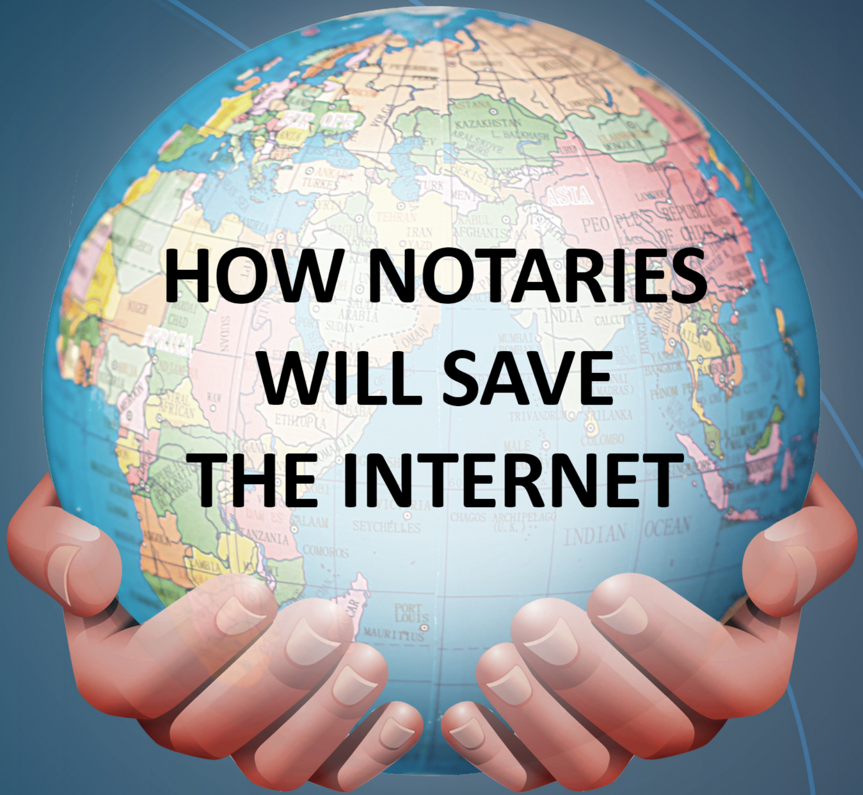
Chapters 1-10

THE FUTURE NEEDS YOU

SECOND EDITION



HOW NOTARIES WILL SAVE THE INTERNET

WES KUSSMAUL

In this book you'll learn why NOTARIES are needed more than ever in the Paperless Digital Age

"Attestation Officers bring urgently needed authenticity to a world awash in inauthenticity."

– Joanna Lilly, President, Empowered Notary
and Former President, American Society of Notaries

The world has entered its second Paperless Age.

In the first Paperless Age, the Roman Tabellio Notaries kept records of deeds on wax tablets, and were paid very well for their important role in society.

Fast forward a couple thousand years. Our paperless digital world is utterly devoid of the accountability that notaries provide.

Result: Pervasive digital identity fraud leading to breaches, ransomware, computer and phone viruses, and on and on.

In this book you'll learn how adding the Attestation Officer designation to your role as a notary public will make you an integral part of the solution to the world's epidemic of ***inauthenticity***.

PKI PRESS

The Future Needs YOU

Second Edition

HOW NOTARIES WILL SAVE THE INTERNET

The significant problems we face cannot be solved at the same level of thinking we were at when we created them.

Albert Einstein

by

Wes Kussmaul

PKI Press
Books about online privacy, security, and authentication

THE FUTURE NEEDS YOU

"Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure," originally published in *Computer Security Journal*, Vol. 16, No. 1, 2000, is reproduced with the kind permission of Carl Ellison and Bruce Schneier. Portions of "Improvements on Conventional PKI Wisdom" from the Proceedings of the First Annual PKI Research Workshop are reproduced with the kind permission of Carl Ellison. The World e-Trust Memorandum of Understanding (MoU) is reproduced by permission of the International Telecommunication Union. Extensive passages from Robin Good's *Guide to P2P File Sharing* are reproduced by permission of Robin Good. The excerpt from *The Design of the OpenBSD Cryptographic Framework*, by Angelos D. Keromytis, Jason L. Wright, and Theo de Raadt is reprinted by permission of Theo de Raadt.

Library of Congress Cataloging-in-Publication Data

Kussmaul, Wes, 1946-
The Future Needs You: *** / by Wes Kussmaul. -- Second edition.
pages cm
Includes index.

Paperback: 978-1-7364316-0-3
eBook: 978-1-63767-021-7
Library of Congress Control Number: 2021930028

1. Telecommunication--Security measures. 2. Internet--Security measures.
3. False personation--Prevention. 4. Privacy. I. Title.
TK5102.85.K87 2013
005.8--dc23 2013003192

FOR

MICKY THEODORIDIS

trusted advisor and friend

Through his pioneering work with Identrus,
and with plans to develop his own systems of trust technology,
Micky was a major force in bringing about an authenticated world
when he, his wife Rahma, and their unborn child
found themselves aboard Flight 11 on September 11, 2001.

He touched the lives of many

He will never be forgotten

He will always be missed

CONTENTS

Something there is that doesn't love a wall…

He says again, "Good fences make good neighbors."

Robert Frost, from "Mending Wall"

Something There Is That Needs a Wall

Something that doesn't love a wall is me
With other internauts, I want to be free.

But some free spirits become disgrace
When liberated in cyberspace.

We're slow to learn that after the Fall
We have not earned such license at all.

(Utopians are never eager to see
The ways that walls make people free.)

But when we meet, we meet in a place
Removed from the crazy highway race.

Something there is that needs a wall:
The preschool, the office, the shopping mall.

And so the mender might glean from his labors
Truly, good fences do make good neighbors.

FOREWORD TO THE FIRST EDITION

BY JACK SETH

With recent historical and life-altering events[1], our lives have been suddenly and tragically transformed. We are a far distance from the seemingly safe environment we took for granted such a short time ago, leading increasingly security-minded lifestyles. People are wary and cautious when undertaking the most simple of tasks, such as air travel or attending a public event—even going to work seems to present new dangers.

As surely as the world around us appears frightening, we as notaries have an important role to play in minimizing the public's fear. Consider what we do. In addition to serving as unbiased witnesses to important transactions, we have experience and skill authenticating the identity of signers. In coming years, the need for that service will grow dramatically as more and more individuals and corporations use the internet or business transactions, meetings, and educational events where, in order to gain access, proof of identity is mandatory. Notaries can and will provide that proof of identity, even if no further notarial act is required. Access to online meetingplaces will become more difficult and eventually impossible without a physical token of authentication, and the notary is the key to that verification.

