1. Record Nr.   UNINA9910820389703321

   Titolo   Communications and information infrastructure security / / edited by
                       John G. Voeller

   Pubbl/distr/stampa Hoboken, New Jersey : , : John Wiley & Sons, , 2014
                       ©2014

   ISBN   1-118-65183-9
                       1-118-65170-7

   Descrizione fisica 1 online resource (124 p.)

   Altri autori (Persone) VoellerJohn G

   Disciplina   005.8

   Soggetti   Computer networks - Security measures

   Lingua di pubblicazione Inglese

   Formato   Materiale a stampa

   Livello bibliografico Monografia

   Note generali   Description based upon print version of record.

   Nota di bibliografia Includes bibliographical references and index.

   Nota di contenuto   Cover; Title Page; Contents; Preface; Chapter 1 Telecommunication:
                       Critical Infrastructure Protection; 1.1 Introduction; 1.2 Overview; 1.3
                       Evolutionary Forces That Shape the Sector; 1.3.1 Unregulated
                       Beginnings; 1.3.2 The Telecom War; 1.3.3 Regulatory Period; 1.7.1 The
                       Hubs: Telecom Hotels; 1.3.4 Deregulated Oligopolies; 1.4 Major
                       Components of the Sector; 1.5 Resiliency of Networks; 1.5.1 Hubs,
                       Clusters, and Betweeners; 1.5.2 Betweenness; 1.6 Resilience Results;
                       1.6.1 Cascade Resiliency; 1.6.2 Flow Resiliency; 1.7
                       Telecommunications Criticality; 1.7.2 Self-Organized Criticality
                       1.8 Final AnalysisReferences; Further Reading; Chapter 2 Strategies for
                       Protecting the Telecommunications Sector; 2.1 Introduction; 2.2
                       Background; 2.2.1 A Historical Perspective; 2.2.2 What Makes Up The
                       Telecommunications Sector?; 2.2.3 How Do We Secure the
                       Telecommunications Sector?; 2.2.4 What are Critical
                       Telecommunications Infrastructure Systems and Assets?; 2.2.5 What is
                       the U.S. Policy on Protecting National Critical Telecommunications
                       Services and Computer-Driven Systems?; 2.3 Threats, Challenges, and
                       Continuous Improvement; 2.3.1 The General Threat Assessment
                       2.3.2 The Threat to America's Telecommunications Components2.3.3
                       The Threat to America's Internet Networks; 2.4 Telecommunications
                       Challenges and Continuous Improvement; 2.5 Conclusions; 2.5.1
                       Performance, Reliability and Efficiency; 2.5.2 The Threat to America's

Telecommunications Sector; 2.5.3 Future Research Direction; 2.5.4 The Prospects for the Future; References; Further Reading; Chapter 3 Wireless Security; 3.1 Scientific Overview; 3.1.1 Voice-Centric Networks; 3.1.2 Data-Centric Networks; 3.2 Mobile and Wireless Security Landscape; 3.2.1 Federal Legislation and Regulation 3.2.2 Federal Standards and Guidance Publications3.2.3 Industry Standards and Guidance Organizations; 3.2.4 Governmental Wireless Communications Initiatives; 3.3 Critical Needs Analysis; 3.3.1 Intrusion Prevention Systems; 3.3.2 Internet-Based Security Protocols; 3.4 Research Directions; 3.4.1 Intrusion Prevention Systems; 3.4.2 Internet-Based Security Protocols; 3.4.3 Overlaying Security Services over IP-based Access Networks; 3.4.4 Mobile Device Security; References; Further Reading; Chapter 4 Detection of Hidden Information, Covert Channels and Information Flows; 4.1 Introduction 4.2 Scientific Overview4.2.1 Hiding Information; 4.3 Countermeasures; 4.3.1 Countermeasures: Detection; 4.3.2 Countermeasures: Disruption; 4.4 Research and Development Trends; 4.4.1 Research Trends; 4.4.2 Development Trends; 4.5 Critical Needs Analysis; 4.6 Research Directions; References; Further Reading; Other Suggested Reading; Chapter 5 Inherently Secure Next-Generation Computing and Communication Networks for Reducing Cascading Impacts; 5.1 Introduction; 5.2 Standards, Guidelines, and Best Practices; 5.3 Standards; 5.3.1 Guidelines; 5.4 Best Practice 5.4.1 Cyber and Control Systems Security Standards in Common Use

| Sommario/riassunto | Communication and Information Systems Security features articles from the Wiley Handbook of Science and Technology for Homeland Security covering strategies for protecting the telecommunications sector, wireless security, advanced web based technology for emergency situations. Science and technology for critical infrastructure consequence mitigation are also discussed. |