

SECURITY IN A WEB2.0+ WORLD

A STANDARDS BASED APPROACH

C. SOLARI

and Contributors



A John Wiley and Sons, Ltd, Publication

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. 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

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-l/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)

1

The World of Cyber Security in 2019

“The semantic Web – what is called Web 3.0¹ – is commonplace in 2019. The start of the Internet and the World Wide Web is the stuff of legacy and lore. Amid the concerns of ICT security is another dimension – the clash of virtual realities such as between the Second Life® virtual world and the physical lives. Decisions in the virtual world drive material reactions in the real world – as they are now one world with no safeguards in place.”

Executive Summary

It is 2019 AD or 28 AW (after the Web), counting in years after the introduction of the World Wide Web.² Contrary to some predictions, ICT systems continue to be one of the primary agents of change in our lifetimes and in the history of humankind. The pace of change has been nothing short of spectacular. There have been many winners and losers as the exponential growth of technology gives rise to new and wider social divisions. This change ripples through societies, cultures and nations with unintended consequences that are too numerous to count.

¹ www.wikipedia.org - Web. 3.0 is one of the terms used to describe the evolutionary stage of the Web that follows Web 2.0.

² www.wikipedia.org - World Wide Web is a system of interlinked hypertext documents accessed via the Internet.

2 *The World of Cyber Security in 2019*

In hindsight, one can see where things went right and where they have gone terribly wrong. Protecting ICT systems has been one of the great challenges. With 12 years of history, Web 2.0 continues to serve, transform and interconnect the world's cultures. Nothing is left untouched by the Web 2.0 generation as worlds that were once physically and logically separate are now inextricably linked. Generation Y and Generation Z (also known as Millennials), born in the age of computers and the Internet, run the physical and virtual worlds. It is a new world, but is it "brave" or is it "foolhardy."

The threats to cyber security in 2019 are many. How did things get to this point? In hindsight, the answer is all too clear. It just happened degree by degree, like the slow-rising temperature in the cauldron. The gradual slide was something that happened even as it is clear that we could have and should have integrated security into our ICT systems. It is not that the technical know-how was missing, nor was it something that came as a surprise. It was a ripening awareness of the vulnerabilities. By the year 2009, it was understood that security had to be an integral part of system design yet by the absence of forethought, understanding and leadership, the vulnerabilities in ICT systems were left unaddressed. It is 2019 and it's time to pay the piper.

It was a sword that cut both ways; the standardization on all-IP systems is what allowed the world of data, voice and video to blend in ways that created the value of next-generation systems. Web 2.0 applications would not have achieved its broad appeal without the convergence of IP systems. It also meant that the vulnerabilities were many and were both *transmuted*³ across the different media and infrastructure domains and replicated across the many nodes in the complexity of the Web 2.0 world. Encryption can be broken with powerful computers. Quantum computing is in our midst; even strongly encrypted national systems are at risk.

³ Transmutation, is used to describe the phenomenon where as an example, a virus delivered by email to compromise computers is now re-crafted for telephony.

2

The Costs and Impact of Cyber Security

It takes considerable knowledge just to realize the extent of your own ignorance.

—Thomas Sowell-economist

Executive Summary

There is a story often told of two men who are walking across the Steppes when they stumble across a lion that has not fed for some time. For the lion, dinner has just come knocking. The two men begin to run for their lives. The slower of the two notices that his partner is not running at full speed, keeping just one step in front and appearing rather undisturbed by the ordeal of being chased by a hungry lion. “What are you doing?” he asks his partner? “I am fast,” the other partner says, “but not faster than the lion. “Still, I don’t need to be faster than the lion, only faster than you, my friend.”

On the surface this story serves as a convenient metaphor for the way in which security is currently practiced in the business world. It is also a cautionary tale for those charged with protecting their firm’s assets. Lions, and for that matter most other predators, follow the law of the jungle preying exclusively on the weakest members of a herd, and hunting only as a means to stave off the threat of starvation and guarantee their survival.

Predators in the world of cyberspace, by contrast, follow a very different code, and their behaviour is far less predictable and far less honorable than that of the lion. For these cyber predators hunting is about conquering and destroying and rarely about survival.

16 *The Costs and Impact of Cyber Security*

In the cyber world, just keeping a step ahead of one's partner is not necessarily sufficient to ward off the attack of a cyber predator. The cyber predator has a different agenda, one that does indeed go after the weak and slow but also the strong and rich prize. They are motivated by more than simple survival; the cyber predator's attacks have more serious consequences with broad implications for national strategy and commercial sustainability.

Each year businesses and government agencies make significant investments to secure their systems and protect their communications networks from all manner of cyber threats. The costs expended in securing these systems are not trivial and cover a broad range of items. There is the cost to build up security infrastructure, to hire security specialists to protect technology systems, to implement security best practices, to meet compliance regulations and, where necessary, to cover the loss from incidents. And these are just some of the direct costs. There is a whole host of indirect costs to consider as well, such as litigation, lost contracts, sales and profits, as well as diminished brand equity.

This chapter evaluates the sources of expense for cyber security and provides an explanation for why the security problem grows more severe despite the ever-increasing investment in security spending. This seemingly inexplicable phenomenon is not as much a mystery as one would think. Spending more and getting increasingly less effective results is, in large part, a result of a lack of rigorous measures that could guide investment decisions.

