the IoT system, but also the entire IoT ecosystem that might form part of a solution.
- Leverage sector- or market-specific best practices and guidelines, where available, to address unique architectural and security approaches or regulation.
- Try to assess industry indicators for which standard will win out in the long term. Backing the wrong standard could result in a system that eventually becomes non-interoperable or obsolete, and this has time and money implications. Look at the standards bodies that the large vendors and industry players are backing. Of course, this could be a challenge if multiple industry-leading IoT companies, such as Cisco, Intel, IBM, GE, and Microsoft, appear to be hedging their bets and working across multiple consortia.

IoT "Standards" and "Guidance" Landscape

The standards, guidelines, consortia, and alliances landscape is broad, with a wealth of options. In the short term, these options likely will increase, but the industry eventually needs to converge to realize the IoT vision. Figure 4-2 shows the main groups that exist in 2017, although this is not an exhaustive list.



IoT Alliances, Consortia & Standards 2017	3GPP	AIOTI Alliance for Internet of Things Innovation	Alexa (Amazon)	AllSeen Alliance	AMQP	AVnu Alliance	Automation ML	BITAG	BLE Bluetooth Low Energy	Bridge Alliance
FIWARE	EyeHub	ETSI	EEBus Initiative	Eclipse IoT Foundation	DLNA	DASH7	CTA Consumer Technology Association	Cloud Security Alliance	Car Connectivity Platform	Brill (Google)
GeoWeb Forum	GMA Global M2M Association	GSMA Mobile IoT Initiative	Home Gateway Initiative	Homekit (Apple)	HomePlug Alliance	HyperCat	I am the Cavalry	IEC 62443 / ISA99	IEC JTC WG10	IEC SG8
Internet of Things Consortium	Internet of Things Architecture Working Group	Internet Governance Forum	ISA 100.11a	Industry 4.0	IIC Industrial Internet Consortium	IETF (CoAP, ACE, T2TRG)	Intelligent Transportation Society of America	IERC European Research Cluster on IoT	IEEE IoT Initiative (including P2413)	IEC TC57 / IEC 62351
Internet of Things Council	Internet of Things Directorate	Internet of Things Privacy Forum	IoT6 Project	IoTivity	IoT Global Council	IoT-GSI Global Standards Initiative	IoTSF IoT Security Foundation	IoT World Alliance	IPSO Alliance IP for Smart Objects	IRTF Internet Research Task Force
NERC-CIP	MUD Manufacturer Usage Description	Motor Control and Motion Association	Microsoft Windows 10 IoT Editions	MEMS Industry Group	MAPI Foundation	M2M Alliance	LoRa Alliance	Li-Fi Consortium	ITU (Study Groups 13,16, 20)	ISO / IEC JTC-1
NFC Forum	NIBS	NIST CPS PWG	NIST NISTIR 7628	NIST Systems Engineering Security	OASIS (IoT, MQTT)	ODVA	OMA Open Mobile Alliance	OMG (DDS)	oneM2M	Online Trust Alliance
Open Management Group	The Open Group	Open IoT Project	Open Home Gateway Forum	Open Fog Consortium	Open Data	OCF Open Connectivity Foundation	OPC / OPC-UA	OAGIS Open Applications Group	OAI Open API Initiative	openADR
Open Mobile Alliance	Open Process Automation	OSIOT Open Source IoT	Open Source Robotics Foundation	OWASP Open Web Application Security Project	Privacy by Design	Secure Technology Alliance	SGIP Smart Grid Interoperability Panel	SMLC Smart Manufacturing Coalition	SmartThings (Samsung)	Thread Group
2017 and Beyond	Z-Wave Alliance	ZigBee Alliance	XMPP	Wi-Sun Alliance	Wireless IoT Forum	WirelessHART	Weightless	Weave (Google)	W3C (WoT, Semantic Sensor)	ULE Alliance

Figure 4-2 *The IoT Standards and Guidance Landscape*

Before looking at an overview of the standards, we need to emphasize the importance of risk. This is usually the first step in deciding what needs to be protected. No specific risk standards exist for IoT, although many IoT or IoT-related standards do contain elements of risk. Internationally recognized standards such as ISO 27001 and ISO 27005, IEC 62443, NIST SP 800-39 and SP 800-37, and the Open Group Risk Taxonomy Standard also cover both the IT and OT angles for IoT. In addition, be sure to keep in mind the proposed new framework we suggest in Chapter 2, "Planning for IoT Security."

The following section outlines the key standards, alliances, consortia, and guidelines in four main areas that need to be considered for IoT systems. The Glossary contains information and links to all 109 resources.

- **Umbrella:** Covers the entire IoT stack, but with no specific market or sector focus
- **Industrial/sector/market:** Covers the entire IoT stack, with a specific market or sector focus
- **NFV/SDN:** Covers NFV or SDN in general, but not specifically for IoT (although some of these groups do have specific IoT focus areas)
- **Security:** Covering security in general, security for IoT specifically, or security for a specific market or sector

Each grouping has a link or a drive for IoT, based on industry direction or market research (whether directly or indirectly focused on IoT); each grouping also has a security element. The security elements of each standard are not called out specifically in this chapter, and additional information is available on the website of each group. The groups are listed in alphabetical order, not in order of importance or applicability.

Architectural or Reference Standards

- **The Alliance for Internet of Things Innovation** (**AIOTI**; https://aioti-space.org/) was founded in March 2015 by the European Commission. Its aim is to create and foster a European IoT ecosystem to accelerate the adoption of IoT. As part of this work, the AIOTI is supporting the convergence of IoT standards, researching how to remove barriers to IoT adoption, and aligning the EU with the rest of the world's IoT activities.
- **The European Telecommunications Standards Institute** (**ETSI**; www.etsi.org and www.etsi.org/technologies-clusters/clusters/connecting-things) has focused its IoT-specific work since May 2015 on ensuring interoperable and cost-effective solutions for M2M, particularly for smart services and applications for IoT. The ETSI is developing standards for data security, data management, data transport, and data processing, with specific initiatives in smart devices, appliances, homes, buildings, connected vehicles, smart grids, and cities. ETSI collaborates with oneM2M in IoT.
- **The Institute of Electrical and Electronics Engineers** (**IEEE**; http://standards.ieee.org/innovate/iot/index.html) has several IoT-focused groups, including the IEEE IoT Initiative, established in 2014, and the IEEE P2413 working group. The IoT Initiative has developed (and continues to develop) a number of standards and is a central point for all IEEE IoT activities. The IEEE P2413 working group focuses on developing an IoT reference architecture, covering basic building blocks, their capability to be integrated into multitiered systems, and security.

- **The ITU Telecommunication Standardization Sector** (**ITU-T**; http://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx) launched its Internet of Things Global Standards Initiative in 2013. Its work is driven by Study Group 20 (SG20), with a focus on IoT and smart cities and communities. Its goals include standardization requirements for the coordinated development of IoT technologies such as M2M and ubiquitous sensor networks, as well as an end-to-end architecture for IoT.

- **The Internet Engineering Task Force** (**IETF**; https://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki) is the leading Internet standards body. It has a specific IoT group that is coordinating related efforts across its working groups, reviewing specifications for consistency, and monitoring IoT-related activities in other standards groups.

- **The Internet Research Task Force** (**IRTF**; https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf), part of the IETF, has been working on various IoT-related initiatives since 2005. Today it has seven working groups, focused on IPv6 over Low-power WPAN (6LoWPAN), Routing Over Low-power and Lossy networks (ROLL), Constrained RESTful Environments (CoRE), 6TiSCH WG (IPv6 over the TSCH mode of IEEE 802.15.4e), Concise Binary Object Representation (CBOR), and IRTF Thing-to-Thing Research Group (T2TRG).

- **IoTivity** (https://www.iotivity.org/) founded its open source framework for IoT device-to-device connectivity in 2016. The project is sponsored by the Open Connectivity Foundation (OCF) and hosted by the Linux Foundation.

- **The IPSO Alliance** (https://www.ipso-alliance.org/) was formed in 2008 with a mission to establish and develop industry leadership for a platform that includes the definition and support of smart objects, with an emphasis on object interoperability on protocol and data layers and also identity and privacy technologies. For IoT smart objects, this includes libraries, repositories, design kits, lifecycle management, and interoperability, with a focus on openness and accessibility.

- **The Object Management Group** (http://www.omg.org/hot-topics/iot-standards.htm) is a technical standards consortium that is developing several IoT standards, including ones that focus on the Data Distribution Service (DDS) and Interaction Flow Modeling Language (IFML), dependability frameworks, threat modeling, and a unified component model for real-time and embedded systems. The Object Management group has also managed the IIC since 2014.

- **The Open Connectivity Foundation** (**OCF**; http://openconnectivity.org/), renamed in 2016 from the previous Open Interconnect Consortium (OIC), develops specification standards, creates interoperability guidelines, and provides a certification program for IoT devices. It is one of the largest IoT organizations (members include Microsoft, Intel, Cisco, and Samsung) and it sponsors the open source IoTivity Project.

- **The Open API Initiative** (https://www.openapis.org/) provides a specification for machine-readable interface files for describing, producing, consuming, and visualizing RESTful API web services as part of the OpenAPI Specification. Development started in 2010, with the OpenAPI Specification released in 2016.
- **The OpenFog Consortium** (**OFC**; www.openfogconsortium.org) was established in November 2015 with the founding members ARM, Cisco, Dell, Intel, Microsoft, and Princeton University Edge Computing Laboratory. OpenFog is a public–private ecosystem formed to accelerate the adoption of fog computing to solve the bandwidth, latency, and communications challenges associated with IoT, Artificial Intelligence, robotics, the tactile Internet, and other advanced concepts. This includes defining a reference architecture of distributed computing, network, storage, control, and resources to support intelligence at the edge of IoT (including autonomous and self-aware machines, things, devices, and smart objects in a variety of disciplines and fields).
- **The Organization for the Advancement of Structured Information Standards** (**OASIS**; https://www.oasis-open.org/) was founded in 1998. It currently promotes industry consensus and produces standards for security, IoT, cloud computing, energy, content technologies, and emergency management.

The main umbrella groups for IoT security are the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance. The section "Specific Security Standards and Guidelines," later in this chapter, covers both.

Industrial/Market Focused

- **The Industrial Internet Consortium** (**IIC**; www.iiconsortium.com) was established March 2014 with the founding members in AT&T, Cisco, GE, IBM, and Intel. The focus of the IIC is to accelerate the industrial IoT, to promote open standards and interoperability for technologies in industrial and machine-to-machine environments. This includes defining use cases and test beds, creating interoperability reference architectures and frameworks, influencing the standards process for the Internet and industrial systems, and facilitating the open sharing of information, ideas, and experiences. The IIC also seeks to build confidence in new approaches to security.
- **The Open DeviceNet Vendors Association** (**ODVA**; www.odva.org) was founded in March 1995 and underwent a 2014 relaunch. Members are suppliers of devices for industrial automation application. Current efforts target transforming industrial automation in integrated cyber-physical systems, with connectivity between things inside and outside the plant. Its approach includes technologies such as SDN, time-sensitive networks (TSN), mobility, cloud, and industrial cybersecurity to make IIoT a reality.
- **The Open Group Open Process Automation** (http://www.opengroup.org/open-process-automation) was established in September 2016, driven by the needs of ExxonMobil. It was standardized by the Open Group because of its applicability

to multiple organizations and industries. The Open Process Automation Forum is an international forum of end users, system integrators, suppliers, academia, and other standards organizations whose aim is to develop a standards-based, open, secure, and interoperable process control architecture. A key element in this is to offer a customer-driven standard, pushing control vendors away from proprietary systems. The standard is a good mix of users and suppliers of process automation systems, and scope covers edge to cloud because of IoT.

- **The Manufacturers Alliance for Productivity and Innovation** (**MAPI**; https://www.mapi.net/forecasts-data/internet-things-industrie-40-vs-industrial-internet) was revived in 2011. It developed Industrie 4.0 for industrial applications of IoT, which focuses on automation and data exchange in manufacturing technologies, including cyber-physical systems, IoT, and cloud computing. Four design principles are central to Industry 4.0: interoperability, or the capability of machines, devices, sensors, and people to communicate with each other via IoT or the Internet of People (IoP); information transparency, or the idea that information can create a virtual copy of the physical world by enriching digital plant models with sensor data; technical assistance, or the capability of assistance systems to support humans in making informed decisions, as well as the capability of cyber-physical systems to physically support humans by doing work deemed unsuitable for people; and decentralized decisions, or the autonomy of decision making for cyber-physical systems.
- **oneM2M** (http://www.onem2m.org/), formed in July 2012, focuses on developing communications architecture and standards, as well as security, interoperability, and specifications for machine-to-machine and IoT technologies. Its framework supports a number of verticals including healthcare, industrial automation, smart grid, connected car, and home automation.
- **OLE for Process Control** (**OPC**; www.opcfoundation.org), founded in 1996, provides an interoperability standard for the secure and reliable exchange of data in the industrial automation space and other industries, including IoT. The developed specifications have been created by industry vendors, end users, and developers. In 2008, OPC-UA (OPC Unified Architecture) was launched, providing a service-oriented architecture to integrate individual OPC specifications into a single framework.
- **The Smart Grid Interoperability Panel** (**SGIP**; http://www.sgip.org/cybersecurity/) was established in December 2009. SGIP focuses on interoperability standards to advance power grid modernization and accelerate the interoperability of smart grid systems and devices. It has a specific IoT effort within the energy industry to incorporate common data models and IoT communication protocols.
- **The Thread Group** (https://www.threadgroup.org/), formed in July 2014, drives an IPv6 networking protocol for IoT to automate home devices such as lighting and security systems on a local wireless mesh network. Thread provides a certification program for Thread-based devices.

The main security standards and regulations for the industrial space include IEC 62443 for industrial control systems, IEC 62351 for power automation, and NERC-CIP for the North American power industry. These are covered in the section "Specific Security Standards and Guidelines," later in this chapter.

Standards for NFV, SDN, and Data Modeling for Services

A 2015 Gartner report recommends a number of principles for IoT solutions architects:

- Design IoT solutions for software-defined things, leveraging a software-defined architecture.
- Build up the technology skills and expertise for the management of large-scale, automated, event-driven systems.
- Invest in technology and expertise in virtualization and software portability, including containerized microservices.
- Choose platforms that offer agility, extensibility, and openness.

These relate directly to the capabilities of NFV and SDN and the level of flexibility, programmability, and automation they provide. NFV and SDN are often used interchangeably, but they are two very distinct technology areas. However, combining them in discussion can bring additional value to some of the complex IoT challenges, as you will see in later chapters of this book. Interestingly, as with IoT, no single standards body exists for NFV or SDN. The SDX Central research repository monitors organizations and standards bodies that exist to enhance SDN, NFV, and NV (network virtualization) adoption and implementation. Its annual report in 2016 listed 138 different organizations. However, we do see a lot of interoperability and openness in the industry to allow different vendor solutions to come together. Not only do we continue to see adoption in the service provider and enterprise spaces, but there is a trend for adoption in the ever-growing IoT space because of the flexibility and features they provide over traditional static network architectures.

Chapter 6, "Evolution and Benefits of SDX and NFV Technologies and Their Impact on IoT," covers NFV and SDN in detail but a brief overview is provided here to give some context in terms of the technology and standards.

Network functions virtualization (NFV) offers a standardized way to architect, implement, and manage networking services. (As we highlight later in this chapter, this can also be extended to other services beyond the network.) The concept involves replacing dedicated network infrastructure devices such as routers and firewalls with standard servers, switches, storage, cloud, or even a fog/edge computing infrastructure. NFV decouples network functions such as routing, switching, and security from proprietary or dedicated hardware appliances, to allow them to run in software.

The aim is to leverage standard IT virtualization technologies to consolidate hardware and to virtualize network functions into building blocks that can connect or chain together to create end-to-end communication services. This can be realized for any control plane function or data plane processing in wired and wireless network environments.

NFV was really born in 2012 when seven of the leading global network service providers came together under the ETSI Industry Specification Group for NFV. This is the main group for developing the requirements and architecture for virtualization for various functions within telecom networks and for the architectural standards for NFV, such as the NFV MANO (Management and Orchestration) architecture. It has become the de facto standard for NFV.

The NFV framework has three main components, as Figure 4-3 shows. The Virtualized Network Functions (VNF) are network functions that are implemented in software and can be deployed in a network functions virtualization infrastructure (NFVI). The NFVI is the overall hardware and software components where VNFs are deployed. The NFV management and orchestration (MANO) environment is the architectural framework that contains the functional blocks, data repositories used by these blocks, and interfaces through which the functional blocks exchange information for the purpose of managing and orchestrating NFVI and VNFs.

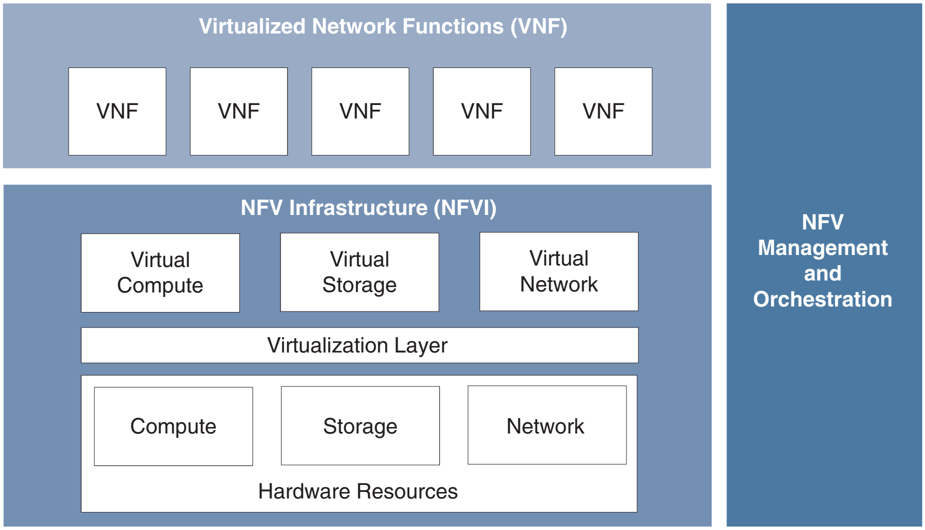


Figure 4-3 *Network Functions Virtualization Overview*

Software-defined networking (SDN) is an approach to design, build, and operate networks by separating the control and data forwarding planes. This enables the network to become directly programmable and dynamic, and it abstracts the lower-level infrastructure functionality. The term arose in the mid-1990s. However, it really became established in 2011 when the Open Networking Foundation was founded to promote SDN and used OpenFlow as the key protocol to describe how to make changes to the network in a standardized way. *SDN* and *OpenFlow* are sometimes used interchangeably, but this is inaccurate. OpenFlow is a protocol, and other communication mechanisms can be used to deliver SDN capabilities.

Several different architectures separate the control logic to off-device resources, but all SDN approaches include an SDN controller and both southbound and northbound APIs (see Figure 4-4).

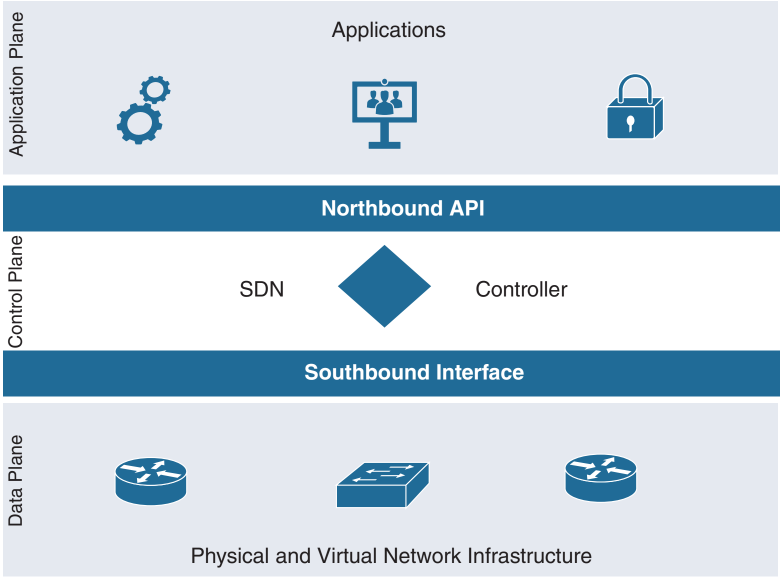


Figure 4-4 *Software-Defined Networking Architecture Overview*

With the close alignment of NFV and SDN as advanced technology areas, some groups are concerned with standards and best practice for SDN, NFV, or often both. The following is a compilation of the key groups and their focus areas, listed alphabetically.

- **The Alliance for Telecommunications Industry Solutions** (**ATIS**; http://www.atis.org/) SDN and NFV Focus Group was launched in January 2014, with a focus on the service chaining of hardware/NFV appliances using SDN concepts. This includes developing application interface APIs and OAM interface APIs for service chaining in an OpenStack and OpenDaylight framework.
- **The Broadband Forum Member** (**BBF**; https://www.broadband-forum.org/) works on both SDN and NFV, with a focus of delivering cloud-based broadband and NFV into the home via service provider networks. In 2017, the BBF entered into a memorandum of understanding (MoU) with the SDN/NFV Industry Alliance to promote the development of network transformation and cloud evolution.

- **The European Telecommunications Standards Institute** (**ETSI**; http://www.etsi.org/technologies-clusters/technologies/nfv) is the main global driver for NFV. The NFV group was founded in November 2012 by seven leading telecoms operators, and ISG NFV became the home of the Industry Specification Group for NFV.

- **The Institute of Electrical and Electronics Engineers** (**IEEE**; https://sdn.ieee.org/) has standardization efforts for SDN underway via two research groups and two study groups. It is examining standardization opportunities in software-defined networks, network functions virtualization, and related areas. The IEEE currently has produced eight standards for SDN.

- **The International Council on Large Electrical Systems** (**CIGRE**; http://www.cigre.org/) has a working group focused on developing the IEEE P1915.1 standard, which specifies the security framework, models, analytics, and requirements for SDN/NFV. CIGRE seeks to understand and address security models, terminology, and analytics (essential components of SDN and NFV environments) to ensure confidentiality, integrity, and availability. It also aims to produce a framework of guidelines for the procurement, deployment, and management of SDN and NFV technologies.

- **The International Telecommunication Union Telecommunication Standardization Sector** (**ITU-T**; http://www.itu.int/en/ITU-T/sdn/Pages/default.aspx) has focused on SDN since November 2012. The ITU-T has adopted Resolution 77 to push for standardization in SDN and also performs SDN-focused work in the group WTSA-12.

- **The Internet Engineering Taskforce** (**IETF**; https://ietf.org) is working on both SDN (through RFC 7426 SDN) and a new IETF SDN standards group (I2RS), to work on southbound programming protocols and NFV and network service chains.

- **The Internet Research Task Force** (**IRTF**; https://irtf.org/concluded/sdnrg) has an SDN group whose aim is to benefit all types of networks, including wireless, cellular, home, enterprise, data centers, and wide-area networks. The Software-Defined Networking Research Group (SDNRG) seeks to identify approaches that can be defined, deployed, and used in the near term, as well identify future research challenges. Key areas of interest include solution scalability, abstractions, and programming languages and paradigms that are particularly useful in the context of SDN. It also provides a forum for researchers to investigate problems in the SDN field, and it provides direct input into standards for other groups, such as ETSI, the IETF and the IEEE.

