Nong Ye

Secure Computer and Network Systems

Modeling, Analysis and Design

WILEY

Secure Computer and Network Systems

Modeling, Analysis and Design

Nong Ye
Arizona State University, USA

John Wiley & Sons, Ltd

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wiley.com

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 42 McDougall Street, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 6045 Freemont Blvd, Mississauga, ONT, Canada L5R 4J3

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

British Library Cataloguing in Publication Data

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

ISBN 978-0-470-02324-2

Typeset in 10/12pt Times by Aptara Inc., New Delhi, India
Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire
This book is printed on acid-free paper responsibly manufactured from sustainable forestry
in which at least two trees are planted for each one used for paper production.

Secure Computer and Network Systems

Preface

Computer and network technologies have empowered us and transformed our business and life in many ways. However, our increasing dependence on computer and network systems has also exposed us to a wide range of cyber security risks involving system vulnerabilities and threats to our assets and transactions on those systems. Computer and network security is concerned with availability, confidentiality, integrity, non-repudiation, trust, and many other aspects of computer and network assets which may be compromised by cyber attacks from external and insider threats through exploiting system vulnerabilities. The protection of computer and network security must cover prevention to reduce system vulnerabilities, detection to identify ongoing cyber attacks that break through prevention mechanisms, and response to stop and control cyber attacks, recover systems and correct exploited system vulnerabilities.

SCOPE AND PURPOSE OF THE BOOK

This book presents a collection of the research work that I have carried out with my students and research associates in the past ten years to address the following issues in protecting computer and network security:

1. Prevention
   (a) How to enhance the architecture of computer and network systems for security protection through the specification and enforcement of digital security policies, with the following research outcome:
      (i) An Asset Protection-Driven Security Architecture (APDSA) which is developed based on a proactive asset protection-driven paradigm of security protection, in comparison with the threat-driven security protection paradigm that is often adopted in existing security products.
   (b) How to manage the admission control, scheduling, reservation and execution of computer and network jobs to assure the service stability and end-to-end delay of those jobs even under Denial of Service attacks or overwhelming amounts of job demands, with the following research outcomes:
      (i) A Batch Scheduled Admission Control (BSAC) method to reduce the variability of job waiting time for service stability, in comparison with no admission control in

the existing best effort service model that is commonly adopted on computers and networks but is a major system vulnerability exploited by Denial of Service (DoS) attacks.

(ii) Several job scheduling methods to schedule the service of jobs on single or multiple computer/network resources for service stability, including the Weighted Shortest Processing Time – Adjusted (WSPT-A) method, the Verified Spiral (VS) method, the Balanced Spiral (BS) method, and the Dynamic VS and BS methods, in comparison with the First-In-First-Out (FIFO) method used in the existing best effort model which can be exploited by DoS attacks.

(iii) Instantaneous Resource reSerVation Protocol (I-RSVP) and a Stable Instantaneous Resource reSerVation Protocol (SI-RSVP) that are developed to allow job reservation and service for instantaneous jobs on computer networks for the end-to-end delay guarantee to those jobs, in comparison with

- the existing Resource reSerVation Protocol (RSVP) based on the Integrated Service (InteServ) model to provide the end-to-end delay guarantee for computer and network jobs with continuous data flows; and
- the existing Differentiated Service (DiffServ) model.

2. Detection

(a) How to achieve the accuracy and earliness of cyber attack detection when monitoring the observed data from computers and networks that contains much noise due to the mixed data effects of an attack and ongoing normal use activities, with the following research outcomes:

(i) the attack norm separation methodology, in comparison with two conventional methodologies of cyber attack detection: signature recognition and anomaly detection.

(ii) the cuscore detection models that are used to perform cyber attack detection based on the attack norm separation methodology, in comparison with

- the Artificial Neural Network (ANN) models based on the signature recognition methodology;
- the univariate Statistical Process Control (SPC) technique, the Exponential Weighted Moving Average (EWMA) control charts, and the Markov chain models of event transitions, which are developed based on the anomaly detection methodology;
- the multivariate SPC technique, the Chi-Square Distance Monitoring (CSDM) method based on the anomaly detection methodology.

(iii) the Clustering and Classification Algorithm – Supervised (CCAS) which is a scalable data mining algorithm with the incremental learning capability to learn signature patterns of attack data and normal use data, in comparison with

- conventional clustering methods, such as hierarchical clustering,
- conventional data mining algorithms, such as decision trees.

(b) How to discover and identify subtle features and characteristics of attack data and normal use data which are the basis of defining the accurate attack and normal use data models to develop attack detection models based on the attack norm separation methodology, with the following research outcomes:

   (i) the statistical methods of extracting the mean, probability distribution and autocorrelation features of attack data and normal use data;

   (ii) the mathematical method of extracting the time-frequency wavelet feature of attack data and normal use data;

   (iii) the statistical and mathematical methods of uncovering attack data characteristics and normal use data characteristics in the mean, probability distribution, autocorrelation and wavelet features;

   (iv) the illustration and summary of the uncovered attack data characteristics of eleven representative attacks, including:

   - the Apache Resource DoS attack
   - the ARP Poison attack
   - the Distributed DoS attack
   - the Fork Bomb attack
   - the FTP Buffer Overflow attack
   - the Hardware Keylogger attack
   - the Software Keylogger attack
   - the Remote Dictionary attack
   - the Rootkit attack
   - the Security Audit attack using Nessus
   - the Vulnerability Scan attack using NMAP.