When the budget for security comes up for review more often than not the CFO is faced with a decision to approve an expenditure for an item that has no strict measure associated with it and no guaranteed results. It is hard to imagine that a CFO would approve such a request if it were made for any other type of investment and yet in the case of security common business sense is temporarily suspended and exceptions made. It is easy to sympathize with the CFO and appreciate the predicament. On the one hand there is an unacceptable absence of rigor and on the other the spectre of potentially devastating consequences to consider. The decision is very often one that is motivated by fear not grounded in reason.

If security cannot be easily measured, how is one to determine the optimal level of spending to achieve desired results? One serious impediment is that an acceptable means for measuring the true cost of a security failure does not today exist. Chief information security officers (CISOs) may consider the cost of breaches from a purely technical perspective. While there is no doubt that this type of evaluation has merit, in the end it only yields one part of a much larger and complex picture. What it may not take into account is the effect of indirect costs that can result from a breach in security, the cost of potential litigation, for example, or the loss of customers, the loss of future business, the impact on brand equity, not to mention the cost of regulatory investigations and even the cost of fines. A true Return on Investment for security expenditures can only be achieved by ultimately quantifying the full extent of direct as well as indirect costs. To do this requires a company's leadership team to work collaboratively and examine the impact of a potential failure on the entire business. This calculation needs additional stakeholders that should be participants in the discussion including legal, compliance, communications and public relations, insurance, sales and human resources. In the case of enterprise risk management, the leadership team must also assess certain types of business risks, such as economic, credit and physical (see appendix Ch. 2, Ref.1).

A historical look at the problem validates this dilemma; despite global increases in security spending, the number and the value of security breaches have not dropped but risen. “The vast majority of cases referred alleged fraud and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was \$239 million with a median loss of \$680 [in 2007] per complaint. This was an increase from \$198.44 million in total reported losses in 2006.”¹ Even the available data is suspect, as much of it remains undisclosed for fear that more harm than good can come from the disclosure of a breach.

The “*extent of our own ignorance*” in this area is significant, yet one might argue that business and government continue on the same path seemingly unable or unwilling to make a correction and change direction. It is more likely that businesses and governments are aware and are willing to make changes as evidenced by the increase in security budgets.

Rod Beckstrom, Director of the National Cyber Security Center for the U.S. Department of Homeland Security, made a presentation at the 2008 inaugural SC Magazine World Congress in New York City. He took a critical first step toward understanding the problems of cyber security from an economic perspective. He proposed a way to answer two fundamental questions: 1) What is the value of a network? and 2) What should we spend to defend it? These are not new questions, and criminals are quite skilled at determining whether they will get a satisfactory return on investment from a cyber attack. To eliminate the motivation for attack one must strengthen the defenses to a point where the cost of the attack is greater than the reward.

To answer the question of how much to spend on protecting an organization, one must answer the first question – what is the value of the network? The economics of security are then determined by subtracting the total security investments and losses (incidents) from the sum of the benefits gained from revenue the network helps the company achieve. Completing this analysis, Beckstrom made the point of different ways to achieve deterrence as the means to drive up the cost to the hacker where attacking the network is no longer lucrative. Rewarding the “good guys” to create “good code” and/or punishing the “bad guys” with “very large fines for companies with bad products” are two forms of strengthening the defenses.

Protecting Web 2.0 systems is of greater consequence when the data about millions of people is stored in databases subject to the pressures of business and government where the interests of the individual are secondary. It is high time that the technology industry resolves this conundrum and learns how to measure security so that an objective cost/benefit analysis can be realized. This way, standard business principles can be applied to how much is spent on security and to ensure that the expense is applied at the most effective points in the process from creating to deploying technology products.

Consider once again the view that treats security as a value life cycle, one where the effort to protect and harden can be measured and has tangible value. The absence of this practice can also be measured – one that removes value from this cycle. Consider also that the problem and solution start at the same place: the point of creation. Transferring these security features within the solutions, forward through the sale of technologies to the consumer, both

¹ “*International Crime Complaint Center 2007 Internet Crime Report*”

18 *The Costs and Impact of Cyber Security*

business and government can carry the security value to the point where technology enables the business or government to function optimally. In an ideal world, both the risks and benefits are taken into account and a balance is achieved.

For businesses, security need not imply additional cost. There are a great number of examples where the cost of security can be returned as business value, directly associated with a brand. In the automotive industry, Volvo® puts safety at the center of its strategy and uses it to differentiate itself from competitors. Similarly, security can be used to competitive advantage by enabling business partners, for example, to exchange information securely as a way of streamlining operations.

The scenario described above starts to form a process called *the Security Value Life Cycle* (“SVL”). This model is one that companies can use to better estimate true ROI from security. It is not particularly novel, but it does reveal what is wrong with the current practice. By using a structured approach to security, this value chain can be made to work with benefit to individuals, companies and governments. Security can be measured and it can be structured so that one can determine its relative value, then baseline the performance. This will allow an organization to understand its true security health over time and make improvements. This is certainly not a panacea, and achieving adequate protection of information doesn’t happen overnight. However, an organization that adopts such an approach can make continuous improvements and minimize the risks to its computing environment. It may take a generation that is unwilling to tolerate incidents to effect a change, but such change must occur or the consequences for all of us will be significant.

