SYNGRESS

RESEARCH METHODS FOR CYBER SECURITY

Thomas W. Edgar | David O. Manz

RESEARCH METHODS FOR CYBER SECURITY

Thomas W. Edgar | David O. Manz

A systematic methodology for improving cyber security research

Research Methods for Cyber Security teaches scientific methods for generating impactful knowledge, validating theories, and adding critical rigor to the cyber security field. This book shows how to develop a research plan, beginning by starting research with a question, then offers an introduction to the broad range of useful research methods for cyber security research: observational, mathematical, experimental, and applied. Each research method chapter finishes with recommended outlines and suggested templates for submission to peer reviewed venues. This book concludes with information on cross-cutting issues within cyber security research.

Cyber security research contends with numerous unique issues, such as an extremely fast environment evolution, adversarial behavior, and the merging of natural and social science phenomena. ***Research Methods for Cyber Security*** addresses these concerns and much more by teaching readers not only the process of science in the context of cyber security research, but providing assistance in execution of research as well.

Key features

- Presents research methods from a cyber security science perspective
- Catalyzes the rigorous research necessary to propel the cyber security field forward
- Provides a guided method selection for the type of research being conducted, presented in the context of real-world usage

Thomas W. Edgar, Senior Cyber Security Scientist, Pacific Northwest National Laboratory

David O. Manz, Senior Cyber Security Scientist, Pacific Northwest National Laboratory

COMPUTER SECURITY

ISBN 978-0-12-805349-2

58995

9 780128 053492

ELSEVIER

SYNGRESS

elsevier.com/books-and-journals

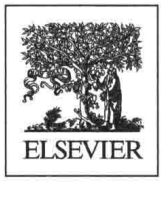
RESEARCH METHODS FOR CYBER SECURITY

Edgar | Manz

SYNGRESS

Research Methods for Cyber Security

Thomas W. Edgar
David O. Manz



SYNGRESS®

Syngress is an imprint of Elsevier
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-805349-2

Publisher: Todd Green
Acquisition Editor: Brian Romer
Editorial Project Manager: Anna Valutkevich
Production Project Manager: Punithavathy Govindaradjane
Cover Designer: Mark Rogers

Typeset by MPS Limited, Chennai, India

Research Methods for Cyber Security

About the Authors

Thomas W. Edgar is a Senior Cyber Security Research Scientist at the Pacific Northwest National Laboratory. He has completed research in the areas of secure communication protocols, cryptographic trust management, critical infrastructure protection, and developing a scientific approach to cyber security. Edgar's research interests include the scientific underpinnings of cyber security and applying scientific-based cyber security solutions to enterprise and critical infrastructure environments. His expertise lies in scientific process, critical infrastructure security, protocol development, cyber forensics, network security, and testbed and experiment construction. Edgar has a B.S. and M.S. in Computer Science from the University of Tulsa with a specialization in information assurance.

David O. Manz is currently a Senior Cyber Security Scientist in the National Security Directorate at the Pacific Northwest National Laboratory. He holds a B.S. in Computer and Information Science from the Robert D. Clark Honors College at the University of Oregon and a Ph.D. in Computer Science from the University of Idaho. Manz's work at PNNL includes enterprise resilience and cyber security, secure control system communication, and critical infrastructure security. Enabling his research is an application of relevant research methods for cyber security (Cyber Security Science). Prior to his work at PNNL, Manz spent 5 years as a researcher on Group Key Management Protocols for the Center for Secure and Dependable Systems at the University of Idaho (U of I). Manz also has experience in teaching undergraduate and graduate computer science courses at U of I, and as an adjunct faculty at Washington State University. Manz has co-authored numerous papers and presentations on cyber security, control system security, and cryptographic key management.

Foreword

The security field—whether one calls it security, cybersecurity, information assurance, information security, or something else—is delightfully frustrating, being an field that both moves at a glacial pace, and literally transforms itself overnight. There are so many challenges! Connect two previously disparate systems, and very often, system security properties (and vulnerabilities) will be entirely different. Change the user community from, say, a highly regulated government agency to a family home, and the methodologies we accept in the name of security become unacceptable. One does not fire the family 5-year old because she writes down a password! As scientists, how do we measure these differences?

