Introduction to Cyberdeception

Neil C. Rowe • Julian Rrushi

Introduction to Cyberdeception

Springer

Neil C. Rowe
US Naval Postgraduate School
Monterey, CA, USA

Julian Rrushi
Western Washington University
Bellingham, WA, USA

ISBN 978-3-319-41185-9 ISBN 978-3-319-41187-3 (eBook)
DOI 10.1007/978-3-319-41187-3

Library of Congress Control Number: 2016943730

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

To Suzanne, who is only occasionally deceptive.

—NCR

To the national hero of Albania, George Castriot, aka Skanderbeg, whose skills in deception helped protect his homeland and the entire Europe from Ottoman conquest.

—JR

Preface

We need new ideas in information security. This book offers a set of interrelated ideas about using deception as a framework for attack and defense of computer systems and networks, and mostly defense. Contrary to popular belief, deception is not always bad and can be a useful tool in cyberspace. Much activity is occurring in regard to cyberdeception, so we try to convey some understanding of what is going on.

This book is intended as an introduction to cyberdeception and can be used in a classroom or for independent study. The intended audience is people who deal with cybersystems in one way or another, especially programmers and people focusing on information security and information assurance. But it also includes managers and policymakers who need to understand the options.

We realize that this book may seem a little cynical. We prefer to think of it as realistic. Deception, like war, is ubiquitous in human society, and it is important to address the world as it is, not as we want it to be. Will this book encourage deception and thus lead to a deterioration of societies? We think not, since there are plenty of books on crime and war, and they have not generally caused higher levels of crime and war. Understanding crime, war, and deception enables doing something about them.

We have tried to provide plenty of references to a variety of work on cyberdeception and supporting topics, for readers who want to further pursue particular topics. (All Rowe's publications are available at http://faculty.nps.edu/ncrowe.) They range from nontechnical to technical. Cyberdeception is an active field of research and development today, so new developments occur frequently. Most of the book does not assume the reader knows much about cybersystems other than the basics of software and architectures. However, the later chapters are more technical for readers who want more details, and appendices are available online to provide examples of implementations.

James Bret Michael and Richard Riehle got us interested in studying cyberdeception. Especially helpful have been Barton Whaley, Dorothy Denning, Paul Thompson, and Glenn Fink. Partial funding for this work has been provided by the U.S. National Science Foundation under the Cyber Trust program.

Monterey, CA Neil C. Rowe
Bellingham, WA Julian Rrushi

Contents