3

Protecting Web 2.0: What Makes it so Challenging?

“Houston, we have a problem”

Executive Summary

In his futuristic cyber crime novel *The Halting State*,¹ Charles Stross takes his readers on a trip through Second Life in the year 2019 (not coincidentally) and describes an environment where the events in a *grid-crime*² can cross over and inspire crimes in the real world that have real consequences and global impact. Although a purely fictional account, Stross’ crime novel, nevertheless, provides an inkling of how Web 2.0 might evolve and shape a world in which virtual tools redraw the relationship between humans and machines narrowing distances between the two and heightening the interaction between them across all senses. The novel also gives the reader pause for thought by demonstrating what can happen when reliance on technology that was considered a source of power suddenly turns into a vulnerability in the wake of a system failure. The source of the failure is a compromised encryption key that has been implemented to protect all commercial and government functions. The repercussions are far-reaching and absolute. No border is sacred and no business or government agency is spared. But before we speculate any further on the evolution of Web 2.0 in 2019, and concern ourselves with the potentially apocalyptic

¹ Charles Stross, *The Halting State*. (Phillips and Nelson Media, 2004)

² Crime that takes place in Second Life. Catherine Holahan, “The Dark Side of Second Life,” *Business Week*, November 21, 2006.

40 *Protecting Web 2.0: What Makes it so Challenging?*

consequences that it implies, let's take a step back and take a closer look at just what Web 2.0 is as a way of getting a better understanding of why it should engender such concerns about security?

There are many definitions of Web 2.0, though any differences likely stem from differing perspectives. In the telecommunications community, it can be defined as next-generation networks in high capacity wireline and wireless broadband. By collapsing the separate legacy and proprietary systems into a single technical infrastructure, a system based on packet switching, the Internet Protocol networks deliver the expanded capacity needed for ubiquitous, unconstrained and un-tethered communications. It is also unified communications where e-mail, voice, text messaging, and facsimile can reach a person as a voice message on any device.

Social networking and collaboration applications such as Facebook³, wikis and blogs are examples of Web 2.0 applications. Companies will expand from their traditional reach in the marketplace; application companies will enter the traditional telecommunications market and telecommunications will deliver Web 2.0 applications. The silos will break down, competition will increase, the traditional information stores from companies in different business verticals will blur with a high potential that privacy controls may be lost in the process.

Like the proverbial blind men describing the elephant, those who attempt to define Web 2.0 are bound to arrive at different conclusions. Web 2.0 is multi-faceted, and it is all of the perspectives of Web 2.0 combined that deliver the next generation of information systems. The promise of the information revolution continues; the first generation was only a taste of things to come.

What makes security so challenging in this new world of Web 2.0 communications and applications? More and more information and applications from both individuals and companies will be delivered in the cloud, not just behind personal or corporate firewalls. If security is partly defined as controlling the system and information assets, in cloud computing, third parties manage the assets. These third parties are expected to deliver services for free (or almost free) in exchange for information that can be used for target marketing. Where are the boundaries of business intelligence derived, and what assurances can these companies make to ensure that their boundaries can't be breached?

There is complexity inherent in making voice, video and data work together over the same infrastructure. The adage that complexity is the breeding place for vulnerabilities applies as much in this case as it ever did before. Add this to the fact that technology companies have historically treated security as a minimal set of design requirements reliant mostly on physical and perimeter isolation. Security in this form is supposed to be provided by a set of aftermarket technologies such as firewalls, detection and prevention systems. With physical isolation in IP networks no longer possible, the conditions are different; highly complex solutions that fail to take security risks into consideration have created an opportunity for those who understand how to exploit this complexity and find vulnerabilities.

³ Facebook is a trademark of Facebook, Inc. All other trademarks used throughout this work are trademarks of their respective owners.

Take a close look inside this technology and the complexity appears in its full clarity – like viewing microbes, invisible to the naked eye, but exposed in detail through a microscope. Aftermarket-based security never did work effectively and it will not serve to protect information systems in the world of Web 2.0, but to change the way the market works will require a sea change. This kind of sea change does not happen by chance or without a significant business driver changing the conditions of how the market behaves.

And, upon closer inspection, there are security challenges posed by the un-tethered communications offered by 3G today and 4G broadband wireless communications soon to come. These next-generation broadband wireless technologies deliver a compelling freedom, yet they harbor a new set of problems for the security community. Wireless broadband delivering services across the full range of voice, video and data has a range of challenges operating together in the shared medium of a radio frequency signal where one bad connection can impact traffic for all the participants on the same Radio Access Network (RAN).

Taken together, these challenges call for a new consideration of how security is applied. The “aftermarket” delivery must change to one in which security is a design consideration at the Point of Creation, and is undertaken at the solution-hardening level and applied consistently. The only parties who can change this relationship are the buyers. The current model is too deeply rooted to be able change of its own accord. The notion of an SVL was introduced earlier to help explain how security works today, and serves to illustrate why this form is so flawed.