- **The Internet Society** (**ISOC**; https://www.internetsociety.org/) has IRTF and IETF groups that focus on NFV and SDN and provide architectural oversight to the Internet Architecture Board (IAB; https://www.iab.org/).

- **The Metro Ethernet Forum** (**MEF**; https://mef.net/), founded in 2001, facilitates industry-neutral implementation environments for service orchestration (OpenLSO) and L2–L7 connectivity services (OpenCS) based on technologies such as SDN and NFV. Its goal is to develop agile, assured, and orchestrated services for the digital economy and the hyperconnected world.

- **The Open Data Centre Alliance** (**ODCA**; https://opendatacenteralliance.org/) was established in October 2010. ODCA is driving a federated cloud architecture with common standards for both hardware and software. It focuses on the widespread adoption of enterprise cloud computing through best practice sharing and collaboration. ODCA has work groups for both SDN and NFV and includes organizations such as BMW, Royal Dutch Shell, and Marriott Hotels.
- **OpenDaylight** (https://www.opendaylight.org/) promotes an open source SDN platform for building programmable and flexible networks. The OpenDaylight Foundation was formed in 2013 and consists of solution providers, individual developers, and end users that include service providers, enterprises, and universities.
- **The Open Networking Foundation** (**ONF**; https://www.opennetworking.org/) is a nonprofit, user-driven organization dedicated to accelerating the adoption of SDN and NFV. The ONF really drove the SDN movement in 2011; it includes companies such as Deutsche Telekom, Facebook, Google, Microsoft, Verizon, and Yahoo! that aim to standardize SDN and OpenFlow. In 2017, ONF announced an Open Innovation Pipeline to guide the industry toward the next generation of SDN and NFV. Network device disaggregation, open source platforms, and software-defined standards are key priorities.
- **The Open Platform for NFV** (**OPNFV**; https://www.opnfv.org), formed in 2014 by the Linux foundation, facilitates the development and evolution of NFV components for open source ecosystems. OPNFV created a reference platform through system-level integration, deployment, and testing, to accelerate the transformation of enterprise and service provider networks. Members include AT&T, Juniper, Brocade, China Mobile, Cisco, Dell, Ericsson, IBM, and Intel.
- **The Optical Internetworking Forum** (**OIF**; http://www.oiforum.com/) has an architecture and signaling working group that is defining interfaces for SDN.

Data Modeling and Services

Data modeling is the process of creating a data model for an information system by applying formal methodologies to model data in a standard, consistent, and predictable way so that it can be managed as a resource. As with everything else, data modeling has a number of competing standards. A data modeling language is required to standardize how we describe and create capabilities and how we can deploy this as a service. For automation and scale into an open heterogenous environment in which any service from any vendor might need to be deployed into any device, we need to leverage a standards-based, model-driven, service-centric approach. This must abstract the service intention from the service instantiation and also separate the instantiation from the devices services will be deployed in. This means being open to device type (multivendor) and also to where the device is deployed (edge, fog, network, data center, or cloud). The standard must also be understood and processed by an NFV- and SDN-based orchestration system.

Many debates have questioned the best choice of modeling language for services in NFV and SDN environments. Typically, the choice comes down to YANG or TOSCA. Both have merits and strengths, but in the context of IoT, with a potentially widely distributed environment with multiple devices from multiple vendors and an architecture that could be very non–cloud focused, YANG has the best applicability. Indeed, YANG has become the standard data modeling language of choice in all environments for a number of reasons, including its applicability throughout an automation and orchestration stack:

- Network infrastructure
- Data plane programmability
- Operating systems
- Controller programmability
- Cloud and virtualization management
- Orchestration and policy

In addition, we have recently seen some of the first IoT- and fog-specific YANG models created for customer implementations in smart cities, automotive manufacturing, oil and gas, and power utilities. All are orchestrated and automated to deliver end-to-end secure customer use cases, leveraging the NFV- and SDN-based platform we describe in Chapter 8. We highlight this new approach later in this section, to show the additional flexibility and capability of YANG.

The IETF uses YANG to specify models, and YANG is also used in many standards-development organizations (SDO), consortia, and open source projects, including the Broadband Forum, IEEE, ITU, MEF, and OpenDaylight, among others. As a data modeling language, YANG is used to model configuration and state data manipulated by the NETCONF network configuration protocol. Figure 4-5 shows an overview of YANG.

YANG can be used to model both configuration data and the state data of network elements, in addition to event notifications from network elements. Data modelers thus can define remote procedure calls that can be invoked on network elements via the IETF standardized NETCONF protocol. YANG is protocol independent and can be converted into any encoding format, such as XML or JSON, that the configuration process supports.

YANG models have traditionally been used to describe networking capabilities and device configurations that leverage the NETCONF protocol. However, it is flexible and powerful enough to be extended to other areas of service definition. As mentioned earlier in this chapter, for IoT, it is essential to include the fog and edge devices, the data pipeline, service assurance, multitenancy, and additional security (see Figure 4-6). The flexibility of YANG enables the extension of the ETSI MANO architecture to encompass these additional areas and address the entire IoT stack.

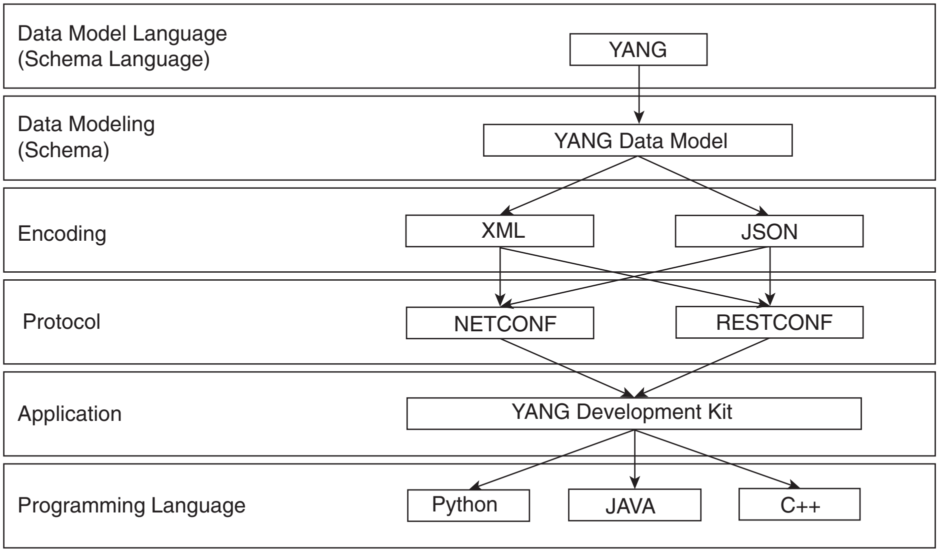


Figure 4-5 *YANG Model Overview*

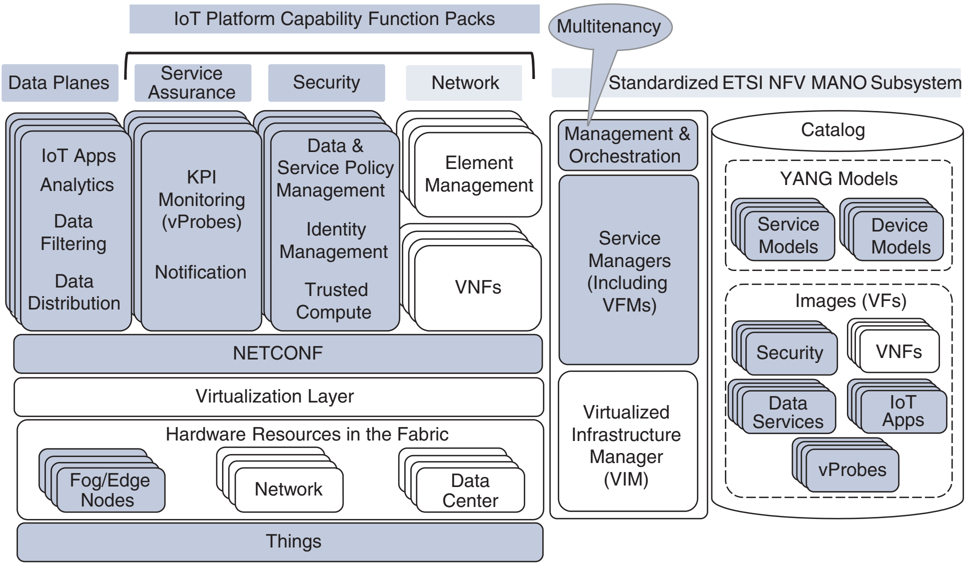


Figure 4-6 *Extending the ETSI MANO Architecture via YANG Service Models*

In the advanced IoT orchestration and automation system that will be detailed in Chapter 8, YANG is the service model language leveraged for both device and service modeling. Chapter 8 outlines how the YANG model works and how the orchestration system leverages it to translate service intent, through to an automated deployment of the service for full use cases via service "function packs." This includes automation capabilities for the complete IoT stack, including infrastructure, virtual network infrastructure, physical devices, virtual environments (VMware, Linux docker, and so on), service assurance, the data pipeline (message brokers, data transformation, and so on), applications and microservices, and, of course, security.

Communication Protocols for IoT

IoT is about connectivity and interoperability, as previously outlined. Without these basic elements, we cannot deliver business value. Therefore, we need communication to happen—and in as uniform a way as possible. As with IoT standards, the standards for protocols and media are heavily fragmented. This section provides an overview of the key communications protocols required for IoT to be successful. It also covers the main wireless offerings that provide the pervasive coverage essential to IoT and touches on some essential wired ones. This section aims to give an overview of the key communications protocols so that you understand what is required from a platform connectivity perspective, especially at the edge and fog layers of the system. This is not designed to be a detailed protocol analysis because much information already exists in this area.

As you have already seen, many emerging and competing networking technologies are being adopted for IoT. Various consortia/alliances, vertical markets, and vendors offer differing technologies for IoT connectivity. Traditional enterprise technologies such as Wi-Fi and Ethernet can be applied for IoT. At the same time, new technologies are being developed specifically to meet the challenges of IoT, especially closer to the edge where specific device, distance, or bandwidth challenges need to be addressed. However we look at it, communications are still the foundational enabler for IoT and are needed for all use cases.

Communication protocols are a set of rules that allow two or more devices in hardware or software to establish a reliable communication system that allows data to be transmitted between them. Rules include syntax, semantics, and synchronization, as well as error recovery mechanisms.

The most common communications model is the Open Systems Interconnection (OSI) model (see the left side of Figure 4-7), which breaks communications into seven functional layers for easier implementation of scalable and interoperable networks. Each layer delivers a specific function and handles clearly defined tasks while interfacing with the layers located directly above and below it. The model is the most widely used in network communications today, with clearly defined layers allowing easier implementation of interoperable and scalable networks.

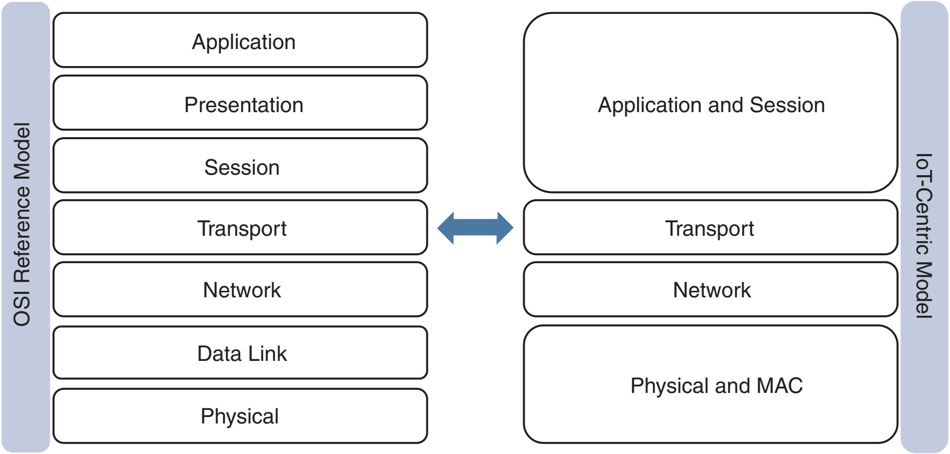


Figure 4-7 *Open Systems Interconnection (OSI) Model*

Although this model is applicable in IoT, it faces certain challenges, especially when devices are very simple and have limited capabilities and computing. A layered approach such as this introduces complexity to the device or software and usually requires more code and memory. It also introduces data overhead because every layer requires additional framing and control messages. More complexity and data transmitted can mean increased power consumption by devices; again, this might not suit an IoT deployment with simple, battery-powered devices. A layered approach does enable more flexibility and scale, however, and also provides the best opportunity for interoperability.

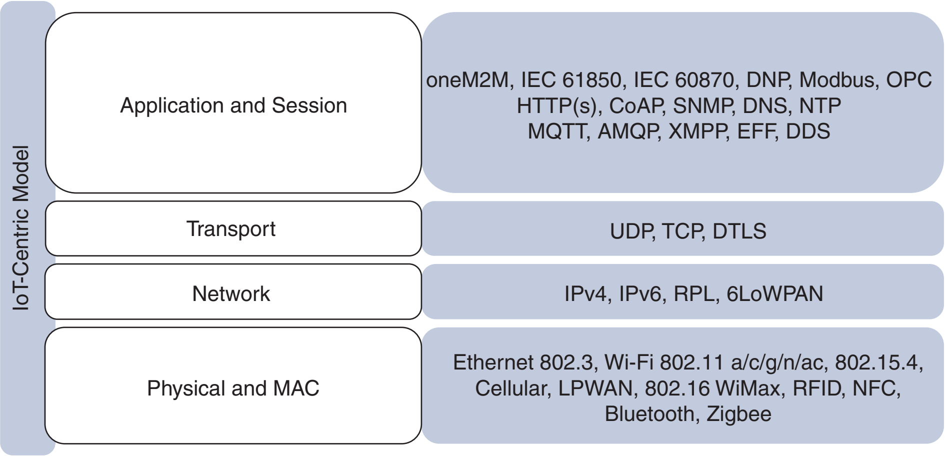
As a result, we see various implementations in IoT. Some use the full OSI reference model, from physical layer to application layer. Others specify only parts of the OSI reference model and leave the remaining aspects of communication up to other technologies. This has led to a more simplistic version of the OSI model for IoT that maps more closely to the TCP/IP model. The right side of Figure 4-7 shows how the model can be simplified for IoT deployments. Some layers are collapsed here, without losing any functionality. This does not mean that one approach is better than the other, particularly because different applications running on top of the communications have different requirements; it simply makes choosing the right option more of a challenge when taking interoperability into account.

This section discusses protocols and communication media, aligning them with the IoT-centric model. Within our focus on communications for data exchange, we look at last-mile communication technologies to the things, or within the fog/edge layers. It is important to make a distinction here because the requirements are different and still emerging. The core networks remain the same and are typically service provider or enterprise based (such as with MPLS). The main change involves connecting the multitude of things together to allow them to communicate between themselves locally or else bringing them back via some kind of backhaul to a central location. Some examples you already are familiar with from the IoT standards overview section; the aim here is to reference the communication elements within them. A fundamental concept to understand is that there is no "one size fits all" approach. A deployment in a smart city might have Ethernet and Wi-Fi connections, whereas a deployment to a remote oil field could be cellular or satellite.

This is extremely important when architecting the system and can dictate architectural and technology decisions. As an example, a gateway might need to be leveraged to provide protocol translation from a legacy system at the edge so that it can be transported through the IoT system by the platform. In another case, a particular function (such as real-time analytics) might have to happen locally because limited bandwidth will not allow a certain amount of data to be transmitted. A more powerful endpoint might thus be deployed to do analytics and data normalization at the fog layer.

From the perspective of the IoT platform, it is important to understand that a wide variety of these protocols need to be addressed as uniformly as possible. This can include IP or non-IP, and different protocols are likely to exist at different levels of the IoT hierarchy. The IoT platform must provide connectivity interfaces for these protocols at the edge or fog layers, whether natively or via a gateway, and must provide a way to securely transport the data flows to their destinations at any level. This applies to both the control and content/data planes.

Following the IoT-centric model, a number of key IoT communication types are mapped out in Figure 4-8.



Application and Session	oneM2M, IEC 61850, IEC 60870, DNP, Modbus, OPC HTTP(s), CoAP, SNMP, DNS, NTP MQTT, AMQP, XMPP, EFF, DDS
Transport	UDP, TCP, DTLS
Network	IPv4, IPv6, RPL, 6LoWPAN
Physical and MAC	Ethernet 802.3, Wi-Fi 802.11 a/c/g/n/ac, 802.15.4, Cellular, LPWAN, 802.16 WiMax, RFID, NFC, Bluetooth, Zigbee

Figure 4-8 *IoT-Centric Communications Model Example*

This model has four layers to cover the communications stack. Although it covers all the functions required, not all of the protocols fit neatly into one level. For example, DTLS fits into the transport, application, and session levels. Similarly, 6LoWPAN fits into the network, physical, and MAC levels. However, this model provides a good starting point for organizing thoughts around communication.

Physical and MAC Layers

This layer covers how a device is physically connected to a network via wired or wireless mechanisms, as well as how devices are uniquely identified by a MAC address (or potentially another method) for physical addressing. Most standards combine the physical and MAC layer protocols; these protocols are essential in establishing communication channels. For IoT, considerations when designing at this level include devices that need to operate with a long battery life, require low power consumption, and have less processing capabilities. Other points to consider are lower bandwidth availability and the need to scale in terms of connecting and operating many more devices in a single environment.

In IoT, wired Ethernet 802.3 and Wi-Fi 802.11 a/b/g/n standards are often leveraged, depending on the environment. Smart cities and manufacturing plant floors are good examples with dense coverage. Other technologies in use include 802.15.4 (802.15.4e, 802.15.4g, WirelessHART, ISA100.11a), cellular (2G, 3G, 4G, CDMA, LTE), Low Power Wide Area Network LPWAN (Long Range Radio LoRa, SigFox, Narrow Band IoT NB-IoT), 802.16 WiMax, RFID, NFC, Bluetooth (including Bluetooth Low Energy BLE), and Zigbee.

Network Layer

This layer focuses on logical addressing and how to deliver packets of information between source and destination endpoints, particularly between different networks. Routing and encapsulation protocols need to be lightweight (constrained devices) and highly scalable (potentially millions of endpoints).

The Internet Protocol (IP) is an essential element of IoT. This includes both IPv4 and IPv6; the latter is essential to address scale. IPv4 provides around 4.3 billion addresses in total, which can create a challenge as we move toward the predicted 20–50 billion endpoints by 2020. IPv6 provides around 340 billion billion billion billion addresses, meaning that the scalability challenge is negated. However, not all IoT devices need a unique or a public address; many will be deployed on private networks that will continue to use private address ranges or will be hidden behind gateways at the edge and fog layers of the network.

The use of IP not only provides interoperability benefits, but also helps with longevity and future-proofing of solutions. With the speed of change of IoT devices and technologies, the physical and data link layers evolve every few years. Using IP provides support for a smooth evolution of technologies, without changing core architectures, affecting the stability of deployments, or introducing new use cases. Even if the endpoints do not support IP, gateways can be deployed at the edge or fog levels to provide connectivity and transport, as well as to support multiple physical and data link layer types.

Many last-mile communication options can be unreliable and unpredictable, so a new routing protocol was created to address routing for constrained devices such as those in wireless sensor networks. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) routes IPv6 traffic over low-power networks and lossy networks (LLN). LLNs are a class of network in which both the devices and their communication mechanisms are constrained. LLN devices are typically constrained by processing power, memory, and battery; their communications are characterized by high loss rates, low data rates, and instability. LLNs can scale from a few dozen up to thousands of devices.

In areas with low-power radio communication, the IPv6 Low Power Wireless Personal Area Network (6LoWPAN) can be leveraged. It was designed with very constrained devices in mind and allows IPv6 to be used over 802.15.4 wireless networks. 6LoWPAN optimizes the transmission of IPv6 packets over LLNs such as IEEE 802.15.4 through header compression.

Transport Layer

This layer addresses secure end-to-end communication, including reliability, bandwidth, and congestion management, as well as sequencing and session maintenance. Operating in constrained and highly geographically dispersed environments, as well as leveraging physical media that is less reliable, makes User Datagram Protocol (UDP) the protocol of choice in place of the more heavyweight Transmission Control Protocol (TCP). Transport Layer Security (TLS) and Datagram TLS (DTLS) are typically leveraged for secure transport.

Application Layer

This layer covers application-level messaging and provides the interface between the user and the desired IoT application. Hypertext Transfer Protocol (HTTP) and Secure HTTP (HTTPS) continue to be leveraged in IoT. In addition, the Constrained Application Protocol (CoAP) is often leveraged as a lightweight alternative to HTTP as a specialized web transfer protocol for use with constrained nodes and constrained networks. It is often used in combination with 6LoWPAN.

To allow data exchange and facilitate control of the data pipeline, a messaging service is often leveraged within IoT deployments. Messaging protocols such as Message Queue Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), and Extensible Messaging and Presence Protocol (XMPP) have been leveraged for some time. More recently, feature-rich message services such as the Cisco Edge Fog Fabric (EFF) have been introduced, providing detailed topologies, strong QoS mechanisms, and real-time analytics capabilities as part of the IoT data/content pipeline management.

Industrial IoT environments and specific markets continue to use more industry-specific protocols that have been designed over many years to address certain vertical or market needs. IEC 61850 Sampled Values (SV), Generic Object Oriented Substation Event (GOOSE), and Manufacturing Message Specification (MMS), IEC 60870, Modbus, Distributed Network Protocol (DNP3), and OLE for Process Control (OPC), provide the core communication mechanisms for industrial environments such as power utilities, manufacturing, oil and gas, and transportation.

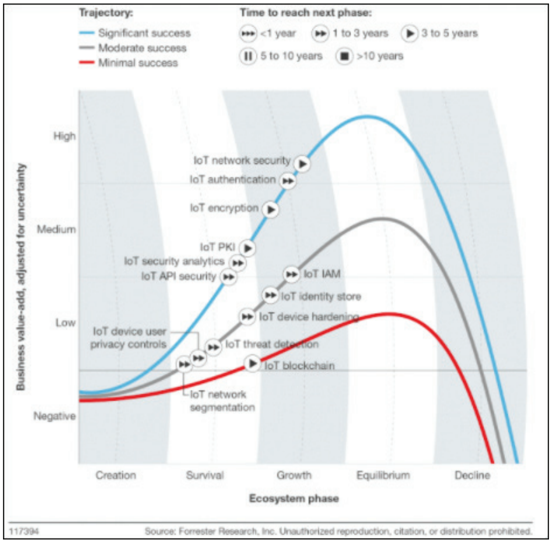
Many IoT environments, particularly industrials, have a requirement to connect legacy devices and sensors. This means that, in addition to IP- and Ethernet-based protocols, serial-based protocols must be connected. This not only adds integration complexity, but it introduces security considerations.

In summary, as well as in practice, different IoT standards use many of these protocols. Choosing the right protocol often comes down to the vendor, the environment, the network topology, the bandwidth available, and the vertical or market in which the use case will be deployed. Other considerations can include power constraints and usage, reliability requirements, and, of course, security. Some of the options listed, such as IEEE 802.15.4, have security mechanisms built in, such as access control, message integrity, replay protection, and message confidentiality.

