

# **SECURITY IN A WEB2.0+ WORLD**

**A STANDARDS BASED APPROACH**

**C. SOLARI**

**and Contributors**



A John Wiley and Sons, Ltd, Publication



# **SECURITY IN A WEB2.0+ WORLD**



# **SECURITY IN A WEB2.0+ WORLD**

**A STANDARDS BASED APPROACH**

**C. SOLARI**

**and Contributors**



A John Wiley and Sons, Ltd, Publication

This edition first published 2009  
© 2009, John Wiley & Sons, Ltd

Registered office

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at [www.wiley.com](http://www.wiley.com).

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

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

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. 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.

ISBN 978-0-470-74575-5

Set in 10/13 Optima by Thomson Digital  
Printed in the USA by Courier Westford

# About the Authors and Contributors. . .

Taking the challenge to write this book it was clear to me that it would need the contributions of many ideas, many hands. These ideas and concepts, and much of the actual writing are a composite of these hands and minds. Dr. Mike Schabel, Ty Sagalow, Bob Thornberry, Marco Raposo and Aleksei Resetko were contributors to Chapters 2 and 3. Mike, in particular, lent his expertise to the topic of wireless broadband communications.

Dr. Jim Kennedy wrote Chapter 4. Uma Chandrashekhar, Andrew McGee, Rao Vasireddy with others at Bell Laboratories were the developers of the Bell Labs Security Framework that became the ITU-T X.805 Recommendation. Their ideas and writings are central to this book particularly with Chapters 5 and 6.

Bob West of Echelon One with the support of Eric Green and Kirsten Francissen contributed throughout bringing the message to conclusion in Chapters 7 and 8. A special mention of Rod Beckstrom and Ty Sagalow; their contributions will open a new area of investigation to understanding the economics of cyber security.

There were a number of reviewers; John Reece in particular added great insight.

Leaving Wyatt Starnes to last is intended to single out his particular contribution. He will see his ideas throughout this book; in effect the central message of this book has been his life's work. We all owe him a great deal of gratitude for his quiet but forceful campaign to get the message through about metrics, about root of creation, about aftermarket security as an ineffective approach.

**vi** *About the Authors and Contributors...*

Thank you Wyatt, and thank you to all that made these important contributions.

To close, we give special acknowledgement to Dan Geer for his foreword. His prose is unmatched - we stand in awe.

**—Carlos Solari**



# Contents

<b>FOREWORD</b>	<b>xi</b>
<i>A seasoned and influential security professional puts the chapters of this book into context by discussing the challenges of cyber security in the Web 2.0+ world.</i>	
<b>PROLOGUE</b>	<b>xv</b>
<b>1 The World of Cyber Security in 2019</b>	<b>1</b>
<i>It is 2019, Web 3.0 has arrived, but it is a destination fraught with the problems of cyber security. With the benefit of hindsight, what went wrong in the development of Web 2.0 is obvious, how to fix it is not so – the challenges abound. This chapter explores the road we travel and why uncorrected it will lead directly to the destination of an uncertain Web.</i>	
<b>2 The Costs and Impact of Cyber Security</b>	<b>15</b>
<i>An increasing number of reporting and regulatory requirements are being placed on businesses, which is resulting in rising compliance costs while yielding poor results in the actual protection against cyber threats. This chapter discusses cyber security from an economic (cost) and risk management perspective, the methods of quantifying potential losses, enhancing business process, and reaping value from enhanced security standards.</i>	
<b>3 Protecting Web 2.0: What Makes it so Challenging?</b>	<b>39</b>
<i>Web 2.0 has begun to impact almost every aspect of everyday life, but comprehensive controls to protect assets, wireless, and content in all of its forms, has yet to be implemented. The lack of security standards could be potentially devastating as virtual life and the</i>	

*physical world begin to meld without the recognition that both need to be protected with the same vigilance.*