Security *designed in* using a standards-based approach is about product and solution makers taking an interest in the security challenges of their customers who face a tremendous set of challenges to secure their respective services, many of them codified in certification and compliance requirements. The SVL introduced in this chapter is a simple concept used to illustrate that systems are tied together like a traditional supply chain. Security must be applied at the beginning or there is no security value to pass downstream to the end customers. The entire process is stuck on the ineffective perimeter security. Technology developers owe it to their customers to get the security right and at the right point. Customers of this technology need to stop buying into this failed form of security, **stop buying complex systems piecemeal and stop acting as the integrators of security.** Push this responsibility back to the developers of this technology and see if the market of product and solution developers won't respond in a positive way.

In Ray Kurzweil's *The Singularity is Near*,⁴ humankind reaches the ultimate point at which the gap between technology and biology no longer exists, as technology reaches deep inside the cortex of the human mind. Never mind the man-machine interfaces for the human senses. It makes for interesting science fiction, and it's an idea that some entertain as a possibility in some very distant future. Yet Mr. Kurzweil speaks of it not as science fiction but as the acceleration of science made real through innovation on a trajectory in near reach for the Millennial generation and even for some baby boomers. It is a mind-boggling analysis

⁴ Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology* (Viking Adult, September 22, 2005).

42 *Protecting Web 2.0: What Makes it so Challenging?*

not easily discounted given the strength of his construct. As innovation has *intertwined risks with benefits*, what are the consequences from the inevitable clash when the worlds of Second Life and the real world collide?

These are interesting questions for the future, but given that the future is shaped by the present, the questions are of more immediate concern. Is this future state attainable where the risks are understood and the measures put into place are a guide for achieving equilibrium? The present path for securing technology has no metrics and has little in the way even to scope the size of the problem. The CSI annual report states year after year that the information gathered is so insubstantial that it makes it difficult to arrive at conclusions with any degree of confidence. One is left with only the anecdotal evidence.

The challenges of securing the technologies and processes of Web 2.0 are significantly larger than the present challenges of strictly enterprise-based technologies that have defined boundaries. It is not that the means and the methods do not exist for securing the present generation of the Web or the future Web 2.0 generation. It is rather that they are not applied in a consistent (and highly transparent) manner. The current path will continue until such time as technology buyers change the dynamics for how technology is acquired from the vendors of the technology by the use of standard methods for security that create transparency in the process.

4

Limitations of the Present Models

The cost of poor security in the United States alone is between \$22.2 and \$59.5 billion per year (NIST)¹

Executive Summary

Information security surveys are released on a regular cycle revealing what should not be surprising – security breaches increase and there seems to be no end to the rising impact. Could it be that the reason is the way information security and technology organizations approach protecting their information?

As the products that are purchased for technology operations are not consistently measured to any given hardening standard (government certification as the exception), one must consider the current models for hardening as complicit in this problem. One needs to look no further than the “aftermarket” security model for applying security. What does this mean?

Hardening is accomplished at two levels. The first level of hardening is supposed to be accomplished by the manufacturer of the technology product. At this level the product development teams should be driving out of the designs the known vulnerabilities in operating systems that can be exploited by criminals and attackers. This includes buffer overflows and back doors left in by software developers during testing. These vulnerabilities such as back doors create the need for a never-ending routine of security patching applied

¹ http://www.nist.gov/public_affairs/releases/n02-10.htm

64 *Limitations of the Present Models*

to operating systems, applications and product software. The second level of hardening involves the information security teams configuring the systems to meet the requirements of the organization.

During product development, the engineers, system designers and architects need to assure their products and solutions with security as a basic property so that critical infrastructure is less susceptible to common attacks. Government agencies have been applying these principles for some time with a degree of success requiring that product vendors harden the equipment and software they sell. There is no such well-followed parallel for systems and software developed for normal business use. Indeed as government agencies also started following the same process of buying technology products as *commercial-off-the-shelf*, there has been little difference in government from business in vulnerability announcements, followed by patching frenzy. For most businesses, it is an ad hoc process, as it is with most governments.

The aftermarket approach to security is the opposite of the hardening described here. As most technology buyers are ill-equipped to redesign the product-solutions they employ to meet their enterprise security requirements, the lack of critical security hardening by product manufacturers and application developers forces information security professionals to react accordingly by applying the approach of protecting their systems at the network perimeter. In this model, the operation utilizes separate specialized components placed at strategic locations in the network such as at the entry-exit points. This self-preservation form of protection involves a growing litany of firewalls, intrusion detection and protection systems (IDS/IPS), separate software protection by employing antivirus detection, content filtering, and so on. But in many cases, the very sophistication incorporated into the security systems used to protect the perimeter and the constantly changing number and types of threats encountered daily make them difficult to configure properly and thus prone to defeat.

In addition to the problem of maintaining perimeter security to protect the enterprise, this model is in direct contrast with the business direction and technology operations movement called deperimeterization.² Most organizations have contractors, consultants, and business partners in addition to their own employees who need to access the systems, and they don't all work behind the same perimeter defenses. This undermines what used to be clear borders around computer networks and makes it much more difficult to protect information. The impact can be seen by the losses of critical data not from within the perimeter of the enterprise but from outside the perimeter on laptops, data being transmitted to outside sources or data storage facilities that are outside of the network they can protect.

