Review of the book

"Network Security A Decision and Game-Theoretic Approach"

by Tansu Alpcan, Tamer Basar

Cambridge University Press, 2010

ISBN: 9780521119320

Reviewed by Sashank Dara

1 Summary of the review

Cyber Security is a complex field that draws applications from variety of theoretical areas. This book is a Decision and Game theoretic book first with few *hypothetical* examples from Network Security. This is in contrary to the title highlighting that it is Network Security book. Over all the book is for graduate students and researchers who want learn applications of highly theoretical concepts like game theory, decision theory, machine learning etc in the field of cyber security.

Note : Importantly this review is from a network security practitioners perspective .

2 Summary of the book

The book is divided into four parts. The first part provides good introduction, motivational examples and basic concepts. The second part is about application of game theory in security. The third part is about application of decision making in security. The fourth part is about applications of machine learning in Intrusion Detection.

2.1 Part I

2.1.1 Chapter 1

This chapter provides a good introduction and motivating examples to the field of network security. The example of using the story of *Blind men and the elephant* metaphor strikingly sets the tone for rest of the chapter. Also the analytical, quantitative approaches needed for this complex field (rather than applying heuristics) is emphasized with examples. Few side thoughts , the tree representation of attackers and defenders moves is not very intuitive.

2.1.2 Chapter 2

This chapter provides a basic introduction to network security. Different types of attacks, attackers, their motivations are explained. Also basic defense mechanisms, security trade offs and risk management are explained.

2.2 Part II

This part is central to theme of the book. Discusses various concepts in Game Theory and its applications.

2.2.1 Chapter 3

This chapter provides a good introduction to deterministic security games. Security games both static and dynamic are provided. Although the static game is provided for illustration purposes, modeling the cost of false-alarm might be useful. In reality too many false-alarms will annoy the defender and even force to turn off few controls subsequently an attacker would gain advantage. The VANET security games presented are of good importance since recent advances in driver-less auto cars. The reviewer has not much expertise in wireless networks so rest of the security games is not commented upon.

2.2.2 Chapter 4

This chapter discusses Stochastic (Markov) security games. The stochastic intrusion detection game is well explained. The challenge in reality though would be providing appropriate costs for *attack* or *no attack* and *defend* or *no defend* actions to determine the game strategies. Finding the optimal attacker and defender strategies in interconnected systems is also an important problem. The malware filter placement game is not really appealing from a practical perspective. In practice the malware filters are placed either at the edge network or before the traffic enters the data centers.

2.2.3 Chapter 5

This chapter discusses Probabilistic (Bayesian) Security games. The Bayesian Intrusion Detection game and Bayesian games for wireless security are explained. Later security games with observation and decision errors are presented. The fictitious play setup is interesting as it accommodates *false-positives* and *false-negatives*.

2.3 Part III

2.3.1 Chapter 6

This chapter is about Quantitative approaches for Security Risk Management. The risk propagation in complex organizations and networks is formulated in an interesting way. Further a probabilistic risk framework and dynamic risk mitigation and control algorithms are presented. The numerical example provided in this section well summarizes the theory.

The challenge in general for applying theory to practice is appropriately formalizing the problem. The example discusses the patching of various systems in the subnet based on number of classes of vulnerabilities existing this sounds good in theory. But in practice, there is yet another dimension to be considered, the impact of each vulnerability would be different from the class of vulnerability. For example , the CVSS scores are assigned for each CVE rather than CWE. Also many factors are considered for patching , the criticality of the server (planned outages, downtime etc are important), these constraints also need to be captured in reality.

The security investment game and co-operative games did not well resonate from a practitioners perspective. These sections seemed to be hypothetical.

2.3.2 Chapter 7

This chapter discusses about optimizing the malware filtering problem using centrality based metrics. Also discusses models for security response and epidemic response.

2.3.3 Chapter 8

This chapter discusses the Usability, Trust and Privacy sub fields of Network Security in a Game theoretic setting. Games related to recommendation algorithms for *sysadmins* , trust games in digital communities and location based privacy games are explained.

2.4 Part IV

2.4.1 Chapter 9

This chapter gives an introduction to machine learning and anomaly detection. It is not clear how this part of the book is connected to the central theme of the book. As it is not related Game theory or Decision theory. Also the classification based on SVM algorithms is out dated by now in this fast moving field. The motivational example given on mobile malware detection based on SMS usage is not at all appealing from a practical view point.

There are number of applications of using machine learning for malware detection like botnet detection, data loss prevention, static and dynamic analysis of suspicious files etc. Such analysis is based on network traffic, file binaries etc. None of these applications are even remotely mentioned.

2.4.2 Chapter 10

This chapter is predominantly about Hypothesis testing. Although few lines are briefly mentioned about usage of this technique in network security, no motivational examples are provided. Most of the chapter is about different types of this testing. The only example provided is detection of misbehavior of wireless nodes which is not well established to be a network security problem. Misbehavior of wireless nodes could be variety of reasons not just from intrusion perspective.

3 What is the book like (style)?

The book is mostly written in text book school for graduate students and researchers. This book is less of a practitioners handbook.

4 Would you recommend this book?

This book might be useful for graduate students and researchers in the field of Game theory, Decision theory. From a practitioner perspective most of the network security examples provided are hypothetical and not realistic. This book is written in 2011 and its high time for a second edition as the field is fast moving and there are many recent advances in the area too.

The reviewer is network security practitioner cum researcher at large multinational company