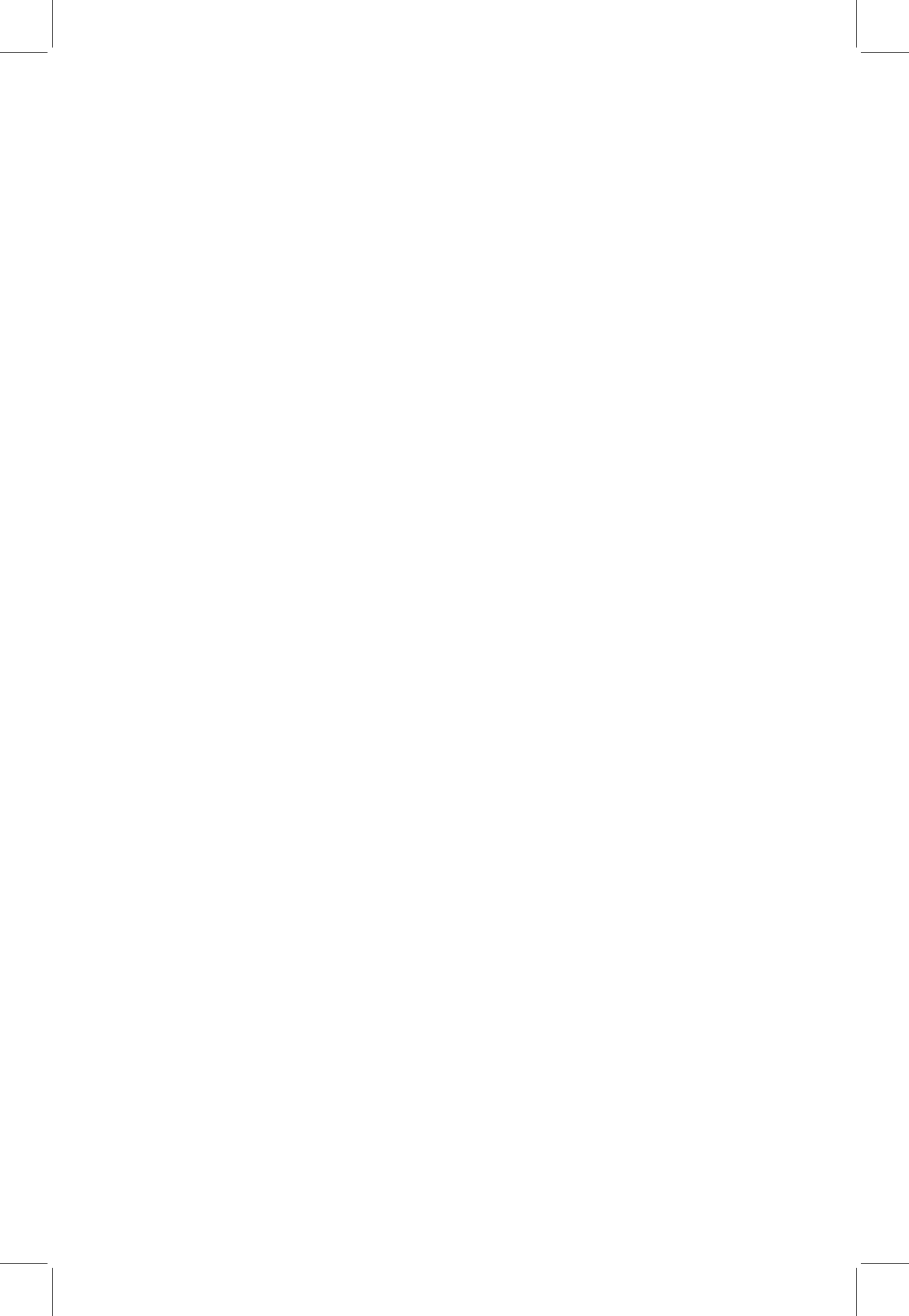


SECURITY IN A WEB2.0+ WORLD



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.

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.

Library of Congress Cataloging-in-Publication Data

[to come, includes ISBN]

A catalogue record for this book is available from the British Library.

