1. Record Nr. UNINA9910143565003321

Autore	Douligeris C (Christos)
Titolo	Network security : current status and future directions / / edited by Christos Douligeris ; Dimitrios N. Serpanos
Pubbl/distr/stampa	Hoboken, N.J., : Wiley Chichester, : John Wiley [distributor], 2007
ISBN	0-470-65356-6 1-280-90006-7 9786610900060 0-470-09974-7 0-470-09973-9
Descrizione fisica	1 online resource (592 p.)
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security
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	Preface. -- Contributors. -- 1. Computer Network Security: Basic Background and Current Issues (Panayiotis Kotzanikolaou and Christos Douligeris). -- 1.1 Some Terminology on Network Security. -- 1.2 ISO/OSI Reference Model for Networks. -- 1.3 Network Security Attacks. -- 1.4 Mechanisms and Controls for Network Security: Book Overview and Structure. -- References. -- Part One Internet Security. -- 2. Secure Routing (Ioannis Avramopoulos, Hisashi Kobayashi, Arvind Krishnamurthy, and Randy Wang). -- 2.1 Introduction. -- 2.2 Networking Technologies. -- 2.3 Attacks in Networks. -- 2.4 State of the Art. -- 2.5 Conclusion and Research Issues. -- References. -- 3. Designing Firewalls: A Survey (Angelos D. Keromytis and Vassilis Prevelakis). -- 3.1 Introduction. -- 3.2 Firewall Classifi cation. -- 3.3 Firewall Deployment: Management. -- 3.4 Conclusions. -- References. -- 4. Security in Virtual Private Networks (Srinivas Sampalli). -- 4.1 Introduction. -- 4.2 VPN Overview. -- 4.3 VPN Benefi ts. -- 4.4 VPN Terminology. -- 4.5 VPN Taxonomy. -- 4.6 IPSec. -- 4.7 Current Research on VPNs. -- 4.8 Conclusions. -- References. -- 5. IP Security