Not unexpectedly there is a constant tug-of-war between how to adequately protect users' sensitive and confidential information and corporate intellectual property, while still being able to provide a ubiquitous mechanism to transact business. One reaction from these stresses has been for national and state governments to impose security regulations, while other industry bodies have developed industry-based security standards to impose a baseline for security within the various industry verticals. Despite this well intentioned reaction, the problem is that these standards and regulations have provided only high-level

² Jericho Forum, www.jerichoforum.org

principles greatly lacking in more specific implementation details. As such, they leave much to the interpretation of the implementer. Depending on the experience, knowledge and capabilities of each respective security practitioner and how they help to develop the policies, practices, standards and controls the outcome is sure to vary from instance to instance. System audits have helped, but many audit findings continue year-after-year with little in sustainable security improvements.

As discussed in earlier chapters, the issue boils down to one of risk. In today's business world, technology is intertwined with all business processes and transactions. Thus, most information that needs to be protected will touch some type of technology systems or network component during its inception, use or destruction and as such needs to be protected appropriately. Also stated earlier are how these risks pale in comparison with what is coming with Web 2.0, a world where the challenges of protecting information are significantly larger in scope.

There is a solution and it begins with metrics embodied in standards that reach deeper in guiding not just at the policy and process level, but to how products and solutions are actually designed, engineered and developed. On the practice side of this problem, one clear goal is to make it so that it does not take a specialized security expert to apply basic security principles in product and solution development. The security features and techniques for the most part already exist – what has been missing is the consistent application of the same. Security *designed in*, not passed to the buyer of technology to purchase aftermarket is good business in the long-term. The practice of applying an ad-hoc, minimum set of hardening controls lacks a well constructed business rationalization, so the default of saving the cost has persisted. This lack of business rationalization cuts across every cycle of technology development, such as requirements, specifications, design, acquisition, installation and operation. If security could be measured, a baseline of its current state could be understood while making better judgments for design, purchase and access.

There are answers to this dilemma that deal with measuring security that will be answered later in this book. It will require a change in the models in use today and the development of new ones based on the ability to measure security and apply the correct business rationality on the use of technology.

5

Defining the Solution – ITU-T X.805 Standard Explained

“The nice thing about standards is that there are so many of them to choose from.”

—Andrew S. Tanenbaum

Executive Summary

There are no shortcuts. As explained in Chapter 4, aftermarket security means the end-user is resigned to perimeter-based security, dependent upon detection capabilities that cannot overcome the zero-day threat. The only remedy is a seemingly endless patching process. This model simply doesn't protect e-commerce environments of the present nor of future Web 2.0 in which data control is further diffused.

Applying security appropriately starts when the product is designed and engineered. This is the foundation for secure technology solutions and services and continues through the Security Value Life Cycle as defined earlier. The need for security metrics is paramount, and it is time to engage in the *how* part of this discussion.

Security design starts by applying the eight security dimensions of the ITU-T X.805 (“X.805”) standard model and building products as component parts in an overall network solution with a direct relationship to the process and policy of certifications and compliance. Chapter 5 starts with a brief examination of the landscape of standards, certifications and regulatory compliance frameworks, postulating that the combination of X.805 and the ISO/IEC 27000 series standards is the right approach.

80 *Defining the Solution – ITU-T X.805 Standard Explained*

The X.805 standard starts to answer one of the primary concerns: a framework to guide beyond the policy and process level to how the security gets applied in practice. The right level of access control, authentication, non-repudiation, communications security, system and data integrity, data confidentiality, system availability and privacy are critical and all of the security dimensions have a key role. As a framework for designing security during product development, it is the missing link between secure product design, secure applications for the end-user, and the standards, certifications and compliance rules.

From theory to practice, it starts with determining the assets that form the product components, the risk profile that allows the engineer to establish the risk zones, and lastly, determining the vulnerabilities and completing the necessary hardening to achieve *sufficient* security. Sufficient is the operative word, as it is well recognized that the right level of security is always relative to the risks that will be present in the environment.

The X.805 standard framework is foundational as it is prescribed at the start of the development life cycle – when and where the products get developed, integrating them in combination with other products constructing systems and functional services. In this process, one can actually start answering and being responsive to the demands of all the security and compliance requirements by embedding security as an integral part of overall technology and business management.

6

Building the Security Foundation Using the ITU-T X.805 Standard: The ITU-T X.805 Standard Made Operational

“By any chance, do you know if this particular solution has been assessed for security using the standard?”

Executive Summary

The transformation of applying security in a product company is no easy task. There are up-front costs in capital, design and engineering effort, and in the long term, the company needs to have the determination to get on and stay the path. Yet this investment has a real benefit that pays for the cost of product differentiation and the ability to compete better and in other intangible ways. For now, consider some of the practical issues with taking the X.805 standard from good theory to real practice.

The experience to date with applying the X.805 standard is still in a formative stage within Alcatel-Lucent. While there is still limited experience (and much to learn as the program matures), the results are already clear enough to draw some early conclusions. This approach is transformative and can identify vulnerabilities consistently. Thus far, they have ranged from those that would have minor impacts if exploited, to security

102 *Building the Security Foundation*

issues that could have significant impacts on an organization. Some of these vulnerabilities should never have been there in the first place. The process to catch these and correct them was missing.

