Preface

Motivation for the Book

This book seeks to present a summary of recent research advances in cyber situation awareness. A multidisciplinary group of leading researchers from the areas of cyber-security, cognitive science, and decision science offer their viewpoints on recent advances in cyber situation awareness.

Today, when a security incident happens, the top three questions a cyber operation center would ask are: What has happened? Why did it happen? What should I do? Answers to the first two questions form the core of cyber situation awareness (SA). Whether the last question can be satisfactorily addressed is largely dependent on the cyber SA capability of an enterprise.

From the perspective of “data to decisions,” cyber SA can be viewed as a main output of a particular data triaging system. Since there are a large variety of sensors monitoring an enterprise network, the cyber operation center will gather a large amount of data coming from these different types of data sources. The data typically represent normal operation status. Stealthy attack-related information could be deeply embedded among the large volume of normal operation data. Thus the signal-to-noise ratio of attack data is normally extremely low. Answering the first two questions through data triaging could be as hard as finding a needle in a haystack.

Although numerous tools have been developed to help security analysts gain a better SA, existing tools are not yet adequate to provide cyber operation centers with highly desirable cyber SA capabilities listed as follows:

- Capability 1: The ability to create problem-solving workflows or processes
- Capability 2: The ability to see the big picture of cyber defense landscape
- Capability 3: The ability to manage uncertainty
- Capability 4: The ability to reason albeit incomplete/noisy knowledge
- Capability 5: The ability to quickly locate needles in haystacks
- Capability 6: The ability to do strategic planning
- Capability 7: The ability to predict the possible next steps an adversary might take

The goal of this work is to present a summary of recent research advances in the development of these highly desirable cyber SA capabilities.

About the Book

Chapters in this book can be roughly divided into the following four areas:

Part I: Overview

- Computer-Aided Human Centric Cyber Situation Awareness

Part II: Computer and Information Science Aspects of the Recent Advances in Cyber Situation Awareness

- An Integrated Framework for Cyber Situational Awareness
- Lessons Learned: Visualizing Cyber Situation Awareness in a Network Security Domain
- Enterprise-Level Cyber Situation Awareness

Part III: Learning and Decision-Making Aspects of the Recent Advances in Cyber Situation Awareness

- Dynamics of Decision-Making in Cyber Defense: Using Multi-Agent Cognitive Modeling to Understand CyberWar
- Studying Analysts Data Triage Operations in Cyber Defense Situational Analysis

Part IV: Cognitive Science Aspects of the Recent Advances in Cyber Situation Awareness

- The Cognitive Sciences of Cyber-Security: A Framework for Advancing Socio-Cyber Systems
- Collaboration on Cybersecurity Situational Awareness

Acknowledgments

We are extremely grateful to all those who contributed to this book. It is a pleasure to acknowledge the authors for their contributions. Special thanks go to Alfred Hofmann, Vice-President Publishing (Editor), Anna Kramer, Assistant Editor, Christine Reiss, Editorial Assistant, and Ingrid Beyer, all from Springer, for their support of this project.

May 2017

Peng Liu
Sushil Jajodia
Cliff Wang

Springer

http://www.springer.com/978-3-319-61151-8

Theory and Models for Cyber Situation Awareness
Liu, P.; Jajodia, S.; Wang, C. (Eds.)
2017, VII, 227 p. 71 illus., Softcover
ISBN: 978-3-319-61151-8