- |          |   |            |
|----------|---|------------|
| <b>4</b> | <b>Limitations of the Present Models</b>  | <b>63</b>  |
|          | <i>This chapter names the problem – a practiced model of security that is bolted on – and why the current models of cyber security are ineffective in transitioning to Web 2.0. Patching, over-reliance on detection and response, and the omnipresence of data in the cloud require a model of greater discipline where security is part of the design, not the afterthought.</i>  |            |
| <b>5</b> | <b>Defining the Solution – ITU-T X.805 Standard Explained</b>   | <b>79</b>  |
|          | <i>Bell Labs introduced a security framework that became Recommendation ITU-T X.805 in 2003. The efficacy of this model for present and Web 2.0 systems is discussed in terms of its overall framework components. As a model it offers a way to apply a disciplined approach to security designed-in, not bolted on. In a security value life cycle, it forms the links in the trust chain from the point of technology creation through technology implemented in security-integrated operational environments.</i> |            |
| <b>6</b> | <b>Building the Security Foundation Using the ITU-T X.805 Standard: The ITU-T X.805 Standard Made Operational</b>   | <b>101</b> |
|          | <i>By using the ITU-T X.805 standard as a framework, this chapter explores how to implement the X.805 framework as a model for trust concepts in applied computing.</i>   |            |
| <b>7</b> | <b>The Benefits of a Security Framework Approach</b>  | <b>113</b> |
|          | <i>Transparency is the primary benefit and one of the key attributes to transform from the present model of aftermarket security to protecting the evolution of Web 2.0. It allows for the proper implementation of security from the beginning stages of product development to the point of delivery while creating a basis for trust, developing a common language, and reducing costs.</i>  |            |
| <b>8</b> | <b>Correcting Our Path – What Will it Take?</b>   | <b>137</b> |
|          | <i>The challenges of protecting Web 2.0 and the solutions toward a more efficient paradigm have been presented, but who will implement these sorely needed changes in the system? Leadership from business, academia, and government is paramount to reshaping the process of how products and solutions are made secure</i>  |            |

*up front in the development life cycle. It will take more than the logic of why it should be done – it will take an active role in these three domains. It starts with the buyers of technology applying the leverage of purchasing in large numbers to change a behavior already ingrained.*

<b>APPENDIX A</b>	<b>151</b>
<b>APPENDIX B</b>	<b>181</b>
<b>APPENDIX C</b>	<b>207</b>
<b>GLOSSARY</b>	<b>217</b>
<b>INDEX</b>	<b>229</b>



# Foreword

Perhaps it does not need saying yet again, but security is a means, not an end. For this reason, and because technological advance is growing faster, the “means” that comprise security today are likely to be short lived, yet means short-lived-ness is not a free pass to ignore them, to put no effort into evolving them. Ends are not short lived.

Most of us who earn our keep in the security trade are well aware of the essentialness of constant adaptation. This constant adaptation is a prerequisite to getting one’s job done; ironically, constant adaptation applies to both Bad Guys and Good Guys. Our problem is that the Bad Guys enjoy a structural advantage over the Good Guys: where in the physical world it is the crook who must engineer the perfect crime and the police who have all the time they need, in the digital world it is the policeman who has to be perfect and the crook who can be patient.

That the Good Guys are at a disadvantage is not a first-principles deduction by some logician – it is merely an observation. Looking back over the last decade, it is easy to observe that the amount of treasure and labor being expended on security has risen very fast indeed. At the same time, the loss of goods and control engineered by the opposition has risen. We are many. They are few. We are losing. They are winning. The reason is structural.

When you are at a structural disadvantage, the first choice might be to just get out of the game. Who wants to play baccarat against a crooked croupier? Or take a spitball when the umpire works for the other team? Better to play at another casino. Better to stand on another diamond. Sadly or not, getting out of the digital security game is not in the cards.

Something else has to happen.