One lesson learned is something already known but not well applied with the global nature of product development: A product development house must adhere to strict quality metrics. The metrics of security apply not just to individual product hardening but to all the components that are part of the overall solution. To have the appropriate level of security, security needs to be part of the fundamental specifications and requirements – right up front in the development cycle. Product hardening can be measured using the X.805 framework and will yield a product that has a higher level of integrity and fewer security issues. As the X.805 framework is used in the long term and more broadly adopted by organizations, the lessons will be better understood and assimilated.

For now, consider this short but helpful story to illustrate the power of this transformation.

In discussion with a business development team about the process and the early results from assessing products with the ITU-T X.805 standard, the question was asked, “By any chance, had there been an assessment of a particular solution?” The answer was “Yes, as it so happens, that assessment was recently completed and the solution yielded excellent results.” The product engineers had done their homework and had been diligent about applying security. What had been up to that point courteous but only mildly interested business development people in the conference room all of a sudden came alive and the questions came fast and with great interest. It turned out that a large and important request for proposal was in the last days of the bid development process and the customer had asked specifically for proof of the security design. The benefits are clear, crystal clear.

Now imagine if the answer had been the opposite: “No, not yet,” or “Yes, the assessment was conducted but the results were not good.” The detriment to the company in this scenario is also clear: opportunity lost.

In another example, a product assessment using the ITU-T X.805 standard revealed a problem that would have been embarrassing had the problem not been discovered and corrected while still in the development stage. Both of these stories are focused on the assessment phase. How much more powerful are the examples with the ITU-T X.805 standard applied not as assessments with the product near completion, but in the design stage? What are the costs that could have been avoided if security had been integrated into the design stage?

At the solution level, the process of system design is expanded, yet remains essentially the same. The engineering team conducts an overall threat analysis, which forms the basis for understanding the vulnerabilities. It continues by taking steps to decompose the solution into the detailed system assets, with each of the assets investigated with respect to the security dimensions for vulnerabilities. Both inherent weaknesses that can be exploited (such as a maintenance interface unprotected from tampering in an end-user device) and well established attacks such as cross-site scripting or buffer overflows.

The identification of assets is followed by a set of decisions to mitigate the vulnerabilities based on criticality and market demands. For each of the system assets and the interactivity between them, a three-step process – *investigation, assessment, appropriate remediation* – delivers a solution hardened to reflect the environment in which it will be implemented. There is no shortcut, but there are clearly efficiencies to be gained by the repetition of a consistent process. There are really not many unique security situations – just different degrees of applying the security dimensions and factors, such as cost and time, to deliver a solution for mitigating risk.

In the long term, preventing vulnerabilities from being implemented in a customer environment will provide not only a better product, but it will also reduce long-term costs for both the product company and the consumer. Some of the costs that can be avoided include retrofitting security, distributing software patches and legal liability. This will create a competitive advantage for those enlightened companies that truly embrace a fundamental change in mind-set.

7

The Benefits of a Security Framework Approach

“All successful revolutions are the kicking-in of rotten doors.”

—John Kenneth Galbraith

Executive Summary

Transparency at the Point of Creation permits transparency at the point of product evaluation and product selection, and it permits transparency at the point of delivery – when the product is inserted as part of a system delivering service in the network. Without transparency at the source of this life cycle, ambiguity and obscurity persist throughout and it creates the problems discussed in previous chapters.

In this chapter the benefits that can be derived from applying the rigor of a good security framework will be addressed. It is primarily to argue that the notion that security is too hard is no longer defensible. Investing in hardening the products at the start does not need to be a business disabler; it is quite the opposite. Security can help businesses and organizations promote quality, lower operating costs, compete better and engender trust. Who is against good quality, lower operating costs, competing better and being considered trustworthy?

The X.805 standard is such a framework – a framework that allows the product and solution developers to establish what kind of security should be applied by first determining the role to be played. For instance, a computer server is generally assigned a role and the security should be appropriate for that role. A network switch is the same. These roles begin to define the needed security measures, as do other factors. The developers must take into account all eight of the dimensions in the X.805 standard, such as privacy, authentication and integrity checking. These

judgments include business decisions as to what environment the developer will market and sell the product in, expecting for instance that for government clients the requirements for security may be more stringent than for a medium size enterprise.

Because these judgments were made within a security framework, the eventual buyer of the technology gets transparency to make better choices and to differentiate not only the functional value, but also the security value of the product. This can now be done without having to recreate a long, specific list of needs; the list is already clear within the framework of the security standard.

It changes the entire dynamic of the seller-buyer relationship by removing the mystery and dealing with the facts, and ultimately making the best choices among the options offered by different vendors. In many respects, as conjured in the image of Figure 7.1, applying the security framework is about recognizing that it takes a closer-in inspection to find and remediate what are inherent vulnerabilities in complex systems. This is transparency at work.

