1.	Record Nr.	UNINA9910821709903321
	Titolo	Comprehensive guide to 5G security / / edited by Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, Mika Ylianttila
	Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, , 2018 [Piscataqay, New Jersey] : , : IEEE Xplore, , [2018]
	ISBN	1-119-29305-7 1-119-29308-1 1-119-29307-3
	Edizione	[1st edition]
	Descrizione fisica	1 online resource (441 pages) : illustrations
	Disciplina	005.8
	Soggetti	Mobile communication systems - Security measures Wireless communication systems - Security measures
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	The Editors xvii -- About the Contributors xxi -- Foreword xxxiii -- Preface xxxv -- Acknowledgements xli -- Part I 5G Security Overview 1 -- 1 Evolution of Cellular Systems 3 /Shahriar Shahabuddin, Sadiqur Rahaman, Faisal Rehman, Ijaz Ahmad, and Zaheer Khan -- 1.1 Introduction 3 -- 1.2 Early Development 4 -- 1.3 First Generation Cellular Systems 6 -- 1.3.1 Advanced Mobile Phone Service 7 -- 1.3.2 Security in 1G 7 -- 1.4 Second Generation Cellular Systems 8 -- 1.4.1 Global System for Mobile Communications 8 -- 1.4.2 GSM Network Architecture 9 -- 1.4.3 Code Division Multiple Access 10 -- 1.4.4 Security in 2G 10 -- 1.4.5 Security in GSM 11 -- 1.4.5.1 IMSI 11 -- 1.4.5.2 Ki 12 -- 1.4.5.3 A3 Algorithm 12 -- 1.4.5.4 A8 Algorithm 13 -- 1.4.5.5 COMP128 14 -- 1.4.5.6 A5 Algorithm 14 -- 1.4.6 Security in IS?]95 14 -- 1.5 Third Generation Cellular Systems 15 -- 1.5.1 CDMA 2000 15 -- 1.5.2 UMTS WCDMA 15 -- 1.5.3 UMTS Network Architecture 16 -- 1.5.4 HSPA 17 -- 1.5.5 Security in 3G 17 -- 1.5.6 Security in CDMA2000 17 -- 1.5.7 Security in UMTS 18 -- 1.6 Cellular Systems beyond 3G 20 -- 1.6.1 HSPA+ 20 -- 1.6.2 Mobile WiMAX 20 -- 1.6.3 LTE 21 -- 1.6.3.1 Orthogonal Frequency Division Multiplexing (OFDM) 21 -- 1.6.3.2 SC?]FDE and SC?]FDMA 21 -- 1.6.3.3 Multi?]

antenna Technique 21 -- 1.6.4 LTE Network Architecture 21 -- 1.7 Fourth Generation Cellular Systems 22 -- 1.7.1 Key Technologies of 4G 23 -- 1.7.1.1 Enhanced MINO 23 -- 1.7.1.2 Cooperative Multipoint Transmission and Reception for LTE?]Advanced 23 -- 1.7.1.3 Spectrum and Bandwidth Management 24 -- 1.7.1.4 Carrier Aggregation 24 -- 1.7.1.5 Relays 24 -- 1.7.2 Network Architecture 24 -- 1.7.3 Beyond 3G and 4G Cellular Systems Security 25 -- 1.7.4 LTE Security Model 26 -- 1.7.5 Security in WiMAX 26 -- 1.8 Conclusion 27 -- References 28 -- 2 5G Mobile Networks: Requirements, Enabling Technologies, and Research Activities 31 /Van?]Giang Nguyen, Anna Brunstrom, Karl?] Johan Grinnemo, and Javid Taheri -- 2.1 Introduction 31 -- 2.1.1 What is 5G? 31.