Specific Security Standards and Guidelines

This leads nicely into the focus area of the book: security. This section explores some of the challenges of standardizing security for the IoT. We look at some key standards and guidelines for security in IoT environments and conclude with some considerations for implementing these as part of the security perspectives discussed in Chapter 2. Standards are available for every layer of the IoT stack, such as Internet Protocol Security (IPsec), Transport Layer Security (TLS), and application layer cryptography. This section does not dive into the technologies themselves, but instead looks at the groups working on bringing technologies together into more of a cohesive approach to security for IoT.

As in the previous sections, standards for security are also widespread and diverse. Many applicable security standards exist, and traditional IT or OT best practices are already being leveraged in many cases. These will continue to be applicable for IoT. With many new security technologies being developed to address new use cases, technologies, and protocols, the landscape is still changing. Research from Forrester (see Figure 4-9) shows that this is set to continue for the foreseeable future, with multiple security requirements still developing for IoT.



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 4-9 *Forrester IoT Security Landscape*

The following standards and guidelines have a specific focus on IoT security, either as an existing best practice that has been applied to the IoT space or as a new best practice generated by IoT demand. Again, these are listed alphabetically, not in order of importance.

- **The European Telecommunications Standards Institute** (**ETSI**; http://www.etsi.org/news-events/news/1015-2015-10-news-etsi-nfv-isg-publishes-security-and-reliability-specifications) has several NFV-focused security areas:
    - Problem statement (NFV-SEC 001)
    - Cataloguing Security Features in Management Software Relevant to NFV (NFV-SEC 002)
    - Security and Trust Guidance (NFV-SEC 003)
    - Privacy and Regulation: Report on Lawful Interception (LI) Implications (NFV-SEC 004)
- **The Institute of Electrical and Electronics Engineers** (**IEEE**; https://standards.ieee.org/develop/project/1915.1.html) P1915.1 standard for SDN and NFV provides a framework to build and operate secure SDN/NFV environments. This standard specifies a security framework, models, analytics, and requirements to secure SDN and NFV.
- **The IoT Security Foundation** (https://iotsecurityfoundation.org/) was established in September 2015 to help secure IoT, accelerate adoption, and maximize potential benefits by providing knowledge and clear security best practices to those who specify, make, and use IoT products and systems.
- **The Open Web Application Security Project** (**OWASP**; https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project) was established to better understand the security issues associated with IoT and to enable better security decisions when building, deploying, or assessing IoT technologies. OWASP has ten IoT security projects to help with this: IoT Attack Surface Areas; IoT Vulnerabilities; Firmware Analysis; ICS/SCADA Software Weaknesses; Community Information; IoT Testing Guides; IoT Security Guidance; Principles of IoT Security; IoT Framework Assessment, Developer, Consumer and Manufacturer Guidance; and Design Principles.
- **The Online Trust Alliance** (**OTA**; https://otalliance.org/), established in 2005, aims to educate users and develop and advance best practices and tools to enhance users' security, privacy, and identity. OTA does this with data sharing and collaboration through working groups, committees, and training. OTA is also a member of other organizations committed to collaboration, law enforcement, and data sharing.
- **The Secure Technology Alliance** (https://www.securetechalliance.org/?utm=scapop), formed in March 2017, is a multi-industry association working to stimulate the understanding, adoption, and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software. This includes secure technologies for authentication, commerce, and IoT

to protect privacy and data. The Secure Technology Alliance was formerly called the Smart Card Alliance; it changed its name in March 2017.

- **IoT IAP** (http://www.iotiap.com/), established in November 2016, addresses security challenges related to IoT. As a working paper, it outlines ideas and approaches to improve today's security situation.
- **The Cloud Security Alliance** (**CSA**; https://cloudsecurityalliance.org/) is a leading organization dedicated to defining and raising awareness of best practices to secure cloud computing environments. CSA offers cloud security-specific research, education, certification, events, and products, including ones focused on IoT.
- **I am the Cavalry** (https://www.iamthecavalry.org/), formed in 2013, aims to ensure that technologies with the potential to impact public safety and human life are worthy of trust and focus on IoT. It accomplishes this in a number of ways, including education, outreach, and research.
- **The National Institute of Standards and Technologies** (**NIST**; https://pages.nist.gov/cpspwg/) launched Cyber Physical Systems in 2014. The Cyber-Physical Systems Public Working Group (CPS PWG) focuses on Cyber-Physical Systems, or "smart" systems, that promise increased efficiency and interaction between computer networks and the physical world. It seeks to enable advances that improve the quality of life, including those in personalized healthcare, emergency response, traffic flow management, and electric power generation and delivery. CPS covers many IoT use cases and includes a consensus vocabulary and reference architecture to facilitate interoperability between elements and systems, as well as promote communication across the breadth of CPS. Timing, dependability, data interoperability, and security are considered first-order design principles for CPS.
- **The National Institute of Standards and Technologies** (**NIST**; https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity) launched its NISTIR 7628 guidelines in September 2014. This three-volume report, *Guidelines for Smart Grid Cybersecurity*, presents an analytical framework that can be used to develop effective cybersecurity strategies based on specific characteristics, risks, and vulnerabilities. It provides methods and supporting information that acts as a guide for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment that includes IoT elements, and it advocates using cybersecurity requirements that also evolve accordingly.
- **The National Institute of Standards and Technologies** (**NIST**; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf) publication SP 800-160 Systems Security Engineering, launched in November 2016, addresses IoT from an engineering-driven perspective and documents actions necessary to develop more defensible and survivable systems (including machine, physical, and human components). It also addresses the capabilities and services delivered by those systems.
- **The International Electrotechnical Commission** (**IEC**; https://www.certsi.es/en/blog/iec62443-evolution-of-isa99) launched the IEC 62443 standard for Cyber

Security for Industrial Control Systems in 2009, based on previous work from ISA99 that was started in 2007. IEC 62443 is the most widely adopted industrial security standard globally; it continues to evolve, particularly in areas such as IoT.

- **The International Electrotechnical Commission** (**IEC**; http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf) launched the IEC 62351standard in 1999. Its focus is on data and communications security in power systems management, along with the associated information exchange. It consists of a series of standards, with a focus on end-to-end security.
- **The North American Electric Reliability Corporation (NERC**: http://www.nerc.com/Pages/default.aspx) launched the Critical Infrastructure Protection regulations for bulk power in North America in 2007. NERC is regulated and requires legal compliance, including cybersecurity.
- **The IoT Global Council** (https://www.iotglobalcouncil.com/), launched in May 2014, is a membership organization for new business leaders of the IoT industry. It focuses on IoT data and security.
- **The Internet Research Task Force** (**IRTF**; https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/) has established security-related works with IoT relevance and focus, launched under the IETF. This includes working groups for DTLS In Constrained Environments (DICE), Authentication and Authorization for Constrained Environments (ACE), and Lightweight Implementation Guidance (LWIG).
- **The Industrial Internet Consortium** (**IIC**; http://www.iiconsortium.org/IISF.htm) is an umbrella type standard with an industrial focus, and has produced a specific cybersecurity framework for the IIoT.

In addition to these established standards and best practices, new ones continue to emerge that focus on interoperability and standardization. A great example is Manufacturer Usage Description (MUD), which introduces a set of network capabilities that provide an additional layer of protection to devices connecting to the IoT system. The focus of this work is security related to smart objects, although it goes further than this. Again, YANG is used as a standardized model to generate and parse manufacturer usage descriptions. Network management systems retrieve these descriptions to instantiate security and communication policies associated with those devices. A manufacturer should know what a device is intended to do; for example, a light bulb should not be communicating with a voice server, but it should be communicating with its controller. The concept, then, is to use the manufacturer's product knowledge to create network policy that can be easily understood and enforced. Put simply, an IoT system should be capable of automatically finding out what a device should be allowed to do and enforcing policies that prevent it from going beyond those limits. At the time of this writing, MUD is currently being reviewed via the standard RFC process; however, organizations (including Cisco) are already working on adoption.

As you have probably concluded from this chapter, many standards and approaches to standards exist for IoT and IoT security. Later chapters of this book zoom in on providing a standardized methodology to deploy and manage security in an open way, leveraging NFV and SDN and automation to ensure that the approach can scale. Instead of competing with existing IoT and security standards, this methodology will actually provide a way to orchestrate and automate the deployment of standards and guidelines, while also bringing a number of enhancements. Security, particularly for IoT, is a multifaceted and difficult challenge, and we will not likely see standards or best practices that completely (or even partly) eliminate the risks of cyber attacks against IoT devices and systems anytime soon. However, a standardized approach to the IoT system, and to the security of the system and by the system, can ensure that deployments meet and even exceed reasonable standards for security. This moves the focus of the approach away from individual devices (which vary greatly in terms of capability) and more toward system-level security (which can more uniformly be provided by an IoT platform).

Summary

As organizations look for the best methods of designing, architecting, and deploying IoT systems, they must consider practical questions:

- What value does a given standard bring to IoT deployment? Are there any demonstrable examples of deployments?
- What are the risks of not using a specific standard—or any standard at all? Do the potential business gains in the short term perhaps outweigh future challenges?
- What are the risks if a chosen standard fails? (A practical option we highlighted earlier was to monitor which industry vendors are backing which standards and make an educated choice.)
- Is there a way to influence a standard? If so, what process or cost is involved? (This can help you understand whether a standard is being driven to truly achieve openness and interoperability, or whether it is being driven for the benefit of one or more participants.)

When looking at standards, whether they focus on IoT, address IoT security in particular, or act as a technology enabler for IoT, remember to consider the security aspects for an IoT deployment. At a minimum, a successful security standard provides the following:

- Scalability and ease of deployment and management. Technologies such as NFV and SDN allow for large-scale automation. This must include policy management, upgrades, and the capability to deploy new devices or use cases without impacting existing ones.
- Protection for devices, no matter where they are deployed in the full IoT stack, from edge to cloud/DC.

- Visibility and monitoring capabilities, in an automated way, to ensure that the system and, ultimately, you are aware of attacks.
- Protection of the end-to-end data pipeline, from initial creation to ultimate consumption.
- Autonomy. IoT often means a devolved and distributed architecture. Devices and lower parts of a system architecture must continue to effectively monitor and enforce security policies and requirements, even if visibility to the system head end is lost.

As the industry moves forward, efforts to evolve and improve standards will consolidate. This is required if we are to deliver technology changes and enable more advanced use cases, applications, and value propositions. The current landscape might be fragmented and complex, but history has shown that we do need standards to minimize complexity in deploying systems and minimize the security attack surface. Standards can help us gain better visibility of security incidents and leverage consistent, best-practice tools to defend, detect, remediate, and report on our IoT deployments.

References

3GPP, http://www.3gpp.org/

Alliance for Internet of Things Innovation (AIOTI), https://aioti-space.org/

AllSeen Alliance, https://allseenalliance.org/

Bluetooth Low Energy (BLE), https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/low-energy

Bridge Alliance, http://www.bridgealliance.com/

Broadband Internet Technical Advisory Group, https://www.bitag.org/

Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/group/internet-of-things/

DASH7, http://www.dash7-alliance.org/

Digital Living Network Alliance (DLNA), https://www.dlna.org/

EEBus Initiative, https://www.eebus.org/en/

EnOCEAN Alliance, https://www.enocean.com/en/

ETSI, http://www.etsi.org/technologies-clusters/clusters/connecting-things

European Committee for Standardisation (CEN), https://www.cen.eu/Pages/default.aspx

FIWARE Foundation, www.fiware.org

Global M2M Association (GMA), http://www.globalm2massociation.com/

GSMA Mobile IoT Initiative, http://www.gsma.com/iot/mobile-iot-initiative/

https://en.wikipedia.org/wiki/Cyber-security_regulation

https://en.wikipedia.org/wiki/Standards_organization

https://www.thethingsnetwork.org/community/thessaloniki/post/50-billion-iot-devices-will-be-connected-by-2020

The Home Gateway Initiative (HGI) http://www.homegatewayinitiative.org/

IEC 62443/ISA99, http://isa99.isa.org/

IEEE IoT Initiative, http://standards.ieee.org/innovate/iot/index.html,

Industrial Internet Consortium (IIC), www.iiconsortium.com

Industry 4.0, https://en.wikipedia.org/wiki/Industry_4.0

International Society of Automation, ISA100.11a, https://www.isa.org/isa100/

Internet Engineering Task Force, https://trac.tools.ietf.org/area/int/trac/wiki/IOTDirWiki

Internet Governance Forum, http://www.intgovforum.org/cms/component/content/article?id=1217:dynamic-coalition-on-the-internet-ofthings

Internet of Things Consortium, http://iofthings.org/

IoT European Research Cluster (IERC), http://www.internet-of-things-research.eu/

IoT Research Council, http://www.theinternetofthings.eu/

IoT Security Foundation (IoTSF), https://iotsecurityfoundation.org/

IoT World Alliance (formerly M2M World Alliance), http://www.iotworldalliance.org

IP for Smart Objects (IPSO Alliance), http://www.ipso-alliance.org/

IRTF Internet Research Task Force, IoT initiatives, https://www.internetsociety.org/publications/ietf-journal-april-2016/internet-things-standards-and-guidance-ietf

ISO/IECJTC-1 https://www.iso.org/isoiec-jtc-1.html

ISOC's Internet of Food SIG, http://internet-of-food.org/

ITU, http://www.itu.int/en/ITUT/studygroups/2013-2016/20/Pages/default.aspx

Li-Fi Consortium, www.lificonsortium.org

LoRa Alliance, https://www.lora-alliance.org/

M2M Alliance, http://www.m2m-alliance.com/

MAPI Foundation, https://www.mapi.net/forecasts-data/internet-things-industrie-40-vs-industrial-internet

OASIS, https://www.oasis-open.org/committees/tc_cat.php?cat=iot

oneM2M, http://www.onem2m.org/

Online Trust Alliance, https://otalliance.org/initiatives/internet-things

Open Connectivity Foundation (OCF), https://openconnectivity.org

Open Group Open Process Automation, http://www.opengroup.org/open-process-automation

OpenFog Consortium (OFC), www.openfogconsortium.org

The Open Management Group, http://www.omg.org/hot-topics/iot-standards.htm

Open Mobile Alliance (OMA), http://openmobilealliance.org/

Open Source Internet of Things (OSIOT), http://osiot.org/

Open Web Application Security Project, https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

Smart Grid Interoperability Panel, http://www.sgip.org/cybersecurity/

Thread Group, https://threadgroup.org

ULE Alliance, https://www.ulealliance.org/

W3C Web of Things (WoT), https://www.w3.org/WoT/

What are open standards?, https://opensource.com/resources/what-are-open-standards

WiHART, https://fieldcommgroup.org/technologies/hart

Wireless IoT Forum, http://www.wireless-iot.org/

Wi-Sun Alliance, www.e.org

The World Wide Web Consortium, https://www.w3.org/

Zigbee Alliance, http://www.zigbee.org/

Z-Wave Alliance, http://z-wavealliance.org/

Index

Symbols

5G, 800

6LoWPAN (IPv6 Low Power Wireless Personal Area Network), 74

802.1X authentication, 363-365

802.1X Flexible Authentication, 366-367

802.11p, 800

A

AAA (authentication, authorization, accounting), 279, 337, 361-362

accounting, 397-398

framework guidelines, 399

requirements, 400-401

centralizing, 268

ODL, 206

standard configuration example, 342-343

tenant/user, 279-280

acceptance, 16

access-accept messages, 362

access-challenge messages, 362

access control

ACLs, 374-376

AWS, 394-397

back-end platform, 637-646

building blocks, 326

complex devices, 345

constrained devices, 345

classes, 345-346

identifying, 348-351

restrictions, 345

data protection, 504

device identification, 336-337

Device Sensor, 340, 343-345

AAA configuration example, 342-343

differentiated authorization privileges, 345

internal/external clients, 341

port security, 341

probe configuration, 344

success, 344

energy limitations, 346-347

equipment health monitoring example, 778-781

IDs, 637-639

Internet draft, 390

ISE profiling, 337-340

Keystone, 640

LDAP, 639

MUD, 390

module, *392*
policy types, *390-391*
process flow, *393-394*
URLs, *emitting*, *390*
multitenancy data sharing, 641, 644
new endpoints, connecting, 639
on demand, 714-718
IPS/IDS, *717-718*
self-service portal, *715-717*
physical access, 505
power for communication, 347-348
RabbitMQ, 546
role-based. *See* RBAC
service deployment, 639-641
SGACLs, 384-388
automation, *388*
benefits, *384*
consumer/provider matrix, *384-386*
east–west, *387*
microsegmentation, *387*
north–south, *387*
SGTs, 376-378
smart city sensors, 708-709
TrustSec, 376-379
classification, *380*
enforcement, *384*
inline tagging, *383*
propagation, *381-383*
Access control lists. *See* ACLs
access-reject messages, 362
access-request messages, 362
accidental incidents, 755
accounting, 397-398
data protection, 505
framework guideline, 399
requirements, 400-401
accreditation, 16
acknowledgeable relationship, 414
ACLs (access control lists), 262
SDN data plane, securing, 262
SGACLs, 384-388
automation, *388*
benefits, *384*
consumer/provider matrix, *384-386*
east–west, *387*
microsegmentation, *387*
north–south, *387*
web-type, 606
acquisition and development phase (SDLC), 14-16
actionable IRM, 413
actions, monitoring, 477
activation sequence example, 472, 474
activation status (VNFs), 474
active networking, 185
Adaptive Network Control (ANC), 446-447
Adaptive Security Appliance virtualized (ASAv), 422-423, 470
ADAS (advanced driver assistance systems), 805
AD-SAL (API-driven service abstraction layers), 209-210
Advanced Malware Protection. *See* AMP
Advanced Message Queuing Protocol (AMQP), 74, 544
Advanced Persistent Threats (APTs), 440-441
AE (application entity), 131
affective computing, 898
aggregators, 101
aggressive mode (IKEv1 phase 1), 582
AGI (Artificial General Intelligence), 891
agility
NFV, 221
OpenFog reference architecture pillar, 135
SDN, 192
AHs (authentication headers), 578
AI (Artificial Intelligence), 98, 878-879

- affective computing, 898
- cognitive computing, 898-899
- components, 891
- contextual awareness, 899
- cybersecurity systems, 878
- DL alignment, 894
- hybrid subsymbolic/symbolic, 892
- ML collaboration, 899
- natural language processing (NLP), 895-896
- people-/user-centric approaches, 98
- subsymbolic, 891-892
- symbolic, 891-892

AIC (availability, integrity, confidentiality), 43

AIOTI (Alliance for the Internet of Things Innovation), 59, 138-140

algorithms

- elliptic curve cryptographic algorithms, 353
- encryption, 580
- hashing, 580
- security events, 445
- state convergence, 475

Alliance for Telecommunications Industry Solutions (ATIS), 65

alliances, standardization efforts, 56

allocating IT staff, 6

always on strategy, 347

AM (authentication manager), 102

Amazon Web Services. *See* AWS

AMP (Advanced Malware Protection), 456, 616

- AnyConnect client, 616
- file policies, 461
- FTD, 459-461
- point-in-time detection, 456-457
- retrospection, 457-458
- sandboxing, 458
- Umbrella service integration, 465

AMQP (Advanced Message Queuing Protocol), 74, 544

analysis

- data, 526
- functional requirements, 15
- nonfunctional security requirements, 15
- protocols, 439
- security assurance requirements, 16

analytics, 5

ANC (Adaptive Network Control), 446-447

ANNs (artificial neural networks), 896-897

anomaly detection. *See* behavioral analysis

anomaly traffic detection, 780-781

ANPR (automatic number plate recognition), 820

anti-tamper and detection, 169

any endpoint, anywhere concept, 25

AnyConnect client, 611-612

- configuration, 612
- deployment, 611
- manufacturing example, 617
  - *authorization, 621*
  - *identity, authentication, posture, 618*
  - *remediation, 619-620*
  - *working components, 618-621*
- modules, 612-616
  - *AMP, 616*
  - *endpoint compliance, 614*
  - *Network Access Manager, 614*
  - *NVM, 615-616*
  - *roaming protection, 614-615*
  - *VPN, 612-613*