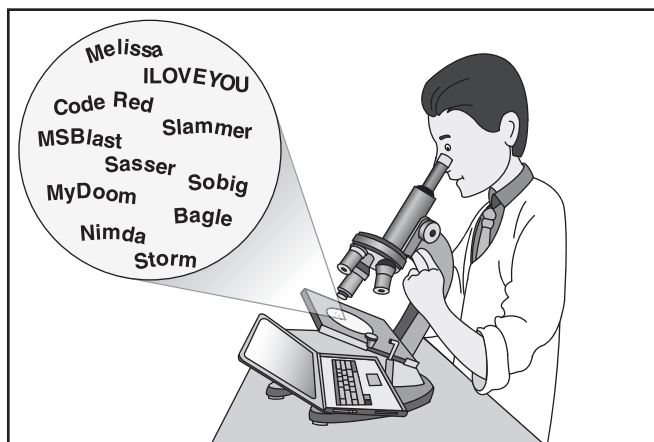


Figure 7.1 Looking through a microscope

Make no mistake about what this means to the product or solution developer; it will take a great deal of effort to adopt the X.805 standard. Yet, it is effort that pays for itself when the product competes and wins in the marketplace – a marketplace that uses the same security framework to remove the mystery of security and is able to apply a better decision in the technology selection process.

The buyer of the technology also benefits from the transparency by being able to insert the technology into a business solution with the knowledge of how the security design satisfies certification and compliance requirements. One can see all the cost savings without much explanation. The added benefits transfer further to the buyer of technology, (Point Two in the SVL) who is further responsible for providing secure systems and services with accountability in customer relationships. Compliance is made simpler by this transparency, where overall quality is improved and the customer relationship is reinforced.

Those who consider only the up front development cost of the effort to *design in* the security are making a fundamental and strategic mistake; the true cost is the combined cost of product recalls, liabilities, loss of sales – lost opportunities. Imagine going in to pitch a particular product to a customer and facing the question:

“Please tell me how your product was designed for security using the ITU-T X.805 standard security framework,” and your response is, “Ah, can you spell out the name of that security framework one more time?”

That is the end of the sales call and the end of the relationship. Imagine now the opposite situation, your response being:

“Yes! I am pleased to do that. Our engineers considered with great precision the risk parameters in your operational environment for this product using the ITU-T X.805 standard model; they have a complete listing of how all eight security dimensions in the standard were considered within your use environment and can, with that same precision, demonstrate how, as an example, access control, authentication, privacy and system integrity are applied commensurate to the risk model. We can also demonstrate that the security designed-in to our product allows you to meet and maintain your ISO/IEC 27000 series standards certifications and also support your Sarbanes-Oxley Act compliance requirements.”

This is a relationship that the buyer will value – no mystery, no obfuscation, no tap dancing – the sale is made, the relationship strengthened, a happy salesperson, a happy CEO and CFO and a more prosperous company. This is opportunity gained, not lost and the cost of the security design recouped many times over with strong profit margins.

Wherever one may be in this life cycle, having transparency in the security design just makes good sense, but it starts at the Point of Creation. In the world of globalization, outsourcing and products made in multiple places, without the use of the security framework there is no way that a product can end up designed secure to its use. Security does not happen by chance – it must be *designed in*, and the downstream elements in the life cycle are the points of enforcement and carry-through.

That is what this chapter is all about – not the problems but the many ways that following the security framework has real benefits, those that look good on your top line as well as the bottom line in the company’s balance sheet. For the government agency it removes layers of bureaucracy to deliver more cost-effective and secure services – the things that engender confidence.

In this chapter, the many benefits of using the X.805 standard security framework to deliver a more secure Web 2.0 will be discussed. Web 2.0 is repeatedly referenced for the reason stated earlier: Web 2.0 is transformational and it is happening right now. It implies a new technical infrastructure – convergence – and new services; Facebook is a good example.

Web 2.0 applications and services create the great potential for businesses to evolve, bringing a virtual connectivity to customers and business partners – the disintermediation or elimination of the so-called middleman between product-services creator and the end customer. The reduction in latency and cost, and the improved operational efficiencies are the benefits and the differentiation for companies. The concept of making explicit the specific security challenges in data storage in the network cloud, as one example, with a third-party company that might have significantly different business agendas and stresses than your business, brings the discussion full circle. It is about transparency.

How does one secure the data in the network cloud when the interests of the client company may vary significantly from those of the provider of these data storage services? It should be clear, the interests are different, but they are not necessarily incompatible. Different is OK; incompatible is not OK and can create great risks.

The specific security solutions for the most part already exist to create the compatible interests within an acceptable level of risk. Other security technologies may be needed – an opportunity for enterprising security companies. The X.805 standard security framework does not prescribe what the solution is in this specific case in the same way that it does not prescribe any of the security solutions. It does, however, name the requirements; it causes developers, sellers, buyers and service providers to acknowledge its presence and creates transparency in how it is answered – or not answered. The choices are now whether the provider of these services is providing methods of security that despite different business models can still be compatible. The power of transparency is clear and it needs to be used to solve the challenges of present-day and Web 2.0 security.

8

Correcting Our Path – What Will it Take?

“To prime the pump it will take organizations coming together”

Executive Summary

The word that best captures the message of this chapter is inertia – the rut in the path so familiar and so ingrained with reinforcing processes that are so difficult to overcome. At the start of this book the story of the frog in the cauldron where the temperature rises slowly to boiling point was another way to make this same point. This path has a name: an aftermarket approach to security placing the security burden where it can least be resolved, with the end-user community, the buyers and users of the technology. This rut in the path is a persistent practice despite a body of people and knowledge well aware that it is an inadequate method; doing something the same way faster with more money will not create a new and better result. It will simply make an inadequate process faster and more expensive.

