1. Record Nr. UNINA9910679617403321

Autore	Wheeler Robert R
Titolo	Oil : from prospect to pipeline / / Robert R. Wheeler, Maurine Whited
Pubbl/distr/stampa	Houston : , : Gulf Pub. Co., Book Division, , 1981
ISBN	0-12-799999-X
Edizione	[Fourth edition.]
Descrizione fisica	1 online resource e (xi, 146 pages) : illustrations
Altri autori (Persone)	WhitedMaurine
Disciplina	333.8/232
Soggetti	Petroleum
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph

2. Record Nr. UNISALENTO991003842239707536

Autore	Gerstein, Larry J.
Titolo	Basic quadratic forms / Larry J. Gerstein
Pubbl/distr/stampa	Providence, R. I. : American Mathematical Society, c2008
ISBN	9780821844656 0821844652
Descrizione fisica	xiii, 255 p. : ill. ; 27 cm
Collana	Graduate studies in mathematics, 1065-7339 ; 90
Classificazione	AMS 11E LC QA243.G47
Disciplina	512.74
Soggetti	Forms, Quadratic Equations, Quadratic Number theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references (p. 245-249) and index

3.	Record Nr.	UNINA9910555293703321
	Autore	Liyanage Madhusanka
	Titolo	IoT security : advances in authentication / / edited by Madhusanka Liyanage, School of Computer Science, University College, Ireland, Centre for Wireless Communication, University of Oulu, Finland, An Braeken, Industrial Engineering, Vrije Universiteit Brussel, Belgium, Pardeep Kumar, Department of Computer Science, Swansea University, UK, Mika Yliantilla, Centre for Wireless Communication, University of Oulu, Finland
	Pubbl/distr/stampa	Hoboken : , : Wiley, , 2020 [Piscataqay, New Jersey] : , : IEEE Xplore, , ©2020
	ISBN	1-119-52794-5 1-119-52796-1 1-119-52797-X
	Edizione	[1st edition]
	Descrizione fisica	1 online resource (318 pages)
	Disciplina	005.8
	Soggetti	Internet of things - Security measures
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Cover; Title Page; Copyright; Contents; About the Editors; List of Contributors; Preface; Acknowledgments; Part I IoT Overview; Chapter 1 Introduction to IoT; 1.1 Introduction; 1.1.1 Evolution of IoT; 1.2 IoT Architecture and Taxonomy; 1.3 Standardization Efforts; 1.4 IoT Applications; 1.4.1 Smart Home; 1.4.2 Smart City; 1.4.3 Smart Energy; 1.4.4 Healthcare; 1.4.5 IoT Automotive; 1.4.6 Gaming, AR and VR; 1.4.7 Retail; 1.4.8 Wearable; 1.4.9 Smart Agriculture; 1.4.10 Industrial Internet; 1.4.11 Tactile Internet; 1.4.12 Conclusion; Acknowledgement; References; Chapter 2 Abstract; 2.1 Introduction2.2 Attacks and Countermeasures; 2.2.1 Perception Layer; 2.2.1.1 Perception Nodes; 2.2.1.2 Sensor Nodes; 2.2.1.3 Gateways; 2.2.2 Network Layer; 2.2.2.1 Mobile Communication; 2.2.2.2 Cloud Computing; 2.2.2.3 Internet; 2.2.3 Application Layer; 2.2.3.1 Smart Utilities -- Smart Grids and Smart Metering; 2.2.3.2 Consumer Wearable IoT (WIoT) Devices for Healthcare and Telemedicine; 2.2.3.3 Intelligent Transportation; 2.2.3.4 Smart Agriculture; 2.2.3.5 Industrial IoT (IIoT); 2.2.3.6 Smart Buildings,

Environments, and Cities; 2.3 Authentication and Authorization; 2.3.1 Authentication; 2.3.2 Authorization2.3.3 Authentication at IoT Layers; 2.3.3.1 Perception Layer; 2.3.3.2 Network Layer; 2.3.3.3 Application Layer; 2.4 Other Security Features and Related Issues; 2.4.1 The Simplified Layer Structure; 2.4.2 The Idea of Middleware; 2.4.3 Cross-Layer Security Problem; 2.4.4 Privacy; 2.4.5 Risk Mitigation; 2.5 Discussion; 2.6 Future Research Directions; 2.6.1 Blockchain; 2.6.2 5G; 2.6.3 Fog and Edge Computing; 2.6.4 Quantum Security, AI, and Predictive Data Analytics; 2.6.5 Network Slicing; 2.7 Conclusions; References; Part II IoT Network and Communication Authentication; Chapter 3 Symmetric Key-Based Authentication with an Application to Wireless Sensor Networks3.1 Introduction; 3.2 Related Work; 3.3 System Model and Assumptions; 3.3.1 Design Goals; 3.3.2 Setting; 3.3.3 Notations; 3.3.4 Attack Model; 3.4 Scheme in Normal Mode; 3.4.1 Installation Phase; 3.4.1.1 Installation of CH; 3.4.1.2 Installation of CN; 3.4.2 Group Node Key; 3.4.3 Individual Cluster Key; 3.4.3.1 CN to CH; 3.4.3.2 CH to CN; 3.4.4 Pairwise Key Derivation; 3.4.5 Multicast Key; 3.4.5.1 Initiation by CH; 3.4.5.2 Derivation by CNs; 3.4.6 Group Cluster Key; 3.5 Authentication; 3.5.1 Authentication by CN3.5.2 Authenticated Broadcast by the CH; 3.5.3 Authenticated Broadcast by the BS; 3.6 Scheme in Change Mode; 3.6.1 Capture of CN; 3.6.2 Capture of CH; 3.6.3 Changes for Honest Nodes; 3.6.3.1 Key Update for Honest Node Replacement; 3.6.3.2 Node Removal and Addition; 3.7 Security Analysis; 3.7.1 Resistance Against Impersonation Attack; 3.7.2 Resistance Against Node Capture; 3.7.3 Resistance Against Replay Attacks; 3.8 Efficiency; 3.8.1 Number of Communication Phases; 3.8.2 Storage Requirements; 3.8.3 Packet Fragmentation; 3.9 Conclusions; Acknowledgement; References; Chapter 4 Public Key Based Protocols -- EC Crypto

Sommario/riassunto

"The Internet of things (IoT) is the network of physical devices such as vehicles, home appliances sensors, actuators and other electronic devices. The development of internet offers the possibility for these objects to connect and exchange data. Since IoT will pay a major role in our lives, it is important to secure the IoT ecosystem for its value to be realized. Among the various security requirements, authentication to the IoT is importance since it is the first step to prevent the impact of attackers. The book offers an insight into the development of various authentication mechanisms to provide IoT authentication in various levels such as user level, device level and network level. The user-level authentication identifies whether the IoT user is a legitimate user to access the smart object services and what kind of authentication mechanisms can be used. Network level authentication is needed to check the identity of connected IoT devices. This book, therefore, offers reference material which will be important for all relative stakeholders of mobile networks such as network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations and security solution developers"--