API (application programming interface), 19

- back-end platform security, 634-635
- deployment preparations, 316

northbound

fog nodes, 662

ODL, 206

northbound (NB APIs), 43

OVS, 197

REST, 634-635

SDN, 191

southbound

fog nodes, 667

ODL, 204

API-driven service abstraction layers (AD-SAL), 209-210

app entities, 139

Apple Face ID/TouchID, 359

application entity (AE), 131

application layers, 46

AIOTI architecture, 138-139

communication, 74

ITU-T Y.2060 reference model, 125

SDN, 191

application programming interfaces. *See* API

application-specific integrated circuit (ASIC), 374

application visibility and control. *See* AVC

applications

access, clientless SSL VPNs, 604-609

authenticity, 271

blockchain distributed ledger, 884

certification, 271

cloud-native functions, 242

cloud-ready functions, 242

detectors, 433

fog-ready functions, 242

future connected car, 815

hierarchy, 36

IoT-A RA, 123

isolating, 271

lifecycles, 704-705

penetration testing, 271

SDN, securing, 252-253, 270-271

secure development, 271

vertical, 679

APTs (Advanced Persistent Threats), 440-441

architectural reference model (ARM), 121, 177

architectures, 32-33

AIOTI, 138-140

ANNs, 897

blockchain, 886

bringing IT and OT technologies together, 157

cloud-centric, 32

cloud computing, 106-112

accessibility, 109

advantages, 109

availability, 109, 112

characteristics, 107

compliance, 110

costs, 109

deployment, 107-108

disadvantages, 110

environmental benefits, 109

extensibility, 109

interoperability, 110

IoT adoption, accelerating, 111

maintenance, 109

privacy, 110

QoS, 112

real-time processing, 112

reliability, 109

scalability, 109

security, 110

Cloud Customer Architecture for IoT, 140-142

data-centric, 104-105

digital roadway, 806

documentation, 27

edge computing, 112-113

enterprise-centric, 32

equipment health monitoring example, 772

Federal Sigma VAMA, 864

fog computing, 112

advantages, 116-118

communications, 114

complexity, 118

costs, 117-118

cross-vertical replicability, 117

data handling, 115

disadvantages, 117

edge computing, compared, 113

governance, 117

heterogeneity, 117

mobility, 116

proximity, 116-117

reliability, 117

requirements, 115

security, 117

speed, 116

full IoT stack, 120

AIOTI, 138-140

Cloud Customer Architecture, 140-142

IEEE P2413, 132-133

IoT-A RA, 120-125

IoTivity framework, 142-144

IoTWF, 126-129

ITU-T Y.2060, 125-126

oneM2M, 129-132

OpenFog Consortium, 133-138

gateway-centric, 32

hub-centric, 32

ICN, 100-104

IEEE P2413, 132-133

IoT-A RA, 120-125

IoTWF reference model, 126-129

ISE integrated, 337

ITU-T Y.2060 reference model, 125-126

Lambda, 119-120

layers, 85-86

middleware, 118

mobile-centric, 32

next-generation IoT platforms, 294-295

NFV ETSI, 229

NVF-based, 154-156

ODL reference, 204-207

OF, 193

oil and gas industry security, 756-757

oneM2M, 129-132

open process automation based on Purdue Model of Control, 159

OpenFog Consortium, 133-138

perspectives, 136

pillars, 133-135

security layers, 137

stakeholder views, 137

OVS, 196

people-centric approach, 98-100

references, 87

SDN, 64-65, 154-156, 189-192

segmented based on Purdue Model of Control, 157

server-side, 99

standards, 59-61

system viewpoint, 89, 106

cloud computing, 106-112

edge computing, 112

fog computing, 112-118

thing-centric, 32

universal, 89, 120

CPwE, 153

GridBlocks, 153-154

IIRA, 144-146

Industry 4.0, 148-149

NFV-based, 154-156

OPC-UA, 150-152

SDN-based, 154-156

user-centric approach, 98-100

X-centric approach, 89-97

cloud-centric, 95-96

enterprise-centric, 96-97

Garner defined-centric views, 97

gateway-centric, 94-95

hub-centric, 94

mobile-centric, 93-94

thing-centric, 92-93

ARMs (architectural reference models), 121, 177

ARP attacks, 41

Artificial General Intelligence (AGI), 891

Artificial Intelligence. *See* AI

artificial neural networks (ANNs), 896-897

Artik, 176

ASAv (Adaptive Security Appliance virtualized), 422-423, 470

ASDM (ASA Security Device Manager), 612

ASI (Artificial Super Intelligence), 891

ASIC (application-specific integrated circuit), 374

assessments, risk, 15, 58

assets

classification, 27

identification, 27

improvements, 742

assurance

IISF, 162

information (IA), 37

sequences, 474-475, 479-481

services, 784-786

ASTM E2158-01, 827

ASTM PS 105-99, 827

ATIS (Alliance for Telecommunications Industry Solutions), 65

attacks

AMP, 456

file policies, 461

FTD, 459-461

point-in-time detection, 456-457

retrospection, 457-458

sandboxing, 458

ARP, 41

authentication, 41

continuum, 11-12

CSRF, 265

data breach costs, 418

Ethernet, 41

identifying risks, 25-28

classification, 27

identification, 25-26

risk scores, 28

jamming, 41

MAC flooding, 41

MITM, 40

oil and gas industry, 755

protocols, 42

TALOS, 456

targets, 39

communication, 41-42

gateways, 40-41

SDN, 42-43

things, 39-40

threat identification, 27

vectors, 38

wireless, 41

attestation, devices, 315

Attribute Value pairs (A/V pairs), 362

audible warning systems, 820

audio systems, police cars, 820

authentication, 38

AAA, 361-362

attacks, 41

A/V pairs, 362

AWS, 395-397
biometrics, 359-360
certificates, 352
Cisco IoT security framework, 170
constrained device limitations, 358
data protection, 504
digital certificates, 352
IEEE 1609.2, 353
PKI, 353-355
revocation, 356-357
SSL pinning, 357
X.509, 352-353
equipment health monitoring example access privileges, 778-780
flexible, 403
HMAC, 264
HTTP, 264
IEEE 802.1X, 363-365
IEEE 802.1X Flexible, 366-367
IPsec peers, 579
MAB (MAC address bypass), 365
MQTT, 533-535
passwords, 357-358
PKI, 351, 354
public key cryptography, 352
RabbitMQ, 547-548
RADIUS, 361-362
REST, 264-267
servers, 363
southbound SDN controller communication, 258
time service, 281
tokens, 265
trust stores, 355

authentication, authorization, and accounting. *See* AAA

authentication headers (AHs), 578

authentication manager (AM), 102

authenticators, 363

authenticity, 271

authorization
ACLs, 374-376
AWS, 394-397
Cisco IoT security framework, 170
data protection, 504
differentiated privileges, 345
dynamic forms, 368
dynamic privileges, 367
equipment health monitoring example access privileges, 778-780
ISE, 368
MQTT, 535-539
northbound SDN controller communications, securing, 267
policy-based, 403
RabbitMQ, 548-549
RADIUS CoA, 368
request commands, 370-371
Request/Response codes, 369
requests, 368-369
session identification, 369
VLAN assignments, 371-374
RBAC dynamic segmentation, 378
remote HMI access, 621
session identification, 369
SGACLs, 384-388
automation, 388
benefits, 384
consumer/provider matrix, 384-386
east–west, 387
microsegmentation, 387
north–south, 387
SGTs, 376-378
TrustSec, 376-379
classification, 380
enforcement, 384
inline tagging, 383
propagation, 381-383

automatic number plate recognition (ANPR), 820

automation, 5

connected cars deployment, 815, 867-870

contextual, 304, 307

driving system levels, 803-804

equipment health monitoring example, 777-778

extranets

orchestration and NFV, 596

software-based, 597

template-based orchestration and NFV, 595

gas and oil industry, 752

IPS/IDS, 717-718

next-generation IoT platforms, 299

oil and gas industry security, 742-763

asset improvements, 742

challenges, 743-744

equipment health monitoring example. See *equipment health monitoring example*

field operations, 789

human efficiency and productivity, 742

trends, 743

reusable templates, 469

secure oil and gas opportunities, 735

security, 876

SGACLs, 388

smart cities, 691-692, 721-725

autonomous vehicles

Ethernet approaches, 825

interoperability, 826, 829

layered approach, 850-851

operational lifecycle, 851

sensor data sharing systems and technologies, 824

standards, 826-829

systems and technologies, 823

autoquarantining versus manual quarantine, 782

autoscaling, KPI, 483

availability, 37, 86

cloud computing, 109, 112

data protection, 505

high, 269

IISF, 162

MQTT, 542-543

NFV, 220

OpenFog reference architecture pillar, 135

RabbitMQ, 550-551

availability, integrity, confidentiality (AIC), 43

AVC (application visibility and control), 423, 433, 437

application subcategories, 434

detection sources, 433

detectors, 434

industrial communication protocol example, 435

MODBUS application filter example, 436-437

A/V pairs (Attribute Value pairs), 362

AV-Test, 455

AWS (Amazon Web Services), 176

Amazon Cognito, 395

device registration process, 331-333

IAM, 395-397

policy-based authorization, 394-395

Ayla IoT Platform, 176

Azure, 176

B

B2B (business-to-business) services, 806

back-end architectural layer, 86

back-end platforms, 631-634

access control, 637-646

API security, 634-635

containerized services management, 649-653

dashboard, 635-637

NFVO, 646-647

NSO, 646

operationalization, 633-634

options, 631

overcloud/undercloud, 634

requirements, 631

REST APIs, 634-635

VFM, 648

VIM, 648-649

backing up data, 570

bandwidth, fog computing, 115

battery management, police vehicles, 821

BBF (Broadband Forum Member), 65

behavioral analysis, 440-441

contextual information with adaptive network control, pairing, 446

encrypted traffic analytics, 450-454

ETA

cryptographic compliance, 454

threat detection, 451-452

WannaCry, 454

NaaS, 444-446

oil and gas pump station example, 447-450

solutions, 441

visibility protocols, 442-444

Flexible NetFlow protocol, 444

NBAR2, 444

NetFlow protocol, 442-443

NSEL (Network Security Event Logging), 444

Big Data, 522-526

Big Data Architectures and the Data Lake (Serra), 523

biometric authentication, 359-360

bitumen, 740

blockchains, 877-880

adoption of IoT, accelerating, 887

architectures, 886

challenges, 886

characteristics, 880

compliance, 887

components, 883

computational resources, 886

consensus algorithm, 883

distributed ledger applications, 884

EdgeChain, 889-890

human skills gap, 886

ledger, 883

private, 884

process flow, 882

public, 884

reactive data protection mechanisms, 572

scalability, 886

startups total funding, 880

storage, 886

transactions, 886

types, 884

Bluemix platform, 177

bookmarks, clientless SSL VPN application access, 604-605

boot integrity, 274-275

bootstrapping, secure, 328

BRSKI, 329-330

immutable identities, 328-329

Bosch IoT Suite, 176

bring your own certificates (BYOC), 333

bring your own device (BYOD), 21

Broadband Forum Member (BBF), 65

brokers, 350

BRSKI (Bootstrapping Remote Secure Key Infrastructure), 329-330

BSI (British Standards Institute), 686-687

BSquare DataV, 176

BSS (business support systems), 223

bug scrubs, 270

building blocks, 35

access control, 326

IISF, 163-164

next-generation IoT platforms, 295-303

fog levels, 302

heterogeneous, 297

infrastructure, 301

management, 297

MANO, 297-301

multitenancy, 296

operation, 297

UIs, 297

virtualization, 297

YANG model, 304-306

buildings, smart cities, 680

business-to-business (B2B), 806

business value, 5

businesses

benefits, 54

business-focused services, 805

needs challenges, 863

processes, 37, 86

support systems (BSS), 223

BYOC (bring your own certificates), 333

BYOD (bring your own device), 21

C

CA (certificate authority), 451

cabinets

fog nodes, 660

monitoring, 705-709

monitoring with event-based video, 709-712

data pipeline security, 713-714

deployment, 710-712

triggers, 710

on demand access control, 714-718

IPS/IDS, 717-718

self-service portal, 715-717

CAN (controller area network), 824

canned policies (ISE), 340

CAP (consistency, availability, and partition) theorem, 568-569

CAPEX reduction, 219

carrier-neutral facility (CNF), 418

Carriots IoT Platform, 177

Casado, Martin, 186

catalogs, security, 656

CCTV (closed circuit television) video security use case, 309

architecture overview, 313

cabinet monitoring, 314

deployment, 316-319

description, 312

preparatory work, 315-316

sequence of events, 319-320

triggers, 312

center architectural layer, 86

center hierarchy, 36

Center for the Protection of National Infrastructure (CPNI), 842

centralized deployment security example, 418-420

activation sequence, 472-474

dynamic mapping, 478

ESC, monitoring, 476-477

ETSI MANO components, 468

fulfillment and assurance sequences, 474-475, 479-480

KPI SESSION_COUNT metric, 482-483

KPI VNF monitoring methods, 479

NSD catalog, 471

NSR, 472

reusable templates, 469

rules, 483-486

VMs, 469, 481

VM_ALIVE script, 480-481

VNFs, monitoring, 475

VNFD catalog, 470

certificate authority (CAs), 451

Certificate Revocation Lists (CRLs), 259, 356

certificates, 352

digital, 352

IEEE 1609.2, 353

PKI, 353-355

revocation, 356-357

SSL pinning, 357

X.509, 352-353

DTLS, 350

managing, 333

SUDI, 328-329

certifications

applications, 271

security, 16

cgroups, 654

chaining services, 494-495

choices provided by standards, 54

CIA (confidentiality, integrity, and availability), 43, 503

CIGRE (International Council on Large Electrical Systems), 66

CIP (Common Industrial Protocol), 428-429, 432

Cisco

Adaptive Security Appliance virtualized (ASAv), 422-423, 470

AnyConnect client. *See* AnyConnect client

CPwE, 153

ENCS, 489

GridBlocks, 153-154

Identity Services Engine (ISE), 336

IoT Cloud Connect, 176

IoT Ready, 329

IoT security framework, 168-171

Kinetic IoT Platform, 177

Next Generational Firewall virtualized (NGFWv), 422-423

NSO, 646

Overlay Transport (OTV), 259

Secure Development Lifecycle, 644

SIO, 456

UCS E-Series servers, 489

citizen experiences, smart cities, 681

City Management Interface, 696

classes, constrained devices, 345-346

classical models versus machine learning, 893

classification

assets, 27

TrustSec, 380

client application detectors, 434

client-based SSL VPNs, 611-612

clientless comparison, 600

configuration, 612

deployment, 611

manufacturing example, 617

authorization, 621

identity, authentication, posture, 618

remediation, 619-620

working components, 618-621

modules, 612-616

AMP, 616

endpoint compliance, 614

Network Access Manager, 614

NVM, 615-616

roaming protection, 614-615

VPN, 612-613

clientless SSL VPNs, 599-611

application access, 604-609

bookmarks, 604-605

plug-ins, 609

port forwarding, 606

smart tunnels, 607

web-type ACLs, 606

client-based comparison, 600

components, 602

DAP, 609

group policies, 602

oil and gas example, 610-611

portal, 602-603

tunnel groups, 601

clients

802.1X, 363

AnyConnect, 611

configuration, 612

deployment, 611

modules, 612-616

Device Sensor, 341

MQTT, 350

vhost, adding, 642

closed circuit television. *See* CCTV video security use case

cloud-centric architecture, 32, 95-96

cloud computing, 106-112

accessibility, 109

advantages, 109

availability, 109, 112

characteristics, 107

compliance, 110

costs, 109

deployment, 107-108

disadvantages, 110

environmental benefits, 109

extensibility, 109

fog computing comparison, 241

fog fusion, 242

hybrid, 107

interoperability, 110

IoT adoption, accelerating, 111

maintenance, 109

privacy, 110

private, 107

public, 107

QoS, 112

real-time processing, 112

reliability, 109

scalability, 109

security challenges, 110

Cloud Customer Architecture for IoT, 140-142

cloud-native functions, 242

cloud-ready functions, 242

Cloud Security Alliance. *See* CSA document

cloud to cloud, 406-408

CNF (carrier-neutral facility), 418

CoA (Certificate of Authenticity)

RADIUS, 368

request commands, 370-371

Request/Response codes, 369

requests, 368-369

session identification, 369

VLAN assignments, 371-374

SGT, 781

CoAP (Constrained Application Protocol), 349-350

cognitive computing, 898-899

Cognito (Amazon), 395

collaborative security, 899

collecting data, 507

command validation, 782-783

Common Industrial Protocol (CIP), 428-429, 432

common service functions (CSFs), 131

common services entity (CSE), 131

communication, 71

application layers, 74

attacks, 41-42

channel vulnerabilities, 839

connected cars, 807-808

data, 790

fog computing, 114
fog nodes, 662-664
IoT-centric model, 72
last-mile, 71
MAC layers, 73
network layers, 73-74
node hierarchy, 36
OSI, 70
physical layers, 73
police vehicles, 821
protocols, 70
SDN controller
east-west, securing, 254-256
northbound, securing, 263-268
southbound, securing, 256-260
security, 658-659
smart cities, 682
technologies, 740
transport layers, 74
complex devices, 345
complexity
connected car security, 835
fog computing, 118
minimizing, 309
compliance
blockchain, 887
cloud computing, 110
cryptographic, 454
security, 5
smart cities, 682
components
AI, 891
blockchain, 883
EFM, 561
ENFV, 486-487
full IoT stacks, 674
ICN architecture, 101
NaaS, 445
NFV framework, 64
OF, 193
oil and gas industry security, 757
smart cities, 679
SSL VPNs, 602
computational resources, 886
computer vision, 898
computing data, 508
concierge services, 805
ConfD, deployment preparations, 316
confidentiality, 37
Cisco IoT security framework, 169
data, 568
data protection, 505
MQTT, 539-540
RabbitMQ, 549
confidentiality, integrity, and availability (CIA), 43, 503
configuring
AAA, 342-343
AnyConnect client, 612
management and control, 17
RabbitMQ, 643
connected cars
automated deployment, 867-870
automated driving system levels, 803-804
autonomous, 823-824
benefits, 811-812
business-focused services, 805
categories, 801
communications, 807-808
customer-focused services, 805
data, 815-817
data enabling solutions, 814
data value, 813
development, 801-802
digital roadway architecture, 806
embedded era, 802

emergency fleet vehicles example, 852-854
- *architecture overview, 854*
- *automation, 867-870*
- *equipment deployment, 865-866*
- *Federal Sigma VAMA, 863-864*
- *intrusion detection and prevention, 858-860*
- *onboard systems deployment, 864-865*
- *OTA secure updates, 855-857*
- *personalized experiences, 862-863*
- *segmentation and zoning, 857-858*
- *Wi-Fi hotspot security, 861-862*

equipment deployment, 865-866

estimated car sales 2015–2021, 798

Ethernet approaches, 825

future applications and services, 815

high-tech entrants, 804

industry trends, 798

infotainment era, 802

interoperability, 826

interoperable infrastructure requirements, 829

intrusion detection and prevention, 858-860

IoT value, 810-812

leadership, 799

low prices of technology, 804

mobility concepts, 805

networks, 824-825

onboard systems deployment, 864-865

operational challenges, 863

operational lifecycle, 851

orchestration platform principles, 848

orchestration requirements, 818

OTA secure updates, 855-857

overview, 800

personalized experiences through identity management, 862-863

police vehicles, 819-821
- *ANPR, 820*
- *audible and visual warning systems, 820*
- *battery management, 821*
- *integrated approach, 821*
- *mobile data terminals, 820*
- *onboard systems and technologies, 819*
- *onboard telematics, 821*
- *operational challenges, 821*
- *orchestrated services, enabling with consolidated orchestrated hardware, 822*
- *radios, 820*
- *speed detection, 820*
- *speed recognition devices, 820*
- *vehicle tracking, 820*
- *video camera and audio systems, 820*
- *wearables, 821*
- *Wi-Fi hotspots, 821*

regulatory and policy constraints, 805

revenue and operational opportunities, 816

security, 830
- *attack surface, 831*
- *challenges, 835*
- *connectivity challenges, 840*
- *considerations, 839*
- *consolidation, 849*
- *data-centric and application-centric fusion, 849*
- *design implementations, 847*
- *driver concerns, 837*
- *encryption, 837*
- *goals, 847-848*
- *industry alliances, 847*
- *layered approach, 850-851*
- *reasons for, 830*
- *safety-criticality, 836*
- *threats, 831-834*
- *U.K. supply chain guidelines, 842-845*
- *upgrades/patches, 840*

U.S. supply chain guidelines, 845-846
vulnerabilities, 836-840
segmentation, 857-858
smart city emergency fleet vehicles integration, 719-721
standards, 826-829
Europe, 827
Japan, 827
SAE International, 827, 829
U.K., 827
U.S., 826
technology transition, 802
trends driving changes, 804
urban customers, 805
V2X era, 802
vehicle maintenance data, 813
vendor ecosystem, 809
Wi-Fi hotspot security, 861-862
zoning, 857-858
connectivity
connected car security, 835
connected cars, 840
IoT, 4
new endpoints, 639
on demand access, 714-718
IPS/IDS, 717-718
self-service portal, 715-717
platforms, 173
connectors, 20, 316
consensus algorithm, 883
consistency, availability, and partition (CAP), 568-569
consistency, next-generation IoT platforms, 291
consolidation
connected car security, 849
smart cities, 698
consortia, standardization efforts, 56
constrainable relationship, 414
Constrained Application Protocol (CoAP), 349-350
constrained devices, 345
classes, 345-346
identifying, 348-351
CoAP, 349-350
MQTT, 350-351
limitations, 358
restrictions, 345
Constrained Object Signing and Encryption (COSE), 409
consumer/provider matrix, 384-386
consumers
ICN, 102
software extensions, 173
spaces, SDN-based IPsec IoT, 592
consumption, data, 526
containerized services, back-end platform management, 649-653
context processing, CN, 102
contextual automation, 304, 307
contextual awareness, 899
contextual relationships, 414
continuous monitoring, 17
control layer, SDN, 190
control planes
data protection, 566-567
SDN, 262
security, 659
controller area networks (CANs), 824
controllers
ODL, 206
power, 702-704
SDN
east-west communications, securing, 254-256
northbound communications, securing, 263-268

securing, 252-253

southbound communications, securing, 256-260

TrustSec, 368-378

controlling

Cisco IoT security framework, 170

configuration, 17

oil and gas industry security, 755

OpenFog Consortium architecture, 136

power, 702

security, 16

converged multifaceted platforms, 246-248

Converged Plantwide Ethernet (CPwE), 153

co-operative awareness basic service standards, 827

core networks hierarchy, 36

Core Root of Trust Management (CRTM), 663

COSE (Constrained Object Signing and Encryption), 409

costs, 16

cloud computing, 109

fog computing, 117-118

CPNI (Center for the Protection of National Infrastructure), 842

CPS PWG (Cyber Physical Systems Public Working Group), 77

CPU, reserving, 278

CPwE (Converged Plantwide Ethernet), 153

crashes, 275

Create, Read, Update, and Delete (CRUD), 628-630

criticality, connected car security, 836

CRLs (Certificate Revocation Lists), 259, 356

cross-certification, 355

cross-fog applications, 136

cross-site scripting (XSS), 635

cross-vertical compound IoT applications, 3

cross-vertical replicability, fog computing, 117

CRSF (cross-site forgery attacks), 265, 636

CRTM (Core Root of Trust Management), 663

CRUD (Create, Read, Update, and Delete), 628-630

cryptography

compliance, 454

D-H (Diffie-Hellman), 580

public key, 352

CSA (Cloud Security Alliance) document, 110, 165-168

IoT-specific security controls, 167

recommended security controls, 165-166

security standards, 77

smart city recommendations, 695

CSDL (Cisco Secure Development Lifecycle), 644-646

CSE (common services entity), 131

CSFs (common service functions), 131

CSRF (cross-site request forgery), 636

CTA (Cognitive Threat Analytics), 453

custom application detectors, 434

customer-focused services, 805

customer profiling, 805

Cyber Physical Systems Public Working Group (CPS PWG), 77

cyberattacks, 454

cybersecurity

connected car standards, 827

connected cars, 830

attack surface, 831

automated deployment, 867-870

challenges, 835

connectivity challenges, 840

considerations, 839

consolidation, 849

data-centric and application-centric fusion, 849

design implementations, 847

driver concerns, 837

emergency fleet vehicles example. See *emergency fleet vehicles example*

encryption, 837

equipment deployment, 865-866

goals, 847-848

industry alliances, 847

intrusion detection and prevention, 858-860

layered approach, 850-851

onboard system deployment, 864-865

operational challenges, 863

operational lifecycle, 851

orchestration platform principles, 848

OTA secure updates, 855-857

personalized experiences through identity management, 862-863

reasons for, 830

safety-criticality, 836

segmentation and zoning, 857-858

threats, 831-834

U.K. supply chain guidelines, 842-845

upgrades/patches, 840

U.S. supply chain guidelines, 845-846

vulnerabilities, 836-840

Wi-Fi hotspots, 861-862

NIST best practices, 659

smart cities, 682, 693-696

Cloud Security Alliance recommendations, 695

threats, 694

standard, 829

D

dACLs (downloadable access control lists), 374

daemons, Docker, 654

DAP (Dynamic Access Policies), 609

dashboard back-end platform, 635-637

dashboards, 627

data

analysis and exposure, 526

anomaly detection. *See* behavioral analysis

app centric, 697

at rest, 518, 521

Big Data, 526

breach costs, 418

categories, 509-511

centricity, 104

collecting, 507

computing, 508

confidentiality, 568

connected cars

analysis technologies, 817

enabling solutions, 814

future services and applications, 815

monetization, 815

consumption, 526

distribution, 527

driver development, 515-516

durability, 529

end-to-end considerations, 18

endpoint collected, 520

flows, oil and gas industry, 790

four Vs, 813

handling, 115, 821

identification, 25-26

information, compared, 524

ingestion, 524

IoT, 4

lakes, 522-524

leveraging, 509

lifecycles, 507-509

categories, 511

collection, 507

computing, 508

data categories, *509*
leveraging, *509*
moving, *508*
management and analytics, 5
mobile terminals, 820
modeling
dynamic mapping, *478*
languages, *68*
standards, *67*, *70*
moving, 508, 527-531
normalization process, 513-517
OpenFog Consortium architecture, 136
permissions, 399
persistency, 529
pipeline
architectural layer, *86*
deployment preparations, *316*
IoT platforms, *288*
security, *713-714*, *786-788*
planes
MQTT. See *MQTT*
protection, *531*
RabbitMQ. See *RabbitMQ*
SDN, *262-263*
security, *659*
preparation, 526
protection, 169, 531
access control, *504*
accounting, *505*
authentication, *504*
authorization, *504*
availability, *505*
backups, *570*
CAP theorem, *568-569*
CIA, *503*
confidentiality, *505*
control plane, *566-567*
data virtualization, *564*
digital twins, *569*
EFM, *560-564*
functions, *504*
integrity, *505*
management plane, *565-566*
MQTT. See *MQTT*
nonrepudiation, *506*
physical access, *505*
proactive mechanisms, *567-571*
RabbitMQ. See *RabbitMQ*
reactive mechanisms, *571-573*
pub/sub systems, 527-530
sanitization, 17
segmentation of responsibilities, 500-502
semistructured, 510
sensor, 824
sharing
multitenancy, *641-644*
security, *9*
smart cities management, 682
stores, 658
structured, 509
topics, 641
transport, 104
unstructured, 511
value, 512, 813
variety, 512, 813
vehicle maintenance, 813
velocity, 813
veracity, 813
volume, 813
warehouses, 521-522
Data Center Interconnect (DCI), 259
data-centric architecture, 104-105
Data Distribution Service (DDS), 105
Data Plane Development Kit (DPDK), 200
databases, IPsec, 589
Datagram Transport Layer Security (DTLS), 74, 349, 612