Set in 10/13pt Optima by Thomson Digital

Manufactured in the United States of America

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

FOREWORD	xi
<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>	
PROLOGUE	xv
1 The World of Cyber Security in 2019	1
<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>	
2 The Costs and Impact of Cyber Security	15
<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>	
3 Protecting Web 2.0: What Makes it so Challenging?	39
<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>	

viii Contents

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

- 4 Limitations of the Present Models** **63**
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.
- 5 Defining the Solution – ITU-T X.805 Standard Explained** **79**
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.
- 6 Building the Security Foundation Using the ITU-T X.805 Standard: The ITU-T X.805 Standard Made Operational** **101**
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.
- 7 The Benefits of a Security Framework Approach** **113**
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.
- 8 Correcting Our Path – What Will it Take?** **137**
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 re-shaping the process of how products and solutions are made secure

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.

APPENDIX A	151
APPENDIX B	181
APPENDIX C	207
GLOSSARY	217



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. That'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

collective best skill if we are not to create something really bad. But how?

The answer is discipline, and discipline in the form of standards and, even, Standards. Sure, standards (or Standards) are sometimes just so much bureaucracy and self-flattery. That is not the case here. Yes, there are people who are so good at what they do that standards (or Standards) just get in the way.

There are too few of those folks to matter, and they won't live forever. If there is anything the last six months in finance have shown, it is that we humans are abundantly capable of building systems more complex than we can understand when in operation. As Mike O'Dell used to say, "Left to themselves creative engineers will deliver the most complex system they think they can debug." Given the stakes in security for Web 2.0, we have to do better, we have to get security right up front, or it is game-over.

Getting it right means using the all-too-rare skills to lay down the path of discipline, using discipline to build security in, and using built-in security to make the world safe for Web 2.0 and all it promises. That's what this book is about – taking the skill now encoded in a Standard, using that Standard to operationalize discipline, and using that discipline to build some security in.

If you have a better idea, all I can say is "Let's hear it" and, maybe, "Where have you been?"

—Daniel E. Geer, Jr., ScD

Prologue

We live in an age of great uncertainty – a period of unprecedented technical innovation that is transforming our lives. It is innovation that accelerates even as we harbor an unquiet sense of the unknown destination; where does all this new technology take us and what becomes of us in the process? Ray Kurzweil, a pre-eminent technology innovator spoke to this point of innovation acceleration at Harvard University, mindful he said of the “intertwined nature of the risks and benefits”. It was February 2005. If only it could be slowed down enough that we can better understand the promise of its benefits and calculate the severity of its risks.

But innovation cannot be slowed; it runs along its own course with a gathering momentum fuelled by competitive global markets and not beholden to any other law than the one that states simply: “technology begets technology at an ever-increasing rate.”

Nowhere is the uncertainty associated with accelerating innovation more pronounced than in the world of cyberspace, where information technology insinuates itself into every nook and corner and then transforms itself with blinding speed. In the world of cyberspace, we are faced with the challenge of trying to secure new territory without having entirely figured out how to protect the present – the cyber security dimension of cyberspace.

It is perhaps easiest to illustrate the challenge we face by recalling the well-known story of the frog in the cauldron of boiling water. A frog that is dropped into a cauldron of boiling water will immediately leap out to save itself. However, if this same frog is placed in a cauldron filled with tepid water that is then only gradually brought to a boil its reaction is very different. Because the increase in temperature is gradual, the frog stays put not realizing its predicament until the water reaches the boiling point and by then it is too late.

Consider in this story similarities with *Security in a Web 2.0+ World*. The present networks remain unprotected; mastery of the security paradigm remains an elusive target. So what is this ill-defined world of Web 2.0?¹ What is the risk today, and how can one address the growing risk tomorrow? The temperature is rising, yet complacency rules. It is time to sense the growing danger and make the necessary response.

There is a dilemma, however, in discussing the topic of cyber security – a problem of communication where policy makers and technologists speak, but in a language that fails to inform one to the other and fails to inject a sound understanding. Simple questions go unasked and unanswered. How serious is the problem of cyber security? Are the issues correctable, and how much time is there to take corrective measures? While risk assessments are done daily, the metrics of assessing the vulnerability of new technologies are not consistently agreed upon and not well practiced.

“We have not been able to easily discern what threats we would face, what the tools of influence would be, or who would become our opponents. The outcome has been a kind of strategic indecision that puts the United States at risk.”²

There is general agreement on a few points, yet, these same points also illustrate why the answers are not easily forthcoming. Security is not intrinsically separate from the business functions; it is a measure of overall business risk represented in the terms of cost. What does it cost the company to lose access to the functions supported by the network and by this determination how much should be spent in security to protect against this loss? This question, addressed in Chapter 2, needs to be answered in order to better calculate business risk. Security metrics, the science of measuring security, remains undefined and so it is not well practiced. There is more to lose in financial terms and in tarnished reputations, but how much, and to what degree of impact remains a degree of conjecture.

