

**4 FREE BOOKLETS**

YOUR SOLUTIONS MEMBERSHIP



# RFID Security

## Protect the Supply Chain

- Learn the Different Types of RFID Attacks: Tag Encoding, Tag Application, Attacking the Backend
- Protect the Consumer and Master Identity Management in RFID
- Avoid Industrial Espionage

**Frank Thornton**

**Brad Haines**

**Anand M. Das**

**Hersh Bhargava**

**Anita Campbell**

**John Kleinschmidt** Technical Editor



# VISIT US AT

**www.syngress.com**

Syngress is committed to publishing high quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our website.

## **SOLUTIONS WEBSITE**

To register your book, visit [www.syngress.com/solutions](http://www.syngress.com/solutions). Once registered, you can access our [solutions@syngress.com](mailto:solutions@syngress.com) web pages. There you will find an assortment of value added features such as free e-booklets related to the topic of this book, URLs of related website, FAQs from the book, corrections, and any updates from the author(s).

## **ULTIMATE CDs**

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

## **DOWNLOADABLE EBOOKS**

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These eBooks are often available weeks before hard copies, and are priced affordably.

## **SYNGRESS OUTLET**

Our outlet store at [syngress.com](http://syngress.com) features over-stocked, out of print, or slightly hurt books at significant savings.

## **SITE LICENSING**

Syngress has a well established program for site licensing our ebooks onto servers in corporations, educational institutions, and large organizations. Contact us at [sales@syngress.com](mailto:sales@syngress.com) for more information.

## **CUSTOM PUBLISHING**

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for use with their organization. Contact us at [sales@syngress.com](mailto:sales@syngress.com) for more information.



# RFID Security

Frank Thornton

Brad Haines

Anand M. Das

Hersh Bhargava

Anita Campbell

John Kleinschmidt Technical Editor

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	GH925537BQ
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

#### **PUBLISHED BY**

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

#### **RFID Security**

Copyright © 2006 by Syngress Publishing, Inc. All rights reserved. Printed in Canada. 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 Canada

1 2 3 4 5 6 7 8 9 0

ISBN: 1-59749-047-4

Publisher: Andrew Williams  
Acquisitions Editor: Jaime Quigley  
Technical Editor: John Kleinschmidt  
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien  
Copy Editor: Judy Eby  
Indexer: Nara Wood

Distributed by O'Reilly Media, Inc. in the United States and Canada.

For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email [matt@syngress.com](mailto:matt@syngress.com) or fax to 781-681-3585.



# Acknowledgments

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

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are 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, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, Rob Bullington, and Aileen Berg.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

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

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.







# Lead Author

**Frank Thornton** runs his own technology consulting firm, Blackthorn Systems, which specializes in wireless networks. His specialties include wireless network architecture, design, and implementation, as well as network troubleshooting and optimization. An interest in amateur radio helped him bridge the gap between computers and wireless networks. Having learned at a young age which end of the soldering iron was hot, he has even been known to repair hardware on occasion. In addition to his computer and wireless interests, Frank was a law enforcement officer for many years. As a detective and forensics expert he has investigated approximately one hundred homicides and thousands of other crime scenes. Combining both professional interests, he was a member of the workgroup that established ANSI Standard “ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information.” He co-authored *WarDriving: Drive, Detect, and Defend: A Guide to Wireless Security* (Syngress Publishing, ISBN: 1-93183-60-3), as well as contributed to *IT Ethics Handbook: Right and Wrong for IT Professionals* (Syngress, ISBN: 1-931836-14-0) and *Game Console Hacking: Xbox, PlayStation, Nintendo, Atari, & Gamepark 32* (ISBN: 1-931836-31-0). He resides in Vermont with his wife.

*Dedicated to my wife, Gerry  
For the many years of love and support*



# Contributors

**Brad ‘RenderMan’ Haines** is one of the more visible and vocal members of the wardriving community, appearing in various media outlets and speaking at conferences several times a year. Render is usually near by on any wardriving and wireless security news, often causing it himself. His skills have been learned in the trenches working for various IT companies as well as his involvement through the years with the hacking community, sometimes to the attention of various Canadian and American intelligence agencies. A firm believer in the hacker ethos and promoting responsible hacking and sharing of ideas, he wrote the ‘Stumbler ethic’ for beginning wardrivers and greatly enjoys speaking at corporate conferences to dissuade the negative image of hackers and wardrivers.

His work frequently borders on the absurd as his approach is usually one of ignoring conventional logic and just doing it. He can be found in Edmonton, Alberta, Canada, probably taking something apart.