Notaries are finding themselves increasingly important in a rapidly changing world, where identity authentication is paramount and identity theft and fraud are rampant. This book reveals the crucial need for stringent measures to prove identity and provides a roadmap into a future that will ensure the enduring significance of the notary public.

As an attorney, former notary, and notary historian, I must strongly emphasize to notaries that it is critical they adhere to proper procedures when identifying any individual appearing before them. Now, more than ever, notaries must carefully and thoroughly authenticate the identity of individuals appearing before them before signing a notarial certificate. A verbal acknowledgment or oath is an imperative component of the notarial ceremony and is often disregarded. Moreover, as always, the notary must determine a signer's willingness to sign and the signer's understanding of the act taking place. In the increasingly technical evolution of commerce today,

[1] This Foreword to the first edition was written not long after the September 11, 2001 attacks.

the notary has fundamental responsibilities that must be implemented with the highest integrity.

Wes Kussmaul has extensive experience in internet communities and business. As the founder of Delphi Internet Services Corporation, he played a major part in ushering in the Digital Age. He understands and applauds the indispensable role the notary has in that electronic environment. Read this book, and understand more about the changing world we live in. Learn how you, the notary, can serve effectively by your growing security-driven participation in the virtual world of online commerce, and help establish a trusted community of securely identified participants. You have a vital role to play in the future … a safe and productive future for all of us.

The future needs you.

(The late) John E. (Jack) Seth
Delegate to the International Union of Latin Notaries
Director Emeritus, American Society of Notaries

AUTHOR'S PREFACE

I began the preface to the first edition with my concern about the future my children face in a world of cybercrime and online mayhem. Now that I can include grandchildren to the subjects of my concern, I find that the threats have evolved more or less as I predicted and that they are even more pronounced today than they were in 2001. I noted then that to underestimate the destructive potential of outlaws in the hopelessly ungoverned and ungovernable open rangeland of the wild online spaces could turn out to be worse than the Allies' underestimation of what was happening in Europe and China in the 1930s. The winds of war are again blowing, but this time the enemy is not a nation but a collection of vandals, thieves, and terrorists, acting with the impunity provided by ungoverned outdoor spaces such as jungles, mountain ranges – and the internet.

Participants in this organized crime version 2.0, unlike the traditional version, can operate from any and all geographical jurisdictions at any time. If we don't do something, we are in for some truly desperate times.

If we do act, and if our actions are well thought out, we can bring the outlaws under control, and materially improve our lives in the process. There is a heretofore unarticulated path to reducing the risks we face while at the same time improving the privacy and quality of our lives. Knowing that is a very strong incentive to get out the message about that path.

An even stronger motivation is the thought that we might continue to rely upon information security technology to meet the challenge, which is to say that we will not meet the challenge at all. In this book I will show that authenticity will succeed where security technology has failed us. This very old thing called authenticity is precisely what we need to keep the world from being taken over by a new borderless organized crime.

I hope you agree with the path to the solution presented here. And if you do, I hope you will help me make it all happen!

This book is about an emerging *new* role for the notary public, an exciting role that secures the lasting significance of the notary office by placing it at the crossroads of tradition and technology. You will read about the distinct advantages of serving the public as an *Attestation Officer*, which involves specific training and certification in addition to the notary notary training and commissions issued by states, provinces, and other jurisdictions.

Of course, a strict adherence to the laws of your commissioning jurisdiction is necessary. As always, a notary must know and follow the law of the commissioning jurisdiction. But just as the Notary Signing Agent designation was created by Scott and Susan Pence as an extra-jurisdictional certification to provide mortgage lenders a more uniform means of reliance on a notary's qualifications, so the Attestation Officer certification originates from outside the notary's commissioning jurisdiction. The word "Officer" in "Attestation Officer" is there to remind people that the certification is in addition to the notary's prior status as a public official, bringing duly constituted public authority to private matters; and along with it all the liabilities and responsibilities of public office..

This book offers an introduction to the procedures to be followed by the Attestation Officer, a designation that every notary interested in the future of the profession will want to learn more about.

Acknowledgments

I'd like to thank the people who helped me with this book, starting with my wife Maria Lewis Kussmaul, for her patience with the time the project has taken and the strong dissent from the assumptions of her industry that it introduces. Thanks also to my daughter, Sara Kussmaul DuBose, and her husband Graham DuBose for their suggestions and for their very professional work on the videos that accompany both this book and two others: *Own Your Privacy a*nd *Quiet Enjoyment*.

A big thank you is owed to Bruce Schneier and Carl Ellison for their permission to reproduce their famous Ten Risks document in its entirety.

Suzanne Niles helped whip the first edition of *Quiet Enjoyment* into shape, and is carving out time from her busy life to help with this book.

The Personal Information Ownership Component is not just a chapter in a book but an actual working prototype, thanks to the considerable talents and efforts of Denise Lochtenbergh, as well as Eddy Nigg's intimate understanding of the operation of a certification authority, help to bring it all out of brainstorm space and into the real world.

Bill Gilpatric, whom I have known since our Air Force days in the 60's, is helping us get the word out on both books. The first editions of both books benefited from the graphic design skills of my daughter Lucinda Booth.

The late Jim Woodhill was a great help in the fine-tuning of the case for a global identity credential, simply by being an intelligent and very tireless debate adversary in advocating for national credentials.

Peter Hadley's suggestions about re-ordering content led to a more readable manuscript, while his holding down the fort on our server and sites allowed me to focus on the writing. Robin Good provided the photograph from the City of Osmio Municipal Charter meeting. He and Ugo Bechini, Luigi D'Ardia, and Alex Ntoko contributed their time and insights to the Charter itself. Alex's help in understanding

the International Telecommunication Union's World e-Trust Initiative was invaluable in putting together the components of QEI.

Michael Krieger of the UCLA Computer Science department was helpful in editing the description of the mathematics of public key cryptography. Joanna Lilly provided helpful early guidance about the intersection of technology and notarial authentication.