2.1.1.1 From a System Architecture Perspective 32 -- 2.1.1.2 From the Spectrum Perspective 32 -- 2.1.1.3 From a User and Customer Perspective 32 -- 2.1.2 Typical Use Cases 32 -- 2.2 5G Requirements 33 -- 2.2.1 High Data Rate and Ultra Low Latency 34 -- 2.2.2 Massive Connectivity and Seamless Mobility 35 -- 2.2.3 Reliability and High Availability 35 -- 2.2.4 Flexibility and Programmability 36 -- 2.2.5 Energy, Cost and Spectrum Efficiency 36 -- 2.2.6 Security and Privacy 36 -- 2.3 5G Enabling Technologies 37 -- 2.3.1 5G Radio Access Network 38 -- 2.3.1.1 mmWave Communication 38 -- 2.3.1.2 Massive MIMO 38 -- 2.3.1.3 Ultra?]Dense Small Cells 39 -- 2.3.1.4 M2M and D2D Communications 40 -- 2.3.1.5 Cloud?]based Radio Access Network 42 -- 2.3.1.6 Mobile Edge and Fog Computing 42 -- 2.3.2 5G Mobile Core Network 44 -- 2.3.2.1 Software Defined Networking 44 -- 2.3.2.2 Network Function Virtualization 44 -- 2.3.2.3 Cloud Computing 46 -- 2.3.3 G End?]to?]End System 46 -- 2.3.3.1 Network Slicing 46 -- 2.3.3.2 Management and Orchestration 47 -- 2.4 5G Standardization Activities 48 -- 2.4.1 ITU Activities 48 -- 2.4.1.1 ITU?]R 49 -- 2.4.1.2 ITU?]T 49 -- 2.4.2 3GPP Activities 49 -- 2.4.2.1 Pre?]5G Phase 49 -- 2.4.2.2 5G Phase I 50 -- 2.4.2.3 5G Phase II 50 -- 2.4.3 ETSI Activities 50 -- 2.4.4 IEEE Activities 51 -- 2.4.5 IETF Activities 52 -- 2.5 5G Research Communities 52 -- 2.5.1 European 5G Related Activities 52 -- 2.5.1.1 5G Research in EU FP7 52 -- 2.5.1.2 5G Research in EU H2020 52 -- 2.5.1.3 5G Research in Celtic?]Plus 53 -- 2.5.2 Asian 5G Related Activities 53 -- 2.5.2.1 South Korea: 5G Forum 53 -- 2.5.2.2 Japan: 5GMF Forum 54 -- 2.5.2.3 China: IMT?]2020 5G Promotion Group 54 -- 2.5.3 American 5G Related Activities 54 -- 2.6 Conclusion 55 -- 2.7 Acknowledgement 55 -- References 55 -- 3 Mobile Networks Security Landscape 59 /Ahmed Bux Abro -- 3.1 Introduction 59 -- 3.2 Mobile Networks Security Landscape 59 -- 3.2.1 Security Threats and Protection for 1G 61 -- 3.2.2 Security Threats and Protection for 2G 61.

3.2.3 Security Threats and Protection for 3G 63 -- 3.2.4 Security Threats and Protection for 4G 63 -- 3.2.4.1 LTE UE (User Equipment) Domain Security 64 -- 3.2.4.2 LTE (Remote Access Network) Domain Security 65 -- 3.2.4.3 LTE Core Network Domain Security 65 -- 3.2.4.4 Security Threat Analysis for 4G 65 -- 3.2.5 Security Threats and Protection for 5G 66 -- 3.2.5.1 Next Generation Threat Landscape for 5G 68 -- 3.2.5.2 IoT Threat Landscape 68 -- 3.2.5.3 5G Evolved Security Model 68 -- 3.2.5.4 5G Security Threat Analysis 69 -- 3.3 Mobile Security Lifecycle Functions 70 -- 3.3.1 Secure Device Management 71 -- 3.3.2 Mobile OS and App Patch Management 71 -- 3.3.3 Security Threat Analysis and Assessment 71 -- 3.3.4 Security Monitoring 72 -- 3.4 Conclusion 73 -- References 73 -- 4 Design Principles for 5G Security 75 /Ijaz Ahmad, Madhusanka Liyanage, Shahriar Shahabuddin, Mika Ylianttila, and Andrei Gurtov -- 4.1 Introduction 75 -- 4.2 Overviews of Security Recommendations and Challenges 76 -- 4.2.1 Security Recommendations by ITU?]T 77 --