Inertia must be understood for how it keeps the status quo. But to actually get out of this rut, change the patterns, the habit of familiarity and the market forces with self-interest to keep it the same, it will take more than good reasoning and sound logic or even the loss of billions of dollars annually. To un-tether from the suction and drag of inertia will take a surge of new energy from different groups pulling together. It will take a clear commitment to a new path of transparency in security, one that starts at the beginning in product development where it always belonged. That is the focus of this chapter, correcting our path – what it will take to get out of the rut of the current path and onto a road to practice a new model where security is *designed in* and it is consistent in each stage of its SVL.

138 *Correcting Our Path – What Will it Take?*

Who are these forces for change? In a broader sense, there are three: business, academia (including research), and government. Specifically, it is leaders in these areas willing to make the investment and step away from the rut of inertia. Closer to ground, it is key organizations willing to lead within these groups, of which there are many. The change must come from all of them, though not necessarily starting together at the same time. The supply side of the security market (security technology companies) has important contributions that provide the key technologies used to mitigate the vulnerabilities, but the impetus to change from aftermarket to *designed in* will not come from the security industry itself; it is too self-invested in the current model. Not that the security industry fails to recognize the need for change, but the inertia feeds this industry, and the security industry will ultimately respond to the demands of customers. The key is with the buyers of the information technology solutions insisting that security be *designed in* with transparency in the form of the security framework described in these previous chapters.

Government must be one of the primary catalysts, as one can argue that it has the most to lose, with the concern over national infrastructure dependent upon communications systems. There are already signs that government gets it; of note is the attention being paid to hardening critical infrastructures from cyber attacks. Consider the Federal Desktop Core Configuration (FDCC) mandate in the U.S. federal government's Office of Management and Budget. By any other name this is about a large customer acting as one buying body demanding that vendors deliver computers in a configuration where the operating system and applications are shipped patched to current levels and stripped of unnecessary features that may create security issues. It is important to note that endpoint computers alone do not make a large complex network, therefore by no means is desktop computer hardening sufficient. It is more than the endpoints, one that includes the network elements, the overall information service delivered with technologies end to end. But this example is a beginning, and it is consistent with the concept. This is a good and hopeful sign.

Businesses must also be primary catalysts and initiators of change. In some vertical markets, such as the world of investment banks, the technology organizations take the practice of security *designed in* as an absolute configuration control applied in every element of the process, not willing to trust anyone but their own well-developed procedures. They take neither endpoint computers, nor any element of networks off the shelf and install it as is. More of this thinking is needed across businesses, though clearly the technical sophistication found in investment banks is a rarity. Businesses in general will need to apply a model of security where it is *designed in* and delivered securely by the product developers – the vendors of technology.

Academia and research laboratories are the final piece that comprises the change agents – the place where engineers and scientists learn their craft, the art and science of innovation and creation. These are the places where security needs to be part of the curriculum, not as a separate function for security engineers. It is an integrated function of sound engineering principles that all engineers learn, and it is in these institutions where it can grow and mature with greater sophistication as a set of principles that come as a body of knowledge with the students who graduate and enter the workforce in product development companies.

It is the entire technology industry that needs to transform, contribute, learn, adapt and integrate security as part of the basic business process. It must follow a standard that is open to contribution and follow an open-source model not held back by a process that is laggard to the pace of business change and to the politics of standards committees. These are not antithetical points; it can be a standard and it can be open to contribution – really open, not just open to companies vying for advantage. It must be open source so all can participate, using the tools already in use, such as blogs and wikis – a standard that matures in small increments, but faster with greater value as it becomes more precise and with greater specification in the various use cases that derive from business in motion.

It must align with the ISO/IEC 27000 series standard as this is the path to certification and compliance, and with certification the needed transparency is developed so that business and governments have a foundation upon which to apply trust. Technology needs to become more trustworthy to its lofty place in our lives – a dependency to every facet of modern society. That can only come from transparency.

How does this pump get primed and get started with sufficient mass that it reaches the critical point, the tipping point, fueled by its own momentum? This question is frequently discussed as the *digital Pearl Harbor*¹ event, a crisis of such magnitude directly attributable to a culprit that can be named and blamed. To be sure, the potential exists for this very scenario. Cyber events are happening today, and they will continue to grow more lucrative due to a variety of motives along with the opportunity presented by vulnerable systems. Be assured that the problem of how to secure complex computer systems will only grow, and its consequence will be more loss in confidence, trust, money and higher costs in trying to correct an uncorrectable situation; one that was designed to fail, or was not designed for survival in a hostile technology environment.

To prime the pump it will take organizations coming together, saying enough is enough. It will take a community of interest for purchasing might and for communicating to its vendor communities that systems will only be acquired that can demonstrate their transparency in accordance with a standard framework. The X.805 standard framework can serve this purpose and get the industry started in correcting its path – a new road moving away from the rut of the path it follows today.

¹ Winn Schwartau, *pearl harbor dot com*, (Interpact Press, 2002)