There is also the question about what security actually means. We might start informally, and say that security means making sure that systems do "what we want." Our next step might be to see whether the system in fact does what we want, and take steps toward designing security in. But—consider categories such as confidentiality, integrity, and availability. These are often used to bin "what we want" into manageable chunks, so as to whether these properties are preserved. If one steps away from pure mathematical rigor, it is easy to spot a problem with designing in security. Security properties are not inherently good or bad. That value judgment is situational. If we are attempting to shut down a spam botnet, many of us hope the "availability" property can be defeated. The owners (or renters) of the botnet might disagree. Is there a way that we can conduct a general experiment to see when availability holds?

As well, new possible security concerns emerging all the time. Two current debates: is privacy a subset of security? What about cyber physical systems—is there a line between fault tolerant approaches that prevent mechanical failures, and security features intended to preserve availability? Does it make a difference if we are talking about a nuclear power plant or an autonomous vehicle? Here is a newer one. Machine learning is ubiquitous—is it a security issue if machine learning algorithms used in job applicant selection (say)

might lead to discrimination against certain parts of the population? What is adversarial machine learning—and can it be detected? There is no shortage of questions, and the field seems more likely to expand than to shrink. As researchers and scientists, we need to decide how to approach these questions in a useful manner.

Fortunately, although the security field does not lend itself to easy answers, progress has been made in how we approach such questions about security, and this has been one of the more important contributions of the emerging Science of Security community. And, as a practical matter, it is in helping the reader discover how to pose and answer such questions using a scientific methodology that this book by Dr. Manz and Mr. Edgar shines. They have included a wealth of ideas that should be helpful to researchers, from how to get started with research in security, to thinking through the kinds of scientific investigation that would be most applicable. They also have more complex considerations involving experimentation, operating in a real-world environment (especially when you cannot afford to break the system under scrutiny!), and how to produce results that will serve as a foundation for other researchers, through replication and other methods. The authors do an excellent job of making it easy to understand how to apply traditional scientific concepts; and this will help both new researchers and more advanced practitioners achieve results that will stand the test of time.

One last thought. Science, like security, is complex. We cannot always control every variable, nor do we always know exactly what to measure. It is important to remember that security itself is a new field, and we have not yet achieved the remarkable precision of measurement that one finds in long-standing disciplines, such as physics, and even in the most upscale physics laboratories, we still today see measurement tools and sensors enhanced with duct tape and foil. Science, like security, is constantly under refinement. Those of us who practice this still-new field of a rigorous approach to security questions are often learning as much about how to conduct that science as we are about security. Many thanks to the authors, who have articulated the scientific approach of today, in hopes that it will support good work in the present, and enable others to do an even better in the future.

Deborah A. Frincke

Preface

PURPOSE

Working as professional researchers at a U.S. national research laboratory has provided us with a couple of unique perspectives. First, we have been uniquely involved in a nexus of academic, government, and industry research, privy to the perceptions and processes of each. Second, we work in an environment where we are often able to work with researchers and rub shoulders across a spectrum of fields: biology, chemistry, ecology, physics, and so on. Through these perspectives we have, over the years, noticed how little the cyber security field understands and leverages scientific methods.

Cyber security is a young field of science. As it naturally grew out of the computer science field, it has a strong grounding in mathematical science. Owing to its relative youth, cyber security academic programs have not matured and do not teach scientific methods to students. We posit this is core to the field's inability to generate general and impactful theories. There is a need for a reference book that presents a scientific approach to cyber security and the importance of rigor in research.