4.2.2 Security Threats and Recommendations by NGMN 78 -- 4.2.3 Other Security Challenges 79 -- 4.2.3.1 Security Challenges in the Access Network 79 -- 4.2.3.2 DoS Attacks 79 -- 4.2.3.3 Security Challenges in the Control Layer or Core Network 80 -- 4.3 Novel Technologies for 5G Security 81 -- 4.3.1 5G Security Leveraging NFV 82 -- 4.3.2 Network Security Leveraging SDN 83 -- 4.3.3 Security Challenges in SDN 84 -- 4.3.3.1 Application Layer 84 -- 4.3.3.2 Controller Layer 85 -- 4.3.3.3 Infrastructure Layer 86 -- 4.3.4 Security Solutions for SDN 86 -- 4.3.4.1 Application Plane Security 86 -- 4.3.4.2 Control Plane Security 87 -- 4.3.4.3 Data Plane Security Solutions 87 -- 4.4 Security in SDN?]based Mobile Networks 88 -- 4.4.1 Data Link Security 88 -- 4.4.2 Control Channels Security 89 -- 4.4.3 Traffic Monitoring 91 -- 4.4.4 Access Control 91 -- 4.4.5 Network Resilience 91 -- 4.4.6 Security Systems and Firewalls 92 -- 4.4.7 Network Security Automation 92.

4.5 Conclusions and Future Directions 94 -- 4.6 Acknowledgement 95 -- References 95 -- 5 Cyber Security Business Models in 5G 99 /Julius Francis Gomes, Marika Iivari, Petri Ahokangas, Lauri Isotalo, Bengt Sahlin, and Jan Mel&eacute;n -- 5.1 Introduction 99 -- 5.2 The Context of Cyber Security Businesses 100 -- 5.2.1 Types of Cyber Threat 101 -- 5.2.2 The Cost of Cyber?]Attacks 102 -- 5.3 The Business Model Approach 103 -- 5.3.1 The 4C Typology of the ICT Business Model 104 -- 5.3.2 Business Models in the Context of Cyber Preparedness 105 -- 5.4 The Business Case of Cyber Security in the Era of 5G 106 -- 5.4.1 The Users and Issues of Cyber Security in 5G 108 -- 5.4.2 Scenarios for 5G Security Provisioning 109 -- 5.4.3 Delivering Cyber Security in 5G 110 -- 5.5 Business Model Options in 5G Cyber Security 112 -- 5.6 Acknowledgment 114 -- References 114 -- Part II 5G Network Security 117 -- 6 Physical Layer Security 119 /Simone Soderi, Lorenzo Mucchi, Matti H&auml;m&auml;l&auml;inen, Alessandro Piva, and Jari Iinatti -- 6.1 Introduction 119 -- 6.1.1 Physical Layer Security in 5G Networks 120 -- 6.1.2 Related Work 121 -- 6.1.3 Motivation 121 -- 6.2 WBPLSec System Model 123 -- 6.2.1 Transmitter 124 -- 6.2.2 Jamming Receiver 126 -- 6.2.3 Secrecy Metrics 126 -- 6.2.4 Secrecy Capacity of WBPLSec 128 -- 6.2.5 Secrecy Capacity of iJAM 129 -- 6.3 Outage Probability of Secrecy Capacity of a Jamming Receiver 131 -- 6.3.1 Simulation Scenario for Secrecy Capacity 134 -- 6.4 WBPLSec Applied to 5G networks 136 -- 6.5 Conclusions 138 -- References 139 -- 7 5G?] WLAN Security 143 /Satish Anamalamudi, Abdur Rashid Sangi, Mohammed Alkatheiri, Fahad T. Bin Muhaya, and Chang Liu -- 7.1 Chapter -- Overview 143 -- 7.2 Introduction to WiFi?]5G Networks Interoperability 143 -- 7.2.1 WiFi (Wireless Local Area Network) 143 -- 7.2.2 Interoperability of WiFi with 5G Networks 144 -- 7.2.3 WiFi Security 144 -- 7.3 Overview of Network Architecture for WiFi?]5G Networks Interoperability 146 -- 7.3.1 MAC Layer 147.

