Advances in Information Security 56

Sushil Jajodia
Paulo Shakarian
V.S. Subrahmanian
Vipin Swarup
Cliff Wang *Editors*

Cyber Warfare

Building the Scientific Foundation

Springer

Advances in Information Security 56

Sushil Jajodia
Paulo Shakarian
V.S. Subrahmanian
Vipin Swarup
Cliff Wang *Editors*

Cyber Warfare

Building the Scientific Foundation

Springer

Advances in Information Security

Volume 56

Series Editor
Sushil Jajodia
Center for Secure Information Systems, George Mason University, Fairfax, VA 22030-4444, USA

More information about this series at http://www.springer.com/series/5576

Sushil Jajodia • Paulo Shakarian
V.S. Subrahmanian • Vipin Swarup • Cliff Wang
Editors

Cyber Warfare

Building the Scientific Foundation

Springer

Editors
Sushil Jajodia
George Mason University
Fairfax, Virginia, USA

Paulo Shakarian
Arizona State University
Tempe, Arizona, USA

V.S. Subrahmanian
Computer Science Department
University of Maryland
College Park, Maryland, USA

Vipin Swarup
The MITRE Corporation
McLean, Virginia, USA

Cliff Wang
Information Sciences Directorate
Triangle Park, North Carolina, USA

ISSN 1568-2633
Advances in Information Security
ISBN 978-3-319-14038-4 ISBN 978-3-319-14039-1 (eBook)
DOI 10.1007/978-3-319-14039-1

Library of Congress Control Number: 2015930093

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

It is imperative, going forward, that we broaden our understanding of the science that underpins cybersecurity.
—General (Ret.) Keith Alexander, Former Commander of U.S. Cyber Command[1]

Modern society's increased reliance on computer systems, smartphones, and the Internet has provided a new target in a time of conflict. Indeed, cyber-warfare has already emerged as an extension of state policies—one needs to look no further than the headlines produced by Stuxnet, Aurora, or the cyber-attacks during the Russian-Georgian war than to gain an understanding of the emerging impact this domain has during a conflict.

While we have seen a plethora of advanced engineering concepts that directly affect cyber-warfare such as the inventions of the firewall, Metasploit, and even advanced malware platforms such as Flame, many of these concepts are built around best practices, rules-of-thumb, and tried-and-true techniques. While these inventions have been of high impact and significance, history has repeatedly taught us (in other disciplines) that the establishment of scientific principles leads to more rapid and remarkable progress.

Hence, this volume is designed to take a step toward establishing scientific foundations for cyber-warfare. Here we present a collection of the latest basic research results toward establishing such a foundation from several top researchers around the world. This volume includes papers that rigorously analyze many important aspects of cyber-conflict including the employment of botnets, positioning of honeypots, denial and deception, human factors, and the attribution problem. Further, we have made an effort to not only sample different aspects of cyber-warfare, but also highlight a wide variety of scientific techniques that can be used to study these problems. The chapters in this book highlight game theory, cognitive modeling, optimization, logic programming, big data analytics, and argumentation to name a few.

It is our sincere hope that this volume inspires researchers to build upon the knowledge we present to further establish scientific foundations for cyber-warfare and ultimately bring about a more secure and reliable Internet.

[1] http://www.nsa.gov/research/tnw/tnw194/article2.shtml.

About the Book

The first three chapters introduce some perspectives and principles of cyber warfare. In Chap. 1, Goel and Hong examine the use of cyber attacks as key strategic weapons in international conflicts, and present game-theoretic models for some cyber warfare problems. In Chap. 2, Elder et al. present a capability based on multi-formalism modeling to model, analyze, and evaluate the effects of cyber exploits on the coordination in decision making organizations. In Chap. 3, Sweeney and Cybenko describe how an attacker who controls the cyber high ground has a distinct advantage in achieving his mission objectives.

The next chapters explore cyber deception and game theoretic approaches. In Chap. 4, Al-Shaer and Rahman develop a game-theoretic framework for planning successful deception plans. In Chap. 5, Kiekintveld et al examine the use of game theory for network security, and present several game-theoretic models that focus on the use of honeypots for network security. In Chap. 6, Heckman and Stech describe cyber-counterdeception, and how to incorporate it into cyber defenses to detect and counter cyber attackers. In Chap. 7, Hamilton addresses the challenges of automatically generating cyber adversary profiles from network observations, even when the adversaries are using deception operations to disguise their activities and intentions. In Chap. 8, Shakarian et al. introduce a formal reasoning system that aids an analyst in the attribution of a cyber operation even when the available information is conflicting or uncertain.

Chapters 9–12 explore social and behavioral aspects of cyber security and cyber warfare. In Chap. 9, Marble et al. review the role of the human factor in cyber security, for both attackers and defenders. In Chap. 10, Ben-Asher and Gonzalez propose using a well-known, multi-agent, cognitive model of decisions from experience to study behavior in cyber-war. In Chap. 11, Puzis and Elovici examine the problem of finding visible nodes in a social network that are most effective at diffusing agents that reveal hidden invisible nodes. In Chap. 12, Paxton et al. review algorithms that discover community structure within networks, and compare them based on the analysis context.

Chapters 13 and 14 are based on large-scale field data from millions of real hosts. In Chap. 13, Dumitras presents results of empirical studies of real-world security using field data collected on over 10 million real hosts. In Chap. 14, Prakash discusses the use of graph mining techniques on large field datasets to solve a range of challenging cybersecurity problems. Finally, in Chap. 15, Ruef and Rohlf discuss how advancements in programming language technology can address fundamental computer security problems, and argue that current research techniques are insufficient to guarantee security.