DataV, 176

DCI (Data Center Interconnect) protocols, 259

DDS (Data Distribution Service), 105

dead-peer detection (DPD), 584

decentralized decisions, Industry 4.0, 148

decentralized environmental notification standards, 827

decision pipeline, end-to-end considerations, 18

decomposing IoT platform, 27

decryption, dynamic, 592-594

Dedicated Short-Range Communications (DSRC), 353, 800, 827

deep learning (DL), 894-895

deep packet inspection (DPI), 430-432

Def Stan 05-138, 829

delivering next-generation IoT platforms, 293

deployment

AnyConnect client, 611

centralized, 418-420

cloud computing, 107-108

connected cars

equipment, 865-866

onboard systems, 864-865

distributed, 420-421

equipment health monitoring example, 766-771, 777-778

event-based video and security use case, 316-319

event-based videos, 710-712

Federal Sigma VAMA architecture, 864

function packs, 317

hybrids, 422

next-generation IoT platforms, 292

OpenStack, 632

OTT, 89

preparations, 315-316

security enforcement, 90

services, 639-641

services-based, 33

smart cities, automating, 723-725

VFs, 317

design

connected car security, 847

IoT platforms, 87

detection, anomaly traffic, 780-781

detectors (application), 433-434

development

connected cars, 801-802

drivers, 515-516

end-to-end considerations, 19

IoT platforms, 178

secure applications, 271

security test and evaluation, 16

Device Level Ring (DLR), 429

Device Sensor, 340-345

AAA configuration example, 342-343

differentiated authorization privileges, 345

internal/external clients, 341

port security, 341

probe configuration, 344

success, 344

devices

attestation and trust, 315

building blocks for access control, 326

complex, 345

constrained, 345

classes, 345-346

identifying, 348-351

limitations, 358

restrictions, 345

discovery, 102

edge, 302

energy limitations, 346-347

ETA, 453

fog, 302

identifying, 26, 336-337

immutable identities, 328-329

IoT, 123

ITU-T Y.2060 reference model, 126

managed devices per IT person in financial and retail customers, 411-412

naming conventions, 327-328

onboarding, 102

power for communication, 347-348

predicted connection rate, 325

provisioning, 326, 330-331

AWS IoT Example, 331-333

Cisco Identity Services Engine example, 334-336

registering, 330-331

AWS IoT example, 331-333

Cisco Identity Services Engine example, 334-336

security, 9

sharing, 315

trust, establishing, 328

trust stores, 355

D-H (Diffie-Hellman) groups, 580

DHCP (Dynamic Host Control Protocol), 390

differentiating IoT platform, 174

digital certificates, 352

IEEE 1609.2, 353

PKI, 353-355

revocation, 356-357

SSL pinning, 357

X.509, 352-353

digital IoT twins, 295

digital marketing, 805

digital roadway architecture, 806

digital signatures

applications, 271

encrypting, compared, 540

digital technology, 735

digital twins, 569

digitization, oil and gas industry, 737-738

oil and gas industry downstream environment, 752

oil and gas industry midstream environment

benefits, 747-748

challenges, 748-749

pipeline management, 747

oil and gas industry upstream environment

automation, 742

challenges, 743-744

trends, 743

pipeline management applications, 744

direct exchanges, 544

disabling services, 270

disposal, hardware and software, 17

disposition phase, SDLC, 14, 17

distributed control systems, 750

distributed deployment, NFVIS example, 486

ENFV components, 486-487

hardware requirements, 488-490

NFVIS benefits, 488

orchestration, 490

service chaining, 494-495

vBranch Function Pack, 490-493

VMs supported, 490

distributed ledger technology. *See* blockchains

distributing data, 527

DLs (data lakes), 522-524

DL (deep learning), 894-895

DLR (Device Level Ring), 429

DLUX (OpenDaylight User Experience), 207

DNS (Domain Name System), 462

DNS-based security, 462

recursive, 462

Umbrella, 463

AMP Threat Grid, 465
healthcare industry protection, 465-466
intelligent proxy services, 464-465
response categories, 463
Docker daemon, 654
Docker security, 653-655
downloadable access control lists (dACLs), 374
downstream environment (oil and gas industry), 734, 749
challenges, 753-754
digitization, 752
distributed control systems, 750
IoT benefits, 752
new business needs, 752
overview, 749
refining and processing architecture, 750
technologies, 750-751
DPD (dead-peer detection), 584
DPDK (Data Plane Development Kit), 200
DPI (deep packet inspection), 430-432
DREAD model, 28
driver safety data, connected cars, 815
drivers
development, 515-516
NEDs, 300
DRTM (Dynamic Root of Trust Management), 663
DSLinks, 563
DSRC (Dedicated Short-Range Communications), 353, 800, 827
DTLS (Datagram Transport Layer Security), 74, 349, 612
durability, data, 529
DW (data warehouses), 521-523
dynamic access policies (DAP), 609
dynamic authorization
ACLs, 374-376
forms, 368
ISE, 368
privileges, 367
RADIUS CoA, 368
request commands, 370-371
Request/Response codes, 369
requests, 368-369
session identification, 369
VLAN assignments, 371-374
SGTs, 376-377
dynamic decryption, 592-594
dynamic mapping, 478
dynamic NAT, 424
Dynamic Root of Trust Management (DRTM), 663
dynamic segmentation, 378-380

E

EAPOL (Extensible Authentication Protocol over LAN), 363
east–west
SDN controller communications, securing, 254-256
SGACLs, 387
ECDH (Elliptic Curve Diffie Hellman), 353
ECDSA (Elliptic Curve Digital Signature Algorithm), 329, 353
ecosystems
CSA document, 165-168
IoT-specific security controls, 167
recommended security controls, 165-166
groupins (smart cities), 683
Edge and Fog Processing Module (EFM), 560-564
edge computing, 112
embedded systems, 237
fog computing, compared, 113, 240
legacy systems, 237
MEC, 237-238

edge devices, 302

edge networks, 36

edge nodes, 35

edge tier

- Cloud Customer Architecture for IoT, 141
- IIRA, 146

EdgeChain, 889-890

EdgeX Foundry platform, 177

EFM (Edge and Fog Processing Module), 560-564

- components, 561
- computation, 562
- data collection, 562
- DSLinks, 563
- permissions, 563
- quarantine, 563

Electronic Security Perimeters (ESP), 23

elliptic curve cryptographic algorithms, 353

Elliptic Curve Diffie Hellman (ECDH), 353

Elliptic Curve Digital Signature Algorithm (ECDSA), 329

embedded era (connected cars), 802

embedded probes, 338

embedded systems (ES), 101, 237

emergency fleet vehicles example, 852-854

- architecture overview, 854
- automation, 867-870
- equipment deployment, 865-866
- Federal Sigma VAMA, 863-864
- intrusion detection and prevention, 858-860
- onboard systems deployment, 864-865
- OTA secure updates, 855-857
- personalized experiences, 862-863
- segmentation and zoning, 857-858
- smart city integration, 719-721
- Wi-Fi hotspot security, 861-862

emergency police vehicles, 821

- ANPR, 820
- audible and visual warning systems, 820
- battery management, 821
- integrated approach, 821
- mobile data terminals, 820
- onboard systems and technologies, 819-821
- onboard telematics, 821
- operational challenges, 821
- orchestrated services, enabling with consolidated orchestrated hardware, 822
- radios, 820
- speed detection, 820
- speed recognition devices, 820
- vehicle tracking, 820
- video camera and audio systems, 820
- wearables, 821
- Wi-Fi hotspots, 821

Encapsulating Security Payload (ESP), 578

Encrypted Traffic Analytics (ETA), 450-454

encryption

- algorithms, 580
- connected cars, 837
- digitally signing, compared, 540
- southbound SDN controller communication, 258
- transport, 532

ENCS (Enterprise Network Compute System), 489

ENCS 5400, 494-495

end-to-end

- development framework, 19
- human interaction, 19
- manageability and orchestration, 17-18

openness, 18
performance, 20
scalability, 20
security, 20, 163-164

endpoints
any endpoint, anywhere concept, 25
architectural layer, 85
compliance module, 614
data collection storage, 520
hierarchy, 35
IDs, 637
IoT, 3
new, connecting, 639
security, 9
transport encryption, 532

energy
efficiency, 220
limitations, 346-348

enforcement (security)
TrustSec, 384
types of deployments, 90

ENFV (Enterprise Network Virtualization), 486-487

enterprise-centric architectures, 32, 96-97, 154-156

Enterprise Resource Planning (ERP), 37

enterprise risks, 12

enterprise software extensions, 173

enterprise tier, 141

entity-based reference model, 123

E&P (exploration and production), 733

equipment health monitoring example, 763-765
access control, 781
access privileges, 778-780
anomaly traffic detection, 780-781
architecture, 772
automated deployment, 777-778
command validation, 782-783
data pipeline security, 786-788
data pipelines, 771
deployment, 766-771, 865-866
limitations, 765
operational lifecycle, 772
preconfiguration checklist, 773-775
quarantines, 782
requirements, 767
service assurance, 784-786

ERP (Enterprise Resource Planning), 37

ES (embedded systems), 101, 237

ESC
KPI rules, 483-485
NSO activation sequence request, 472-474
NSO fulfillment and assurance sequences, 474-475
VNFs, monitoring, 475
actions, 477
dynamic mapping, 478
metrics, 476
prerequisites, 475

E-Series servers, 489

ESP (Electronic Security Perimeters), 23

ESP (Encapsulating Security Payload), 578

ETA (Encrypted Traffic Analytics), 451
cryptographic compliance, 454
threat detection, 451-452
WannaCry, 454

Ethernet
attacks, 41
connected cars, 825
inline tagging format, 383

EtherNet/IP, 429

ETL (Extract-Transform-Load) model, 521

ETSI (European Telecommunications Standards Institute), 18, 59, 187
architectural standards, 59

MANO, 18

centralized security example, 468

NFV centralized components, 419

NFV

architecture, 229

standards, 66

NFV MANO, 225

benefits, 232

challenges, 229

decoupling service intentions from instantiation process, 230-231

implementation, 231-232

LSO, 226-229

OpenFog convergence, 243-245

OSS/BSS interoperability, 232

security standards, 76

TS 102 637, 827

TS 102 637-1, 827

TS 102 637-2, 827

TS 102 637-3, 827

TS 102 637-4, 827

EUIs (Extended Unique Identifiers), 327

European connected car standards, 827

European Lighthouse Integrated Project, 120

European Telecommunications Standards Institute. *See* ETSI

event-based videos

security use case, 309

architecture overview, 313

cabinet monitoring, 314

deployment, 316-319

description, 312

preparatory work, 315-316

sequence of events, 319-320

triggers, 312

smart cities, 709-714

data pipeline security, 713-714

deployment, 710-712

triggers, 710

evolution of IoT, 236

evolving technology IoT landscape, 670-671

exchanges

IKEv2, 584-586

RabbitMQ, 544

explicit trust, 355

exploration and production (E&P), 733

exposure, data, 526

Extended Unique Identifiers (EUIs), 327

extensibility

cloud computing, 109

OPC UA, 151

Extensible Authentication Protocol over LAN (EAPOL), 363

Extensible Messaging and Presence Protocol (XMPP), 74, 258

external clients, 341

Extract-Transform-Load (ETL) model, 521

extranets, 594

automating with orchestration and NFV, 596

automating with template-based orchestration and NFV, 595

software-based automation, 597

traditional approach, 594

F

Face ID, 359

fanout exchanges, 544

FCAPS (fault management, configuration management, accounting management, performance management, and security management), 126

FD.io (Fast Data–input/output), 198

Federal Sigma VAMA, deployment
- equipment, 865-866
- onboard systems, 864-865

FFV
- ETSI architectural framework, 229
- MANO, 223-232
  - *benefits, 232*
  - *challenges, 229*
  - *decoupling service intentions from instantiation process, 230-231*
  - *implementation, 231-232*
  - *LSO, 226-229*
  - *OSS/BSS interoperability, 232*

FIB (forwarding information base), 199

field operations automation, oil and gas industry, 789

file policies, 461

Filet-o-Firewall vulnerabilities, 42

filtering
- CIP, 432
- filters, applying, 432
- packets
  - *firewalls, 426-427*
  - *sanity checking, 431*
  - *user definable, 432*

financial services, connected cars, 806

fingerprint IDs, 359

Firefox percentage of web pages, 450

firepower-based application detectors, 434

Firepower Management Center (FMC), 459

Firepower Threat Defense (FTD), 459-461

Firepower Threat Defense virtualized (FTDv), 422

firewalls
- APTs, 440-441
- ASAv, 423
- AVC, 433-437
- behavioral analysis, 440-441
  - *contextual information with adaptive network control, pairing, 446*
  - *Flexible NetFlow protocol, 444*
  - *NaaS, 444-446*
  - *NetFlow protocol, 442-443*
  - *oil and gas pump station example, 447-450*
  - *visibility protocols, 442-444*
- defined, 422
- DPI, 430-432
- encrypted traffic analytics, 450-454
- ETA
  - *cryptographic compliance, 454*
  - *threat detection, 451-452*
  - *WannaCry, 454*
- Filet-o-Firewall, 42
- FTD, 459-461
- IDS/IPS, 437
  - *pattern matching, 438-439*
  - *protocol analysis, 439*
  - *weaknesses, 439-440*
- industrial protocols, 428
  - *CIP, 428-429*
  - *lack of security, 429*
  - *potential solutions, 430*
- IPS, 438
- NAT, 424
- NGFWv, 423
- overlapping, 425
- packet filtering, 426-427
- PAT, 425

Fitbit Aria IoT IAM example, 406
- cloud to cloud, 406
- device to device, 409
- native applications to cloud, 408
- self-registration, 408

fleet management, connected cars, 806

flexibility
authentication, 403
NFV, 220
Flexible NetFlow (FNF), 444, 447
FlexRay networks, 824
flows
data, oil and gas industry, 790
Fitbit Aria example, 408
MUD, 393-394
flows per second (FPS), 443
FMC (Firepower Management Center), 459
FNF (Flexible NetFlow) protocol, 444
fog computing, 112
advantages, 116-118
cloud computing comparison, 241
cloud fusion, 242
communications, 114
complexity, 118
containerized services, 650
costs, 117-118
cross-vertical replicability, 117
data handling, 115
disadvantages, 117
edge computing, compared, 113, 240
governance, 117
hierarchy, 36
heterogeneity, 117
levels, 302
mobility, 116
nodes, 240
data analysis, 526
data at rest, 521
operating systems, 664
RabbitMQ orchestrated security example, 552-558
security, 660-666
southbound APIs, 667
OpenFog convergence with NFV MANO, 243-245
proximity, 116-117
reliability, 117
requirements, 115
SDX/NFV role, 243
security, 117, 666
smart traffic example, 238-241
speed, 116
Forbes IoT platform key areas, 288
forwarding
graphs, NFV, 222-224
information base (FIB), 199
P4, 202
ports, 606
four Vs of data, 813
FPS (flows per second), 443
FQDN (fully qualified domain name), 602
fracking, 739
frameworks
accounting, 399
Cisco IoT, 168-171
IIAF, 144
IISF, 160-165
assurance, 162
building blocks, 163-164
implementation, 164
recommendations, 162-163
system characteristics, 162
trustworthiness, 161
IoTivity, 142-144
NFV, 63
components, 64
standards, 65-67
Nirvana Stack, 212
OWASP, 168
P4, 201

front-end UIs security, 630, 657

FTD (Firepower Threat Defense), 459-461

FTDv (Firepower Threat Defense virtualized), 422

fulfillment sequences, 474-475, 479-481

full IoT stack architectures, 120

addressing, 670

AIOTI, 138-140

Cloud Customer Architecture, 140-142

components, 674

IEEE P2413, 132-133

IoT-A RA, 120-125

IoTivity framework, 142-144

IoTWF, 126-129

ITU-T Y.2060, 125-126

next-generation IoT platforms, 293

oneM2M, 129-132

OpenFog Consortium, 133-138

fully qualified domain name (FQDN), 602

Function Packs

deploying, 316-317

next-generation platforms, 675

smart cities, 722

YANG model, 306

functional architectures

IoT-A RA, 124

oneM2M, 131

functional requirements, 15, 827

functions

cloud-native, 242

cloud-ready, 242

data protection, 504

fog-ready, 242

OF, 194

OVS, 197

VFs, 298

Future Internet, 3

G

Gartner-defined centric views, 97

Gartner Hype Cycle for Emerging Technologies 2017, 879

Gartner IoT platform recommendations, 289-290

gateways

architecture, 32, 94-95

attacks, 40-41

hierarchy, 35

IoT-A RA, 123

GDPR (General Data Protection Regulation), 499, 571

General Electric Predix, 177

Google Cloud Platform, 176

governance

fog computing, 117

security, 5

smart cities, 682

graph nodes, 199

GridBlocks, 153-154

group policies, SSL VPNs, 602

guidelines

accounting framework, 399

implementation, 53

oil and gas industry, 757

H

handling data

fog computing, 115

police vehicles, 821

hardware

connected cars, 827

disposal, 17

gateway, 40

specific platforms, 173

Hash Based Message Authentication (HMAC), 264

hashing algorithms, 580

header exchanges, 546

healthcare

industry protection with Umbrella, 465-466

smart cities, 681

heterogeneity, 86

fog computing, 117

next-generation IoT platforms, 297

Hewlett-Packard Enterprise Universal of Things Platform, 176

hierarchical data flow model, 158

hierarchy

applications, 36

architecture layers, 85

business processes and services, 86

center/back-end, 86

data pipeline and processing, 86

infrastructure and transport, 85

integration, 86

security, 86

things and endpoints, 85

business processes, 37

center, 36

communication nodes, 36

core networks, 36

edge networks, 36

edge nodes, 35

endpoints, 35

fog networks, 36

gateways, 35

microservices, 36

services, 37

things, 35

high availability

NFV, 220

SDN orchestration, 269

high-level architecture, smart cities, 701

high-level groups, identification, 25

high reliability, next-generation IoT platforms, 293

HMAC (Hash Based Message Authentication), 264

HMI (Human Machine Interface), remote access, 617

authorization, 621

identity, authentication, posture, 618

remediation, 619-620

working components, 618-621

horizontal approaches, smart cities, 685

HTTP (Hypertext Transfer Protocol), 74, 264

HTTPS (HTTP over TLS), 598

HTTPS (Secure HTTP), 74

hub-centric architecture, 32, 94

human efficiency and productivity, oil and gas industry automation, 742

human interaction, end-to-end considerations, 19

human layer, 44

Human Machine Interface. *See* HMI

hybrid clouds, 107

hybrid deployments, 422

hybrid mode, 190

hybrid subsymbolic/symbolic AI, 892

Hypertext Transfer Protocol (HTTP), 74, 264

I

I am the Cavalry, 77

IA (information assurance), 37

IaaS (infrastructure-as-a service), 108, 173

IACS (Industrial Automation and Control System), 21

IAM (identity and access management)

AWS, 394-397

existing, 325

IoT

Fitbit Aria example, 406-409

OAuth 2.0, 404-405

OpenID Connect 1.0, 405

requirements, 403-404

scaling, 402

self-registration, 408

IBM

Bluemix, 177

Watson, 176

ICN (information-centric network), 100-104

challenges, 103

components, 101

data transport, 104

existing technologies, 103

features, 101

middleware, 102

migration, 104

scalability, 103

security, 103

ICS (Industrial Control Systems), 38

Purdue Model of Control reference model, 160

hierarchical data flow model, 158

open process automation, 159

segmented architecture based on, 157

IDs (identities), 637-639

device registration, 330-331

AWS IoT example, 331-333

Cisco Identity Services Engine example, 334-336

immutable, 328-329

LDAP management, 639

naming conventions, 327-328

personalized connected car experiences, 862-863

trusted devices, establishing, 328

identifying

assets, 27

constrained devices, 348-351

CoAP, 349-350

MQTT, 350-351

data elements, 25-26

device types, 26

devices, 336-337

encrypted network traffic threats, 451-453

equipment health monitoring example access privileges, 778-780

high-level groups, 25

risk, 25

classification, 27

identification, 25-26

risk scores, 28

threat modeling, 27

sessions, 369

subgroups, 26

threats, 27, 878

identities. *See* IDs

identity and access management. *See* IAM

Identity Relationship Management (IRM), 326, 413-414

Identity Services Engine. *See* ISE

IDMZ (Industrial DMZ), 158, 759

IDS (intrusion detection system), 437

connected cars, 858-860

pattern matching, 438-439

protocol analysis, 439

smart city services on demand connectivity, 717-718

weaknesses, 439-440

IEC (International Electrotechnical Commission)

2020 Platform Whitepaper, 155

62351 standard, 78

62443 standard, 78, 500-502, 756

IoT platform definition, 88

IEEE (Institute of Electrical and Electronics Engineers), 59
- 802.1X authentication, 363-365
- 802.1X Flexible Authentication, 366-367
- 802.11-2012 Standard for Information Technology, 826
- 1455-1999, 826
- 1609.1-2006, 826
- 1609.2-2016, 826
- 1609.2 certificates, 353
- 1609.3-2016, 826
- 1609.4-2016, 827
- 1609.12-2016, 827
- architectural standards, 59
- P2413 architecture, 132-133
- SDN standards, 66
- security standards, 76
- smart city recommendations, 683
- smart city standards, 685

IETF (Internet Engineering Task Force), 60
- architectural standards, 60
- RFC 6241, 258
- SDN/NFV standards, 66

IIAF (Industrial Internet Architecture Framework), 144

IIC (Industrial Internet Consortium), 61, 144
- industrial/market standards, 61
- security standards, 78