7.3.2 Network Layer 147 -- 7.3.3 Transport Layer 148 -- 7.3.4 Application Layer 149 -- 7.4 5G?]WiFi Security Challenges 150 -- 7.4.1 Security Challenges with Respect to a Large Number of Device Connectivity 151 -- 7.4.2 Security Challenges in 5G Networks and WiFi 151 -- 7.5 Security Consideration for Architectural Design of WiFi?]5G Networks 156 -- 7.5.1 User and Device Identity Confidentiality 156 -- 7.5.2 Integrity 156 -- 7.5.3 Mutual Authentication and Key Management 157 -- 7.6 LiFi Networks 158 -- 7.7 Introduction to LiFi?] 5G Networks Interoperability 159 -- 7.8 5G?]LiFi Security Challenges 160 -- 7.8.1 Security Challenges with Respect to a Large Number of Device Connectivity 160 -- 7.8.2 Security Challenges in 5G Networks and LiFi 160 -- 7.9 Security Consideration for Architectural Design of LiFi?]5G Networks 160 -- 7.10 Conclusion and Future Work 161 --

References 161 -- 8 Safety of 5G Network Physical Infrastructures 165 /Rui Travanca and Jo&atilde;o Andr&eacute; -- 8.1 Introduction 165 -- 8.2 Historical Development 168 -- 8.2.1 Typology 168 -- 8.2.2 Codes 170 -- 8.2.3 Outlook 170 -- 8.3 Structural Design Philosophy 171 -- 8.3.1 Basis 171 -- 8.3.2 Actions 174 -- 8.3.3 Structural Analysis 179 -- 8.3.4 Steel Design Verifications 180 -- 8.3.4.1 Ultimate Limit States 180 -- 8.3.4.2 Serviceability Limit States 181 -- 8.4 Survey of Problems 181 -- 8.4.1 General 181 -- 8.4.2 Design Failures 182 -- 8.4.3 Maintenance Failures 183 -- 8.4.4 Vandalism or Terrorism Failures 186 -- 8.5 Opportunities and Recommendations 188 -- 8.6 Acknowledgement 190 -- References 191 -- 9 Customer Edge Switching: A Security Framework for 5G 195 /Hammad Kabir, Raimo Kantola, and Jesus Llorente Santos -- 9.1 Introduction 195 -- 9.2 State?]of?]the?]art in Mobile Networks Security 197 -- 9.2.1 Mobile Network Challenges and Principles of Security Framework 200 -- 9.2.2 Trust Domains and Trust Processing 202 -- 9.3 CES Security Framework 203 -- 9.3.1 DNS to Initiate Communication 205 -- 9.3.2 CETP Policy?]based Communication 206.

9.3.3 Policy Architecture 208 -- 9.3.4 CES Security Mechanisms 209 -- 9.3.5 Realm Gateway 210 -- 9.3.6 RGW Security Mechanisms 211 -- 9.3.6.1 Name Server Classification and Allocation Model 212 -- 9.3.6.2 Preventing DNS Abuse 212 -- 9.3.6.3 Bot?]Detection Algorithm 213 -- 9.3.6.4 TCP?]Splice 213 -- 9.4 Evaluation of CES Security 213 -- 9.4.1 Evaluating the CETP Policy?]based Communication 214 -- 9.4.1.1 Security Testing 216 -- 9.4.1.2 Outcomes of the Security Testing 216 -- 9.4.2 Evaluation of RGW Security 217 -- 9.5 Deployment in 5G Networks 222 -- 9.5.1 Use Case 1: Mobile Broadband 224 -- 9.5.1.1 Deployment and Operations 224 -- 9.5.1.2 Security Benefits 224 -- 9.5.1.3 Scalability 225 -- 9.5.1.4 Reliability 225 -- 9.5.2 Use Case 2: Corporate Gateway 225 -- 9.5.2.1 Deployment and Operations 225 -- 9.5.2.2 Security Benefits 226 -- 9.5.2.3 Scalability 226 -- 9.5.2.4 Reliability 226 -- 9.5.3 Use Case 3: National CERT Centric Trust Domain 226 -- 9.5.3.1 Deployment and Operations 226 -- 9.5.3.2 Security Benefits 227 -- 9.5.3.3 Scalability 227 -- 9.5.3.4 Reliability 227 -- 9.5.4 Use Case 4: Industrial Internet for Road Traffic and Transport 227 -- 9.5.4.1 Deployment and Operations 227 -- 9.5.4.2 Security Benefits 228 -- 9.5.4.3 Scalability 228 -- 9.5.4.4 Reliability 228 -- 9.6 Conclusion 228 -- References 230 -- 10 Software Defined Security Monitoring in 5G Networks 231 /Madhusanka Liyanage, Ijaz Ahmad, Jude Okwuibe, Edgardo Montes de Oca, Mai Hoang Long, Oscar Lopez Perez, and Mikel Uriarte Itzazelaia -- 10.1 Introduction 231 -- 10.2 Existing Monitoring Techniques 232 -- 10.3 Limitations on Current Monitoring Techniques 233 -- 10.4 Use of Monitoring in 5G 234 -- 10.5 Software?]Defined Monitoring Architecture 235 -- 10.6 Expected Advantages of Software Defined Monitoring 238 -- 10.7 Expected Challenges in Software Defined Monitoring 240 -- 10.8 Conclusion 242 -- References 243 -- Part III 5G Device and User Security 245 -- 11 IoT Security 247 /Mehrnoosh Monshizadeh, and Vikramajeet Khatri.

