Cyberspace mimic defense

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Cyberspace mimic defense : generalized robust control and endogenous security / by Jiangxing Wu

Auteur(s) : Wu, Jiangxing (1953-....)

Publication : Cham : Springer

Date de copyright : C 2020

Description matérielle : 1 vol. (L-735 p. : ill., graph., diagr., tabl. ; 25 cm

Collection : Wireless networks 2366-1186

ISBN : 978-3-030-29843-2

EAN : 9783030298432 rel.

Appartient à la collection : Wireless networks (Cham. Print) 2366-1186

Classification décimale Dewey : 364.168 2

Note sur les bibliographies et les index : Bibliogr. en fin de chapitres

Note sur le contenu : 1 Security Risks from Vulnerabilities and Backdoors 2 Formal Description of Cyber Attacks 3 Conventional Defense Technologies 4 New Approaches to Cyber Defense 5 Analysis of diversity, randomness and dynamicity 6 Revelation of Heterogeneous Redundancy Architecture 7 DHR Architecture 8 Original Meaning and Vision of Mimic Defense 9 Theory of Cyberspace Mimic Defense 10 Engineering & Implementation of Mimic Defense 11 Foundation and Cost of Mimic Defense 12 Examples of Mimic Defense Application 13 Testing and Evaluation of the Mimic Defense Principle Verification System 14 Application Demonstration and Current Network Testing of Mimic Defense

Résumé ou extrait : La 4e de couv. indique : "This book discusses uncertain threats, which are caused by unknown attacks based on unknown vulnerabilities or backdoors in the information system or control devices and software/hardware. Generalized robustness control architecture and the mimic defense mechanisms are presented in this book, which could change "the easy-to-attack and difficult-to-defend game" in cyberspace. The endogenous uncertain effects from the targets of the software/hardware based

on this architecture can produce magic "mimic defense fog", and suppress in a normalized mode random disturbances caused by physical or logic elements, as well as effects of non-probability disturbances brought by uncertain security threats. This book provides a solution both in theory and engineering implementation to the difficult problem of how to avoid the uncontrollability of product security caused by globalized marketing, COTS and non-trustworthy software/hardware sources. It has been proved that this revolutionary enabling technology has endowed software/hardware products in IT/ICT/CPS with endogenous security functions and has overturned the attack theories and methods based on hardware/software design defects or resident malicious codes. This book is designed for educators, theoretical and technological researchers in cyber security and autonomous control and for business technicians who are engaged in the research on developing a new generation of software/hardware products by using endogenous security enabling technologies and for other product users. Postgraduates in IT/ICT/CPS/ICS will discover that (as long as the law of "structure determines the nature and architecture determines the security is properly used), the problem of software/hardware design defects or malicious code embedding will become the swelling of Achilles in the process of informationization and will no longer haunt Pandora's box in cyberspace. Security and opening-up, advanced progressiveness and controllability seem to be contradictory, but there can be theoretically and technologically unified solutions to the problem."

Sujet - Nom commun : Protection de l'information (informatique)
Systèmes de communication sans fil
Radiocommunications mobiles
Électrotechnique