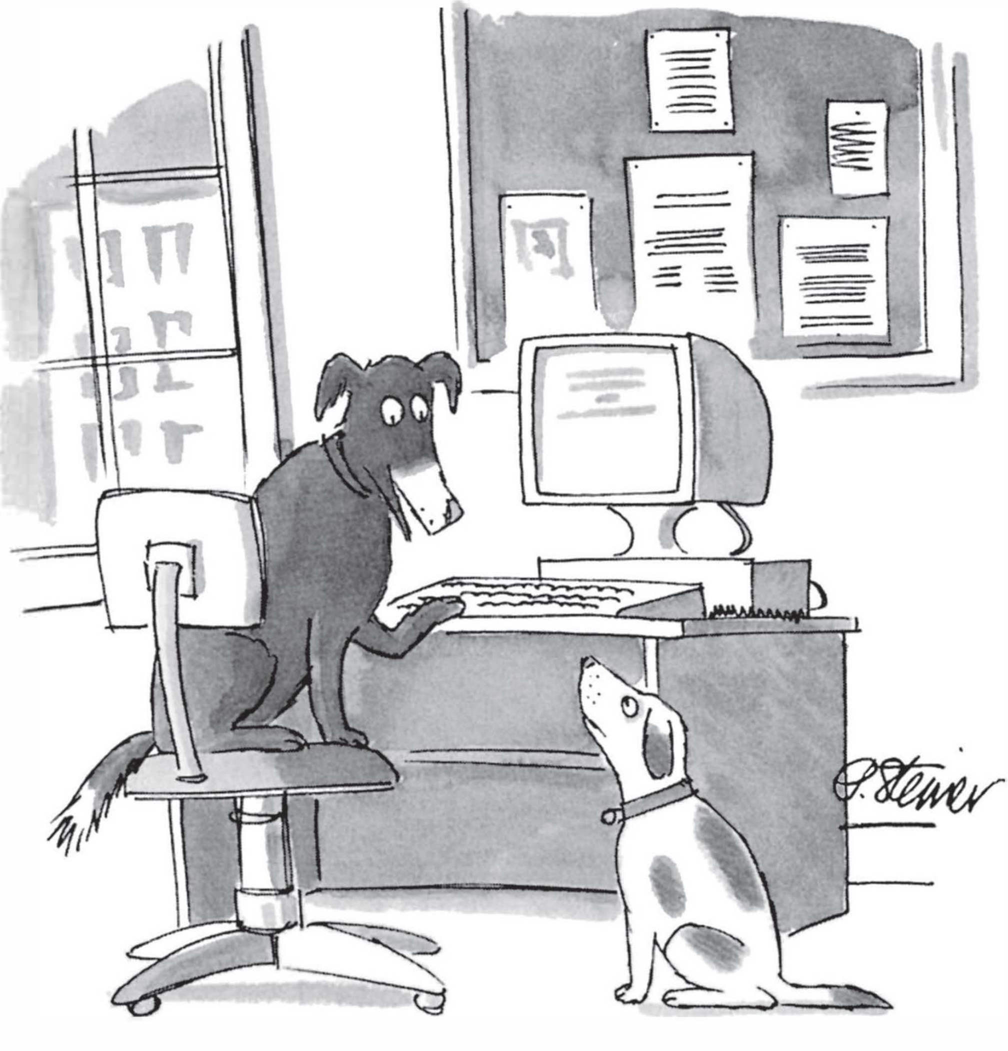
As I write this Rochelle Mensidor is applying her considerable design skills to make my work look good, as she has done so well with my previous books.

And of course I must again thank Jack Seth, this time posthumously, for his insightful foreword.

Wes Kussmaul
Boston, Massachusetts
September, 2020

PART 1

The Practice of Attestation in the Paperless Digital Age



"On the Internet, nobody knows you're a dog."

1

The Future Needs You

As a notary, you've learned how to take steps to ensure that a signer is who they claim to be. But as the world goes paperless, the old procedures may seem less relevant. The role of the notary public has been characterized by some as an anachronism, having no place in the paperless digital age.

That happens to be incorrect.

In fact, ***the reality is the exact opposite of that characterization.***

The paperless digital age has ushered in an epidemic of inauthenticity: fraud, malware, phishing attacks, breaches, ransomware, anonymous payment for anonymously solicited crime, human trafficking, and on and on. A new form of organized crime is taking over our systems of commerce and communication.

With a third of a trillion dollars spent every year on systems security, how could that be happening?

The reason is astoundingly simple: our information systems have been designed and built with utter disregard for the need for the accountability that comes from measurably reliable identities of the people using those systems. Technologists have relentlessly pursued a catch-the-bad-guys strategy without stopping to think why that strategy will never work.

Until recently, people have shown a remarkable willingness to pay for security that does not work. But that's changing fast. You and I together will demonstrate how accountability built upon measurably reliable identities fixes a multitude of problems at less cost.

You, the notary public, are the key to bringing measurably reliable identities into the world's information infrastructure.

If you don't read another page of this book, please keep this message in your head and heart: ***the future needs you, the notary, to bring authenticity to the information and communication systems*** *upon which everyone on Earth has become so completely dependent.*

Also, if you can't find the time to read the whole book, then watch two short videos about something called PKI: *What is PKI* and *PKI Done Right*. You'll find both videos at https://tabelio.org.

If you absorb the messages in those two short videos you will have a better understanding of the solution to security problems than is the case with almost all security experts – who generally do not understand this thing called PKI.

2

Become an Attestation Officer

As a practicing notary public you may be thinking “I know how to do acknowledgments and affidavits and I even know how to do a second mortgage closing; but what has that got to do with internet security?”

Good question.

We have a good answer for you, but before we get into the description of what an Attestation Officer does, let’s note one facet of the job which you will probably agree is very important:

Attestation Officers Will Be Well Paid.

To repeat: the Attestation Officer role pays well.

As an Attestation Officer you will be paid well for a procedure that will be very much in demand and which doesn’t take a lot of time. Unlike a mortgage closing, this process takes place in your home or office and only takes minutes.

Better yet, your relationship with the enrollment client is permanent. You’ll receive a variety of fees, some annual, some for upgrade services, some for restoring the client’s credential when their phone is lost or stolen. If the client chooses to have you maintain an escrow file containing their credential’s digital keys, you’ll be paid annually just for taking that responsibility, with no extra effort on your part. We’ll go into that in a little more detail in the next chapter.

The Attestation Officer role is new. And so while there are no guarantees, that fact also means that those who do take the training and become qualified early will reap the greatest reward.

Notaries in Latin Law countries are paid very well for the same kind of work that notaries in common law jurisdictions have never been adequately compensated. The Attestation Officer role will change that. Did we mention that Attestation Officers will be well paid?

Back to the Job Description

First, let's start by noting that you already have the word "Officer" in the job title covered. When you were commissioned by your jurisdiction, you were made a public official. You are empowered to apply duly constituted public authority in testamentary matters, public and private. As a police officer is an officer of the public, so are you. Both you and the police officer are empowered to apply public authority in your work, although in different realms of responsibility.

Every procedure you perform as a notary, that is, as an officer of the public, involves identity verification. You know how to check ID, right?

You're probably also aware that many U.S. states have launched Remote Online Notary (RON) programs, where notarial processes are performed over a video link using a video conferencing application such as Zoom, Webex, InDoors, Microsoft Teams, GoToMeeting, etc. In the case of such online notarial procedures, obviously the process of checking ID is different from one in which you hold the client's driver's license in your hand as you copy its number into your log book.

