# SECURITY IN A WEB2.0+ WORLD

## A STANDARDS BASED APPROACH

**C. SOLARI**

**and Contributors**

WILEY

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**

WILEY

A John Wiley and Sons, Ltd, Publication

This edition first published 2009

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

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.

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

# 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. Them'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