(IPSec) (Anirban Chakrabarti and Manimaran Govindarasu). -- 5.1 Introduction. -- 5.2 IPSec Architecture and Components. -- 5.3 Benefi ts and Applications of IPSec. -- 5.4 Conclusions. -- References. -- 6. IDS for Networks (John C. McEachen and John M. Zachary). -- 6.1 Introduction. -- 6.2 Background. -- 6.3 Modern NIDSs. -- 6.4 Research and Trends. -- 6.5 Conclusions. -- References. -- 7. Intrusion Detection Versus Intrusion Protection (Luis Sousa Cardoso). -- 7.1 Introduction. -- 7.2 Detection Versus Prevention. -- 7.3 Intrusion Prevention Systems: The Next Step in Evolution of IDS. -- 7.4 Architecture Matters. -- 7.5 IPS Deployment. -- 7.6 IPS Advantages. -- 7.7 IPS Requirements: What to Look For. -- 7.8 Conclusions. -- References. -- 8. Denial-of-Service Attacks (Aikaterini Mitrokotsa and Christos Douligeris). -- 8.1 Introduction. -- 8.2 DoS Attacks. 8.3 DDoS Attacks. -- 8.4 DDoS Defense Mechanisms. -- 8.5 Conclusions. -- References. -- 9. Secure Architectures with Active Networks (Srinivas Sampalli, Yaser Haggag, and Christian Labonte). -- 9.1 Introduction. -- 9.2 Active Networks. -- 9.3 SAVE Test bed. -- 9.4 Adaptive VPN Architecture with Active Networks. -- 9.5 (SAM) Architecture. -- 9.6 Conclusions. -- References. -- Part Two Secure Services. -- 10. Security in E-Services andApplications (Manish Mehta, Sachin Singh, and Yugyung Lee). -- 10.1 Introduction. -- 10.2 What Is an E-Service? -- 10.3 Security Requirements for EServices and Applications. -- 10.4 Security for Future EServices. -- References. -- 11. Security in Web Services (Christos Douligeris and George P. Ninios). -- 11.1 Introduction. -- 11.2 Web Services Technologies and Standards. -- 11.3 Web Services Security Standard. -- 11.4 Conclusions. -- References. -- 12. Secure Multicasting (Constantinos Boukouvalas and Anthony G. Petropoulos). -- 12.1 Introduction 205 -- 12.2 IP Multicast. -- 12.3 Application Security Requirements. -- 12.4 Multicast Security Issues. -- 12.5 Data Authentication. -- 12.6 Source Authentication Schemes. -- 12.7 Group Key Management. -- 12.8 Group Management and Secure Multicast Routing. -- 12.9 Secure IP Multicast Architectures. -- 12.10 Secure IP Multicast Standardization Efforts. -- 12.11 Conclusions. -- References. -- 13. Voice Over IP Security (Son Vuong and Kapil Kumar Singh). -- 13.1 Introduction. -- 13.2 Security Issues in VoIP. -- 13.3 Vulnerability Testing. -- 13.4 Intrusion Detection Systems. -- 13.5 Conclusions. -- References. -- 14. Grid Security (Kyriakos Stefanidis, Artemios G. Voyiatzis, and Dimitrios N. Serpanos). -- 14.1 Introduction. -- 14.2 Security Challenges for Grids. -- 14.3 Grid Security Infrastructure. -- 14.4 Grid Computing Environments. -- 14.5 Grid Network Security. -- 14.6 Conclusions and Future Directions. -- References. -- 15. Mobile Agent Security (Panayiotis Kotzanikolaou, Christos Douligeris, Rosa Mavropodi, and Vassilios Chrissikopoulos).
15.1 Introduction. -- 15.2 Taxonomy of Solutions. -- 15.3 Security Mechanisms for Mobile Agent Systems. -- References -- Part Three Mobile and Security. -- 16. Mobile Terminal Security (Olivier Benoit, Nora Dabbous, Laurent Gauteron, Pierre Girard, Helena Handschuh, David Naccache, Stephane Soci, and Claire Whelan). -- 16.1 Introduction. -- 16.2 WLAN and WPAN Security. -- 16.3 GSM and 3GPP Security. -- 16.4 Mobile Platform Layer Security. -- 16.5 Hardware Attacks on Mobile Equipment. -- 16.6 Conclusion. -- References. -- 17. IEEE 802.11 Security (Daniel L. Lough, David J. Robinson, and Ian G. Schneller). -- 17.1 Introduction. -- 17.2 Introduction to IEEE 802.11. -- 17.3 Wired Equivalent Privacy. -- 17.4 Additional IEEE 802.11 Security Techniques. -- 17.5 Wireless Intrusion Detection Systems. -- 17.6 Practical IEEE 802.11 Security Measures. -- 17.7 Conclusions. -- References. -- 18. Bluetooth Security (Christian Gehrmann). -- 18.1