11.1 Introduction 247 -- 11.2 Related Work 248 -- 11.3 Literature Overview and Research Motivation 249 -- 11.3.1 IoT Devices, Services and Attacks on Them 250 -- 11.3.2 Research Motivation 253 -- 11.4 Distributed Security Platform 254 -- 11.4.1 Robot Data Classification 254 -- 11.4.2 Robot Attack Classification 255 -- 11.4.3 Robot Security Platform 256 -- 11.4.3.1 Robot Section 257 -- 11.4.3.2 Mobile Network Section 257 -- 11.5 Mobile Cloud Robot Security Scenarios 259 -- 11.5.1 Robot with SIMcard 259 -- 11.5.2 SIMless Robot 260 -- 11.5.3 Robot Attack 263 -- 11.5.4 Robot Communication 263 -- 11.6

Conclusion 263 -- References 265 -- 12 User Privacy, Identity and Trust 267 /Tanesh Kumar, Madhusanka Liyanage, Ijaz Ahmad, An Braeken, and Mika Ylianttila -- 12.1 Introduction 267 -- 12.2 Background 268 -- 12.3 User Privacy 269 -- 12.3.1 Data Privacy 269 -- 12.3.2 Location Privacy 271 -- 12.3.3 Identity Privacy 272 -- 12.4 Identity Management 273 -- 12.5 Trust Models 274 -- 12.6 Discussion 277 -- 12.7 Conclusion 278 -- References 279 -- 13 5G Positioning: Security and Privacy Aspects 281 /Elena Simona Lohan, Anette Al&eacute;n?]Savikko, Liang Chen, Kimmo J&auml;rvinen, Helena Lepp&auml;koski, Heidi Kuusniemi, and P&auml;ivi Korpisaari -- 13.1 Introduction 281 -- 13.2 Outdoor versus Indoor Positioning Technologies 283 -- 13.3 Passive versus Active Positioning 283 -- 13.4 Brief Overview of 5G Positioning Mechanisms 285 -- 13.5 Survey of Security Threats and Privacy Issues in 5G Positioning 291 -- 13.5.1 Security Threats in 5G Positioning 291 -- 13.5.1.1 Security Threats Affecting Several or All Players 291 -- 13.5.1.2 Security Threats Affecting LISP 292 -- 13.5.1.3 Security Threats Affecting LBSP 293 -- 13.5.1.4 Security Threats Affecting the 5G User Device or LIC 293 -- 13.6 Main Privacy Concerns 294 -- 13.7 Passive versus Active Positioning Concepts 295 -- 13.8 Physical?] Layer Based Security Enhancements Mechanisms for Positioning in 5G 296 -- 13.8.1 Reliability Monitoring and Outlier Detection Mechanisms 296.

