Review of the book

"Network Intrusion Detection and Prevention"
by Ali A. Ghorbani, Wei Lu and Mahbod Tavallaee
Springer, 2010

ISBN: 978-0-387-88770-8

Mark Daniel
Envieta, LLC

1 Summary of the review

Network Intrusion Detection and Prevention provides an overview of the field from an academic perspective. Breadth is emphasized over depth – while many topics are considered, details are generally left to the references. Researchers may find the book useful as an annotated guide through the field's research literature (circa 2005). Prospective audiences not already familiar with the topic (students, security professionals) will find it to be of less value.

2 Summary of the book

The book consists of eight chapters and an appendix.

- **Chapter 1: Network Attacks**
  A discussion of general attack taxonomies is followed by more specific comments on particular types of attacks (Probes, Denial of Service (DOS), Worms, *etc.*).
- **Chapter 2: Detection Approaches**
  Approaches to intrusion detection are characterized as belonging to one of three broad categories: *Misuse Detection*, *Anomaly Detection*, or *Specification-Based Detection*. Examples of existing Intrusion Detection Systems (IDSs) implementing these three approaches are discussed.
- **Chapter 3: Data Collection**
  Data Collection depends on where the IDS operates. Options for *Host–Based*, *Network–Based* and *Application–Based* IDSs are presented.
- **Chapter 4: Theoretical Foundations of Detection**
  A survey of anomaly detection techniques is presented with an emphasis on *machine learning* methods.
- **Chapter 5: Architecture and Implementation**
  The prominent architectural distinction is between *Centralized* and *Distributed* systems. Distributed systems dominate the discussion, and a number of examples are presented.
- **Chapter 6: Alert Management and Correlation**
  As the size of the monitored network increases, management and correlation of alert information becomes more difficult. Techniques for handling the increased amount of data are presented.
- **Chapter 7: Evaluation Criteria**
  Measuring the performance of an IDS is a challenging task. A number of different methods are discussed for evaluating *Accuracy*, *Performance* and other characteristics of IDSs.

- **Chapter 8: Intrusion Response**
  Passive IDSs simply alert a system administrator when an intrusion is detected, while *Active* IDSs may respond with countermeasures when triggered. A number of approaches to automated response are discussed.

- **Appendix A: Examples of Commercial and Open Source IDSs**
  The title is self explanatory.

3 What is the book like (style)?

In the book's Acknowledgements, the authors recognize five additional contributors and assign them variously to the eight chapters. This is telling, because the book itself reads more like a collection of eight distinct papers than a unified volume. References between chapters are rare, and in some cases material is duplicated. For example, chapters five and six both have subsections titled "Cooperative Intrusion Detection", and both reproduce (from a referenced paper) essentially identical ten point lists of "basic principles". One wonders whether the author of chapter five read chapter six (or vice versa). Perhaps more aggressive editing would have helped.

The chapters themselves read like academic survey articles. The style is terse, and sprinkled with references. Much of the text consists of single paragraph summaries of research articles. Few specific ideas receive more than a single paragraph of treatment. Chapter four is an exception, with more thorough discussions of the fundamentals of various theoretical detection topics. However, even there, details of the application of these topics to intrusion detection is mostly left to the references.

The book has a decidedly mid–2000s feel. When discussing worms (1.5), the authors state, "Some examples of recent worms include Slammer, Blaster, and Nachi." All three of these worms are from 2003. The Conficker worm (2008) is not mentioned, despite the book's 2010 publication date. In the appendix, they refer to the "ETHEREAL" network protocol analyzer, even though its name was changed in 2006 to "Wireshark".

4 Would you recommend this book?

This book holds some value for researchers in the field of IDS design. Its brief summary paragraphs provide suitable points of departure for further reading in the body of research literature.

While the authors explicitly state that their intended audience is students and security professionals, I would not recommend this book to either. The book's survey article style and overall lack of unity lessen its suitability as a textbook, or for self–study. Security professionals charged with the task of selecting/installing/managing a NIDS would be better served by conuslting any of the more practically focused books in the existing literature.

The reviewer is a Senior Security Analyst at Envieta, LLC.