In the real world, perfection is scarce. As any bar bouncer will confirm, high quality fake drivers' licenses abound; it makes little difference whether you're verifying them in a face to face setting or an online video setting. There is only so much responsibility you can be asked to assume in a world of fake IDs.

And that is a fundamental premise behind the Attestation Officer's role. As an Attestation Officer you will be asked to record a variety of forms of ***Evidence of Identity*** presented by, or accompanying, your enrollment client. The apparent validity of their government-issued ID is only one piece of the puzzle. Specifically, it is one part of one eighth of the puzzle. We need more than an easily-faked driver's license or even passport to have measurable confidence in your claimed identity. *That* is what this job is all about.

The important word above is "record". In most cases the process is merely making a record of what you see, using the tools you've been given. While there are occasional judgment calls to be made, you can always call for help and backup in making those calls.

You'll be asked to record the existence of various forms of Evidence of Identity. Those forms of Evidence of Identity fall into eight categories. Each of the eight Dimensions of Identity Quality is measured using a scale of 0 to 9, with 0 being the lowest rating in a particular dimension.

The Eight Dimensions of Identity Quality

1. **Degree of Protection of Personal Assets.** Does the user have "skin in the game" or are their employer's assets the only ones at risk? (The only reliable way to prevent credential sharing at work is with credentials that protect the user's financial, reputational, and identity assets.) To what extent

does the identity protect those personal assets? An enrollee's ownership of the credential itself (rather than an employer-owned credential) is part of this criterion, as the credential itself should be a valuable personal asset. If a higher score is requested (and paid for), you will be provided a means to check that a bank account in their name is under their control.

2. **Quality of Enrollment Practices.** What type of enrollment procedure was used? Did it involve corroboration of personal information? (You'll be provided tools to administer the PII corroboration test (often called knowledge-based authentication or KBA)? Was it an in-person enrollment or remote, via a video session? Or are you merely serving as the Attestation Officer of record for a free low-quality self-service enrollment where only email and SMS verification have taken place? (Later when a relying party requires a higher Enrollment Quality Score, you will be the one to earn the fee for the upgrade service.) Each risk profile and highest protected digital asset value will call for a particular enrollment procedure. Of course the higher the required Enrollment Qualty, the higher your fee. A company in the electric power generation and distribution industry found a quoted enrollment fee of fifteen hundred dollars per person to be quite acceptable. The higher the identity quality score, the higher the fee.
3. **Quality of Means of Assertion. A well-used identity is a more reliable identity; the more places it is used, the better.** You'll be provided with instructions and tools to determine whether the credential supports OpenID, FIDO, Shibboleth, CardSpace and others.
4. **Quality of Authoritative Attestation.** In most cases this will be automatic. As an Attestation Officer you are applying the duly constituted public authority of a certification authority called the Osmio Vital Records Department or Osmio VRD. Since this Identity Quality Assurance system may be used to measure any claim of identity backed by anyone, this metric #4 exists to make the process universal. For example the U.S. government has a system of identity quality called LOA 800-63. While there is no current provision for it, in the future you may be asked to rate the quality of the identity claim of a government contractor.
5. **Quality of Other Attestations.** To what extent do colleagues of the subject corroborate the subject's claim of identity? The more acquaintances willing to put their own identity quality scores at risk, and the higher those scores are, the higher this score will be. You'll be given tools that give you an objective means to rate this metric.
6. **Quality of the Credential.** Here you'll be given a list of credential types. You'll simply look up the credential on the list and record the number between zero and nine that appears next to it on the list. There may be qualifications about the way the credential is used that require further consideration. In that case you'll simply contact the engineer on duty to

make the determination. You won't be asked to participate in judgment calls on this metric.

7. **Quality of Assumption of Liability.** If fraud is committed with the use of the credential, who carries the liability? As with the previous metric, you will be given a table that shows the various bonding sources. You'll record what the lookup table tells you to record. If the identity claim is bonded by an entity that's not in the table, you'll simply get in touch with Metric 7 administrators, who will make the determination for you.
8. **Reputation of the Credential.** How long has the credential been used without revocation or reported compromise? How many transactions and authentication events has it been used for in total? The longer a credential has been used without incident, the more reliable it tends to be. Note that the reputation of the credential is not the same thing as the reputation of the subject. For example, if a subject with a very good reputation has a habit of lending his or her credential to family members and colleagues, resulting in documented confusion over who is responsible for what, then the reputation of the credential is greatly diminished.

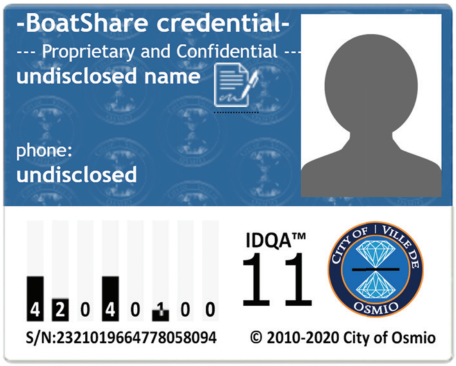
Here again, the determination will be made by Metric 8 administrators.

Aggregate Identity Quality Goes from 0 to 72

Adding all eight dimensions for a particular identity yields an Identity Quality Score between 0 and 72. That is the objective measure by which a relying party will know whether the claimed identity is sufficiently reliable.

Each of the eight component scores is reported reported by the Osmio VRD certification authority when a certificate status query is made, because different relying parties will value the forms of Evidence of Identity differently.

There will be cases where a website will want to let users know the identity quality score of, for instance, a blog reader who has submitted a comment. For that purpose IDQA badge is provided for display by the site. Here;s an example of an IDQA badge:



IDQA badge:
Note that the badge carries the branding of the organization that generated the enrollment – in this case it's a hypothetical organization called BoatShare. If you are responsible for bringing Authenticity to an organization and getting them on board, you will be entitled to a fee for your role.

IDQA can be used to evaluate, record and report the value of an identity claim represented by any credential technology. However, IDQA integrates best with the Authenticity Infrastructure, which is a system that is built upon the truly remarkable technology and methodology of PKI. We'll explain PKI shortly, but first let's take another look at the recurring revenue that's generated by the Attestation Officer role. After that we'll see why PKI is needed, that is, why commonly used security technology is failing.

3

Passive Recurring Revenue

Take **another** look at this famous cartoon:

© 1993 Peter Steiner, The New Yorker Collection / The Cartoon Bank

"On the Internet, nobody knows you're a dog."

A few years after that first appeared, MIT's Technology Review came out with this cover story:

All these years, after security companies and their customers have spent multiple trillions of dollars on the solution, the problem not only has not been solved; in fact the problem has gotten worse.