(c) How to select the smallest set of attack data characteristics for monitoring to reduce the computational overhead of running attack detection models, with the following research outcome:

   (i). the Integer Programming (IP) formulation of an optimization problem to select the smallest set of attack data characteristics that produce a unique combination or vector of attack data characteristics for each attack to allow the unique attack identification at the lowest computational overhead of running attack detection models.

3. Response

   (a) How to correlate the attack data characteristics associated with events that occur at various spatial and temporal locations in the cause–effect chain of a given attack for security incident assessment, with the following research outcome:

   (i) the attack profiling method of assessing a security incident by spatially and temporally correlating security events and associated attack data characteristics of the

> incident in the cause–effect chain of attack progression and propagation. The attack profile of a given attack allows using the attack signals from attack detection models, which monitor attack data characteristics at various spatial and temporal locations of the cause–effect chain of the attack, to gain a quick, accurate, comprehensive picture of the attack progression and its propagating effects for security incident assessment. The quick, accurate and comprehensive assessment of a security incident is the key in planning the response to stop and control an attack, recover the affected computer and network system, and correct exploited system vulnerabilities for preventing the future occurrence of the attack.

The comparison of the new research outcomes with the existing methods points out the drawbacks of the existing methods that the new research outcomes have overcome.

This book contains various design, modeling and analytical methods which can be used by researchers to investigate the security of computer and network systems. This book also describes new design principles and algorithms, along with new knowledge about computer and network behavior under attack and normal use conditions, which can be used by engineers and practitioners to build secure computer and network systems or enhance security practice. Known cyber attacks and existing security protection methods are reviewed and analyzed to give the background and point out the need to develop the new security protection methods presented in the book. Statistical and mathematical materials for analysis, modeling and design of the new methods are provided.

ORGANIZATION OF THE BOOK

This book is divided into seven parts. Part I, including Chapters 1 and 2, gives an overview of computer and network security. Chapter 1 traces cyber security risks to three elements: assets, vulnerabilities, and threats, which must coexist to pose a security risk. The three elements of security risks are defined with specific examples. An asset risk framework is also defined to capture the security risk elements along the cause–effect chain of activities, state changes and performance changes that occur in a cyber attack and the resulting security incident. Chapter 2 describes three important aspects of protecting computers and networks against security risks: prevention, detection, and response, and gives an overview of existing methods in the three areas of security protection.

Part II, including Chapters 3-6, presents the research outcomes for attack prevention and Quality of Service (QoS) assurance. As more business transactions move online, it has become imperative to provide the QoS assurance on the Internet which does not currently exist. Specifically, Chapter 3 describes the Asset Protection-Driven Security Architecture to enhance computer and network security through the specification and enforcement of digital security policies. Digital security policies are systematically defined according to the asset, vulnerability and threat elements of security risks. Chapter 4 addresses job admission control, and describes the development and testing of the Batch Scheduled Admission Control (BSAC) method. Chapter 5 presents several job scheduling methods developed to achieve service stability by minimizing the variance of job waiting times. Chapter 6 addresses the lack of job reservation and service protocol to provide the end-to-end delay guarantee for instantaneous computer and network jobs (e.g., jobs generated by email and web browsing applications) in previous work, although there exists RSVP for the service guarantee of computer and network jobs with continuous data flows (e.g., for the video streaming application). The development and testing of the Instantaneous Resource reSerVation Protocol (I-RSVP) and the Stable Instantaneous Resource reSerVation Protocol (SI-RSVP) are described in Chapter 6.

Chapter 7 in Part III describes the procedure of collecting the Windows performance objects data under eleven attack conditions and two normal use conditions of text editing and web browsing. The collected data is used for training and testing the detection models described in Parts IV, V and VI. Chapters 8–11 in Part III describe the statistical and mathematical methods of extracting the mean, probability distribution, autocorrelation and wavelet features of attack data and normal use data, respectively. Chapter 8 focuses on the simple mean feature of attack data and normal use data and the mean shift attack data characteristics. The wavelet feature described in Chapter 11 and the autocorrelation feature described in Chapter 10 reveal relations of data observations over time. The autocorrelation feature focuses on the general autocorrelation aspect of time series data, whereas the wavelet feature focuses on special forms of time-frequency data patterns. Both the wavelet feature in Chapter 11 and the probability distribution feature described in Chapter 9 are linked to specific data patterns of spike, random fluctuation, step change, steady change and sine–cosine wave with noise which are observed in the data. The distribution feature describes the general pattern of the data, whereas the wavelet feature reveals time locations and frequencies of those data patterns. The new knowledge about the data characteristics of attacks and normal use activities, which is not available in previous literature, is reported. For example, it is discovered that the majority of the data variables on computers and networks have some degree of autocorrelation. Moreover, the majority of the data variables on computers and networks follow either a skewed distribution or a multimodal distribution. Such information is important in modeling data of computer and network systems and building computer and network models for simulation and analysis. The attack data characteristics in the mean, probability distribution, autocorrelation and wavelet features for eleven representative attacks, which are revealed using the statistical and mathematical methods described in Chapters 8–11, are also summarized with an illustration of specific examples. Both the similarity and the difference between the attacks are revealed.

