Preface

Motivation for the Book

This book seeks to establish the state of the art in the cyber situational awareness area and to set the course for future research. A multidisciplinary group of leading researchers from cyber security, cognitive science, and decision science areas elaborate on the fundamental challenges facing the research community and identify promising solution paths.

Today, when a security incident occurs, the top three questions security administrators would ask are in essence: What has happened? Why did it happen? What should I do? Answers to the first two questions form the core of Cyber Situational Awareness. Whether the last question can be satisfactorily answered is greatly dependent upon the cyber situational awareness capability of an enterprise.

A variety of computer and network security research topics (especially some systems security topics) belong to or touch the scope of Cyber Situational Awareness. However, the Cyber Situational Awareness capability of an enterprise is still very limited for several reasons:

- Inaccurate and incomplete vulnerability analysis, intrusion detection, and forensics.
- Lack of capability to monitor certain microscopic system/attack behavior.
- Limited capability to transform/fuse/distill information into cyber intelligence.
- Limited capability to handle uncertainty.
- Existing system designs are not very “friendly” to Cyber Situational Awareness.

The goal of this book is to explore ways to elevate the Cyber Situational Awareness capability of an enterprise to the next level by measures such as developing holistic Cyber Situational Awareness approaches and evolving existing system designs into new systems that can achieve self-awareness. One major output of this book is a set of scientific research objectives and challenges in the area of Cyber Situational Awareness.

About the Book

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

- Cyber SA: Situational Awareness for Cyber Defense
- Overview of Cyber Situation Awareness

The Reasoning and Decision Making Aspects

- RPD-based Hypothesis Reasoning for Cyber Situation Awareness
- Uncertainty and Risk Management in Cyber Situational Awareness

Macroscopic Cyber Situational Awareness

- Employing Honeynets For Network Situational Awareness
- Assessing Cybercrime Through the Eyes of the WOMBAT

Enterprise Cyber Situational Awareness

- Topological Vulnerability Analysis
- Cross-Layer Damage Assessment for Cyber Situational Awareness

Microscopic Cyber Situational Awareness

- A Declarative Framework for Intrusion Analysis
- Automated Software Vulnerability Analysis

The Machine Learning Aspect

- Machine Learning Methods for High Level Cyber Situation Awareness

Acknowledgements

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 Susan Lagerstrom-Fife, Senior Publishing Editor for Springer, and Sharon Palleschi, Editorial Assistant at Springer for their support of this project. Special thanks also go to Shengzhi Zhang at Penn State University, who helped transform several chapters from MS Word to LaTex.

Sushil Jajodia
Peng Liu
Vipin Swarup
Cliff Wang