PLEASE READ BEFORE PROCEEDING

Dear Syngress Customer:

This PDF document is digitally signed by Syngress Publishing. It is recorded as being licensed exclusively to the single-user who purchased it from www.syngress.com. Other than the initial password required to open the document, none of the navigation, print, copy, or edit functions have been disabled. We have done this so that you as an IT Professional can derive the maximum benefit from our product. Once you have saved the document, you may even disable the password requirement by using Adobe Acrobat's "Security Options" menu.

Please read this license, and if it is not acceptable, notify us at customercare@syngress.com within three days of your purchase for a refund. We appreciate your loyalty and thank you in advance for protecting your purchase and our intellectual property.

SYNGRESS PUBLISHING Single-User Ebook License Agreement

This is a legal agreement between you, the end user and Syngress Publishing, Inc. regarding your use of this Syngress copyrighted ebook. (collectively, "Ebook"). By proceeding beyond this page, you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, do not download the Ebook. Promptly notify Syngress Publishing at customercare@syngress.com for a complete refund of your purchase.

1. Grant of License. Syngress hereby grants to you (an individual) the revocable, personal, non-exclusive, and nontransferable right to install and activate the Ebook on two separate computers solely for your personal and non-commercial use. Sharing this Ebook with other individuals, or allowing other individuals to view the contents of this Ebook, is in violation of this license. You may not make the Ebook available on a network, or in any way provide the Ebook to multiple users, unless you have first purchased a multi-user workstation license from Syngress.
2. Copyright. The Ebook is owned by Syngress and protected by United States and international copyright law. You may not remove or conceal any proprietary notices, labels or marks from the Ebook.
3. Restrictions on Use. Except as noted hereunder, you may not, and you may not permit others modify, distribute, or create derivative works of the Ebook; copy (other than one back-up copy), distribute, publicly display, transmit, sell, rent, lease or otherwise exploit the Ebook. You may use any of the features available in The Adobe Acrobat readers to comment, highlight, print, or otherwise annotate the Ebook so long as no change is made to the original content of the Ebook
4. Term of Agreement. The term of this Agreement begins upon download of this Ebook and shall terminate 10 years from the date of purchase. Syngress reserves the right to terminate this Agreement at any time if you violate any provision of this Agreement. If the Agreement is terminated for any reason, you agree immediately to return to Syngress all copies of this Ebook and all accompanying items.

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work. There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state. In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

SYNGRESS®

"This novel is scarily realistic."

—James A. Whittaker, Ph.D., Chief Scientist and Founder of Security Innovation

THE Mezonic Agenda

HACKING THE PRESIDENCY

A Novel by

Dr. Herbert H. Thompson

Spyros Nomikos

What People are Saying About *The Mezonic Agenda*

"Hackers and spies, what an appealing mix… I can't wait for the sequel!"

—Sarah Gordon, Security Researcher

"Cyber threat hits home in a very realistic manner. This really could happen"

—Greg Miles,Ph.D., CISSP, President Security Horizon, Inc.

"This novel is scarily realistic and I know Herbert Thompson well enough that I am sure whoever he is voting for will win the next election!"

—James A. Whittaker, Ph.D., Chief Scientist and Founder of Security Innovation

"Entertainment is the best way to communicate complex ideas. *The Mezonic Agenda: Hacking the Presidency* is an enjoyable electronic crime novel that simplifies complex technologies and reveals the dangers of electronic voting, a page-turner that shows how people in power might manipulate electronic voting and undermine democracy - and how they might be stopped."

—Richard Thieme, Author of "Islands in the Clickstream"

Imagine a scenario whereby the U.S. presidential election could be manipulated through ingenuity, stealth, and the exploitation of flaws inherent in the technology used to tabulate the vote. Now imagine that the flawed technology isn't cardboard chads, rather, it's the allegedly hack-proof software used by the Federal Elections Committee to gather and calculate the popular vote. What's more, the culprits aren't overworked precinct monitors; instead they're brilliant programmers working for a foreign corporation committed to a favorable election outcome at any cost. You now have the essence *The Mezonic Agenda.*

Register for Free Membership to

solutions@syngress.com

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2000*, Brian Caswell and Jay Beale's *Snort 2.0 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy to search web page, providing you with the concise, easy to access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

SYNGRESS®

THE Mezonic Agenda

HACKING THE PRESIDENCY

HACK ALONG WITH THE HEROES AND VILLAINS AS THE AMERICAN PRESIDENCY HANGS IN THE BALANCE OF CYBER-SPACE

Dr. Herbert H. Thompson
Spyros Nomikos

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	67GAW5PLDR
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

The Mezonic Agenda: Hacking the Presidency

Copyright © 2004 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 1-931836-83-3

Publisher: Andrew Williams
Acquisitions Editor: Christine Kloiber
Technical Reviewer: Russ Rogers
Cover Designer: Michael Kavish
Copy Editor: Adrienne Rebello
Page Layout and Art: Patricia Lupien

Distributed by O'Reilly & Associates in the United States and Canada.
For information on rights and translations, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

Jeff Moss and Ping Look from Black Hat, Inc. You have been good friends to Syngress and great colleagues to work with. Thank you!