IIoT (Industrial Internet of Things), 3

IIRA (Industrial Internet reference architecture), 144-146

IISF (Industrial Internet Security Framework), 160-165
- assurance, 162
- building blocks, 163-164
- implementation, 164
- recommendations, 162-163
- system characteristics, 162
- trustworthiness, 161

IKE (Internet Key Exchange), 578, 589

IKE_AUTH exchange, 586

IKEv1
- IKEv2 comparison, 586
- phase 1, 579-582, 586-587
  - *aggressive mode, 582*
  - *authentication method, 579*
  - *D-H (Diffie-Hellman) groups, 580*
  - *encryption algorithms, 580*
  - *hashing algorithms, 580*
  - *main mode, 580-581*
- phase 2, 582-584, 588
  - *PFS, 584*
  - *quick mode, 582-583*

IKEv2 (Internet Key Exchange Protocol Version 2), 584-586
- exchange process, 584-586
- IKEv1 comparison, 586
- phase 1 attributes, 586-587
- phase 2 attributes, 588

images
- computer vision, 898
- Docker, 654

immutable identities, 328-329

immutable relationships, 413

implementation
- end to end security, 164
- ETSI FNV MANO, 231-232
- guidelines, 53
- Industry 4.0, 148
- ODL, 208
- P4, 203
- policies, 53
- procedures, 54
- reference, 87
- regulations, 53
- requirements, 86

SDLC, 14-16

standards, 53

inband SGT propagation, 381

inbound packet filtering, 426

incident handling standard, connected cars, 829

incident management standard, connected cars, 828

incompatibility, 49

independent network applications, 207

Industrial Automation and Control System (IACS), 21

industrial communication protocols AVC example, 435

Industrial Control Systems. *See* ICS

Industrial DMZ (IDMZ), 158

industrial environments

IIRA, 144-146

IISF, 160-165

assurance, 162

building blocks, 163-164

implementation, 164

recommendations, 162-163

system characteristics, 162

trustworthiness, 161

Industry 4.0, 148-149

NFV-based, 154-156

OPC-UA, 150-152

Purdue Model of Control Hierarchy framework, 5, 160

hierarchical data flow model, 158

open process automation, 159

segmented architecture based on, 157

SDN-based, 154-156, 592

industrial-focused standards, 61-63

Industrial Internet Architecture Framework (IIAF), 144

Industrial Internet Consortium. *See* IIC

Industrial Internet Reference Architecture (IIRA), 144-146

Industrial Internet Security Framework. *See* IISF

Industrial Internet of Things (IIoT), 3

industrial protocols

CIP, 428-429

lack of security, 429

potential solutions, 430

Industry 4.0, 148-149

industry compliance standards, 23

industry convergence and multifaceted platforms, 246-248

Industry Specification Group (ISG), 187

information

assurance (IA), 37

data, compared, 524

modeling, 151

preservation, 17

security, 828

technology security awareness and training standard, 829

technology standard, 826

transparency, 148

information-centric network. *See* ICN

infotainment era (connected cars), 802, 805

infrastructure

architectural layer, 85

connected car interoperable, 829

next-generation IoT platforms, 301

operational efficiency (smart cities), 681

SDN, 189

control plane, 262

data, 262-263

management, 261

operations, 261

security, 260-263

infrastructure-as-a service (IaaS), 108, 173

ingestion, data, 524

initiation phase (SDLC), 14-15

inline tagging, 383

innovation, NFV, 221

input nodes, 199

insecure devices, 9

inspection, 16

Institute of Electrical and Electronics Engineers. *See* IEEE

integration

architectural layer, 86

Cloud platform, 177

system, 16

integrity, 37

boot, 274-275

data protection, 505

MQTT, 540-542

RabbitMQ, 549

Intel IoT Platform, 177

intelligent proxy services, 464-465

Intelligent Transportation Systems (ITS), 826-827

intended outcomes, next-generation IoT platforms, 303-308

contextual automation, 307

model-driven, 304-306

service-centric, 304-306

service chaining, 306-307

interfaces. *See also* UIs

HMI remote access, 617

authorization, 621

identity, authentication, posture, 618

remediation, 619-620

working components, 618-621

OpenFlow, 257

SDN-based IPsec flow protection, 590-591

smart cities, 696

internal application detectors, 434

International Council on Large Electrical Systems (CIGRE), 66

International Telecommunications Union (ITU), 2

Internet Engineering Task Force. *See* IETF

Internet Key Exchange (IKE), 578, 589

Internet Key Exchange Protocol Version 2. *See* IKEv2

Internet of People (IoP), 98

Internet Protocol (IP), 73, 169

Internet Reliable Transaction Protocol (IRTP), 60

Internet Research Task Force. *See* IRTF

Internet Security Association and Key Management Protocol (ISAKMP), 578

Internet Security Research Group (ISRG), 451

Internet Society (ISOC), 66

Internet of Things. *See* IoT

Internet of Things Architecture Reference Architecture (IoT-A RA), 120-125

interoperability, 49, 86

cloud computing, 110

connected car requirements, 829

connected cars, 826

ETSI FNV MANO, 232

Industry 4.0, 148

IoT platforms, 178

next-generation IoT platforms, 299

next-generation platforms, 672

standards, 50, 54-55

Inter-Vertical Interface, 696

Intra-Application Connectivity Interface, 696

intrusion detection system. *See* IDS

intrusion prevention system. *See* IPS

I/O, single root virtualization, 283-285

IoP (Internet of People), 98

IoT (Internet of Things)

building blocks, 35

business value, 5

Cloud Connect, 176
communication, 72
connectivity, 4
cross-vertical compound applications, 3
custom, 7
data, 4
devices, 123
endpoints, 3
entities, 139
evolution, 236
Global Council, 78
IAM
Fitbit Aria example, 406-409
OAuth 2.0, 404-405
OpenID Connect 1.0, 405
performance, 403
policy-based authorization, 403
privacy, 403
requirements, 403-404
scalability, 403
scaling, 402
security best practices, 404
IAP, 77
implementation, 86
interest over time, 2
ITU definition, 2
next-generation. *See* next-generation IoT
open standard/open architecture systems, 7
people and processes, 3-4
platforms
architecting, 32-33
building out solutions, 175
data pipeline, 288
decomposing, 27
design, 87
development, 178
differentiating, 174
improvements, 179-182
interoperability, 178
key areas, 288
market, 172
maturity, 174
next-generation. See *next-generation IoT*
orchestration, 288
recommendations, 289-290
security, 178-179
top IoT platforms for 2018, 176-177
Ready, 329
SaaS, 7
scalability, 5
security, 8-9
Security Foundation, 76
servers, 102
staff allocation, 6
Suite platform, 176
things, 3
threats, 8
transformation into PaaS, 7
IoT-A RA (Internet of Things Architecture Reference Architecture), 120-125
entity-based reference model, 123
functional architecture, 124
reference model, 121
IoT layer, AIOTI architecture, 138
IoTivity, 60, 142-144
IoTWF (IoT World Forum) reference model, 126-129
IP (Internet Protocol), 73, 169
iPhone Face ID system, 360
IPS (intrusion prevention system), 438
connected cars, 858-860
pattern matching, 438-439
protocol analysis, 439
smart city services on demand connectivity, 717-718
weaknesses, 439-440

IPsec

AHs (authentication headers), 578

databases, 589

ESP, 578

IKE, 578

IPsec/IKE within NSF, 589

peer authentication, 579

SA negotiation, 582-584

SDN-based

dynamic decryption, *592-594*

flow protection, *589-591*

IoT application, *592-594*

site-to-site VPNs, 576

IKEv1 phase 1, *579-582*

IKEv1 phase 2, *582-584*

IKEv1/v2 phase 1 attributes, *586-587*

IKEv1/v2 phase 2 attributes, *588*

IKEv2, *584-586*

IKEv2 versus IKEv1, *586*

Software-Defined Networking (SDN)-based IPsec Flow Protection Internet draft, 588

IPSO Alliance, 60

IPv6 Low Power Wireless Personal Area Network (6LoWPAN), 74

IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), 73

IRM (Identity Relationship Management), 326, 413-414

IRTF (Internet Research Task Force), 60

SDN standards, 66

security standards, 78

IRTP (Internet Reliable Transaction Protocol), 60

ISAKMP (Internet Security Association and Key Management Protocol), 578

ISE (Identity Services Engine), 336

authorization, 368

canned policies, 340

collector and analyzer, 338

consumer/provider matrix, 384-386

CSDL, 644-646

embedded probes, 338

integrated architecture, 337

on demand access control example, 715-717

profiling, 337-340

provisioning, 334-336

SGACLs, 387-388

TrustSec controller, 378

ISG (Industry Specification Group), 187

ISO 27-35, 828

ISO 9797-1, 828

ISO 12207, 828

ISO 15408, 828

ISO 27001, 828

ISO 27002, 828

ISO 27010, 828

ISO 27018, 828

ISO 27034, 828

ISO 29101, 828

ISO 29119, 829

ISOC (Internet Society), 66

isolation

applications, 271

multi-administrator, 282-283

performance and latency, 278

ISRG (Internet Security Research Group), 451

IT

bringing together with OT technologies, 157

connected cars standard, 828

OT convergence, 156

staff allocation, 6

IT/OT

convergence, 159

integration, 788

technology separation, 758-759

ITS (Intelligent Transportation Systems), 826-827

ITU (International Telecommunications Union), 2

ITU-T (ITU Telecommunication Standardization Sector), 60, 66

ITU-T Y.2060 reference model, 125-126

J

jamming attacks, 41

Japan connected car standards, 827

JavaScript, 635

JOSE (JavaScript Object Signing and Encryption), 409

K

Kaa platform, 177

Kantara Initiative, 413-414

Key Performance Indicators. *See* KPIs

keys

- BRSKI, 329-330
- IKE, 578
- PKI, 353-355
- private, 276-278
- PSKs, 41, 579
- public, 352
- QKD, 276

Keystone, 640

Kinetic IoT Platform, 177

KPIs (Key Performance Indicators), 20, 274

- autoscaling, 483
- rules, 483-485
- SESSION_OUT metric, 482-483
- VM_ALIVE script, 480-481
- VM_SCALING metric, 481
- VNF monitoring, 475, 479

Kubernetes security best practices, 656-658

L

L2MP (Layer 2 Multipath), 259

Lambda architectures, 119-120

languages

- data modeling, 68
- natural language processing (NLP), 895-896

last-mile communication, 71

latency

- fog computing, 115
- performance struggle, 278

Layer 2 Multipath (L2MP), 259

Layer 3 inline tagging format, 383

layered data bus, 146

layered security, 43

- application, 46
- device, 45
- human, 44
- network, 45-46
- physical, 44

layers

- AIOTI architecture, 138
- application, 74, 125, 138-139
- architectural, 85-86
- Cloud Customer Architecture for IoT, 141
- connected car security, 850-851
- device, 126
- IoT, 138
- MAC, 73
- MQTT, 532
- network
  - *AIOTI architecture, 138*
  - *communication, 73-74*
  - *ITU-T Y.2060 reference model, 125*
- ODL, 204-207
  - *AAA, 206*
  - *controllers, 206*

DLUX, 207

independent network applications, 207

MD-SAL, 205

NeXT UI, 207

northbound APIs, 206

plug-ins, 204

southbound APIs, 204

OPC UA, 150

physical, 73

SDN, 189-192

applications layer, 191

control layer, 190

infrastructure layer, 189

service support, 125

transport, 74

LDAP (Lightweight Directory Access Protocol)

data pipeline security, 713-714

data topics, 641

ID management, 639

Keystone comparison, 640

MUD URLs, emitting, 390

multitenancy data sharing, 641, 644

RabbitMQ queries, 548

vhost clients, adding, 642

least privilege, SDN orchestration, 269

ledger, blockchains, 883

legacy systems, 237

legislation standards, 54

Let's Encrypt, 451

Level 1 vehicles, 804

Level 2 vehicles, 804

Level 3 vehicles, 804

Level 4 vehicles, 804

Level 5 vehicles, 804

levels of automated driving systems, 803-804

leveraging data, 509

lifecycle service orchestration (LSO), 226-229

lifecycles

data, 507-509

categories, 511

collection, 507

computing, 508

data categories, 509

leveraging, 509

moving, 508

secure remote management, 704-705

system (SDLC), 13

LINs (local interconnect networks), 824

lldpSystemDescription variable, 343

LLN (low-power and lossy networks), 73

local interconnect networks (LINs), 824

local service gateway (LSG), 101

local sys_admin accounts, creating, 399

logging SDN orchestration, 270

logical segmentation, 22

loops, attacks, 41

low-power and lossy networks (LLNs), 73

lower power strategy, 347

LSG (local service gateway), 101

LSO (lifecycle service orchestration), 226-229

LTE-V (LTE-Vehicle), 800

LTI Mosaic, 177

M

M2M (Machine-to-Machine), 3, 173

M4 Rack Server, 489

MAB (MAC address bypass), 365

MAC addresses

EUIs, 327

flooding, 41

layers, 73

machine learning. *See* ML

main mode (IKEv1 phase 1), 580-581

maintenance

cloud computing, 109

oil and gas industry, 752

malicious incidents, oil and gas industry security, 755

Malware Block policy, 387

malware protection

AMP, 456

file policies, 461

FTD, 459-461

point-in-time detection, 456-457

retrospection, 457-458

sandboxing, 458

TALOS, 456

man-in-the-middle attacks (MITM), 40

managed device count per IT person for financial and/or retail customers, 411-412

management

configuration, 17

containerized services, 649-653

data, 5

IoT-A RA, 124

next-generation IoT platforms, 297

police vehicle systems, 821

publish-subscribe, 102

management planes

data protection, 565-566

SDN, 261

security, 658

management UIs (user interfaces), 627-628

MANO (Management and Orchestration), 18

end-to-end considerations, 17-18

next-generation IoT platforms, 297-301

next-generation platforms, 671

NFV, 223-232, 243-245

NFV ETSI, 225

benefits, 232

challenges, 229

decoupling service intentions from instantiation process, 230-231

implementation, 231-232

LSO, 226-229

OSS/BSS interoperability, 232

OpenFog Consortium architecture, 136

manual versus autoquarantining, 782

manufacturer usage description. *See* MUD

Manufacturers Alliance for Productivity and Innovation (MAPI), 62

manufacturing

AnyConnect client example, 617

authorization, 621

identity, authentication, posture, 618

remediation, 619-620

working components, 618-621

clientless portal example, 603

CPwE, 153

GridBlocks, 153-154

segmentation of data responsibilities, 500, 502

Manufacturing 4.0, 3

Manufacturing Execution (MES), 37

manufacturing focused approaches

CPwE, 153

GridBlocks, 153-154

Manufacturer Usage Description. *See* MUD

MAPI (Manufacturers Alliance for Productivity and Innovation), 62

market-focused standards, 61-63

market IoT platform, 172

Marz, Nathan, 120

maturity, IoT platform, 174

mbed platform, 177

McKeown, Nick, 186

MD5 (Message Digest Algorithm), 580

MD-SAL (model-driven service abstraction layer)

AD-SAL, comparison, 209-210

ODL, 205

MEC (Multi-access Edge Computing), 237-238

Media Oriented Systems Transport (MOST), 825

media sanitization, 17, 829

mediums, 41

MEF (Metro Ethernet Forum), 66

memory, reserving, 278

menu access permissions, 399

MES (Manufacturing Execution), 37

message authentication codes, 828

Message Digest Algorithm (MD5), 580

Message Queue Telemetry Transport. *See* MQTT

message sets for vehicle/roadside communications standard, 826

metrics

monitoring, 476

VMs, scaling, 481

Metro Ethernet Forum (MEF), 66

microsegmentation, 387

microservices, 36

Microsoft

Azure, 176

DREAD model, 28

middleware

architectures, 118

ICN, 102

midstream environment (oil and gas industry),734, 744

challenges, 748-749

digitization, 747

new business needs, 747

pipeline, 744-748

migration, ICN challenges, 104

million packets per second (MPPS), 199

MindSphere, 176

minimizing complexity, 309

MITM (man-in-the-middle attacks), 40

ML (machine learning), 98, 878-879, 893

AI collaboration, 899

classical models approach, comparison, 893

connected cars, 815

deep learning (DL), 894-895

neural networks, 896-897

people-/user-centric approaches, 98

supervised, 894

mobile-centric architectures, 32, 93-94

mobile data terminals, police vehicles, 820

mobility, fog computing, 116

Mocana by Mocana platform, 177

MODBUS application filter example, 436-437

models

intended outcomes, 304-306

reference, 87

service abstraction layer (MD-SAL), 205

modules

AnyConnect client, 612-616

AMP, 616

endpoint compliance, 614

Network Access Manager, 614

NVM, 615-616

roaming protection, 614-615

VPN, 612-613

MUD, 392

pluggable authentication (PAM), 646

monitoring

actions, 477

continuous, 17

event-based videos, 709-712

data pipeline security, 713-714
deployment, 710-712
triggers, 710
metrics, 476
police vehicle systems, 821
power, 702
street cabinets, 705-709
VNFs, 475
dynamic mapping, 478
ESC, 476-477
fulfillment and assurance sequences, 479-480
KPI monitoring methods, 479
prerequisites, 475
VM alive script, 480-481
Mosaic, 177
MOST (Media Oriented Systems Transport), 825
moving data, 508, 527-531
MPPS (million packets per second), 199
MQTT (Message Queuing Telemetry Transport Protocol), 350-351, 532-533, 540
authentication, 533-535
authorization, 535-539
availability, 542-543
brokers, 350
clients, 350
confidentiality, 539-540
integrity, 540-542
layers, 532
repudiation, 543
transport protection, 532
MUD (Manufacturer Usage Description), 78, 390
driver development, 516
Internet draft, 390
module, 392
policy types, 390-391
process flow, 393-394
telemetry sensors, adding to street cabinets, 707
URLs, emitting, 390
Multi-access Edge Computing (MEC), 237-238
multi-administrator isolation, 282-283
multitenancy
data sharing, 641, 644
deployment preparations, 315
next-generation IoT platforms, 296
smart cities, 698
TEEs, 666
user profiles/roles, 628-630

N

NaaS (Network as a Service), 444-446
NAC (Network Access Control), 42
namespaces, 654
naming conventions, 327-328
naming services, 102
NAT (network address translation), 424-425
National Highway Traffic Safety Administration (NHTSA), 803, 845-846
National Institute of Standards and Technologies. *See* NIST
National Service Framework (NSF), 589
native applications, 408
NAT-T (NAT-Traversal), 583
natural intelligence (NI), 890
natural language processing (NLP), 895-896
navigation services, 805
NB APIs (northbound APIs), 43
NBAR2 (Network-Based Application Recognition), 444
NEDs (Network Element Drivers), 300, 316
NERC (North American Electric Reliability Corporation), 78

NETCONF (IETF RFC 6241), 258

NetFlow protocol, 442-443

Netrounds, 784

Network Access Control (NAC), 42

Network Access Manager, 614

network address translation (NAT), 424-425

Network as a Service (NaaS), 444-446

Network-Based Application Recognition (NBAR2), 444

Network Element Drivers (NEDs), 300, 316

network enforced policies, 170

network functions virtualization. *See* NFV

network functions virtualization infrastructure. *See* NFVI

network layer, 45-46

- AIOTI architecture, 138
- communication, 73-74
- ITU-T Y.2060 reference model, 125

Network Security Event Logging (NSEL), 444

Network Services Descriptors (NSD) catalog, 471

network services entity (NSE), 131

Network Services Orchestrator. *See* NSO

Network Storage Resource (NSR), 472

Network Visibility Module (NVM), 615-616

networks

- active networking, 185
- AIOTI architecture, 139
- connected cars, 824-825
- IoT-A RA, 123
- low-power and lossy, 73
- proximity, 146
- smart cities, 682

neural networks, 896-897

next-gen IPS (NGIPS), 423

Next Generation Firewall virtualized (NGFWv), 422-423

next-generation IoT, 291

- architecture, 294-295
- building blocks, 295-303
  - *fog levels, 302*
  - *heterogeneous, 297*
  - *infrastructure, 301*
  - *management, 297*
  - *MANO, 297-301*
  - *multitenancy, 296*
  - *operation, 297*
  - *UIs, 297*
  - *virtualization, 297*
- complexity, minimizing, 309
- consistency, 291
- delivery, 293
- deployment, 292
- event-based video and security use case, 309-321
  - *architecture overview, 313*
  - *cabinet monitoring, 314*
  - *description, 312*
  - *preparatory work, 315-316*
  - *triggers, 312*
- evolving technology landscape, 670
- full IoT stacks, 293, 670
- Function Packs, 675
- high reliability, 293
- intended outcomes, 303-308
  - *contextual automation, 307*
  - *model-driven, 304-306*
  - *service-centric, 304-306*
  - *service chaining, 306-307*
- interoperability, 299, 672
- MANO, 671
- reference architecture, 293
- requirements, 308
- scaling, 293

services, 299
standards, 292

NeXT UI, 207

NFV (network function virtualization), 7, 63, 187
adoption acceleration, 218
agility, 221
architectures, 154-156
CAPEX reduction, 219
challenges, 233-235
components, 64
energy efficiency, 220
extranet automation, 596
flexibility, 220
fog computing, 243
forwarding graphs, 222-224
high availability, 220
history, 187
innovation, 221
IoT enabling capabilities, 235
MANO, 243-245
multi-administrator isolation, 282-283
NFVI, 222-223
ODL alignment (OPNFV), 67, 211
OPEX reduction, 219
SDN, compared, 187
security, 272
authenticated time service, *281*
backdoors, *281-282*
boot integrity, *274-275*
multi-administrator isolation, *282-283*
performance isolation, *278*
private keys, *276-278*
secure crash, *275*
SRIOV, *283-285*
tenant/user AAA, *279-280*
threat landscape, *273*
SRIOV, 283-285
standards, 65-67
telecom benefits, 219-221
template-based extranet automation, 595
VNFC, 221

NFVI (network functions virtualization infrastructure), 222-223, 486
ENFV components, 486-487
hardware requirements, 488-490
NFVIS benefits, 488
orchestration, 490
service chaining, 494-495
vBranch Function Pack, 490-493
VMs supported, 490

NFVO (NFV orchestrator), 226
back-end platform, 646-647
containerized services, 650
NSO, 646

NGFWv (Next Generation Firewall virtualized), 422-423

NGIPS (next-gen IPS), 423

NHTSA (National Highway Traffic Safety Administration), 803, 845-846

NI (natural intelligence), 890

Nirvana Stack, 212

NIST (National Institute of Standards and Technologies), 77
CPS PWG, 77
cybersecurity best practices, 659
NISTIR 7628 guidelines, 77
security recommendations, 15
SP 800-30, 829
SP 800-50, 829
SP 800-61, 829
SP 800-88, 829
SP 800-1600 Systems Security Engineering publication, 77