We are dependent on the kind of networked cooperation made possible such a short time ago with the appearance of Mosaic (March

14, 1993, to be precise). The rate of change, even in the short retrospect of sixteen years, proves that predicting future change is an unlikely business. The one prediction that seems assured is that we may think we are dependent on networked communications today, but we ain't seen nothin' yet! Web 2.0 will see to that because, if nothing else, it is already doing so – a kind of proof-by-demonstration that William Gibson's famous bon mot embraces, "the future is already here, just unevenly distributed." If we are going to be so dependent on Web 2.0 that society literally could not survive without it, and do that in a world where the opposition has an all-but-permanent structural advantage, it really is time to get serious. As the 44th President said in his Inaugural Address, "In the words of Scripture, the time has come to set aside childish things."

This book is about setting aside childish things, such as assuming that somehow we'll muddle through. Marcus Ranum may have sounded cynical to some ears when he said: "Will the future be more secure? It'll be just as insecure as it possibly can, while still continuing to function. Just like today." But he didn't sound cynical to my ear. The difference is that the complexity of the Web 2.0 + world and our dependence on it makes the core of Ranum's remark, "while still continuing to function," the core of whatever debate there still is.

(Look,) It is entirely clear that convergence of nearly all communications-based functions in the economy and in society to Internet-based communications is inevitable if not already true. It is entirely unarguable that increasing quantities of data that make all this convenience work are held not on one's desk but on the Web itself. It is entirely predictable that the more dependent we are on something, the more its vulnerabilities matter and the more our opponents will invest in R&D aimed at it. So, Points #1 and #2: Web 2.0 is irresistible so long as it works, and the only real failure would be a loss of trust after some unignorable security shortcoming – everything else is fungible.

There is a joking restatement of the Three Laws of Thermodynamics that goes like this:

You can't win  
 You can't break even  
 You can't get out of the game

That is where we are: we cannot get out of the security game because we cannot get out of the Web 2.0 game, even if we wanted to. (Which we don't.) That we are at a structural disadvantage is just a restatement that we can't win. That we can't break even says that what

we do for security will be judged as all risk management is judged: by what did not happen as much as by what did. There's the breaks.

Behavioral psychologists will tell you that you begin to change outcome the minute you begin visibly taking data. If security is a process in its operation and a mindset otherwise, then it is time we took some data. In a structural disadvantage where success is when nothing happens, our aim is to be a less attractive target than someone else so that the things that must happen, happen to that someone else. This isn't jaded. This is Real Politik.

The authors of this book have set out to do a difficult thing, and that is to transmit what they know about how to think. In a complex world addicted to convenience, how to think often seems like an expensive hobby compared to what button to press, what exactly to do. As complexity grows, what button to press may be the only thing all but the few can do. How to think is not so quick, and it is never cut-and-dried. How to think doesn't tell you what button to press, and knowing what button to press proves nothing except that you can follow instructions. Knowing what button to press is nevertheless good enough when you don't have sentient opponents, only accidents and stray alpha particles. Knowing what button to press is useless when the opponent is sentient and is gaming you. When sentient opponents are what you are up against, you need to be able to think. You need to be able to out-think.

We all know from long experience that (1) there are never enough experts to go around, and (2) that security must be built-in rather than bolted-on. In our current world situation, it is probably fair to say that the demand for security expertise so outstrips supply that the charlatan fraction is rising. As such, some way to extend the reach of the expertise we do have would be a Very Good Thing. Because we all know that an ounce of built-in security is worth many, many pounds of field upgrades. No rational observer would argue other than that the scarce expertise absolutely must be deployed at the earliest possible stage of development, which is to say where the supply-demand imbalance is least and the leverage on what supply we do have is greatest.

Thus we come to the point of this book. By whatever precise definition you choose, Web 2.0 is the future, it is already here if unevenly distributed, and it needs security built-in, not bolted on. The best expertise we have needs to be in the front end of every Web 2.0 construction. Sure, some constructions have already been done, and, let us hope, done well. But there is a lot more to come and it needs our