**Anita Campbell** is a consultant, speaker, and writer who closely follows trends in technology, including the development of the RFID market. She writes for a number of publications, and serves as the Editor for the award-winning RFID Weblog, named to the CNET Blog 100, and syndicated on MoreRFID.com. She is a part-time instructor at the University of Akron and is also the host of her own talk radio program/podcast series on the VoiceAmerica.com Internet radio network.

Anita has held a variety of senior executive positions culminating in the role of CEO of an information technology subsidiary of Bell & Howell. She also has served on a number of Boards, including Vice Chair of the Advisory Board, Center for Information Technology and eBusiness at the University of Akron. Anita holds a B.A. from Duquesne University and a J.D. from the University of Akron Law School.

**Anand M. Das** has seventeen plus years of experience creating and implementing business enterprise architecture for the Department of Defense (DOD) and the commercial sector. He is founder and CTO of Commerce Events, an enterprise software corporation that pioneered the creation of RFID middleware in 2001. Anand is a founding member of EPCglobal and INCITS T20 RTLS committee for global RFID and wireless standards development. He formulated the product strategy for AdaptLink™, the pioneer RFID middleware product, and led successful enterprise wide deployments including a multi-site rollout in the Air Force supply chain. Previously he was Vice President with SAIC where he led the RFID practice across several industry verticals and completed global rollouts of RFID infrastructure across America, Asia, Europe and South Africa. He served as the corporate contact for VeriSign and played a key role in shaping the EPCglobal Network for federal and commercial corporations. Earlier, he was chief architect at BEA systems responsible for conceptualizing and building the Weblogic Integration suite of products. He has been a significant contributor to ebXML and RosettaNet standard committees and was the driving force behind the early adoption of service-oriented architecture. Anand has held senior management positions at Vitria, Tibco, Adept, Autodesk and Intergraph.

Anand has Bachelor of Technology (Honors) from IIT Kharagpur and Master of Science from Columbia University with specialization in computer integrated manufacturing. He served as the past chairman of NVTC's ebusiness committee and is a charter member of TIE Washington, DC. Anand and his wife, Annapurna, and their two children live in Mclean, VA.

*Anand also contributed to the technical editing of this book.*

**Hersh Bhargava** is the founder and CTO of RafCore Systems, a company that provides RFID Application Development and Analytics platform. He is the visionary behind RafCore's mission of making enterprises respond in real-time using automatic data collection techniques that RFID provides. Prior to RafCore Systems, he

founded AlbumNet Technologies specializing in online photo sharing and printing. With 15 years of experience in building enterprise strength application, he has worked in senior technical positions for Fortune 500 companies. He earned a Bachelor of Technology in Computer Science and Engineering from IIT-BHU.

*Hersh also contributed to technical editing of this book.*



## Technical Editor

**John Kleinschmidt** is a self-taught, staunch wireless enthusiast from Oxford, Michigan. John is a security admin for a large ISP in Oakland County, Michigan. He spends much of his time maintaining [personalwireless.org](http://personalwireless.org) and enjoys reading up on IT security. John is also a moderator for [netstumbler.org](http://netstumbler.org).

*Special thanks to John Pineau for allowing me to pick his brain, and of course, my wife for putting up with me when I'm stuck to the computer.*

# Contents

<b>Part I: Overview</b>	<b>1</b>
<b>Chapter 1 What Is RFID?</b>	<b>3</b>
Introduction	4
What This Book Is and Is Not	5
RFID Radio Basics	9
Why Use RFID?	11
RFID Architecture	13
Tag/Label	13
Passive vs. Active Tags	14
Reader	16
Middleware	16
Data Communications	17
Tag Data	17
Electronic Product Code	18
Protocols	19
Physical Form Factor (Tag Container)	21
Cards	22
Key Fobs	23
Other Form Factors	24
Summary	27
Links to Sites	27

<b>Chapter 2 RFID Uses</b>	<b>29</b>
Introduction	30
Applied Use	33
Wholesale	35
Retail	37
Standards in the Marketplace	38
Failures in the Marketplace	40
Benetton	41
Metro Group	41
Lessons Learned	41
RFID for the Consumer: Case Studies	44
Wal-Mart	44
Implementation	44
Results	45
US Department of Defense (DoD)	46
Implementation	46
Results	47
E-ZPass	48
Implementation	48
Results	49
SpeedPass and Contactless Payment Systems	49
Implementation	50
Results	50
Livestock Tagging	51
Implementation	51
Results	51
Summary	54
References	54