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly is incredible and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Lynn Schwartz, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, and Rob Bullington.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack, and Krista Leppiko, for making certain that our vision remains worldwide in scope.

David Buckland, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.

Authors

Herbert H. Thompson, Ph.D., is Director of Security Technology at Security Innovation Inc. (www.securityinnovation.com). He earned his Ph.D. in Applied Mathematics from the Florida Institute of Technology and is co-author of *How to Break Software Security: Effective Techniques for Security Testing* (Addison-Wesley, 2003). Herbert has over 50 academic and industrial publications on software security, and frequently writes for industrial magazines including: *Dr. Dobbs Journal*, *IEEE Security and Privacy*, *Journal of Information and Software Technology*, *ACM Queue* and *Better Software Magazine*. He has spoken on software security throughout the United States, Europe, and Asia at conferences such as STAR, Quality Week, SD Expo, RSA, Gartner, RUC, ACM SAC and COMPSEC to name a few. He has won numerous best presentation awards for his lectures and is often asked to give conference keynotes. At Security Innovation, he leads research efforts on software security and trains security testers at some of the world's largest software companies. Herbert is also the principal investigator on several grants from the U.S. Department of Defense.

Spyros Nomikos holds a BS and MS in Chemical Engineering from the Florida Institute of Technology. He has worked for numerous fuel cell companies developing future hydrogen systems. His expertise is in systems design, safety analysis, and new product development. He is published and presented in various conferences on subjects such as hyperthermophillic bacteria, fuel cells and hydrogen.

Technical Reviewer

Russ Rogers (CISSP, CISM, IAM) is a Co-Founder, Chief Executive Officer, and Principle Security Consultant for Security Horizon, Inc; a Colorado-based professional security services and training provider and veteran owned small business. Russ is a key contributor to Security Horizon's technology efforts and leads the technical security practice and the services business development efforts. Russ is a United States Air Force Veteran and has served in military and contract support for the National Security Agency and the Defense Information Systems Agency. Russ is also the editor-in-chief of 'The Security Journal' and occasional staff member for the Black Hat Briefings. Russ holds an associate's degree in Applied Communications Technology from the Community College of the Air Force, a bachelor's degree from the University of Maryland in computer information systems, and a master's degree from the University of Maryland in computer systems management. Russ is a member of the Information System Security Association (ISSA) and the Information System Audit and Control Association (ISACA). He is also an Associate Professor at the University of Advancing Technology (uat.edu), just outside of Phoenix, Arizona. Russ is the author of *Hacking a Terror Network: The Silent Threat of Covert Channels* (Syngress, ISBN 1-928994-98-9). He has contributed to many books including: *Stealing the Network: How to Own a Continent* (Syngress, ISBN: 1-931836-05-1), *Security Assessment: Case Studies for Implementing the NSA IAM* (Syngress, ISBN 1-932266-96-8), *WarDriving, Drive, Detect, Defend: A Guide to Wireless Security* (Syngress, ISBN: 1-931836-03-5) and *SSCP Study Guide and DVD Training System* (Syngress, ISBN: 1-931846-80-9).

Contents

Part I

The Mezonic Agenda: Hacking the Presidency 1

In six days Chad Davis will testify before Congress on the security, stability, and safety of Advice Software Inc.'s e-vote software. He is a world-renowned expert on software security, and his testimony will determine if the software will be implemented for use during the 2004 U.S. Presidential Elections. All is well until he receives a cryptic CD on the software from a notorious hacker, which ignites a string of murders and uncovers a dangerous conspiracy. A race against the clock, Davis must use his knowledge of buffer overflows, format string vulnerabilities and zero-day exploits to penetrate physical and cyber defenses, ultimately uncovering Advice's plot to fix the US presidential elections. What's the software's secret? Will Davis find out before his testimony? What is *The Mezonic Agenda*?