13.8.2 Detection, Location and Estimation of Interference Signals 297 -- 13.8.3 Backup Systems 298 -- 13.9 Enhancing Trustworthiness 299 -- 13.10 Cryptographic Techniques for Security and Privacy of Positioning 299 -- 13.10.1 Cryptographic Authentication in Positioning 300 -- 13.10.2 Cryptographic Distance?]Bounding 301 -- 13.10.3 Cryptographic Techniques for Privacy?]Preserving Location?]based Services 303 -- 13.11 Legislation on User Location Privacy in 5G 304 -- 13.11.1 EU Policy and Legal Framework 304 -- 13.11.2 Legal Aspects Related to the Processing of Location Data 306 -- 13.11.3 Privacy Protection by Design and Default 306 -- 13.11.4 Security Protection 307 -- 13.11.5 A Closer Look at the e?]Privacy Directive 307 -- 13.11.6 Summary of EU Legal Instruments 308 -- 13.11.7 International Issues 308 -- 13.11.8 Challenges and Future Scenarios in Legal Frameworks and Policy 309 -- 13.12 Landscape of the European and International Projects related to Secure Positioning 311 -- References 312 -- Part IV 5G Cloud and Virtual Network Security 321 -- 14 Mobile Virtual Network Operators (MVNO) Security 323 /Mehrnoosh Monshizadeh and Vikramajeet Khatri -- 14.1 Introduction 323 -- 14.2 Related Work 324 -- 14.3 Cloudification of the Network Operators 325 -- 14.4 MVNO Security 326 -- 14.4.1 Data Security in TaaS 327 -- 14.4.2 Hypervisor and VM Security in TaaS 328 -- 14.4.2.1 SDN Security in TaaS 329 -- 14.4.2.2 NFV Security in TaaS 331 -- 14.4.2.3 OPNFV Security 332 -- 14.4.3 Application Security in TaaS 333 -- 14.4.4 Summary 334 -- 14.4.5 MVNO Security Benchmark 335 -- 14.5 TaaS Deployment Security 338 -- 14.5.1 IaaS 338 -- 14.5.2 PaaS 340 -- 14.5.3 SaaS 340 -- 14.6 Future Directions 340 -- 14.7 Conclusion 341 -- References 342 -- 15 NFV and NFV?]based Security Services 347 /Wenjing Chu -- 15.1 Introduction 347 -- 15.2 5G, NFV and Security 347 -- 15.3 A Brief Introduction to NFV 348 -- 15.4 NFV, SDN, and a Telco Cloud 351 -- 15.5 Common NFV Drivers 353 -- 15.5.1 Technology Curve 353.

15.5.2 Opportunity Cost and Competitive Landscape 353 -- 15.5.3 Horizontal Network Slicing 354 -- 15.5.4 Multi?]Tenancy 354 -- 15.5.5 Rapid Service Delivery 354 -- 15.5.6 XaaS Models 354 -- 15.5.7 One Cloud 355 -- 15.6 NFV Security: Challenges and Opportunities 355 -- 15.6.1 VNF Security Lifecycle and Trust 355 -- 15.6.2 VNF Security in

Operation 358 -- 15.6.3 Multi?]Tenancy and XaaS 359 -- 15.6.4 OPNFV and Openstack: Open Source Projects for NFV 360 -- 15.7 NFV?]based Security Services 364 -- 15.7.1 NFV?]based Network Security 365 -- 15.7.1.1 Virtual Security Appliances 365 -- 15.7.1.2 Distributed Network Security Services 366 -- 15.7.1.3 Network Security as a Service 366 -- 15.7.2 Policy?]based Security Services 366 -- 15.7.2.1 Group?] based Policy 367 -- 15.7.2.2 Openstack Congress 368 -- 15.7.3 Machine Learning for NFV?]based Security Services 369 -- 15.8 Conclusions 370 -- References 370 -- 16 Cloud and MEC Security 373 /Jude Okwuibe, Madhusanka Liyanage, Ijaz Ahmed, and Mika Ylianttila -- 16.1 Introduction 373 -- 16.2 Cloud Computing in 5G Networks 374 -- 16.2.1 Overview and History of Cloud Computing 375 -- 16.2.2 Cloud Computing Architecture 376 -- 16.2.3 Cloud Deployment Models 377 -- 16.2.4 Cloud Service Models 378 -- 16.2.5 5G Cloud Computing Architecture 379 -- 16.2.6 Use Cases/Scenarios of Cloud Computing in 5G 380 -- 16.3 MEC in 5G Networks 381 -- 16.3.1 Overview of MEC Computing 381 -- 16.3.2 MEC in 5G 383 -- 16.3.3 Use Cases of MEC Computing in 5G 384 -- 16.4 Security Challenges in 5G Cloud 385 -- 16.4.1 Virtualization Security 385 -- 16.4.2 Cyber?] Physical System (CPS) Security 386 -- 16.4.3 Secure and Private Data Computation 386 -- 16.4.4 Cloud Intrusion 387 -- 16.4.5 Access Control 387 -- 16.5 Security Challenges in 5G MEC 388 -- 16.5.1 Denial of Service (DoS) Attack 389 -- 16.5.2 Man?]in?]the?]Middle (MitM) 389 -- 16.5.3 Inconsistent Security Policies 389 -- 16.5.4 VM Manipulation 390 -- 16.5.5 Privacy Leakage 390 -- 16.6 Security Architectures for 5G Cloud and MEC 391.

