Network Security

A Decision and Game-Theoretic Approach

Covering attack detection, malware response, algorithm and mechanism design, privacy, and risk-management, this comprehensive work utilizes unique quantitative models derived from decision, control, and game theories to address diverse network security problems. It provides the reader with a system-level theoretical understanding of network security, and is essential reading for researchers interested in a quantitative approach to key incentive and resource allocation issues in the field. It also provides practitioners with an analytical foundation that is useful for formalizing decision-making processes in network security.

Tansu Alpcan is an Assistant Professor at the Technical University of Berlin, and is concurrently affiliated with Deutsche Telekom Laboratories. His research involves applications of distributed decision-making, game theory, and control to various security and resource allocation problems in complex and networked systems. Dr. Alpcan, who has numerous publications in security, networking, control, and game theory, is the recipient of multiple best paper awards from IEEE and research achievement awards from the University of Illinois. He has chaired and played an active role in the organization of various conferences, including GameSec, GameComm, and GameNets, and is currently chairing the Interest Group on Security in Media Processing and Communications within the IEEE Technical Committee on Multimedia Communications.

Tamer Başar holds several academic positions at the University of Illinois at Urbana-Champaign, including the titles of Swanlund Endowed Chair and Center for Advanced Study Professor of Electrical and Computer Engineeering. He is currently the Editor-in-Chief of Automatica, Series Editor for Systems and Control: Foundations and Applications, and Managing Editor of the Annals of the International Society of Dynamic Games (ISDG). He is a member of the US National Academy of Engineering, Fellow of the IEEE and IFAC, Founding President of the ISDG and Current President of the AACC. Dr. Başar has won a number of awards, including the Isaacs Award of ISDG, Bellman Control Heritage Award of the AACC, the Bode Lecture Prize of the IEEE CSS and the Quazza Medal and Outstanding Service Award of IFAC.

Network Security

A Decision and Game-Theoretic Approach

Tansu Alpcan
Deutsche Telekom Laboratories,
Technical University of Berlin, Germany

and

Tamer Başar
University of Illinois at Urbana-Champaign, USA

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

4843/24, 2nd Floor, Ansari Road, Daryaganj, Delhi - 110002, India

79 Anson Road, #06-04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521119320

First published 2011

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging in Publication data
Alpcan, Tansu, 1975–
Network security : a decision and game-theoretic approach / Tansu Alpcan, Tamer Basar.
p. cm.
Includes bibliographical references.
ISBN 978-0-521-11932-0 (hardback)
1. Computer networks–Security measures. 2. Game theory.
I. Basar, Tamer. II. Title.
TK5105.59.A45 2010
005.8–dc22
2010027364

ISBN 978-0-521-11932-0 Hardback

To

Alper, Altay, and Özlem (T.A.)

and

Tangül, Gözen, Elif, and Altan (T.B.)

Contents

Cambridge University Press
978-0-521-11932-0 — Network Security
Tansu Alpcan , Tamer Başar
Frontmatter
More Information

Preface

We are a lucky generation for witnessing the microprocessor and Internet revolutions, the type of technological marvels that mark the start of a new era: *the information age*. Just like electricity, railroads, and automobiles, the information technologies have a profound effect on our way of life and will stay with us for decades and centuries to come. Thanks to these advances, we have been building complex communication and computing networks on a global scale. However, it is still difficult today to predict how this information age will progress in the future or to fully grasp its consequences. We can hope for a complete understanding perhaps in decades to come, as past history tells us.

Although we have engineered and built the *Internet*, the prime example of the information revolution, our (mathematical) understanding of its underlying systems is cursory at best, since their complexity is orders of magnitude greater than that of their predecessors, e.g. the plain telephone network. Each disruptive technology brings its own set of problems along with enormous opportunities. Just as we are still trying to solve various issues associated with automobiles, the challenges put forward by the information and communication networks will be there not only for us but also for the next generations to address.

An important challenge today is *security* of complex computing and communication networks. Our limited understanding of these systems has a very unexpected side-effect: partial loss of "observability" and "control" of the very systems we build. Who can claim today full knowledge and control of all the running computing and communication processes on their laptop, corporate network, or country at all times? The science-fiction literature has always focused on fears of losing control of "intelligent machines." It is ironic that very few people imagined losing control of our dumb but complex and valuable systems to our malicious yet very own fellow human beings.