The reason is astoundingly simple. Security technology is almost always built on the catch-the-bad-guys approach, that is, on determining the character and intentions of the sender of a stream of bits.

Isn't that like telling an office building's lobby receptionist to determine the intentions and character of everyone who walks through the door? Wouldn't that be impossible?

Instead, wouldn't you ask the lobby receptionist to get some ID - a business card or driver's license - in order to establish who is accountable for what happens while the visitor is in the building?

Good security is about accountability. Security is only secondarily about what do do after a bad guy has broken in and stolen something.

The result of that tragically mistaken reliance on cops-and-robbers security, the problems caused by lack of accountability, have turned the internet into a worsening epidemic of identity theft and identity fraud. Identity problems lead to phishing attacks, breaches, ransomware, viruses. Anonymous solicitation with anonymous payment is a gift to human traffickers, drug dealers and other criminals.

What the world needs now is: accountability.

And accountability comes from measurably reliable identities.

As a notary, you've learned how to take steps to ensure that a signer is who they claim to be.

***As a notary, YOU* are the key to reversing the epidemic of identity theft and identity fraud**

YOU are needed for enrollment procedures.

But that's just the beginning of the story.

It's just the beginning of the story because accountability calls for permanent universal identity credentials that carry a measure of their own reliability. A person's whole administrative life – insurance, employment, tax payments and refunds – even their connection to social media – will be tied up in that universal credential.

So What happens when that person loses their credential?

Answer: *YOU*, as their designated Attestion Officer, hold the keys to connecting their records to a new credential. Whether you actually were paid annually for keeping the keys in escrow, or you repeated the process of gathering evidence of identity before applying the user-supplied keys to the new credential, you are they gatekeeper to continued availability of their personal credential and access to their personal store of personal information.

In other words, the future needs you.

And Then There Are Upgrades

A user's new job may require a higher identity quality score. Or, a user may just want a higher identity quality score. Or the user may need access to a database that calls for a higher score.

what happens when a new relying party requires (and pays for) a higher level of identity reliability?

Answer: *YOU,* as their designated Attestion Officer, are the one to perform additional procedures to gather additional Evidence of Identity and record the higher score.

What happens when any of another set of identity events causes them to go back to the person who enrolled them?

Answer: *YOU,* as their designated Attestion Officer, will have a permanent relationship with the person whose identity you validated and recorded.

Self-service enrollment is free, or, internet marketing language, a "freemium" offer. It doesn't involve you, except that you will probably want to be the Attestation Officer of record for your fair share of self-service enrollees.

That's because when that person sees how important their credential is to their life in their increasingly paperless online lifestyle, and as they are encouraged to sign up for escrow services with their designated Attestation Officer, that person will remain your client, paying you an annual fee, for as long as you maintain that escrow relationship.

And that doesn't include revenue from upgrade and restoration and other services you may provide – or simply Authenticity related third party services for which you earn a commission based simply on your relationship with the user.

Recurring revenue – for you.

Passive revenue – for you.

PART 2

Security Technology is The New Bloodletting

Let our advance worrying become advance thinking and planning.

Sir Winston Churchill

4

Bad News and Good News

"Wes, you know the cartoon. 'On the internet, no one knows you're a dog.' What are we going to do?"

Kip Bryan, our VP of Engineering, was wrestling with the looming problem. Our successful social networking service, where members enjoyed both privacy and mutual accountability, would have to make the leap to the internet, where it appeared they would have neither.

"Our members value their privacy and they value that other members are accountable for their actions. But on the internet anyone can be whoever they want to be. They become just users instead of members. There's no security, no privacy, no accountability. It's a disaster waiting to happen."

So went one of the many conversations at Delphi, the company I had founded in 1981, as it faced a difficult transition. Delphi was in the business of providing online social network gathering places. Online, that is, but not on the internet.

Simultaneous privacy and accountability were essential constituents of the value we had provided to individual users and groups for nearly a decade. But how could we continue to do that in this new environment, where internet service providers simply dump users onto the open, public, outdoor information highway?

As it turned out, our concerns didn't matter. The writing was on the wall. The prohibitions on commercial activity on the internet came down in the early '90's, meaning that we and our rivals AOL, CompuServe, and Prodigy would have to become internet service providers. Our enclosed, walled, protected online spaces would have to become part of the outdoor public transport system, the Information Superhighway.

The Disaster Waited, Then Happened

Fast forward a decade. "The Internet Is Broken" proclaimed the title of an *MIT Technology Review* cover story, while Stanford University's Clean Slate Initiative explored the idea of scrapping the existing Net and starting over.

Then things got worse.

As was inevitable.

A decade and a half after that article appeared, the use of the Internet, which now includes phone networks, has changed drastically. Participation in social media has grown by a factor of thousands, Chinese social networks have merged ecommerce with social, and a huge variety of services have been introduced. Half the world's population makes regular use of internet-based services.

But the problems cited in the article have only gotten worse. Spam brings us phishing attacks that deliver malware that in turn builds botnets. Fraud and predation pervade everyday online experience. Identities – and cash – are stolen in batches. Ransomware and other threats have been added to the mayhem. As the information security industry assures us "we're working on it," people grow ever more wary of their internet experience even as they come to depend upon it more and more.

Because the inevitable train wreck that is internet security and privacy took place over decades, people resigned themselves, like citizens of some hopelessly corrupt banana republic, to a permanent state of fraud, theft, and predation.

Inevitable, that is, when people keep their files, hold their meetings, and let their kids hang out in a crowded outdoor rest area alongside a busy information highway or in cardboard boxes by the side of an online city street. Though the term has gone out of fashion, the Information Highway continues to live up to its name.

We Can't Live in Cardboard Boxes

The problem is not a broken internet. That highway serves well as an outdoor public transport system. From the underlayment and substrate and pavement to the traffic controls and painted lines and signage on the surface – that is, the Web – it's truly a marvel of engineering, delivering a set of smoothly paved high speed roadways that transport packet vehicles around the world with incredible speed.

No, the problem is rather with *the way we use* the internet. We do things on the outdoor highway that should be done indoors. We keep our files, hold our meetings, and let our kids hang out in a busy outdoor rest stop alongside the highway, instead of moving our files, desks, play spaces, and meeting halls to indoor spaces.

Put it another way: our online lives resemble the lives of defenseless homeless folks, living in cardboard boxes alongside the road. Appropriately, we are constantly vigilant for the inevitable threats that our living conditions invite. Life on the streets is dangerous.

Whose idea was it to live like this, anyway?

Good News

The good news is simply this: a complete solution is available – and its component pieces are old and proven. It's just that the old and proven pieces are invisible to technologists whose field of vision is limited to technology. In this book, and in actual practice, we have brought those old and proven pieces together with the technology pieces. And now we've brought the whole thing into the field of vision of decision makers.

