

1. Record Nr.	UNINA9910812555603321
Autore	Ben Mahmoud Mohamed Slim
Titolo	Risk propagation assessment for network security : application to airport communication network design // Mohamed Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano
Pubbl/distr/stampa	Hoboken, N.J., : ISTE Ltd/John Wiley and Sons Inc, 2013
ISBN	1-118-57994-1 1-118-58101-6 1-299-47554-X 1-118-57873-2
Edizione	[1st ed.]
Descrizione fisica	1 online resource (139 p.)
Collana	Focus series in networks and telecommunications
Altri autori (Persone)	LarrieuNicolas PirovanoAlain
Disciplina	387.740426
Soggetti	Computer networks - Security measures - Design Aeronautics - Communication systems - Design and construction
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	Title Page; Contents; LIST OF FIGURES; LIST OF TABLES; INTRODUCTION; PART 1. NETWORK SECURITY RISK ASSESSMENT; CHAPTER 1. INTRODUCTION TO INFORMATION SYSTEMSECURITY RISK MANAGEMENT PROCESS; 1.1. On the importance of network security for network designers; 1.2. On the impact of risk assessment in the decision-making process for network security designers; 1.3. Quantitative versus qualitative risk assessment approaches; 1.4. Network security risk propagation concept; 1.4.1. Impact of node correlation; 1.4.2. Network security risk transitivity 1.4.3. Network security risk propagation illustrative caseCHAPTER 2. SECURITY RISK MANAGEMENTBACKGROUND; 2.1. Qualitative security risk management methods; 2.1.1. CRAMM; 2.1.2. OCTAVE; 2.1.3. EBIOS; 2.1.4. MEHARI; 2.1.5. CORAS; 2.1.6. Discussion; 2.2. Quantitative security risk assessment approaches; 2.3. Toward a quantitative propagation-based risk assessment methodology; CHAPTER 3. A QUANTITATIVE NETWORK RISK ASSESSMENT METHODOLOGY BASED ON RISK PROPAGATION; 3.1. Quantifying

methodology parameters; 3.1.1. Network risk decomposition; 3.1.2. Node value; 3.1.3. Enhanced node value  
3.1.4. Impact of threats 3.1.5. Likelihood of threats; 3.2. Network security risk assessment process; 3.3. Conclusion; PART 2.  
APPLICATION TO AIRPORT COMMUNICATION NETWORK DESIGN;  
CHAPTER 4. THE AEROMACS COMMUNICATION SYSTEM IN THE SESAR PROJECT; 4.1. Overview of the European SESAR project; 4.2. Overview of aeronautical communications operating concept and requirements; 4.3. Introduction to the AeroMACS communication system; 4.3.1. AeroMACS protocol stack; 4.3.2. AeroMACS reference network architecture; 4.3.3. AeroMACS security considerations; 4.3.3.1. Analysis of AeroMACS security weaknesses  
4.3.4. AeroMACS reference network topology 4.3.4.1. Isolated AeroMACS network architecture; 4.3.4.2. End-to-end AeroMACS network architecture; CHAPTER 5. AERONAUTICAL NETWORK CASE STUDY; 5.1. Experimental parameters; 5.1.1. Testbed infrastructure; 5.1.2. Aeronautical node values instantiation; 5.1.3. Aeronautical services instantiation; 5.1.4. Isolated vs. end-to-end emulation scenarios; 5.2. AeroMACS case study: experimental results; 5.2.1. Main inputs for emulation scenarios; 5.2.2. Isolated AeroMACS scenario: preliminary results; 5.2.2.1. Individual risks; 5.2.2.2. Propagated risks 5.2.2.3. Node and network risks 5.2.3. Isolated AeroMACS scenario: EAP vs. RSA sub-scenario; 5.2.4. Preliminary AeroMACS security enhancement guidance; 5.2.5. AeroMACS implementation improvements: isolated scenario without operational server vulnerabilities; 5.2.5.1. Experimental inputs; 5.2.5.2. Network topology; 5.2.5.3. Vulnerability statistics; 5.2.5.4. Individual risk results; 5.2.5.5. Propagated risk results; 5.2.5.6. Network risk results; 5.2.6. AeroMACS topological improvements: isolated scenario with two ASN gateways; 5.2.6.1. Experimental inputs; 5.2.6.2. Network topology 5.2.6.3. Vulnerability statistics

---

## Sommario/riassunto

The focus of this book is risk assessment methodologies for network architecture design. The main goal is to present and illustrate an innovative risk propagation-based quantitative assessment tool. This original approach aims to help network designers and security administrators to design and build more robust and secure network topologies. As an implementation case study, the authors consider an aeronautical network based on AeroMACS (Aeronautical Mobile Airport Communications System) technology. AeroMACS has been identified as the wireless access network for airport surface communication

---