Security is a challenge stemming not only from the complexity of the systems surrounding us but also from the users' relative lack of experience with them. Unlike other complex systems, such as vehicle traffic, ordinary users receive very little training before obtaining access to extremely powerful technologies. Despite this (or maybe because of it), users' expectations of their capabilities are very high. They often expect everything to function as simply and reliably as, for example, the old telephone network. However, even for advanced users, bringing all aspects of a connected computer under control is a very time-consuming and costly process. The most diligent efforts can unfortunately be insufficient when faced with a determined and intelligent attacker.

These facts when combined with unrealistic expectations often result in significant disappointment in the general public regarding security.

In spite of its difficulty, securing networked systems is indisputably important as we enter the information age. The positive productivity benefits of networks clearly overcome the costs of any potential security problems. Therefore, there is simply no turning back to old ways. We have to live with and manage the security risks associated with the new virtual worlds which reflect our old selves in novel ways.

The emerging security challenges are multifaceted ranging from complexity of underlying hardware, software, and network interdependencies to human and social factors. While individuals and organizations are often very good at assessing security risks in real life, they are quite inexperienced with the ones they encounter on networked systems, which are very different in complexity and timescale. Although many lessons from real-world security can be transferred to the network security domain, there is a clear need for novel and systematic approaches to address the unique issues the latter brings about. It is widely agreed by now that security of networked systems is not a pure engineering problem that can be solved by designing better protocols, languages, or algorithms. It will require educating users and organizations, changing their perspectives, and equipping them with better tools for assessing and addressing network security problems.

Although many aspects of the network security problem are new, it also exhibits constraints familiar to us, which we often encounter in real life. Many resources available to malicious attackers and defending administrators of networks are limited. They vary from classical resources, such as bandwidth, computing speed and capability, energy, and manpower, to novel ones such as time, attention span, and mental load. Network security involves decision making by both attackers and defenders in multiple levels and timescales using the limited resources available to them. Currently, most of these decisions are made intuitively and in an ad-hoc manner.

This book, which is the first of its kind, aims to present *a theoretical foundation for making resource allocation decisions that balance available capabilities and perceived security risks in a principled manner*. We focus on analytical models based on game, information, communication, optimization, decision, and control theories that are applied to diverse security topics. At the same time, connections between theoretical models and real-world security problems are highlighted so as to establish the important feedback loop between theory and practice. Hence, this book should not be viewed as an authoritative last word on a well-established field but rather as an attempt to open novel and interesting research directions, hopefully to be adopted and pursued by a broader community.

Scope and usage

This book is aimed mainly at researchers and graduate students in the field of network security. While the emphasis is on theoretical approaches and research for decision-making in security, we believe that it would also be beneficial to practitioners, such as system administrators or security officers in industry, who are interested in the latest theoretical research results and quantitative network security models that build on control, optimization, decision, and game-theoretic foundations. An additional objective is the introduction of the network security paradigm as an application area to researchers well versed in control and game theory.

The book can be adopted as a reference for graduate-level network security courses that focus on network security in diverse fields such as electrical engineering, computer science and engineering, and management science. A basic overview of the mathematical background needed to follow the underlying concepts is provided in the Appendix.

Part I of the book is a very basic introduction to relevant network security concepts. It also discusses the underlying motivation and the approach adopted, along with three example scenarios. It is accessible to a general audience.

Part 2 presents security games and illustrates the usage of various game-theoretic models as a way to quantify the interaction between malicious attackers and defenders of networked systems. Deterministic, stochastic, and limited-information security games are discussed in order of increasing complexity.

Part 3 focuses on decision making for security and provides example applications of quantitative models from optimization and control theories to various security problems. Among the topics presented are "security risk-management," "optimal allocation of resources for security," and social side of security: "usability, trust, and privacy." Chapters in this part are not dependent on each other and can be read independently.

Part 4 studies distributed schemes for decentralized malware and attack detection. First, a distributed machine learning scheme is presented as a nonparametric method. Subsequently, centralized and decentralized detection schemes are discussed, which provide a parametric treatment of decentralized malware detection. Hence, this part builds a bridge between security and statistical (machine) learning.