One of those old and proven pieces consists of the application of duly constituted public authority into the whole system. That is of course exactly what the practice of the notary public is all about – right?

Further, the root of our internet problems is also the root of all sorts of other problems: financial, governance, health care, critical infrastructure, social, and interpersonal. And the solution that fixes our internet problems also fixes those "offline" problems.

Almost everything about the practice of security is deeply flawed, and the solution is neither technology nor training of users to be more security conscious.

In fact you, the notary public, are the heart of the solution. You are the key to a comprehensive solution to not just problems of security but a multitutde of other problems as well.

Authenticity Works Where Security Technology Has Failed Us

As the fault is not with the information highway, neither is it with us users of the highway. We do things outdoors for the simple reason that online buildings do not exist. Let's remedy that.

Buildings are about providing spaces where, among other things, we have confidence in the identities of the others who share the space with us, and who have access to its file cabinets and other resources. You share a room with others in an entirely different manner from the way you would share a highway with them. Buildings provide a measure of accountability, which in turn yields a measure of authenticity.

And there's the magic word: authenticity.

Mankind over the centuries has developed a superb set of methods and procedures for establishing authenticity. New digital "construction materials" combined with these old processes will deliver precisely what we're looking for: privacy, security, reliability, authenticity. The security that is provided as a byproduct of authenticity is superior to the stopgap measures currently dominating what web guru Bruce Schneier aptly calls the "security theatre" market, with its antivirus software, firewalls, and intrusion prevention systems. **Authenticity works where security technology has failed us.**

Let's take a good look at this very new and very old way of fixing the internet's problems.

5

The New Bloodletting

And all that the Lorax left here in this mess was a small pile of rocks with the one word… "UNLESS"

Dr. Seuss

Are you familiar with the intricacies of firewalls, malware signatures, intrusion detection, intrusion prevention systems, security incident analysis tools, advanced persistent threat mitigation, DLP?

No?

Good!

Because those things don't work.

The more of yourself – your time, your skills, your self-image, the space inside your skull – that you have invested in working with those things, the harder it will be to let them go.

For hundreds of years physicians practiced bloodletting, the draining of blood from a patient in order to rid the person of an overabundance of a certain type of "humor," despite plentiful evidence that bloodletting was useless at best, and surely despite some skeptical looks from patients and their families. No one likes to confront evidence that something in which they've invested their professional lives is useless. I am not a practitioner of information security because I have seen that the practice of information security does not produce information security any more than the practice of bloodletting produces health.

Authenticity, on the other hand, is a goal worthy of the efforts needed to achieve it. And in producing authenticity we get an important byproduct: information security.

When I have engaged in discussions both online and face-to-face about authenticity, people often assume that I'm talking about a character attribute or a desired value in human relationships. "People should be authentic with each other."

Well sure, but that's not what this is about.

The authenticity this book advocates and enables comes from knowing the accuracy of others' claims of identity with measurable reliability, and being able to hold the identified parties accountable for their actions while using that claim of identity, while not knowing the identified person's name, location, or any other item of information about them.

Anonymous accountability. Accountable anonymity.

We can have it, and we can have it pervasively. Then and only then can we have reliable online buildings.

Time to Blow the Whistle

Early in the new millennium the Secretary General of the International Telecommunication Union, a United Nations agency, appointed me to serve on the High Level Experts Group of its Global Cybersecurity Agenda. I was appointed because of an observation that I've been pretty vocal about:
security problems are the effect of a bigger problem.
That problem is *inauthenticity*.

This book is about a specific set of procedures and technologies that will solve the inauthenticity problem.

To understand it, we need to step back – way back – and examine where the problems came from in the first place.

Authenticity: Where It Went, How to Get It Back

People all want privacy for themselves, and accountability from everyone else.

Our car registrations illustrate how we can have both at the same time. Everyone can see your license plate number, but others can only know your identity under certain circumstances, such as when your car is in an accident with theirs.

The question is, who keeps the file that maps car registrations to drivers' licenses? In a social network, that translates to, who keeps the mapping of user names to real names? The practices of that back office must be visible, monitorable, and secure. Technology and practice must scrupulously obey the rules of due process in disclosing names only to those with a need and a right to know them.

With something called the Internet of People protocol, it's impossible to find the identity of a person in that database directly. The database can only tell the identity of the Attestation Officer who is responsible for the enrollment of that person.

Wouldn't it be great to be in complete control of the use of information about yourself? You, the notary public, are the key to making that possible.

How We Got into This Mess

Delphi Internet Services Corp. was launched at the beginning of the '80s, before the epidemic of inauthenticity. Some years later new internet companies doubled in value overnight, and suddenly investment banks were clamoring to get on the bandwagon, hyping new dot coms while paying little attention to their merit. It seemed that the more ridiculous the business, the more they could get people to buy stock. Later we learned that at the same time the analysts and their employers were singing the praises of those ill-conceived companies to individual investors, among themselves they were laughing at both the companies and their gullible investors.

The results were predictable. Those who got swept up in the market bubble got a quick and costly lesson in what happens when hype and emotion trump common sense.

But the big trouble didn't end with the dotcom debacle. Many of the ensuing offenders have become household names: Enron, WorldCom, HealthSouth, Parmalat, BCCI.

Do you remember wondering what happened to integrity, thinking that things couldn't possibly get worse than Enron and Worldcom? But of course they did get worse.

A whole new set of companies played fast and loose with the facts. Investment banks and accounting firms attested to the fantasies of value in securitized no-doc mortgages, loans to borrowers who pay a higher rate of interest so they can lie about their income. As in any Ponzi scheme, those who got out early did quite well by sticking it to the later investors.

ARTHUR
ANDERSEN

Mortgage originators and the securities industry came up with a very imaginative new process for turning low-grade mortgage ore into golden marketable securities. Each step made the underlying junk debt look a little prettier. The two technical terms for this process are securitization and…fraud.

And what happened to those who attested to the authenticity of all this…stuff? The firms went under, their investors lost everything, but management collected their bonuses and moved on.

Wall Street's inauthenticity reached preposterous proportions. But it's not just Wall Street.

Here's a little from that MIT Technology Review cover story that proclaimed the emperor to be naked; that "The Internet is Broken":

> In his office within the gleaming-stainless-steel and orange-brick jumble of MIT's Stata Center, Internet elder statesman and onetime chief protocol architect David D. Clark prints out an old PowerPoint talk. Dated July 1992, it ranges over technical issues like domain naming and scalability. But in one slide, Clark points to the Internet's dark side: its lack of built-in security.

