TACTICAL WIRELESS COMMUNICATIONS AND NETWORKS: DESIGN CONCEPTS AND CHALLENGES

BY GEORGE F. ELMASRY

WILEY, 2012, ISBN 978-1-119-95176-6, HARDCOVER, 301 PAGES

REVIEWER: JANUSZ GOZDECKI

George F. Elmasry has prepared a comprehensive guidebook on solutions and network architectures used in military tactical wireless networks where security, information assurance, and network operations must be met.

The book consists of 11 chapters divided into three main parts. In the first of them, a general overview of protocol stack layers in tactical networks is described, starting from the mapping of the OSI model to a tactical network layer model. Here, the theoretical background for the physical, data link, MAC, and network layers of military wireless networks is presented. For each layer the solutions used in tactical and commercial radio systems are compared. The second part describes the details of different generations of wireless tactical data systems, starting from non-IP networks, through systems that integrate non-IP systems with IP core networks, to IP-based tactical networks. The challenges of the cognitive radio in the context of wireless tactical networks are also discussed. In the last part of the book, the application of the open architecture model and reuse of solutions from commercial networks for next generation military networks are presented. The introduction of the open architecture is a new paradigm in the tactical radio and a new approach for network system development in comparison with closed solutions known from military systems. The use of an open architecture can bring competition between vendors and service providers to military systems, as well as cost reductions and more innovation in comparison with legacy closed systems. Additionally, the security and network management challenges in tactical networks are discussed, including use of Policy Based Network Management and game theory.

The book helps in understanding the concept of tactical wireless radios and military networks with special requirements regarding security, information assurance, and systems resilience. The author addresses a likely evolution of military networks, pointing out potential reuse of solutions from commercial networks and following the open architecture paradigm to develop military communication systems. The book is written in easy to understand English, although many abbreviations and terminology specific to the military world are used. Each chapter is complemented with an interesting concluding summary with historical background, and with the bibliography related to the discussed topic. I would like to recommend the book for graduate students, engineers and researchers interested in a general understanding of military wireless network technologies, architectures, and challenges facing future generations of this type of networks.

FISMA AND THE RISK MANAGEMENT FRAMEWORK: THE NEW PRACTICE OF FEDERAL CYBER SECURITY

BY STEPHEN D. GANTZ AND DANIEL R. PHILPOTT

SYNGRESS, 2013, ISBN 978-1-59749-641-4, SOFTCOVER, 562 PAGES

REVIEWER: TOMASZ CHMIELECKI

The Federal Information Security Management Act (FISMA) is the U.S. federal law that is the basis of IT security planning and its implementation in all American federal agencies. During the 12 years since its passage, a number of documents drilling down different aspects of IT security the bill enforces have been published. The ambition of this book is to give a picture of the approach taken by the act and its derivative documents to IT security. The authors successfully present the picture from all perspectives, starting with a global overview, going through the purpose of preparing the system of documents and standards as a whole, and finishing with a fully detailed explanation of all the relevant components.

Chapter 1 introduces FISMA, acquainting readers with a general overview of the topic and introducing the key concepts. There is a comparison of strengths and shortcomings of the approach as well. Chapter 2 describes the U.S. government viewpoint on security and familiarizes the reader with federal information security fundamentals. One can find information about the history of legislative requirements regarding information security applicable to federal agencies. Chapter 3 is focused on risk management. Starting from the definition of key terms, such as trust, distrust, trustworthiness security, assurance, or risk, the authors show a position and importance of information security management as a core component of enterprise risk management. Chapter 4 describes types of government systems and elaborates on different approaches to their management, emphasizing aspects like IT investments, enterprise architecture, FISMA requirements, and regulatory compliance. Chapter 5 presents tools supporting successful execution of Risk Management Framework (RMF) processes by pointing out prerequisites, constraints, and factors influencing the effectiveness of organizational security management practices.

The Risk Management Framework (RMF) is precisely presented in Chapters 6 to 9. Chapter 6 concentrates on planning and initiation, discussing system-level and organizational activities undertaken to start the RMF process. The authors emphasize the significance of careful determination of the resources and analysis of dependencies between them. In Chapter 7, tasks and requirements associated with categorization of information and selection of security controls are described. Security controls, their implementation, and assessment are the subject of Chapter 8. The next chapter covers two closing steps of the RMF: authorizing information systems and security controls monitoring.

The System Security Plan, which is the foundational document in RMF and the primary reference point for federal information system security data, is described in Chapter 10. The Security Assessment Report, which is the most important output of the security control assessment process, is discussed in Chapter 11. Chapter 12 describes the development and maintenance of the Plan of Actions and Milestones, a key document in the security authorization package. Chapter 13, focusing on NIST SP 800-39, the central documents for RMF, characterizes the risk management process, comprising risk framing, risk assessment, risk response, and risk monitoring activities. Chapter 14 covers the Continuous Monitoring process, describing system-specific and organizational activities performed as its components. Chapter 15 explains the relationship between contingency planning and related activities, such as disaster recovery and incident response. Chapter 16 specifies various requirements prescribing federal agency obligations for protecting different types of personal information stored in federal IT systems. The last chapter briefly summarizes key federal initiatives that impact security management in federal agencies.

Readers of this book will feel that the authors are security practitioners who decided to write for the security practitioners. For the person who needs to build a solid IT system and get it through the process of security authorization, this work will be a perfect source. The authors structured the contents logically, which makes it easy to find information. The book can be used as a compendium of security knowledge, to which one can return many times to find important details when needed. Although it deals with American recommendations, the book can also be very useful for European security professionals, who are used to ISO 27000-related standards in their daily work. For them, this will be an excellent source of knowledge of another fundamental approach to security.