Acknowledgements

We are extremely grateful to the numerous contributors to this book. In particular, it is a pleasure to acknowledge the authors for their contributions. Special thanks go to Susan Lagerstrom-Fife, senior publishing editor at Springer for her support of this project. We also wish to thank the Army Research Office for their financial support under the grant numbers W911NF-14-1-0116 and W911NF-13-1-0421.

Contents

Contributors

Myriam Abramson Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Ehab Al-Shaer University of North Carolina at Charlotte, Charlotte, USA

Noam Ben-Asher Department of Social and Decision Sciences, Dynamic Decision Making Laboratory, Carnegie Mellon University, Pittsburgh, PA, USA

Joseph Coyne Information Technology Division, Naval Research Laboratory, Washington, DC, USA

George Cybenko Thayer School of Engneering at Dartmouth College, Hanover, NH, USA

Tudor Dumitraş Electrical and Computer Engineering Department, University of Maryland, College Park, MD, USA

Robert J. Elder System Architectures Laboratory, George Mason University, Fairfax, VA, USA

Yuval Elovici Telekom Innovation Laboratories and Department of Information Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel

Sanjay Goel University at Albany, State University of New York, New York, USA

Cleotilde Gonzalez Department of Social and Decision Sciences, Dynamic Decision Making Laboratory, Carnegie Mellon University, Pittsburgh, PA, USA

Samuel N. Hamilton Siege Technologies, Manchester, USA

Kristin E. Heckman The MITRE Corporation, McLean, VA, USA

Yuan Hong University at Albany, State University of New York, New York, USA

Paul Hyden Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Christopher Kiekintveld Computer Science Department, University of Texas at El Paso, El Paso, USA

W. F. Lawless Paine College, GA, Augusta, USA

Alexander H. Levis System Architectures Laboratory, George Mason University, Fairfax, VA, USA

Viliam Lisý Agent Technology Center, Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Prague, Czech Republic

Julie L. Marble Advanced Physics Laboratory Senior Human Factors Scientist Asymetric Operations Sector, Johns Hopkins University, Laurel, MD, USA

Ranjeev Mittu Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Geoffrey Moores Department of Electrical Engineering and Computer Science, U.S. Military Academy, West Point, NY, USA

Ira S. Moskowitz Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Radek Píbil Agent Technology Center, Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Prague, Czech Republic

Simon Parsons Department of Computer Science, University of Liverpool, Liverpool, UK

Napoleon C. Paxton Information Technology Division, Naval Research Laboratory, Washington, DC, USA

B. Aditya Prakash Department of Computer Science, Virginia Tech., Blacksburg, VA, USA

Rami Puzis Telekom Innovation Laboratories and Department of Information Systems Engineering, Ben-Gurion University of the Negev, Beer-Sheva, Israel

Mohammad Ashiqur Rahman University of North Carolina at Charlotte, Charlotte, USA

Chris Rohlf Yahoo Inc., New York, USA

Andrew Ruef Trail of Bits, New York, USA

Stephen Russell Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Paulo Shakarian Arizona Sate University, Tempe, AZ, USA

Ciara Sibley Information Technology Division, Naval Research Laboratory, Washington, DC, USA

Gerardo I. Simari Department of Computer Science and Engineering, Universidad Nacional del Sur, Bahìa Blanca, Argentina

Frank J. Stech The MITRE Corporation, McLean, VA, USA

Patrick Sweeney Thayer School of Engneering at Dartmouth College, Hanover, NH, USA

Bahram Yousefi System Architectures Laboratory, George Mason University, Fairfax, VA, USA

Chapter 1
Cyber War Games: Strategic Jostling Among Traditional Adversaries

Sanjay Goel and Yuan Hong

Abstract Cyber warfare has been simmering for a long time and has gradually morphed into a key strategic weapon in international conflicts. Doctrines of several countries consider cyber warfare capability as essential to gain strategic superiority or as a counterbalance to military inferiority. Countries are attempting to reach consensus on confidence building measures in cyber space while racing with each other to acquire cyber weaponry. These attempts are strongly influenced by the problem of clear attribution of cyber incidents as well as political imperatives. Game theory has been used in the past for such problems in international relations where players compete with each other and the actions of the players are interdependent. Problems in cyber warfare can benefit from similar game theoretic concepts. We discuss in this book chapter the state of cyber warfare, the key imperatives for the countries, and articulate how countries are jostling with each other in the cyber domain especially in the context of poor attribution and verification in the cyber domain. We present game theoretic models for a few representative problems in the cyber warfare domain.

1.1 Introduction

Cyber warfare started as a low intensity activity among nations and was initially used for nuisance attacks such as website defacement and denial of service attacks but it has developed into a fierce cyber arms race among countries. Cyber warfare now figures prominently in doctrines of major military superpowers and terrorist organizations. There have been cyber warfare incidents in the past where attacks were launched on Estonia and Georgia in context of political conflicts with Russia. There have also been attacks on South Korea and Japan related to regional political conflicts involving similar modes of attacks. Aside from these overt attacks, there have been several covert attacks involving espionage across different countries where both the

S. Goel (✉) · Y. Hong
University at Albany, State University of New York, New York, USA
e-mail: goel@albany.edu

Y. Hong
e-mail: hong@albany.edu

S. Jajodia et al. (eds.), *Cyber Warfare,* Advances in Information Security 56,
DOI 10.1007/978-3-319-14039-1_1