1. Record Nr. UNINA9910254984103321

Autore	Rowe Neil C
Titolo	Introduction to Cyberdeception / / by Neil C. Rowe, Julian Rrushi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-41187-X
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XIV, 334 p. 61 illus., 49 illus. in color.)
Disciplina	005.8
Soggetti	Computer security Computer communication systems Application software Data encryption (Computer science) Systems and Data Security Computer Communication Networks Information Systems Applications (incl. Internet) Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction -- Psychology of Deception -- Professional Deception -- Deception Methods for Defense -- Deception Methods for Offense -- Delays -- Fakes -- Defensive Camouflage -- False Excuses -- Defensive Social Engineering -- Measuring Deception -- Planning Cyberspace Deception -- Software Engineering of Deceptive Software and Systems -- Decoy I/O Devices -- Deception for the Electrical Power Industry -- Law and Ethics for Software Deception. .
Sommario/riassunto	This book is an introduction to both offensive and defensive techniques of cyberdeception. Unlike most books on cyberdeception, this book focuses on methods rather than detection. It treats cyberdeception techniques that are current, novel, and practical, and that go well beyond traditional honeypots. It contains features friendly for classroom use: (1) minimal use of programming details and mathematics, (2) modular chapters that can be covered in many orders, (3) exercises with each chapter, and (4) an extensive reference list. Cyberattacks have grown serious enough that understanding and using

deception is essential to safe operation in cyberspace. The deception techniques covered are impersonation, delays, fakes, camouflage, false excuses, and social engineering. Special attention is devoted to cyberdeception in industrial control systems and within operating systems. This material is supported by a detailed discussion of how to plan deceptions and calculate their detectability and effectiveness. Some of the chapters provide further technical details of specific deception techniques and their application. Cyberdeception can be conducted ethically and efficiently when necessary by following a few basic principles. This book is intended for advanced undergraduate students and graduate students, as well as computer professionals learning on their own. It will be especially useful for anyone who helps run important and essential computer systems such as critical-infrastructure and military systems. .