Currently, the cyber security field is in a red queen's race, defensive researchers are expending great amounts of resources to maintain status quo with attackers. However, ground is being lost. Tremendous effort is spent on trying to come up with the next killer app or an exploit for the last years app. There is an insufficient amount of effort to discover the fundamental science of cyber security. In our journey to discover how to define and measure cyber security, we have come to the belief that our field needs to progress through the use of research methods. The purpose of this book is to provide an introduction to research methods that we, or our colleagues, have found useful in performing cyber security research.

AUDIENCE

This book is intended for undergraduate students, graduate students, and faculty who seek to understand how to execute cyber security research. Additionally, the information in this text can both be used by researchers as an introductory text for scientific research in the context of cyber security, or as a guide and reference for those seeking to execute specific research. By reading straight through the book, a perspective on cyber security science and an understanding of the various issues and methods of executing research can be gained. However, if a reader has a specific research question they would like to investigate and answer, then the book provides a path to help drive straight to the most appropriate chapter that is of relevance and help.

While designed for university coursework, the information in this book can also be useful and beneficial for professional cyber security practitioners. Obviously, this book can be used as a reference and refresher for cyber security researchers and developers. Cyber forensics investigations require rigorous, procedural methodology. Applying scientific methodology and concepts can provide the necessary rigor of developing supporting evidence as well as bringing a skeptical eye to the challenge. Cyber incident response and analysis is largely a process of asking questions and answering hypotheses of what occurred. Observational and experimental research methods are helpful techniques in these endeavors. Our hope is that this book can bring a new perspective and thought process to the entire field of cyber security for researchers and practitioners.

ORGANIZATION AND STYLE

This book is organized around two pathways of use. The first is the common straight read-through to learn all of the concepts and techniques. Reading each chapter in sequence will provide an overview of all research methods as well as approaches to answering research questions. Information in earlier chapters are leveraged and built upon in later chapters. Additionally, a second style of use is for readers who have a specific research question or project they would like to execute. Chapter 3 provides logic and reasoning for selecting a research approach and method and then provides directions to the appropriate chapter covering those topics. This enables users who are after guidance and reference to quickly get to the information they need.

This book is separated into six different parts. Each part covers a grouping of information: an introduction to science and cyber security, observational research, formal research, experimental research, applied research, and useful ancillary materials. Within each part, there are multiple chapters. Each

chapter covers a specific topic. The research method chapters leverage example research to help show the process in and reasoning behind using specific methods. The examples are loosely based on real research, we or colleagues, we know have performed in the past. All data and results are fictional and were designed to highlight aspects and issues of the research process.

We purposely used a more informal style in this book. Our goal is to teach the concepts and practice of research in an approachable, everyday manner. Our hope is that readers find this style readable and unintimidating. As professional researchers, we are aware of and have to deal with the realities of performing research and, while some philosophy of science is discussed, we try to address limitations in the text.

To provide extra insights and fun discussions we have provided breakout boxes throughout the text. There are two types of breakout boxes: *Did You Know?* and *Dig Deeper*. The *Did You Know?* boxes provide fun and interesting facts surrounding information that is covered in the text. *Dig Deeper* boxes discuss topics in more depth and direct readers to where further information on a topic can be found. The intent of these boxes are to provide a fun pedagogical aid for students and readers.

Acknowledgments

We appreciate the expertise and hard work provided by our colleagues in assisting with topics needed to fill the full spectrum of research methods:

Chapter 1 Mark Tardiff

Chapter 6 Satish Chikkagoudar, Samrat Chatterjee, Dennis G. Thomas, Thomas E. Carroll, George Muller

Chapter 7 Thomas E. Carroll

Special thanks goes to our publisher team at Elsevier; Brian Romer for supporting the idea for this book and Anna Valutkevich for her extreme patience and guidance in helping us reach the finish line.

Finally, our most heartfelt thanks goes out to our spouses and children: Sharon Edgar, Alexis Edgar, Caitlin Manz, Matthew Manz, and Henry Manz. Our wives' support and patience with this process allowed this book to come to fruition and our children were always helpful in keeping a smile on our faces through this long process. Additional thanks goes to Caitlin Manz for providing her editorial eye and review skills to turn our professorial babbling into clear and concise text.