NISTIR 7628 guidelines, 77

NLP (natural language processing), 895-896

nodes

- edge, 35
- fog, 240
    - *cabinets, 660*
    - *communications, 664*
    - *core software, 662-664*
    - *data analysis, 526*
    - *data at rest, 521*
    - *drives, 664*
    - *northbound communications, 662*
    - *operating system security, 664*
    - *RA, 662*
    - *RabbitMQ orchestrated security example, 552-558*
    - *runtime environments, 665*
    - *security, 660-662, 666*
    - *southbound APIs, 667*
    - *virtualization, 665*
- graph, 199
- input, 199

nonfunctional security requirements analysis, 15

nonrepudiation, 38

- data protection, 506
- MQTT, 543
- northbound SDN controller communications, securing, 267-268
- RabbitMQ, 552

normal off power strategy, 347

normalization, data, 513-517

North American Electric Reliability Corporation (NERC), 78

northbound APIs (NB APIs), 43

- fog nodes, 662
- ODL, 206
- OVS, 197
- SDN, 191

northbound SDN controller communications, securing, 263-266

- authorization, 267
- checks and balances, 268
- nonrepudiation, 267-268
- REST authentication, 264-267

north–south SGACLs, 387

NSD (Network Services Descriptors) catalog, 471

NSE (network services entity), 131

NSEL (Network Security Event Logging), 444

NSF (National Service Framework), 589

NSO (Network Services Orchestrator), 646

- centralized security example, 469
    - *activation sequence, 472-474*
    - *fulfillment and assurance sequences, 474-475*
    - *NSD catalog, 471*
    - *NSR, 472*
    - *VNFD catalog, 470*
- PAM, 646
- scalability, 647

NSR (Network Storage Resource), 472

NVM (Network Visibility Module), 615-616

O

OAM (operation and management), 192

OASIS (Organization for the Advancement of Structured Information Standards), 61

OAuth 2.0

- IoT IAM, 404-405
- MQTT authorization, 537-539

Object Management Group, 60

OCF (Open Connectivity Foundation), 60, 142

OCSP (Online Certificate Status Protocol), 259

ODCA (Open Data Centre Alliance), 67
ODD (operational design domain), 804
ODL (OpenDaylight), 203-212
AD-SAL versus MD-SAL, 209-210
implementation, 208
Nirvana Stack, 212
objectives, 204
OPNFV, 211
reference architecture, 204-207
AAA, 206
controllers, 206
DLUX, 207
independent network applications, 207
MD-SAL, 205
NeXT UI, 207
northbound APIs, 206
plug-ins, 204
southbound APIs, 204
SDN standards, 67
SDNi, 254
ODVA (Open DeviceNet Vendors Association), 61
OF (OpenFlow), 186, 192-195
components, 193
functions, 194
interface, 257
ONF, 193
strength, 192
OFC (OpenFog Consortium), 61
architecture, 133-138
NFV MANO convergence, 243-245
perspectives, 136
pillars, 133-135
security layers, 137
stakeholder views, 137
offloading traffic, 198
OIF (Optical Internetworking Forum), 67
oil and gas industry, 729
clientless SSL VPNs, 610-611
data flows, 790
demand and consumption, 730
digital technology investments, 735
downstream environment, 749
activities, 734
challenges, 753-754
digitization, 752
distributed control systems, 750
IoT benefits, 752
new business needs, 752
overview, 749
refining and processing architecture, 750
technologies, 750-751
E&P (exploration and production), 733
equipment health monitoring, 763-765
access control, 781
access privileges, 778-780
anomaly traffic detection, 780-781
architecture, 772
automated deployment, 777-778
command validation, 782-783
data pipelines, 771, 786-788
deployment, 766-771
limitations, 765
operational lifecycle, 772
preconfiguration checklist, 773-775
quarantines, 782
requirements, 767
service assurance, 784-786
fatality rate, 731
field operations automation, 789
future communication requirements, 790
IoT and digitization examples, 737-738
IoT goals, 731
IoT impact, 789
IT/OT integration, 788
maintenance, 752
midstream environment, 744

activities, *734*

challenges, *748-749*

digitization, *747*

IoT benefits, *747-748*

new business needs, *747*

pipeline architecture, *744*

pipeline management applications, *744-746*

new requirements, 788

price per barrel of oil, 730

secure automation opportunities, 735

security, 754-763

accidental incidents, *755*

architectures, *756-757*

automation requirements, *762-763*

budget constraints, *762*

components, *757*

control systems, *755*

IDMZ, *759*

IEC 62443 approach, *756*

IT/OT technology separation, *758-759*

malicious incidents, *755*

requirements, *760-761*

risk outcomes, *755*

standards and guidelines, *757*

vulnerabilities, *754*

upstream environment

activities, *733*

automation, *742-743*

challenges, *743-744*

communication and solution technologies, *740*

fracking, *739*

oil sands mining, *740*

overview, *739*

value, 731-734

oil sands mining, 740

OLE for Process Control (OPC), 62

on demand access control, 714-718

IPS/IDS, 717-718

self-service portal, 715-717

onboard systems, deployment, 864-865

onboard telematics, 821

onboarding

attack target, 40

devices, 102, 334-336

smart city sensors, 706-707

oneM2M architecture, 129-132

CSFs, 131

functional architecture, 131

industrial/market standards, 62

layered model, 130

ONF (Open Networking Foundation), 67, 186, 193, 257

Online Certificate Status Protocol (OSCP), 259, 357

Online Trust Alliance. *See* OTA

OPC (OLE for Process Control), 62

OPC Foundation, 152

OPC-UA (OPC Unified Architecture), 150-152

Open API Initiative, 61

Open Connectivity Foundation (OCF), 60, 142

Open Data Centre Alliance(ODCA), 67

Open DeviceNet Vendors Association (ODVA), 61

Open Group Open Process Automation, 61

open interoperable standards, 55

Open Networking Foundation (ONF), 67, 186, 193, 257

Open Platform for NFV (OPNFV), 67, 211

open platforms, smart cities, 677

open process automation architecture, Purdue Model of Control, 159

open standards, 55

Open Systems Interconnection (OSI), 70

Open vSwitch. *See* OVS

Open Web Application Security Project (OWASP), 76, 168

OpenDaylight. *See* ODL

OpenDaylight User Experience (DLUX), 207

OpenFlow. *See* OF

OpenFog Consortium. *See* OFC

OpenID Connect 1.0, 405

openness, 86

end-to-end considerations, 18

OpenFog reference architecture pillar, 135

SDN, 192

smart city platforms, 697

OpenStack platform, 632

operation and management (OAM), 192

operation support systems (OSS), 223

operational design domain (ODD), 804

operational lifecycle, 772

operational plane, 261

Operational Technology (OT), IT convergence, 156-157, 788

operationalization, back-end platforms, 633-634

operations

challenges, 821, 863

next-generation IoT platforms, 297

requirements, 86-87

operations and maintenance phase (SDLC), 14, 17

OPEX reduction, 219

OPNFV (Open Platform for NFV), 67, 211

Optical Internetworking Forum (OIF), 67

Oracle Integrated Cloud, 177

orchestration, 5

connected cars, 818, 848

extranet automation, 596

IoT capabilities, 288, 691

NFVIS distributed deployment, 490

police vehicles, 822

RabbitMQ fog node level security example, 552-558

SDN, 268-270

smart cities, 690, 697

system of systems platform for smart cities, 699-700

template-based extranet automation, 595

Organization for the Advancement of Structured Information Standards (OASIS), 61

OSCP (Online Certificate Status Protocol), 357

OSI (Open Systems Interconnection) model, 70

OSS (operation support systems), 223

OT (Operational Technology), IT convergence, 156-157, 788

OTA (Online Trust Alliance), 76

lifecycle management, 821

secure updates, 855-857

security standards, 76

OTA (over-the-air), 821

OTT (over the top), 89, 673

OTV (Cisco Overlay Transport), 259

out of band SGT propagation, 381

outbound packet filtering, 426

overcloud, 634

overlapping firewalls, 425

OVS (Open vSwitch), 195-198

architecture, 196

capabilities, 196

features, 198

functions, 197

traffic management, 197

traffic offloading, 198

Ovum Research IoT platform recommendations, 290

OWASP (Open Web Application Security Project), 76, 168

P

P4 (Programming Protocol-Independent Packet Processors), 201-203
- forwarding model, 202
- framework, 201
- implementation, 203

PaaS (Platform as a Service), 7, 108

packets
- DPI, 430-432
- filtering
  - *firewalls, 426-427*
  - *sanity checking, 431*
  - *user definable, 432*
- vector, 198-200

PAD (Peer Authorization Database), 589

PAM (pluggable authentication modules), 646

partial solutions, 88

passwords, authentication, 357-358

PAT (port address translation), 425

patches, 840

pattern matching, 438-439

PCI-SIG (PCI Special Interest Group), 284

peer systems, 124

penetration testing, 271

people (IoT), 4

people-centric architecture approach, 98-100

Perfect Forward Secrecy (PFS), 584

performance
- end-to-end considerations, 20
- IoT IAM, 403
- isolation, 278
- OpenFog Consortium architecture, 136
- V2V standard requirements, 827

permissions
- data, 399
- EFM, 563
- menu access, 399
- RabbitMQ, 546

persistency, data, 529

personal health monitoring services, 805

personalized connected car experiences, 815, 862-863

perspective approach. *See* system viewpoint

PFS (Perfect Forward Secrecy), 584

phasor measurement unit (PMU) zones, 23

PHY (physical layers), 213

physical access, 505

physical entities, 123

physical layers (PHY), 73, 213

physical security, 9, 38, 44

physical segmentation, 21

pillars
- IA, 37
- OpenFog reference architecture, 133-135

pipelines (oil and gas)
- architecture, 744
- challenges, 748-749
- data security, 786-788
- digitization, 747
- IoT benefits, 747-748
- management applications, 744-746
- new business needs, 747

PKI (Private Key Infrastructure), 351-355

placement, platforms, 89

planning security, 16

Platform as a Service (PaaS), 7

Platform Exchange Grid (pxGrid), 446

platforms
- back-end, 631-634
  - *access control, 637-646*
  - *API security, 634-635*
  - *containerized services management, 649-653*

dashboard, 635-637
NFVO, 646-647
operationalization, 633-634
options, 631
overcloud/undercloud, 634
requirements, 631
REST APIs, 634-635
VFM, 648
VIM, 648-649
converged and multifaceted, 246-248
definition, 88
independence, 151
open, 677
OTT IoT, 673
placement, 89
public shared, 89
Smart City, 692-693
plug-ins
clientless SSL VPN application access, 609
ODL, 204
RabbitMQ, 548
pluggable authentication modules (PAM), 646
PMU (phasor measurement unit) zones, 23
point-in-time protection, 456-457
police vehicles, 821
ANPR, 820
audible and visual warning systems, 820
battery management, 821
integrated approach, 821
mobile data terminals, 820
onboard systems and technologies, 819-821
onboard telematics, 821
operational challenges, 821
orchestrated services, enabling with consolidated orchestrated hardware, 822
radios, 820
smart city integration, 719-721
speed detection, 820
speed recognition devices, 820
vehicle tracking, 820
video camera and audio systems, 820
wearables, 821
Wi-Fi hotspots, 821
policies
authorization, 403
implementation, 53
MUD, 390-391
network enforced, 170
port address translation (PAT), 425
portals
self-service, 714-717
SSL VPNs, 602-603
ports
application detectors, 434
forwarding, 606
security, 341
posture, 28, 618
power
communication, 347-348
monitoring and controlling in smart cities, 702
virtualization, 702-704
preconfiguration checklist, 773-775
Predix, 177
presentation, 5
preserving information, 17
preshared keys. *See* PSKs
preventing threats. *See* IPS
preventive automated maintenance, 742
privacy
cloud computing, 110
Cloud Customer Architecture for IoT, 142
connected cars standard, 828
IISF, 162

IoT-A RA, 124
IoT IAM, 403
people-/user-centric approaches, 100
private blockchain, 884
private clouds, 107
private keys, 276-278
privileges, dynamic authorization, 367
proactive data protection mechanisms, 567-571
proactive mode (SDN), 190
probes
Device Sensor, 344
embedded within ISE, 338
ISE profiling capability leveraging, 338
procedures, 17, 54
processes, 4, 393-394
processing
architectural layer, 86
context, 102
profile provisioning, 330-331
AWS IoT example, 331-333
attributes, associating, 331
certificate and associated key pair, 332
certificate management, 333
connection kit, downloading, 332
temperature sensor, adding to registry, 331
Cisco Identity Services Engine example, 334-336
profiles, users, 628-630
profiling ISE process, 337-340
Programming Protocol-Independent Packet Processors. *See* P4
propagation, TrustSec, 381-383
protecting data, 531
backups, 570
CAP theorem, 568-569
control plane, 566-567
data virtualization, 564
digital twins, 569
EFM, 560-564
components, 561
computation, 562
data collection, 562
DSLinks, 563
permissions, 563
quarantine, 563
management plane, 565-566
MQTT, 532-533
authentication, 533-535
authorization, 535-539
availability, 542-543
confidentiality, 539-540
integrity, 540-542
layers, 532
nonrepudiation, 543
transport encryption, 532
proactive mechanisms, 567-571
RabbitMQ, 544-547
access control, 546
authentication, 547-548
authorization, 548-549
availability, 550-551
confidentiality, 549
exchanges, 544
fog node orchestration example, 552-558
integrity, 549
nonrepudiation, 552
permissions, 546
plug-ins, 548
vhosts, 546-547
reactive mechanisms, 571-573
protocols, 41
6LoWPAN, 74
AMQP, 74
analysis, 439
CIP, 428

CoAP, 349-350
communication, 70
DCI, 259
DTLS, 74, 612
Flexible NetFlow, 444
HTTP, 74, 264
HTTPS, 74, 598
IKE, 578
IKEv1, 579, 586-587
aggressive mode, 582
authentication mode, 579
D-H groups, 580
encryption algorithms, 580
hashing algorithms, 580
IKEv2 comparison, 586
main mode, 580-581
IKEv2, 584-588
exchange process, 584-586
IKEv1 comparison, 586
industrial
CIP, 428-432
lack of security, 429
potential solutions, 430
IP, 73
IPsec. *See* IPsec
L2MP, 259
MQTT. *See* MQTT
NetFlow, 442-443
OCSP, 259, 357
OTV, 259
OVS supported, 196
RPL, 73
SNMP, 259
SXP, 381
TCP, 74
TLS, 74
UDP, 74
vulnerabilities, 42
VXLAN, 259
XMPP, 74, 258
prototype with OAuth2, 410
provisioning devices, 326, 330-331
AWS IoT example, 331-333
Cisco Identity Services Engine example, 334-336
proximity
fog computing, 116-117
IIRA, 146
PSKs (preshared keys), 349
cracking, 41
IPsec peer authentication, 579
public blockchains, 884
public clouds, 107
public keys, 352
public platforms, 89
public services, on demand access control, 714-718
IPS/IDS, 717-718
self-service portal, 715-717
public shared platforms, 89
publish-subscribe management, 102
pub/sub systems, 527-530
Purdue Model of Control, 157-160
hierarchy, 5, 158
open process automation, 159
segmentation of data responsibilities, 500-502
segmented architecture based on, 157
pxGrid (Platform Exchange Grid), 446

Q

QKD (quantum key distribution), 276
QoS (Quality of Service), cloud computing, 112
quadruple silo, 683
quarantines
EFM, 563
equipment health monitoring example, 782

R

RA (remote attestation), 662

RabbitMQ, 544-547

access control, 546

authentication, 547-548

authorization, 548-549

availability, 550-551

confidentiality, 549

configuring, 643

exchanges, 544

fog node level orchestration example, 552-558

fog node running TEEs deployment, 554

orchestrated transaction, 556-558

tenant administrator responsibilities, 555-556

integrity, 549

nonrepudiation, 552

permissions, 546

plug-ins, 548

vhosts, 546-547

Radio Frequency Identification (RFID), 327

radios, police vehicles, 820

RADIUS, 361-362

A/V pairs, 362

CoA, 368

request commands, 370-371

Request/Response codes, 369

requests, 368-369

session identification, 369

VLAN assignments, 371-374

message types, 362

RAMI 4.0, 148

ransomware programs, 454

rating threats, 28

RawPublicKey, 349

RBAC (role-based access control), 169

Cisco IoT security framework, 169

dynamic segmentation based on, 378

multitenancy data sharing, 644

reactive data protection mechanisms, 571-573

reactive mode (SDN), 189

real-time processing, cloud computing, 112

recommendations, IoT platforms, 289-290

recursive DNS, 462

reference architectures, 87

IIRA, 144-146

next-generation IoT platforms, 293

ODL, 204-207

AAA, 206

controllers, 206

DLUX, 207

independent network applications, 207

MD-SAL, 205

NeXT UI, 207

northbound APIs, 206

plug-ins, 204

southbound APIs, 204

OpenFog Consortium, 133-138

perspectives, 136

pillars, 133-135

security layers, 137

stakeholder views, 137

RAMI 4.0, 148

reference implementation, 87

reference models, 87

AIOTI architecture, 138

GridBlocks, 153-154

IoT-A RA, 121

IoTR-A RA entity-based, 123

ITU-T Y.2060, 125-126

IoTWF, 126-129

Purdue Model of Control, 157-160

hierarchical data flow model, 158
open process automation, 159
segmented architecture based on, 157
reference standards, 59-61
registering devices, 330-331
AWS IoT example, 331-333
Cisco Identity Services Engine example, 334-336
regulations, 53
regulatory bodies, 56
RelayR IoT Middleware Platform, 177
reliability, 86
cloud computing, 109
fog computing, 115-117
high, 293
IISF, 162
OpenFog reference architecture pillar, 135
SDN, 190
standards, 54
remediation
remote HMI access, 619-620
threats, 878
remote access
connected cars, 806
Human Management Interface (HMI), 617
VPNs, 598
remote access SSL-based VPNs, 598
AnyConnect client, 611
configuration, 612
deployment, 611
manufacturing example, 617-621
modules, 612-616
client-based, 600, 612
clientless, 599-611
application access, 604-609
client-based comparison, 600
components, 602
DAP, 609
group policies, 602
oil and gas example, 610-611
portal, 602-603
tunnel groups, 601
HTTPS, 598
multiple solutions, 599
reverse proxy, 599
remote attestation (RA), 662
remote management, 704-705
repeatability, 597
reporting, 16
Representational State Transfer. ***See*** **REST**
Request/Response codes (CoA), 369-371
requirements
accounting, 400-401
back-end platform security, 631
connected car interoperability infrastructures, 829
connected car orchestration, 818
equipment health monitoring example, 767
fog computing, 115
IoT IAM, 403-404
IoT implementation and operation, 86
next-generation IoT platforms, 308
NFVIS hardware, 488-490
oil and gas industry, 760-761, 788-790
SDN-based IPsec flow protection interface, 590
security, 75
reserving CPU/memory, 278
resilience, IISF, 162
REST (Representational State Transfer), 349
APIs, 634-635
authentication, 264-267
CoAP, 349-350
data at, 518, 521

restrictions, constrained devices, 345

retrospection malware detection, 457-458

reusable templates, 469

reverse proxy, 599

revocation, 259, 267, 356-357

RFID (Radio Frequency Identification), 327

risks

- assessing, 15, 58, 829
- biometric authentication, 360
- identifying, 25
  - *classification, 27*
  - *identification, 25-26*
  - *risk scores, 28*
  - *threat modeling, 27*
- oil and gas industry security malicious/accidental attacks, 755
- scores, 28

roaming protection, AnyConnect client, 614-615

Rockwell Automation, 153

role-based access control. *See* RBAC

roles

- IDs, 637-639
- users, 628-630

RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks), 73

RSA-encrypted nonces, 579

RSA signatures, 579

rules, centralized security, 483-486

runtime environments, 665

S

SAs, 582-584

SaaS (Software as a Service)

- cloud computing deployment, 108
- IoT, 7

SAD (Security Association Database), 589

SAE (Society of Automotive Engineers)

- automated driving system levels, 803-804
- International connected car standards, 827-829
- J2735, 827
- J2945/1, 827
- J3061, 827
- J3101, 827

safety

- IISF, 162
- standards, 54

SA_INIT Exchange, 585

Salesforce IoT Cloud, 176

Samsung Artik, 176

sandboxing, 458

sanity checking, 431

SANS paper, Security Evaluation of Z-Wave Wireless Protocol, 40

SAP Cloud Platform, 177

SASL (Simple Authentication and Security Layer), 547

scalability, 86, 191

- blockchain, 886
- cloud computing, 109
- data-centric architectures, 105
- end-to-end considerations, 20
- ICN, 103
- IoT, 5
- IoT IAM, 402-403
- IRM, 413
- KPI, 483
- next-generation IoT platforms, 293
- NSO, 647
- OpenFog reference architecture pillar, 135
- standards, 54
- VMs, 481

SDK (software development kits), 20

SDLC (System Development Lifecycle), 13

acquisition and development, 14-16

assessment, 14

disposition, 14, 17

implementation, 14-16

initiation, 14-15

operations and maintenance, 14, 17

SDN (software-defined networking), 7, 64-65, 185, 188

agility, 192

applications, 270-271

architectures, 154-156, 189-192

applications layer, 191

control layer, 190

infrastructure layer, 189

northbound API, 191

southbound API, 191

attacks, 42-43

controllers

east-west communication, securing, 254-256

northbound communication, securing, 263-268

securing, 252-253

southbound communication, securing, 256-260

history, 185

infrastructure

control plane, 262

data, 262-263

management, 261

operations, 261

securing, 260-263

IPsec

dynamic decryption, 592-594

flow protection, 588-591

IoT application, 592-594

NFV, compared, 187

OAM, 192

ODL, 203-212

AD-SAL versus MD-SAL, 209-210

implementation, 208

Nirvana Stack, 212

objectives, 204

OPNFV, 211

reference architecture, 204-207

OF, 192-195

components, 193

functions, 194

ONF, 193

strength, 192

openness, 192

orchestration, 268-270

OVS, 195-198

architecture, 196

capabilities, 196

features, 198

functions, 197

traffic management, 197

traffic offloading, 198

P4, 201-203

forwarding model, 202

framework, 201

implementation, 203

reliability, 190

scalability, 191

SDR, 212-214

SDX

challenges, 233-235

fog computing, 243

IoT enabling capabilities, 235

security

applications, 270-271

controller, 252-253

controller east-west communications, 254-256 *controller northbound communications, 263-268*

controller southbound communications, 256-260

infrastructure, 260-263

orchestration, 268-270

services, 270-271

underlying operating system, 253

services, 270-271

standards, 65-67

strengths, 186-191

underlying operating system, 253

VPP, 198-200

data plane programmability, 200

directed graph of nodes, 199

DPDK, 200

WANs, 214-217

SDNi (SDN Controller Inter-communication), 254-255

SDO (standards development organizations), 130

SD-PHY (software-defined PHY), 213

SDR (software-defined radio), 212-214

SD-WANs (software-defined wide-area networks), 186

SDWN (software-defined wireless networking), 186

SDX (software-defined X), 186

challenges, 233-235

fog computing, 243

history, 186

IoT enabling capabilities, 235

secure boot, 274-275

secure bootstrapping, 328

BRSKI, 329-330

immutable identities, 328-329

secure crash, 275

Secure Hash Algorithm (SHA), 580

Secure HTTP (HTTPS), 74

Secure Key Exchange Mechanism (SKEME), 578

Secure Sockets Layer. *See* SSL

Secure Technology Alliance, 76

Secure Unique Device Identification (SUDI), 328-329

security, 8-9

architectural layer, 86

assurance requirements analysis, 16

attack continuum, 11-12

automating, 876

catalogs, 656

cloud computing, 110

collaborative, 899

communications, 658-659

compliance and governance, 5

connected cars, 830

attack surface, 831

challenges, 835

connectivity challenges, 840

considerations, 839

consolidation, 849

data-centric and application-centric fusion, 849

design implementations, 847

driver concerns, 837

encryption, 837

goals, 847-848

industry alliances, 847

layered approach, 850-851

reasons for, 830

safety-criticality, 836

threats, 831-834

U.K. supply chain guidelines, 842-845

upgrades/patches, 840

U.S. supply chain guidelines, 845-846

vulnerabilities, 836-840

control, 16

control planes, 659

data pipelines, 713-714

data planes, 659

data sharing, 9

data stores, 658

DNS-based. *See* DNS-based security

Docker, 653-655

end-to-end considerations, 20

endpoints, 9

enforcing, 90

fog agents, 666

fog computing, 115-117

ICN, 103

insecure devices, 9

IoT-A RA, 124

IoT platforms, 178-179

Kubernetes best practices, 656-658

layers, 43

- *application, 46*
- *device, 45*
- *human, 44*
- *network, 45-46*
- *physical, 44*

management planes, 658

NFV, 272

- *authenticated time service, 281*
- *backdoors, 281-282*
- *boot integrity, 274-275*
- *multi-administrator isolation, 282-283*
- *performance isolation, 278*
- *private keys, 276-278*
- *secure crash, 275*
- *SRIOV, 283-285*
- *tenant/user AAA, 279-280*
- *threat landscape, 273*