> In others, he observes that sometimes the worst disasters are caused not by sudden events but by slow, incremental processes -- and that humans are good at ignoring problems. “Things get worse slowly. People adjust,” Clark noted in his presentation...
>
> At the same time, the Internet’s shortcomings have resulted in plunging security and a decreased ability to accommodate new technologies. “We are at an inflection point, a revolution point,” Clark now argues. And he delivers a strikingly pessimistic assessment of where the Internet will end up without dramatic intervention. “We might just be at the point where the utility of the Internet stalls -- and perhaps turns downward.”
>
> Indeed, for the average user, the Internet these days all too often resembles New York’s Times Square in the 1980s. It was exciting and vibrant, but you made sure to keep your head down, lest you be offered drugs, robbed, or harangued by the insane...
>
> That’s why Clark argues that it’s time to rethink the Internet’s basic architecture, to potentially start over with a fresh design -- and equally important, with a plausible strategy for proving the design’s viability, so that it stands a chance of implementation. “It’s not as if there is some killer technology at the protocol or network level that we somehow failed to include,” says Clark.

So far so good. But then...

> “We need to take all the technologies we already know and fit them together so that we get a different overall system.

See, there is the problem. Clark goes on...

> This is not about building a technology innovation that changes the world but about architecture -- pulling the pieces together in a different way to achieve high-level objectives.”

Architecture? Well, yes, now he’s getting somewhere. Architecture is needed.

But in the world of information technology, “architecture” doesn’t carry the same connotations as the traditional usage of the word.

In the physical world, architects are professionally licensed by public authority. They sign their drawings and the applications for occupancy permits for the buildings they design, and they are legally responsible if problems arise.

If David Clark wants an architectural approach to make a difference in his re-imagined internet, then “taking all the technologies we already know” will not do it. The difference between the practice of physical architecture and information architecture is that one requires an individual professional accountability that is unheard of in the other.

The article calls for a clean slate, and Stanford University responded with its Clean Slate Initiative. From the paper[2] that launched the Stanford University Clean Slate Initiative:

> Shortcomings of the Internet
>
> Designed over 30 years ago, the success of the Internet is a testament to the foresight of a handful of visionary researchers. Hundreds of millions of users rely on it for business and pleasure; and it is now hard to imagine a world without it. But our reliance on the Internet makes us victims of its success, and vulnerable to its shortcomings. Some of the shortcomings are self-evident, such as the plague of security breaches, spread of worms, and denial of service attacks. Even without attacks, service is often not available due to failures in equipment or fragile routing protocols. And its behavior is unpredictable making it unsuitable for time-critical applications. Other shortcomings are less obvious: The Internet was designed for computers in fixed locations, and is ill-suited to support mobile end-hosts; it uses packet-switching making it hard to take advantage of improvements in optical switching technology; it neither ensures anonymity, nor facilitates accountability; and the demise and restructuring of most network service providers suggests that providing network service is not profitable. In summary, we don’t believe that we can or should continue to rely on a network that is often broken, frequently disconnected, unpredictable in its behavior, rampant with (and unprotected from) malicious users, and probably not economically sustainable.

[2] *Clean-Slate Design For The Internet*, a paper produced by “a group of faculty from the Departments of Electrical Engineering, Computer Science, and Management Science and Engineering,” edited by Nick McKeown and Bernd Girod, Stanford University.

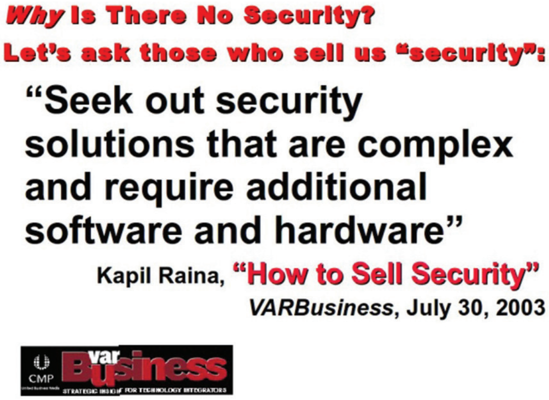
But the MIT-Stanford slate wasn't clean at all. It addressed internet technology, but not the root cause of the problems. And that's why it failed.

Epistemology is the study of the ways we come to know things. If only Stanford had involved its Department of Epistemology in addition to its the Departments of Electrical Engineering, Computer Science, and Management Science and Engineering in coming up with its Clean Slate, the group might have addressed the question, "How do we protect anonymity and provide accountability at the same time?"

Unfortunately Stanford couldn't do that because it, and as far as I can tell every other university, does not have an epistemology department. Someone needs to tell the world that it desperately needs epistemologists. I'll start.

As long as we don't know the real identity of the source of a stream of bits – the person who sent them directly or who is responsible for the software that sends them – we are left to guess at the sender's real intentions and character. That's a pretty iffy exercise. The information technology industry loves iffy exercises, as they provide opportunities to sell expertise and software without being accountable for real solutions.

Solving Problems Is Unprofitable



Why Is There No Security?
Let's ask those who sell us "security":

"Seek out security solutions that are complex and require additional software and hardware"

Kapil Raina, "How to Sell Security"
VARBusiness, July 30, 2003

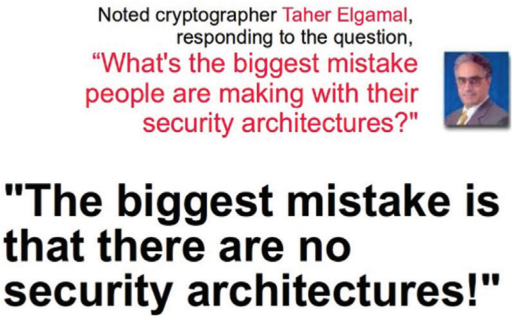
To see how that works, let's ask an expert why there are so many security problems online and offline. Here's a candid answer from an expert in the marketing of security technology:

Pause a moment to look at this advice from a magazine for people who sell information technology to you and me. For seventeen years the "security" industry has got the world to spend literally trillions of dollars on snake oil that still delivers, as Bruce Schneier puts it, "security theater" rather than security.

The advice of Kapil Raina, a knowledgeable security expert, seems to be: Do not solve the customer's information security problems! Because if you solve those problems with a well-thought-out and well-architected solution, then you deprive yourself of ongoing revenue.

Kapil Raina's quote explains one reason why there are no security architectures, as another distinguished security expert, the author of the Elgamal asymmetric cryptography algorithm, points out.

No security architectures? The world has spent hundreds of billions of dollars, conceivably a trillion dollars, on information security. That investment has produced no security architectures at all?



Noted cryptographer Taher Elgamal,
responding to the question,
“What's the biggest mistake
people are making with their
security architectures?"

"The biggest mistake is
that there are no
security architectures!"