Cambridge University Press
978-0-521-11932-0 — Network Security
Tansu Alpcan , Tamer Başar
Frontmatter
More Information

Acknowledgments

We would like to thank several individuals, particularly Kien Nguyen, Michael Bloem, Jeff Mounzer, Yalin Sagduyu, Stephan Schmidt, Jean-Pierre Hubaux, Nick Bambos, Christian Bauckhage, Sonja Buchegger, Walid Saad, M. Hossein Manshaei, Ann-Miura Ko, Maxim Raya, Albert Levi, and Erkay Savaş, whose research has provided a basis for various sections of this book. They have also kindly supported us in the writing process and provided feedback on relevant parts. We also thank Florin Ciucu for his careful reading of some of the chapters and for providing feedback.

Tansu Alpcan wishes to thank Deutsche Telekom Laboratories and its managing director Peter Möckel for their kind support in the writing of this book.

Finally, we would like to thank our editor Julie Lancashire and the team at Cambridge University Press, particularly Sarah Finlay and Sabine Koch, for their continuous and kind support during the preparation of this manuscript.

Tansu Alpcan	Tamer Başar
Berlin, Germany	Urbana, Illinois, USA
March, 2010	March, 2010

Artwork

The cover image is created by Tansu Alpcan using *Google SketchUp 7*[1] software for 3D design and *Kerkythea*[2] open source software for 3D rendering.

Almost all of the graphics in the book, except for scientific graphs and those listed below, are created originally by Tansu Alpcan using the *Inkscape*[3] open source software and (in some cases) public domain graphics from the *Open Clip Art Library*.[4]

The scientific graphs in the book (e.g. in Figures 3.3, 3.6 to 3.9, 4.2, 10.5, etc.) are generated using the *MATLAB* software by Mathworks Inc.

The image in Figure 1.1 is courtesy of the Intel Corporation and included with permission. The image in Figure 1.2 is a partial representation of the Linux 2.6.22 kernel and is generated by Tansu Alpcan using the scripts provided by *Linux Kernel Graphing Project*.[5]

Figure 6.1 is after an idea by Nick Bambos and Figure 6.6 is based on an earlier drawing by Jeff Mounzer. Figures 7.1 and 8.5 are inspired from earlier images by Michael Bloem. The figures in Chapter 10 are made in collaboration with Kien Nguyen.

[1] http://sketchup.google.com
[2] http://www.kerkythea.net
[3] http://www.inkscape.org
[4] http://www.openclipart.org
[5] http://fcgp.sourceforge.net/lgp

CAMBRIDGE
Cambridge University Press
978-0-521-11932-0 — Network Security
Tansu Alpcan , Tamer Başar
Frontmatter
More Information

Notation

Some of the notational conventions adopted in this book are listed below.

Symbol	Description
x	vector or scalar as a special case
x_i	i-th element of vector x
$y = [y_1, \dots, y_n]$	row vector y
M	matrix
$M_{i,j}$	entry at the i-th row and j-th column of matrix M
x^T, M^T	transpose of a vector x or matrix M
$\mathcal{S}$	set
$\mathcal{P}^A$	(set of) attacker player(s) in security games
$\mathcal{P}^D$	(set of) defender player(s) in security games
$\mathbb{R}$	set of real numbers
$\{0,1\}$	set with two elements: 0 and 1
$[0,1)$	right-open line segment $\{x \in \mathbb{R} : 0 \le x < 1\}$
$[0,1]$	closed unit interval $\{x \in \mathbb{R} : 0 \le x \le 1\}$
$f(x)$, $V(x)$	real valued functions or functionals with argument x (vector or scalar)
$\text{diag}(x)$	diagonal matrix with diagonal entries x
$\approx$	approximately equal
$:=$	definition; term on the left defines the expression on the right
I	identity matrix, $I := \text{diag}([1,\dots,1])$
$\|x\|$, $\|M\|$	norm of a vector x or of a matrix M
min, max	minimum and maximum operations
inf, sup	infimum and supremum operations
NE	Nash equilibrium (or Nash equilibria)
FP	fictitious play

Please see Appendix A for further information and definitions.