Prologue: Seattle, WA 3
October 2, 2003

Chapter 1: Seattle, WA 5
University of Washington, Six Months Later

Chapter 2: Macau, China 8
Mezonic Corporation: Corporate Headquarters

Chapter 3: Amsterdam, the Netherlands 13
RSA Conference: RAI Convention Center

Chapter 4: Amsterdam, the Netherlands 27
Schiphol International Airport

Chapter 5: Amsterdam, the Netherlands 30
RSA Conference

Chapter 6: Amsterdam, the Netherlands 45
Baff Lexicon's Apartment

Chapter 7: Amsterdam, the Netherlands 50
Victoria Hotel

Chapter 8: Amsterdam, the Netherlands 52
Red Light District

Chapter 9: Amsterdam, the Netherlands 55
Apartment of Baff Lexicon

Chapter 10: Amsterdam, the Netherlands 58
The Holland Casino and Hard Rock Café

Chapter 11: Seattle, WA 61
Advice Software, Inc.

Chapter 12: Amsterdam, the Netherlands 64
Chad Davis's Hotel Room, Victoria Hotel

Chapter 13: Amsterdam, the Netherlands 67
Schiphol Airport

Chapter 14: Amsterdam, the Netherlands 70
Schiphol Airport

Chapter 15: Seattle, WA 78
Chad Davis's Home

Chapter 16 Seattle, WA 80
Chad Davis's Home

Chapter 17: Washington, D.C. 84
Senator Shift's Home

Chapter 18: Seattle, WA 88
Chad Davis's Home

Chapter 19: Amsterdam, the Netherlands 102
Red Light District

Chapter 20: Seattle, Washington 104
Saturday: Starbucks

Chapter 21: Seattle, WA 119
Starbucks

Chapter 22: Seattle, WA 127
Chris Payne's Home

Chapter 23: Seattle, WA 130
Chad Davis's Home

Chapter 24: Washington, D.C. 134
Senator Shift's Home

Chapter 25: Seattle, WA 137
Chad Davis's Home

Chapter 26: Seattle, WA 140
Chad Davis's Home

Chapter 27: Seattle, WA 154
Chris Payne's Home

Chapter 28: Seattle, WA 158
Chad Davis's Home

Chapter 29: Seattle, WA 162
Chad Davis's Home

Chapter 30: Seattle, WA 170
Outside of Elizabeth Davis's Middle School

Chapter 31: Seattle, WA 175
En route to Airport

Chapter 32: Washington, D.C. 177
Dulles International Airport

Chapter 33: Washington, D.C. 182
Chris Payne's Hotel Suite

Chapter 34: Washington, D.C. 193
Chad Davis's Hotel Room

Chapter 35: Washington, D.C. 202
Chad Davis's Hotel Room

Chapter 36: Washington, D.C. 204
Chris Payne's Suite

Chapter 37: Washington, D.C. 209
U.S. Congress: Waiting Room

Chapter 38: Washington, D.C. 212
U.S. Congress

Chapter 39: Washington, D.C. 216
U.S. Congress

Chapter 40: Washington, D.C. 235
U.S. Congress

Epilogue 239
Flight 304, Washington D.C. to Seattle, WA

Part II 243

The Technology behind *The Mezonic Agenda*

In *The Mezonic Agenda*, Chad Davis is a computer expert who must use all of his skills and knowledge to unlock the CD and solve the secret of Advice's software. The story may be fiction, but the science is all too real. Every day, real-life security experts use the methodology and tactics implemented by Davis in the story. The following appendices touch upon these technologies, their history, and their role in the present-day. From the origins of voting to the modern-era realm of buffer overflows, you'll be given a tour of the technology behind *The Mezonic Agenda*.

Appendix A A Brief History of Voting: Origins to Modern Implementations 245

Introduction 246
A Brief Review of the Electoral College 246
Voting Systems and Their History 249
Paper Ballots 252
Mechanical Lever Machines 253
Punch Cards 254
Votomatic 255
Datavote 255
Optical Scan Ballots (Marksense) 258
Direct Recording Electronic Systems 260
How Do DREs Work? 261
Diebold (www.diebold.com) 264
Election Systems & Software (www.essvote.com) 266
Sequoia 269

Hart InterCivic (www.eslate.com) 269
SERVE and Internet Voting 270
California's Internet Voting Report 271
Voting Over the Internet (VOI) 271
SERVE 271
VoteHere (www.votehere.net) 272
The Attacks 273
But I've Bought Stuff Online Using my Credit Card… and That's Secure, Right? .274
Certifying Software 276
Conclusion: What's the Right Answer? 277
References 278