Introduction. -- 18.2 Bluetooth Wireless Technology. -- 18.3 Security Architecture. -- 18.4 Security Weaknesses and Countermeasures. -- 18.5 Bluetooth Security: What Comes Next? -- References. -- 19. Mobile Telecom Networks (Christos Xenakis and Lazaros Merakos). -- 19.1 Introduction. -- 19.2 Architectures Network. -- 19.3 Security Architectures. -- 19.4 Research Issues. -- 19.5 Conclusions. -- References. -- 20. Security in Mobile Ad HocNetworks (Mike Burmester, Panayiotis Kotznanikolaou, and Christos Douligeris). -- 20.1 Introduction. -- 20.2 Routing Protocols. -- 20.3 Security Vulnerabilities. -- 20.4 Preventing Attacks in MANETs. -- 20.5 Trust in MANETs. -- 20.6 Establishing Secure Routes in a MANET. -- 20.7 Cryptographic Tools for MANETs. -- References. -- 21. Wireless Sensor Networks (Artemios G. Voyiatzis and Dimitrios N. Serpanos). -- 21.1 Introduction. -- 21.2 Sensor Devices. -- 21.3 Sensor Network Security. -- 21.4 Future Directions. -- 21.5 Conclusions. -- References. -- 22. Trust (Lidong Chen). -- 22.1 Introduction. -- 22.2 What Is a trust Model?.
22.3 How Trust Models Work? -- 22.4 Where Trust Can Go Wrong? -- 22.5 Why Is It Diffi cult to Defi ne Trust? -- 22.6 Which Lessons Have We Learned? -- References. -- Part Four Trust, Anonymity, and Privacy. -- 23. PKI Systems (Nikos Komninos). -- 23.1 Introduction. -- 23.2 Origins of Cryptography. -- 23.3 Overview of PKI Systems. -- 23.4 Components of PKI Systems. -- 23.5 Procedures of PKI Systems. -- 23.6 Current and Future Aspects of PKI Systems. -- 23.7 Conclusions. -- References. -- 24. Privacy in Electronic Communications (Alf Zugenmaier and Joris Claessens). -- 24.1 Introduction. -- 24.2 Protection from Third Party: Confidentiality. -- 24.3 Protection from Communication Partner. -- 24.4 Invasions of Electronic Private Sphere. -- 24.5 Balancing Privacy with Other Needs. -- 24.6 Structure of Privacy. -- 24.7 Conclusion and Future Trends. -- References. -- 25. Securing Digital Content (Magda M. Mourad and Ahmed N. Tantawy). -- 25.1 Introduction. -- 25.2 Securing Digital Content: Need and Challenges. -- 25.3 Content Protection Techniques. -- 25.4 Illustrative Application: EPublishing of E-Learning Content. -- 25.5 Concluding Remarks. -- References. -- Appendix A. Cryptography Primer: Introduction to Cryptographic Principles and Algorithms (Panayiotis Kotzanikolaou and Christos Douligeris). -- A.1 Introduction. -- A.2 Cryptographic Primitives. -- A.3 Symmetric-Key Cryptography. -- A.4 Asymmetric-Key Cryptography. -- A.5 Key Management. -- A.6. Conclusions and Other Fields of Cryptography. -- References. -- Appendix B. Network Security: Overview of Current Legal and Policy Issues (Andreas Mitrakas). -- B.1 Introduction. -- B.2 Network Security as a Legal Requirement. -- B.3 Network Security Policy Overview. -- B.4 Legal Aspects of Network Security. -- B.5 Self-Regulatory Security Frameworks. -- B.6 Conclusions. -- References. -- Appendix C. Standards in Network Security (Despina Polemi and Panagiotis Sklavos). -- C.1 Introduction. -- C.2 Virtual Private Networks: Internet Protocol Security (IPSec).
C.3 Multicast Security (MSEC). -- C.4 Transport Layer Security (TLS). -- C.5 Routing Security. -- C.6 ATM Networks Security. -- C.7 Third-Generation (3G) Mobile Networks. -- C.8 Wireless LAN (802.11) Security. -- C.9 E-Mail Security. -- C.10 Public-Key Infrastructure (X. 509). -- Index. -- About the Editors and Authors.

Sommario/riassunto

A unique overview of network security issues, solutions, and methodologies at an architectural and research level Network Security provides the latest research and addresses likely future developments in network security protocols, architectures, policy, and implementations. It covers a wide range of topics dealing with network

security, including secure routing, designing firewalls, mobile agent security, Bluetooth security, wireless sensor networks, securing digital content, and much more. Leading authorities in the field provide reliable information on the current state of security protocols, architectures, implementations, and policies. Contributors analyze research activities, proposals, trends, and state-of-the-art aspects of security and provide expert insights into the future of the industry. Complete with strategies for implementing security mechanisms and techniques, Network Security features: * State-of-the-art technologies not covered in other books, such as Denial of Service (DoS) and Distributed Denial-of-Service (DDoS) attacks and countermeasures * Problems and solutions for a wide range of network technologies, from fixed point to mobile * Methodologies for real-time and non-real-time applications and protocols.