Part IV demonstrates the signature recognition methodology through the application of two techniques: (1) Clustering and Classification algorithm – Supervised (CCAS) in Chapter 12; and (2) Artificial Neural Networks (ANN) in Chapter 13, to cyber attack detection. The performance problem of these techniques in detection accuracy and earliness is illustrated with a discussion that points out their lack of handling the mixed attack and normal use data and dealing with subtle features and characteristics of attack data and normal use data.

Chapters 14 and 15 in Part V present the development and testing of the univariate and multivariate SPC techniques including the EWMA control charts and the Chi-Square Distance Monitoring (CSDM) method, as well as the Markov chain models of event transitions, all of which are developed based on the anomaly detection methodology for cyber attack detection. The anomaly detection techniques share with the signature recognition techniques in Part IV the same performance problem in detection accuracy and earliness and the drawback in lack of handling the mixed attack and normal use data and dealing with subtle features and characteristics of attack data and normal use data.

After clearly illustrating the performance problem of two conventional methodologies for cyber attack detection, the new attack norm separation methodology, which has been developed to overcome the performance problem of the two conventional methodologies, is presented in

Part VI. The attack norm separation methodology requires the definition of attack data models and normal use data models to deal with the mixed effect of attack data and normal use data, by first using the normal use data model to cancel the effect of normal use data in the data mixture, and then using the attack data model to identify the presence of a given attack in the residual data that is left after canceling the effect of normal use data. Chapter 16 in Part VI describes the statistical and mathematical methods of defining attack data models and normal use data models based on the characteristics of attack data and normal use data. Chapter 17 presents the cuscore detection models which are used to implement the attack norm separation methodology. For each combination of a given attack and a given normal use condition, a cuscore detection model is developed using the attack data model and the normal use data model. Chapter 17 shows the superior detection performance of the cuscore detection models for attack norm separation compared to that of the EWMA control charts for anomaly detection and that of the ANN technique for signature recognition.

Part VII focuses on security incident assessment. Specifically, Chapter 18 first addresses the selection of an optimal set of attack data characteristics to minimize the computational overhead of monitoring attacks that occur with various normal use conditions. An Integer Programming (IP) problem is formulated to solve this optimization problem. Chapter 18 then presents the attack profiling method of spatially and temporally correlating the selected attack data characteristics along the cause–effect chain of a given attack, and mapping those attack data characteristics to the events in the cause–effect chain of the attack for security incident assessment.

ACKNOWLEDGEMENTS

The research work presented in this book is made possible through the funding support of the U.S. Air Force Research Laboratory (AFRL), the U.S. Air Force Office of Scientific Research (AFOSR), the U.S. Defense Advanced Research Projects Agency (DARPA), the U.S. Department of Defense through the Multidisciplinary University Research Initiative (MURI) in Cyber Infrastructure Protection (CIP) Program, the Advanced Research and Development Activities (ARDA) of the U.S. Intelligence Community, Symantec Corporation, and General Dynamics C4 Systems. I have enjoyed working with many of my program managers and collaborators at these organizations. I would like to thank them for their interest in my research work and their support. A special thank you goes to Joseph Giordano at AFRL who truly is a pioneer and a visionary leader in the field of computer and network security. I appreciate not only his interest and support for my research work in the past ten years but also his kindness and understanding that he generously shares with people working with him. It is a true pleasure working with him and some others at AFRL, including John Faust and Patrick Hurley.

I would also like to thank Gary Hogg, Peter Crouch, and Ronald Askin for their encouragement and support of my research work at Arizona State University in many ways. I gratefully acknowledge the research assistance from my students. In addition to those students whose joint research papers with me have been published and are listed in the references of this book, I would like to thank Napatkamon Ayutyanont for her research assistance in a timely manner throughout several years, although our joint research papers have not yet been published.

It is my pleasure to work with many people at John Wiley & Sons who worked with me on this book project, and I appreciate their generous and professional help in publishing this book.

Mostly, I would like to thank my husband, Baijun Zhao, and our daughter, Alice Zhao. This book would not have been possible without their love and support.

Nong Ye
Arizona State University
USA

Contents

Part II Secure System Architecture and Design

Part IV Cyber Attack Detection: Signature Recognition

Part V Cyber Attack Detection: Anomaly Detection

Part VI Cyber Attack Detection: Attack Norm Separation

Part VII Security Incident Assessment