

1. Record Nr.	UNINA9910807161003321
Titolo	Information assurance : dependability and security in networked systems // [edited by] Yi Qian ... [et al.]
Pubbl/distr/stampa	Amsterdam ; ; Boston, : Elsevier/Morgan Kaufmann, c2008
ISBN	1-281-09617-2 9786611096175 0-08-055588-8
Edizione	[1st edition]
Descrizione fisica	1 online resource (577 p.)
Collana	The Morgan Kaufmann series in networking The Morgan Kaufmann series in computer security
Altri autori (Persone)	QianYi <1962->
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer networks - Reliability 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	Front Cover; Information Assurance; Copyright Page; Table of Contents; Preface; Contributors; Chapter 1. Information Assurance; 1.1 Introduction; 1.2 Information Assurance: Dependability and Security of Networked Information Systems; 1.3 Book Organization; 1.4 Conclusion; References; Part I: Foundational Background on Security and Dependability Techniques; Chapter 2. Network Security; 2.1 Introduction; 2.2 Network Attacks and Security Issues; 2.3 Protection and Prevention; 2.4 Detection; 2.5 Assessment and Response; 2.6 Conclusion; References Chapter 3. Security for Distributed Systems: Foundations of Access Control 3.1 Introduction; 3.2 Identification and Authentication; 3.3 Access Control; 3.4 Access Control in Distributed Systems; 3.5 Digital Identity Management; 3.6 Conclusion; References; Chapter 4. Network Survivability; 4.1 Introduction; 4.2 Prevention Techniques; 4.3 Survivable Network Design and Traffic Restoration Concepts; 4.4 Transport Network Recovery Techniques; 4.5 Survivable Network Design Techniques; 4.6 Multilayer Issues; 4.7 Conclusion and Future Research Areas; References; Chapter 5. System Survivability

5.1 Introduction and Background 5.2 Survivability and the Impact of Fault Models; 5.3 Design for Survivability; 5.4 Decentralized Storage; 5.5 Survivability of Large Distributed Systems; 5.6 Borrowing from Well-established Fields; 5.7 Conclusion; References; Part II: Modeling the Interaction Between Dependability and Security; Chapter 6. Taxonomy and Framework for Integrating Dependability and Security; 6.1 Introduction; 6.2 Basic Concepts and Related Work; 6.3 Proposed Taxonomy and Framework; 6.4 Dependability, Security, and their Attributes; 6.5 The Means to Attain Dependability and Security 6.6 Conclusion References; Chapter 7. Stochastic Modeling Techniques for Secure and Survivable Systems; 7.1 Introduction; 7.2 Analytical Modeling Techniques; 7.3 Security Modeling; 7.4 Survivability Modeling; 7.5 Conclusion; Acknowledgment; References; Chapter 8. Integrated Dependability and Security Evaluation Using Game Theory and Markov Models; 8.1 Introduction; 8.2 Stochastic Modeling; 8.3 Predicting Attacker Behavior; 8.4 Defining and Solving the Game; 8.5 Tuning the Game Parameters; 8.6 Case Study: DNS Service; 8.7 Conclusion; References
Chapter 9. Scenario Graphs Applied to Network Security 9.1 Introduction; 9.2 Algorithms for Generating Scenario Graphs; 9.3 Attack Graphs are Scenario Graphs; 9.4 Network Attack Graphs; 9.5 Example Network; 9.6 Attack Graph Analysis; 9.7 Practical Experience; 9.8 Related Work; 9.9 Future Work and Conclusion; Acknowledgments; References; Chapter 10. Vulnerability-Centric Alert Correlation; 10.1 Introduction; 10.2 Review of Alert Correlation and Related Techniques; 10.3 Attack Graph; 10.4 Alert Correlation, Hypothesis, Prediction, and Aggregation; 10.5 Conclusion; 10.6 Acknowledgments
References

Sommario/riassunto

In today's fast paced, info centric environment, professionals increasingly rely on networked information technology to do business. Unfortunately, with the advent of such technology came new and complex problems that continue to threaten the availability, integrity, and confidentiality of our electronic information. It is therefore absolutely imperative to take measures to protect and defend information systems by ensuring their security and non-repudiation. Information Assurance skillfully addresses this issue by detailing the sufficient capacity networked systems need to operate while under