16.6.1 Centralized Security Architectures 391 -- 16.6.2 SDN?]based Cloud Security Systems 392 -- 16.7 5GMEC, Cloud Security Research and Standardizations 392 -- 16.8 Conclusions 394 -- References 394 -- 17 Regulatory Impact on 5G Security and Privacy 399 /Jukka Salo and Madhusanka Liyanage -- 17.1 Introduction 399 -- 17.2 Regulatory Objectives for Security and Privacy 401 -- 17.2.1 Generic Objectives 401 -- 17.3 Legal Framework for Security and Privacy 402 -- 17.3.1 General Framework 402 -- 17.3.2 Legal Framework for Security and Privacy in Cloud Computing 403 -- 17.3.3 Legal Framework for Security and Privacy in Software Defined Networking and Network Function Virtualization 405 -- 17.4 Security and Privacy Issues in New 5G Technologies 405 -- 17.4.1 Security and Privacy Issues in Cloud Computing 405 -- 17.4.2 Security and Privacy Issues in Network Functions Virtualization 407 -- 17.4.3 Security and Privacy Issues in Software Defined Networking (SDN) 409 -- 17.4.4 Summary of Security and Privacy Issues in the Context of Technologies under Study (Clouds, NFV, SDN) 410 -- 17.5 Relevance Assessment of Security and Privacy Issues for Regulation 411 -- 17.6 Analysis of Potential Regulatory Approaches 412 -- 17.7 Summary of Issues and Impact of New Technologies on Security and Privacy Regulation 413 -- References 417 -- Index.

Sommario/riassunto

The first comprehensive guide to the design and implementation of security in 5G wireless networks and devices Security models for 3G and 4G networks based on Universal SIM cards worked very well. But they are not fully applicable to the unique security requirements of 5G networks. 5G will face additional challenges due to increased user privacy concerns, new trust and service models and requirements to support IoT and mission-critical applications. While multiple books already exist on 5G, this is the first to focus exclusively on security for the emerging 5G ecosystem. 5G networks are not only expected to be faster, but provide a backbone for many new services, such as IoT and the Industrial Internet. Those services will provide connectivity for

everything from autonomous cars and UAVs to remote health monitoring through body-attached sensors, smart logistics through item tracking to remote diagnostics and preventive maintenance of equipment. Most services will be integrated with Cloud computing and novel concepts, such as mobile edge computing, which will require smooth and transparent communications between user devices, data centers and operator networks. Featuring contributions from an international team of experts at the forefront of 5G system design and security, this book: . Provides priceless insights into the current and future threats to mobile networks and mechanisms to protect it. Covers critical lifecycle functions and stages of 5G security and how to build an effective security architecture for 5G based mobile networks. Addresses mobile network security based on network-centricity, device-centricity, information-centricity and people-centricity views. Explores security considerations for all relative stakeholders of mobile networks, including mobile network operators, mobile network virtual operators, mobile users, wireless users, Internet-of things, and cybersecurity experts Providing a comprehensive guide to state-of-the-art in 5G security theory and practice, A Comprehensive Guide to 5G Security is an important working resource for researchers, engineers and business professionals working on 5G development and deployment.