Appendix B Reverse Engineering 281
Introduction 282
Who's Doing Reverse Engineering and Why? . . .285
Underground Reverse Engineers 286
Governments 286
Corporations 287
Academia 287
Tools of the Trade 288
Static Analysis Tools 289
Hex Editors 289
Disassemblers 289
Decompilers 290
Other Tools 290
Dynamic Analysis Tools 290
Debuggers 291
Emulators 291
Other Tools 291
The Reverse-Engineering Process 292
Reverse Engineering and the Law 300

A Legal History of Software Copyrights in the United States 300
Reverse Engineering 303
DMCA 304
Exceptions 305
Safe Harbors 308
First Legal Challenges to the DMCA 309
Beyond U.S. Copyright Law 312
Legal Implications of Reverse Engineering . . . 312
Reverse Engineering in The Mezonic Agenda . . .313
References 314

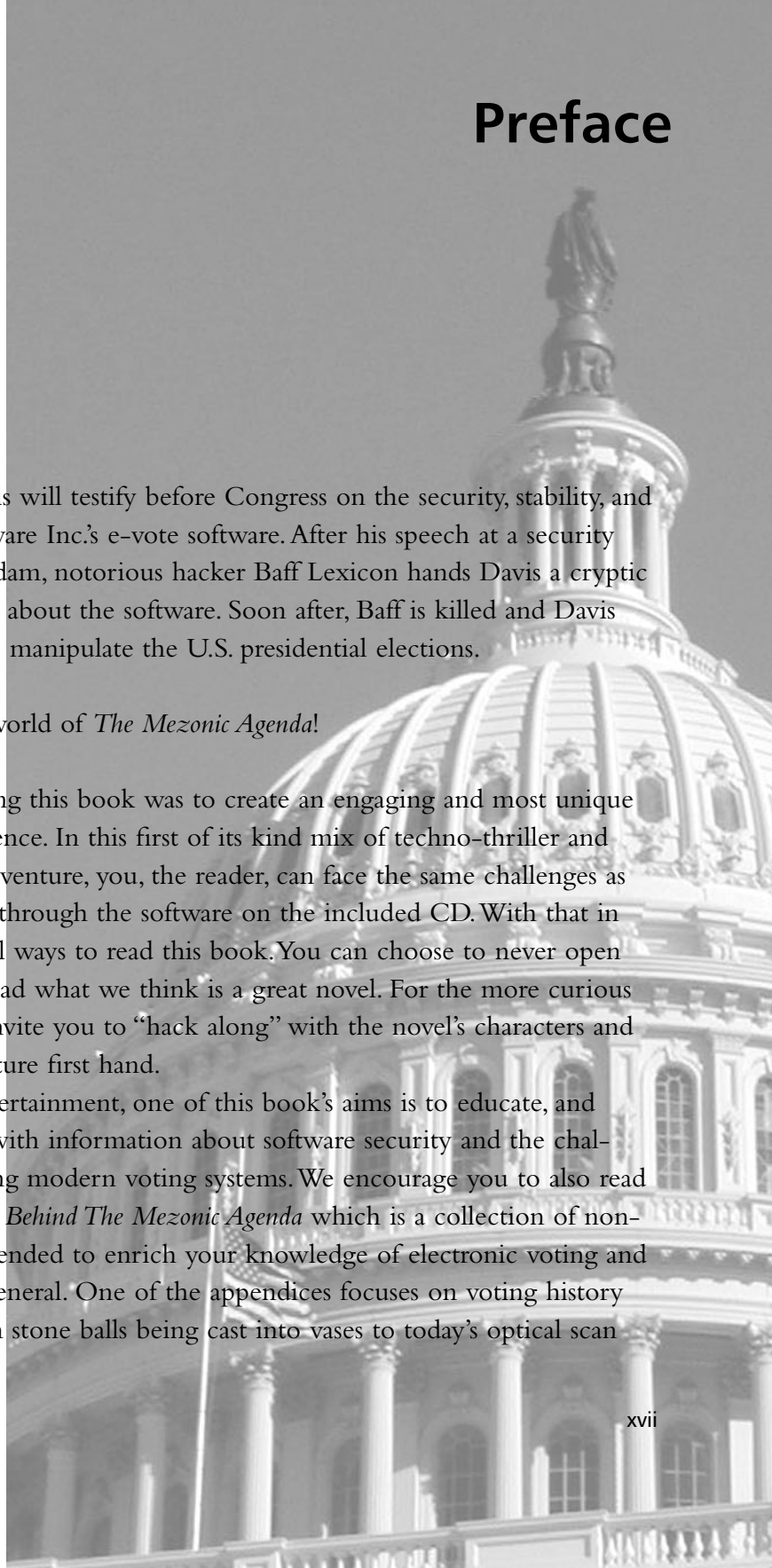
Appendix C Cryptography 317
History of Cryptography 318
Symmetric Encryption 321
Block Ciphers 322
Monoalphabetic Substitution Ciphers 324
Polyalphabetic Substitution Ciphers 325
Asymmetric Encryption 325
RSA 326
ElGamal 326
Cryptography and The Mezonic Agenda 327
References 328