NIST recommendations, 15

oil and gas industry, 754-763

- *accidental incidents, 755*
- *architectures, 756-757*
- *automation requirements, 762-763*
- *budget constraints, 762*
- *components, 757*
- *control systems, 755*
- *IDMZ, 759*
- *IEC 62443 approach, 756*
- *IT/OT technology separation, 758-759*
- *malicious incidents, 755*
- *new requirements, 788*
- *requirements, 760-761*
- *risk outcomes, 755*
- *standards and guidelines, 757*
- *vulnerabilities, 754*

OPC UA, 151

OpenFog Consortium architecture, 136

OpenFog reference architecture pillar, 134

physical, 9, 38, 44

planning, 16

police vehicles, 821

requirements, 75

risk assessments, 15

SDN

- *applications, 270-271*
- *controller, 252-253*
- *controller east-west communications, 254-256*
- *controller northbound communications, 263-268*
- *controller southbound communications, 256-260*
- *infrastructure, 260-263*
- *orchestration, 268-270*
- *services, 270-271*
- *underlying operating system, 253*

smart cities, 681, 693-696

- *Cloud Security Alliance recommendations, 695*
- *threats, 694*

spanning the enterprise, 12

standards, 54, 75-78

technology lifecycles, 9

threats, 8

Security Association Database (SAD), 589

Security Evaluation of Z-Wave Wireless Protocol, 40

security events algorithms, 445

Security Group Firewall (SGFW), 384

Security Group Tag ACL (SGACL), 384

Security Group Tags. *See* SGTs

Security Intelligence Operations (SIO), 456

Security Policy Database (SPD), 589

segmentation, 21-25

architectures, 157

connected car security, 857

data responsibilities, 500-502

dynamic decryption, 592

dynamic RBAC-based, 378

industry compliance standards, 23

logical, 22

physical, 21

security policies, 22

self-registration workflow, 334-336

self-service portals, 714-717

semantics, people-/user-centric approaches, 99

semistructured data, 510

sensors

data, sharing, 824

smart cities

access control, *708-709*

onboarding, *706-707*

sequences

activation, 472-474

event-based video and security use case, 319-320

fulfillment and assurance, 474-481

Serra, James, 523

servers

architecture, 99

authentication, 363

IoT, 102

UCS E-Series, 489

services

architectural layer, 86

assurance, 784-786

catalogs, 656

chaining, 306-307

next-generation IoT platforms, *304*

NFVIS distributed deployment, *494-495*

cloud computing deployment, 108

connected cars, 805

containerized, managing, 649-653

deployment, 33, 639-641

disabling SDN orchestration, 270

discovery, 102

future connected car, 815

hierarchy, 37

ICN, 102

intelligent proxy, 464-465

intended outcomes, 304-306

IoT-A RA, 123

microservices, 36

naming, 102

network orchestrator. *See* NSO

next-generation IoT platforms, 299, 304

SDN, 270-271

smart cities, 691-692

support layer, 125

SESSION_OUT metric, 482-483

sessions

IDs, 369, 533

tickets, 533

SGACL (Security Group Tag ACL), 384

automation, 388

benefits, 384

consumer/provider matrix, 384-386

east–west, 387

microsegmentation, 387

north–south, 387

SGFW (Security Group Firewall), 384

SGIP (Smart Grid Interoperability Panel), 62

SGT (Security Group Tag), 376-377

dynamic assignment, 380

enforcement, 384

equipment health monitoring example, 781

inline tagging, 383

NetFlow records information, 447

propagation, 381-383

RBAC-based segmentation, 378

static assignment, 380

static/dynamic assignment, 380

SGT Exchange Protocol (SXP), 381

SHA (Secure Hash Algorithm), 580

sharing

data, 9, 641, 644

devices, 315

sensor data, 824

Shenker, Scott, 186

show authentication session command, 371

Siemens MindSphere, 176

signatures, 579

siloed systems, police vehicles, 821

silos, 683

Simple Authentication and Security Layer (SASL), 547

Simple Network Management Protocol (SNMP), 259

single root I/O virtualization (SRIOV), 283-285

SIO (Security Intelligence Operations), 456

SIoT (social IoT), 98

site-to-site IPsec VPNs, 576

IKEv1, 586-588

IKEv1 phase 1, 579-582

aggressive mode, 582

authentication method, 579

D-H (Diffie-Hellman) groups, 580

encryption algorithms, 580

hashing algorithms, 580

main mode, 580-581

IKEv1 phase 2, 582-584

NAT-T (NAT-Traversal), 583

PFS, 584

quick mode, 582

IKEv2, 584-586

exchange process, 584-586

phase 1 attributes, 586-587

phase 2 attributes, 588

versus IKEv1, 586

SKEME (Secure Key Exchange Mechanism), 578

smart cities

automation, 721-722

benefits, 693

buildings, 680

challenges, 684

citizen experience, 681

city-wide platforms, 692-693

common components, 679

common platform implementation, 696

compliance, 682

connected cars, 806

consolidation, 698

cybersecurity, 682

data-app centric, 697

data management, 682

defined, 676

deployment automation, 723-725

economic impact of IoT deployments, 688

ecosystem groupings, 683

emergency vehicle fleet management, 719-721

event-based video, 709-714

governance, 682
growth, 678
healthcare, 681
high-level architecture, 701
horizontal approaches, 685
infrastructure operational efficiency, 681
interface types, 696
investments, 676
IoT orchestration capabilities, 691
market segments, 676
multitenancy, 698
networking and communications, 682
open platforms, 677
orchestration, 690, 697
platform openness, 697
power monitoring and control, 702
public service connectivity on demand, 714-718
IPS/IDS, 717-718
self-service portal, 715-717
quadruple silo, 683
secure remote application lifecycle management, 704-705
security, 681, 693-696
sensors, 706-709
services benefiting from automation capabilities, 691-692
standards, 685-687
street cabinet monitoring, 705-709
system of systems, 690, 699-700
threats, 678
traditional city operating models, 685
transportation and urban mobility, 680
vendors, 689
vertical applications overview, 679
virtualization of power controllers, 702, 704
workforces, 681

Smart City Platform, 692-693

smart factories, 148

Smart Grid Interoperability Panel (SGIP), 62

smart traffic system fog example, 238-241

smart tunnels, 607

SMC (Stealthwatch Management Console), 445, 453

SNMP (Simple Network Management Protocol), 259

social IoT (SIoT), 98

Society of Automotive Engineers. *See* SAE

software
connected cars, 828-829
disposal, 17
extranet automation, 597
lifecycle processes, 828

Software as a Service. *See* SaaS

software-defined networking. *See* SDN

software-defined PHY (SD-PHY), 213

software-defined radio (SDR), 212-214

software-defined wide-area networks (SD-WANs), 186

software-defined X. *See* SDX

software development kits (SDK), 20

solution technologies, oil and gas upstream environment, 740

Sourcefire Vulnerability Research team (VRT), 456

southbound APIs
fog nodes, 667
ODL, 204
SDN, 191

southbound SDN controller communications, securing, 256-259
authentication, 258
checks and balances, 260
encryption, 258
revocation, 259
SNMP, 259

SP 800-1600 Systems Security Engineering publication, 77

SPD (Security Policy Database), 589

speed

detection services, 820

fog computing, 116

recognition devices, 820

SRIOV (single root I/O virtualization), 283-285

SSL (Secure Sockets Layer), 598

AnyConnect client, 611

configuration, 612

deployment, 611

manufacturing example, 617-621

modules, 612-616

client-based, 600, 612

clientless, 599-611

application access, 604-609

client-based comparison, 600

components, 602

DAP, 609

group policies, 602

oil and gas example, 610-611

portal, 602-603

tunnel groups, 601

HTTPS, 598

multiple solutions, 599

pinning, 357

reverse proxy, 599

stakeholder views, OpenFog Consortium, 137

standards

advantages, 57

alignment, 50

alliances, 56

architectural, 59-61

bodies, 56

business benefits, 54

choices, 54

choosing, 57

connected cars, 826-829

Europe, 827

Japan, 827

SAE International, 827-829

U.K., 827

U.S., 826

considerations, 50-52, 57

consortia, 56

data modeling, 67, 70

defining, 54-56

history, 50

implementation, 53

industrial-focused, 61-63

interoperability, 50-55

legislation, 54

main groups, 58

market-focused, 61-63

next-generation IoT platforms, 292

NFV, 65-67

oil and gas industry security, 757

open, 55

regulatory bodies, 56

reliability, 54

safety, 54

scalability, 54

SDN, 65-67

security, 54, 75-78

smart cities, 685-687

standards bodies, 56

standards development organizations (SDO), 130

state convergence algorithm, 475

static NAT, 424

static SGT assignment, 380

Stealthwatch Flow Collector, 445, 453

Stealthwatch Management Console (SMC), 445

storage
- blockchain, 886
- endpoint collected data, 520
- ICN, 102

structured data, 509

subgroups, identifying, 26

subsymbolic AI, 891-892

SUDI (Secure Unique Device Identification), 328-329

supervised ML, 894

supply chain guidelines, 842-845

SXP (SGT Exchange Protocol), 381

symbolic AI, 891-892

system
- application detectors, 433
- hierarchy
  - *applications, 36*
  - *business processes, 37*
  - *center, 36*
  - *communication nodes, 36*
  - *core networks, 36*
  - *edge networks, 36*
  - *edge nodes, 35*
  - *endpoints, 35*
  - *fog networks, 36*
  - *gateways, 35*
  - *microservices, 36*
  - *services, 37*
  - *things, 35*
- integration, 16
- interaction, 5

System Development Lifecycle. ***See*** **SDLC**

system of systems, smart cities, 690, 699-700

system viewpoint, 89, 106
- cloud computing, 106-112
  - *advantages, 109*
  - *characteristics, 107*
  - *deployment, 107-108*
  - *disadvantages, 110*
- edge computing, 112-113
- fog computing, 112
  - *advantages, 116-118*
  - *communications, 114*
  - *data handling, 115*
  - *disadvantages, 117*
  - *edge computing, compared, 113*
  - *requirements, 115*
- OpenFog reference architecture, 136

T

TALOS (Advanced Malware Protection), 456

TAM (ternary content addressable memory), 374

targeted marketing, connected cars, 815

targets, attacks, 39
- communication, 41-42
- gateways, 40-41
- SDN, 42-43
- things, 39-40

TCP (Transmission Control Protocol), 74

technical assistance, Industry 4.0, 148

technologies
- downstream environment (oil and gas), 750-752
- Gartner Hype Cycle for Engineering Technologies 2017, 879
- lifecycles, 9
- oil and gas industry, 744
- transition, 802
- upstream environment (oil and gas), 739

TEEs (trusted execution environments), 302, 666, 711

telecom industry
- NFV benefits, 219-221
- revenue gap, 218

telemetry sensors, adding to street cabinets, 706-707

Telit Application Enablement Platform, 177

templates

extranet automation, 595

reusable, 469

tenants

AAA, 279-280

execution environments, 302, 666, 711

multitenancy, 296

ternary content addressable memory (TAM), 374

testing

developmental security test and evaluation, 16

penetration, 271

Tetra (Terrestrial Trunked Radio), 820

thing-centric architecture, 32, 92-93

Thing Shadow, 397

things

architectural layer, 85

attack target, 39

attacks, 40

hierarchy, 35

IoT, 3

ThingWorx IoT platform, 176

Thread Group, industrial/market standards, 62

Threat Grid, 458, 465

threats, 8

AI cybersecurity systems, 878

AMP, 456

file policies, 461

FTD, 459-461

point-in-time detection, 456-457

retrospection, 457-458

sandboxing, 458

AnyConnect protection, 616

APTs, 440-441

attack continuum, 11-12

connected cars, 831-834

data breach costs, 418

detecting. *See* IDS

documenting, 27

encrypted network traffic, 451-453

identifying, 27, 878

modeling, 27

NFV, 273

preventing. *See* IPS

public shared platforms, 89

rating, 28

remediation, 878

SDN orchestration, 269

smart cities, 678, 694

TALOS, 456

WannaCry, 454

tiers

Cloud Customer Architecture for IoT, 141

IIRA, 146

time service, 281

TLS (Transport Layer Security), 74, 539

TND (Trusted Network Detection), 613

tokens

authentication, 265

biometric, 360

top IoT platforms for 2018, 176-177

topic exchanges, 545

TouchID, 359

TPM (Trust Platform Module), 355

traditional city operating models, 685

traffic

APTs, 440-441

behavioral analysis, 440-441

contextual information with adaptive network control, pairing, 446

NaaS, 444-446

oil and gas pump station example, 447-450

solutions, 441

visibility protocols, 442-444

encrypted analytics, 450-454

equipment health monitoring example, 780-781

ETA

cryptographic compliance, 454

threat detection, 451-452

WannaCry, 454

offloading, 198

OVS management, 197

packet filtering, 426-427

transactions

blockchain, 886

people-/user-centric approaches, 99

transferable relationships, 414

Transmission Control Protocol (TCP), 74

transport architectural layer, 85

transport encryption, 532

Transport Layer Security (TLS), 74, 539

transport layers, communication, 74

transportation

smart cities, 680

smart traffic fog computing example, 238-241

triggers, smart city event-based video, 710

trust

CRTM, 663

devices, 315, 328

DRTM, 663

execution environments, 302, 666, 711

explicit, 355

IISF, 161

relationships, 171

stores, 355

Trust Platform Module (TPM), 355

Trusted Network Detection (TND), 613

TrustSec, 376-379

classification, 380

controllers, 368

enforcement, 384

fields (Flexible NetFlow), 447

inline tagging, 383

propagation, 381-383

tunnels

smart, 607

SSL VPNs, 601

Twistlock, 654

U

UCS C220 M4 Rack Server, 489

UCS E-Series servers, 489

UDP (User Datagram Protocol), 74

UIs (user interfaces), 297

front-end, 630, 657

management, 627-628

next-generation IoT platforms, 297

U.K. connected car standards, 827

Umbrella, 463

AMP Threat Grid, 465

healthcare industry protection, 465-466

intelligent proxy services, 464-465

response categories, 463

umbrella groups for IoT security, 61

undercloud, back-end platforms, 634

underlying operating systems, securing, 253

uniform resource indicators (URIs), 327

unique identifiers

EUIs, 327

SUDI, 328-329

universal architectures, 89, 120

CPwE, 153

GridBlocks, 153-154
IIRA, 144-146
Industry 4.0, 148-149
NFV-based, 154-156
OPC-UA, 150-152
SDN-based, 154-156
Universal IoT Platform, 176
Universal Plug and Play (UPnP), 42
unstructured data, 511
updates
OTA secure, 855-857
SDN orchestration, 270
upgrading connected car security, 840
UPnP (Universal Plug and Play), 42
upstream environment (oil and gas industry), 733
automation, 742-743
challenges, 743-744
communication and solution technologies, 740
fracking, 739
oil sands mining, 740
overview, 739
urban mobility, smart cities, 680
URIs (uniform resource indicators), 327
U.S.
connected car standards, 826
supply chain guidelines, 845-846
User Datagram Protocol (UDP), 74
users
application detectors, 433
architecture, 98-100
IDs, 637-639
interfaces. *See* UIs
interaction, 124
packet filtering, 432
roles/profiles, 628-630

V

V2C (vehicle-to-cloud), 807
V2D (vehicle-to-device), 808
V2G (vehicle-to-grid), 808
V2I (vehicle-to-infrastructure), 807
V2P (vehicle-to-pedestrian), 807
V2V (vehicle-to-vehicle), 807, 827
V2X (vehicle-to-everything), 802, 808
validation, commands, 782-783
value
automating security, 876
data, 512, 813
oil and gas, 731-734
variety, data, 512, 813
vBranch Function Pack, 490-493
Vector Packet Processing (VPP), 198-200
vectors, attack, 38
vehicle-to-cloud (V2C), 807
vehicle-to-device (V2D), 808
vehicle-to-everything (V2X), 802, 808
vehicle-to-grid (V2G), 808
vehicle-to-infrastructure (V2I), 807
vehicle-to-pedestrian (V2P), 807
vehicle-to-vehicle (V2V), 807, 827
vehicles
care services, 806
maintenance services, 813
tracking, 820
velocity, 813, 876
vendors
ecosystem, 809
smart cities, 689
veracity, data, 813
vertical applications, 679
VFs (virtual functions), 298, 317

VFM (Virtual Function Manager), 245, 300

back-end platform, 648

containerized services, 650

vhosts

clients, adding, 642

RabbitMQ, 546-547

video

cameras, police vehicles, 820

computer vision, 898

event-based, 709-714

data pipeline security, 713-714

deployment, 710-712

triggers, 710

security use case, 309-321

architecture overview, 313

cabinet monitoring, 314

deployment, 316-319

description, 312

preparatory work, 315-316

sequence of events, 319-320

triggers, 312

VIM (Virtual Infrastructure Manager), 228, 300

back-end platform, 648-649

containerized services, 650

Virtual Extensible Lan (VXLAN), 259

Virtual Function Manager. *See* VFM

virtual functions (VFs), 298, 317

Virtual Infrastructure Manager. *See* VIM

virtual LANs. *See* VLANs

Virtual Machines. *See* VMs

virtual network function component (VNFC), 221

Virtual Network Function Descriptor (VNFD) catalog, 470

virtual network functions. *See* VNFs

virtual routing and forwarding (VRF), 23

virtualization

centralized deployment. *See* centralized deployment security example

data, 564

distributed deployment, 486-495

fog nodes, 665

next-generation IoT platforms, 297

power controllers, 702-704

single root I/O, 283-285

VNFs, 278

visibility

Cisco IoT security framework, 170

NaaS, 444-446

protocols, 442-444

visual warning systems, police cars, 820

visualization, 627

VLANs (virtual LANs)

assignments via CoA, 371-374

logical segmentation, 22

VMs (Virtual Machines)

alive rule, 484

centralized security example, 469

NFVIS supported, 490

overloaded/underloaded rules, 484

scaling, 481

SRIOV, 283-285

VM_ALIVE KPI script, 480-481

VM_ALIVE rule, 484

VM_OVERLOADED rule, 484

VM_UNDERLOADED_EMPTY rule, 484

VMware IoT platform key areas, 288

VNFs (virtual network functions), 154, 187

activation status, 474

centralized deployment, 419

crashes, 275

fulfillment and assurance sequences, 474-475 monitoring, 475

dynamic mapping, 478

ESC, 476-477

fulfillment and assurance sequences, 479-480

KPI monitoring methods, 479

prerequisites, 475

VM alive script, 480-481

OFL alignment, 67, 211

performance isolation, 278

private keys, 276-278

time service authentication, 281

virtualization, 278

VNFC (virtual network function component), 221

VNFD (Virtual Network Function Descriptor) catalog, 470

VNFM (VNF manager), 227, 274

volume, data, 813

VPNs

AnyConnect client, 612-613

extranets. *See* extranets

remote access SSL-based. *See* remote-access SSL-based VPNs

site-to-site IPsec, 576

IKEv1 phase 1, 579-582, 586-587

IKEv1 phase 2, 582-584, 588

IKEv2 phase 1, 586-587

IKEv2 phase 2, 584-588

IKEv2 versus IKEv1, 586

VPP (Vector Packet Processing), 198-200

VRF (virtual routing and forwarding), 23

VRT (Vulnerability Research team), 456

vulnerabilities

connected cars, 836-840

JavaScript, 635

oil and gas industry security, 754

VXLAN (Virtual Extensible Lan), 259

W

WANs (wide-area networks), 214-217

WannaCry, 454

Watson, 176

WAVE (Wireless Access in Vehicular Environments) standards, 826

weaknesses, IDS/IPS, 439-440

wearables, police vehicles, 821

web application detectors, 434

websites

AIOTI, 59

ATIS, 65

BBF, 65

BRSKI Internet Draft, 330

CIGRE, 66

Cisco Kinetic IoT Platform, 177

CPwE, 153

CSA, 77

DDS, 105

EdgeX Foundry, 177

ETSI, 59, 66, 76

FD.io, 198

GridBlocks, 153

I am the Cavalry, 77

IBM Bluemix, 177

IEC 62351 standard, 78

IEC 62443 standard, 78

IEEE, 59, 66, 76

IETF, 60, 66

IIC, 61, 78

Intel IoT Platform, 177

IoT

IAP, 77

Global Council, 78

IoTivity, 60

Security Foundation, 76

IPSO Alliance, 60

IRTF, 60, 66, 78

ISOC, 66
ITS, 826
ITU-T, 60, 66
MAPI, 62
MEF, 66
NERC, 78
NIST, 77
NIST SP 800-1600 Systems Security Engineering publication, 77
OASIS, 61
Object Management Group, 60
OCF, 60
ODCA, 67
ODVA, 61
OFC, 61
OIF, 67
oneM2M, 62
ONF, 67
OPC, 62
Open API Initiative, 61
Open Group Open Process Automation, 61
OpenDaylight Foundation, 67
OPNFV, 67
OTA, 76
OWASP, 76, 168
PCS PWG, 77
RelayR IoT Middleware, 177
SAP Cloud Platform, 177
Secure Technology Alliance, 76
SGIP, 62
Telit Application Enablement Platform, 177
Thread Group, 62

web-type ACLs, 606

wide-area networks (WANs), 214, 217

Wi-Fi hotspots

police vehicles, 821
security, 861-862

wireless attacks, 41

Wireless Access in Vehicular Environments (WAVE), 826

workforces, smart cities, 681

X

X.509 certificates, 352-353, 390

X-centric architecture, 89-97

cloud-centric, 95-96
data-centric, 104-105
enterprise-centric, 96-97
Gartner-defined centric views, 97
gateway-centric, 94-95
hub-centric, 94
information-centric. *See* ICN
mobile-centric, 93-94
people-/user-centric, 98-100
thing-centric, 92-93

XMPP (Extensible Messaging and Presence Protocol), 74, 258

XSS (cross-site scripting), 635

Y

YANG, 68

building blocks, 304-306
deployment preparations, 316
Function Pack, 306
MUD, 391

Z

zoning

connected car security, 857-858
PMU, 23

ZT (ZeroTouch), 667