¹ According to the definition available at www.wikipedia.org, “Web 2.0” describes the changing trends in the use of World Wide Web technology and web design that aim to enhance creativity, communications, secure information sharing, collaboration and functionality of the web. Note: this and other definitions obtained from the Wikipedia are licensed under the GNU Free Documentation License.

² CSIS Commission on Cybersecurity for the 44th Presidency. *Securing Cyberspace for the 44th Presidency*. (p. 12). Washington: Government Printing Office, 2008.

To begin to answer these questions requires putting in place the foundational constructs of technical and process metrics, the economics of loss in the era of “*cyber-value*”, and to communicate the concepts of cyber security from policy to technology clearly. In the absence of these constructs, one can anticipate what is already happening: policy disconnected from reality and bureaucracy that exacerbates rather than remedies. There are many already arguing this point with Sarbanes-Oxley³ and the California Senate Bill 1386 (SB 1386).⁴ Policy without the metrics to determine its effectiveness often ends up creating a spiral of increasing costs without the intended benefits.

To better understand and communicate the issues of cyber security between policy maker and technologist requires an effort to speak to both in a manner that each can understand. With this intention, each chapter in this book begins with its own executive summary; speaking to the policy maker: the business executive, the academician, and government executive. Transitioning to the body of each chapter, the target audience shifts. It is meant not just for the security professional, but for all makers and developers of the information communications technology (ICT) systems, a term applied in this book encompassing traditional “IT” or information technology (thought of with data networks) and telecommunications systems (thought of with telephony and video systems). To embed security in the ICT systems, will require first that one begin with explaining the principles of good practice for security design to the engineers who make the products and systems.

The target audience is thus a broad population, ranging from those who need to know enough about cyber security to make effective policy decisions to the engineers who design the ICT systems. The book does not cover how to encrypt data, but where it should be considered and in what measure it should be applied. In this manner, it aims to lessen the mystery surrounding cyber security and present it as sound engineering principles that need to be applied in the right measure.

Three key points will be stated and reinforced in later chapters. The first is that there is not much time; years cannot be spent to begin the process of embedding security into current and future systems. The second is that there is a need for models that allow one to measure security in the design stage, in deployment and in production. With

³ www.soxlaw.com

⁴ http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

the use of better security models, one can expect a lessening of the dependency on cyber security experts and transform the practice of security more to the science of metrics, baselines and business-rational remediation. This book proposes two models that can help make this transformation – the X.805 standard⁵ and the security value life cycle. Both of these models will work toward creating greater transparency as a way to bring a more finely grained trust context into computing transactions.

The final point is that the stakes could not be higher. This will be said repeatedly: Information communications technology is embedded in the whole of technology and becoming more so with each day that we automate to improve operational efficiency and compete in the global markets.

To understand the issue of *how much time*, one needs to look no further than the *convergence* of technology and the emergence of Web 2.0 computing. *Convergence* is the move from separate infrastructures and technologies for voice, video and data to one technology platform – Internet Protocol (IP) – and toward a unified infrastructure, not separate plants.

Convergence is happening around the world – one can recognize it in the marketing speak of *triple play*⁶ and IPTV,⁷ as two examples. When the convergence is done, it will be too late and too expensive to redesign these systems and protect them against a hostile environment of hackers working with organized crime

There is little time to ensure that security is engineered into the systems that the wonderful benefits of convergence and Web 2.0 computing are designed to withstand the rigors of the inherent risk. As an example, “new pay-TV market data indicates that IPTV will grow by an estimated 32 percent annually over the next six years to nearly 79 million subscribers globally by the end of 2014.”⁸ The dependency is deep and more intertwined in everyday life.

⁵ <http://www.itu.int/rec/T-REC-X.805-200310-I/en>

⁶ www.wikipedia.org - tripleplay: In telecommunications, the triple play service is a marketing term for the provisioning of the two broadband services, high-speed Internet access and television, and one narrowband service, telephone, over a single broadband connection. Triple play focuses on a combined business model rather than solving technical issues or a common standard.

⁷ www.wikipedia.org - IPTV is a system where a digital television service is delivered using Internet Protocol over a network infrastructure, which may include delivery by a broadband connection.

⁸ Richard Grigonis, “IPTV (Telco TV) Tops Pay-TV Platform Growth at 32 Percent”, <http://www.tmcnet.com/channels/3g-voip-iptv-performance/articles/48691-iptv-telco-tv-tops-pay-tv-platform-growth.htm> (January 14, 2009)