Appendix D Buffer Overflows 329
Introduction 330
Stack Overflows 331
Exploiting Stack Overruns: An End-to-End Windows Example 339
Heap Overflows 349
Buffer Overflows in The Mezonic Agenda 354
References 355

Appendix E Steganography 357
Introduction 358
Types of Stego 358
Insertion Stego 360
Substitution Stego 362
How Does It Work? 362
A Quick Example 364
Generation Stego 364
Steganography in The Mezonic Agenda 365
References 368

Contest Rules 369

Preface



In six days Chad Davis will testify before Congress on the security, stability, and safety of Advice Software Inc.'s e-vote software. After his speech at a security conference in Amsterdam, notorious hacker Baff Lexicon hands Davis a cryptic CD with information about the software. Soon after, Baff is killed and Davis must unravel a plot to manipulate the U.S. presidential elections.

Welcome to the world of *The Mezonic Agenda*!

Our goal in writing this book was to create an engaging and most unique entertainment experience. In this first of its kind mix of techno-thriller and interactive hacking adventure, you, the reader, can face the same challenges as the novel's characters through the software on the included CD. With that in mind, there are several ways to read this book. You can choose to never open the CD and simply read what we think is a great novel. For the more curious reader, however, we invite you to "hack along" with the novel's characters and experience the adventure first hand.

In addition to entertainment, one of this book's aims is to educate, and empower the reader with information about software security and the challenges of implementing modern voting systems. We encourage you to also read Part II: *The Technology Behind The Mezonic Agenda* which is a collection of non-fiction appendices intended to enrich your knowledge of electronic voting and software security in general. One of the appendices focuses on voting history and its evolution from stone balls being cast into vases to today's optical scan

and electronic systems. The other appendices take a piercing look at software security, cryptography, steganography, reverse engineering and software exploits.

We hope you enjoy reading this book as much as we've enjoyed researching and creating it. Please visit the books companion website at www.mezonica-genda.com for new challenges and more information on all of the topics discussed in the novel. Thanks and enjoy!

Herbert H. Thompson
Spyros Nomikos
August 2004

About the CD

Now you can hack along with the heroes and villains of *The Mezonic Agenda*! Don't just read it, experience it!

Notorious hacker Baff Lexicon has just handed internationally renowned software security expert Dr. Chad Davis a cryptic CD. Davis must decrypt this CD's contents to reveal the secrets behind Advice Software's e-voting system, a secret that has cost the lives of several people and holds the American Presidency in the balance.

Hack along with Davis as he tries to unlock the CD's mysteries. Unzip the contents to access the data on the CD. You will then have three files, and your first challenge is to decrypt one of them: encrypted.dat, where you will receive several more challenges. The CD's mysteries will be revealed in the story and you can either: read the novel and ignore the CD, perform the hacks as they appear in the novel, or the more aspiring techie can try and decrypt the CD contents without reading too far into *The Mezonic Agenda*. Do you have what it takes to expose Advice Software Inc. and ultimately save the Nation's general election from disaster? There's only one way to find out…

Visit www.mezonicagenda.com for more information and new challenges!

About the Contest

The Mezonic Agenda: Hacking the Presidency Contest challenges you, the reader, to interact with the book and CD, decrypt its contents, and ultimately control the fate of a mock U.S. Presidential Election. Contestants will attempt to vote for themselves as the winning candidate during our "simulated" election to be held in early 2005. Contestants must use their hacking skills, along with strategy, to manipulate the results of the Mezonic "mock" election. Visit www.mezonicagenda.com to enter.

Any eligible contestant can download the software from the Mezonic Agenda: Hacking a Presidency website (www.mezonicagenda.com) without having to purchase the book. The book, though, will help the reader better understand how the software works, teach them software hacking skills and ultimately aid in its exploitation.

Prizes include a free pass to the 2005 Black Hat Briefings in Las Vegas and a suite of security books from Syngress Publishing.

Syngress may require any participant receiving any prize to provide Syngress with proof that he or she is eligible to participate according to the eligibility requirements hereunder. See "The Mezonic Agenda Hack Contest Rules" in the back of the book or visit www.mezonicagenda.com for complete contest rules.