According to the distinguished cryptographer Taher Elgamal, that is exactly the case.

The pervasive lack of security architectures is a consequence of the rampant inauthenticity we see all the time in information technology, combined with some worn out assumptions. If we examine those old assumptions we'll learn about architecture. Not computer technology, but architecture. The less you know about bloodletting, er, information security technology, the more prepared you will be to understand what we mean by architecture.

We'll build upon something we learned at Delphi: how to ensure that people are accountable for their actions while online, while at the same time ensuring that their privacy is protected.

Worn-Out Assumptions

Some would have you believe that we all must give up our privacy in order to have security. That is nonsense, propagated by organizations whose principal money-making balance sheet asset is your personal information – kind of like a respected museum that finds itself with stolen artworks in its inventory and doesn't want to give them back, and most definitely does not want to discuss its own role in the theft of the asset. These companies have a lot to lose. The information is not theirs to begin with, and nevertheless they fear losing it.

Another misguided assumption is that the tools to fix the problem must involve new technology. We will show that the answer to the question, “Why is the internet broken if the tools and materials to fix it are available and proven?” is precisely the same as the answer to a question asked by the inventors of steel and reinforced concrete in 1847.

We'll look at that answer, but first, let's take a closer look at why information security technology does not produce information security.

6

Why Is There No Security?

In his May 24, 2011, column in *InfoWorld*'s Security Central[3], security advisor Roger Grimes noted that

> In reality, hacking is easy once you know what you're doing. Defending is hard. If you want to truly impress the world, develop systems and applications that will be used by a lot of people while being resistant to easy hacking.
>
> **Hacking is all too easy**
>
> Hacking is as easy as 1-2-3: Locate target. Identify software and version. Research possible vulnerabilities. Attack. Compromise. In my nine years as a penetration tester, I broke into every company I was hired to test, all in one hour or less (apart from one project that took three hours). These targets included banks, hospitals, energy companies, media firms, and three-letter government agencies.
>
> I'm not even that good at hacking. On a scale 1 to 10, I'm probably a 5. When I worked at Foundstone and led an Ultimate Hacking class, I taught hundreds of students, in a matter of days, how to break into the average company with minimal effort.

A long chapter entitled "Our Disastrous Networks" in the first edition of this book cited lots of examples of the failure of our information infrastructures to provide elementary security. Things have gotten so much worse since then that the chapter is no longer needed. The plainly visible truth is that computers and networks have become intolerably vulnerable.

[3] http://www.infoworld.com/d/security/make-your-mark-stopping-hackers-920, May 24, 2011.

In spite of hundreds of billions, perhaps a trillion dollars, spent on information security by business and government, network security practically does not exist.

And still, getting people to believe that new acronyms will fix everything is sadly not a difficult sell. Like health and wealth, security falls into the "desperately desired" category that gets people to peddling miracle cures for dread diseases, video courses that will turn you into an overnight millionaire, software that will put snarling guard dogs at the entrance to your personal computer, and magic boxes that can tell just from their appearance which packets of information entering your organization's network were sent by bad guys.

And sadly, the people who make this stuff often believe it can work.

But it also dangerously distracts everyone from real solutions. It generates a class of believers who fail to question fundamental assumptions, and are unprepared for a fresh approach.

It Takes a Great Mind...

Until now I purposely neglected the title and subhead of the Roger Grimes *InfoWorld* column:

"Make Your Mark by Stopping Hackers

Anyone can hack a system, but it takes a great mind to build secure systems that can keep bad guys at bay."

Do better, general readership! Try harder! It's worthy of a coach's halftime pep talk in a game that the adversaries, the serious hackers, are decisively winning.

Stupendous irony: the inherent inconsistency in that title and subtitle sums up the information security situation brilliantly. It is absolutely true: anyone can hack a system, but *using existing assumptions about security*, it takes a great mind to build secure systems that can keep bad guys at bay. It's on that seemingly minor caveat, "using existing assumptions," that the whole thing turns.

As it happens, even an abundance of great minds will not solve the problem. Grimes puts forth his pantheon of the 22 greatest minds in information security (wisely including a disproportionate number of his fellow Microsoft employees): Dr. Daniel J. Bernstein, Theo de Raadt, Michael Howard, Kim Cameron, David LeBlanc, Crispin Cowin, Steve Lipner, Aaron Margosis, Robert Hensing, Dr. Niels Provos, Bruce Schneier, Lance Spitzner, Dr. Dorothy Denning, Ross Greenberg, Clifford Stoll, Paul Ferguson, Lenny Zeltser, Dr. Eric Cole, Jason Fossen, Ed Skoudis, Dr. Eugene Schultz, Stephen Northcutt.

If you look at the examples given of the kinds of software the great minds are wrapped up in, you'll note a pattern. It's all complex software developed for demanding environments to be sure, but it's also software that tends to deal with core services, removed from the messy business of applications.

To illustrate, let's pick on Theo de Raadt and his superb OpenBSD operating system. The OpenBSD kernel is indeed built like a steel ball. It's actually better than its reputation of having only two discovered vulnerabilities in the last decade, because those vulnerabilities were not in the kernel at all but rather in the part that's outside the kernel. That's the part that's closer to the applications, ie closer to the software that real people use in their daily work and play.

OpenBSD, and for that matter most of the software that those great minds produce, may be compared to the vaults and security systems at Fort Knox. It provides security in a setting that is most demanding.

But how many attacks does Fort Knox have to withstand, compared with the number of times people try to mess with cash registers, bank branches, ATMs, convenience store surveillance and alarm systems?

Security professionals sometimes refer to the "attack surface," meaning the total set of places that are exposed to potential attackers. The attack surface of Fort Knox is like a postage stamp compared to the thousands of acres covered by all the places in the economy where cash is gathered and dispensed, sensitive information is exposed, and children in social networks are vulnerable.

The software produced by the millions of application programmers working in the real world serves a role more like a bank branch, an ATM, or a cash register than a big-budget national vault. Fort Knox is surely a more exacting security setting, but that setting isn't exposed to millions of diverse interactions with millions of people every day, as are our bank, ATM, cash register – and applications software.

So let's recap.

- Hacking is easy once you know what you're doing.
- Defending is hard.
- The greatest minds are able to secure a subset of the software that has a much smaller attack surface than does application software.
- The vast preponderance of software that is directly exposed to masses of users, providing the biggest attack surface, is application software.

So either we must come up with an abundance of great minds to solve the problem, or we must come up with new assumptions about security.

The former is beyond unlikely; but building on a new set of assumptions will in fact solve most information security problems. As a bonus, building on those new assumptions with the new tools and methods will make our computers more useful and our lives easier.

Introducing the Solution

The first paragraph of the Grimes article serves as a perfect introduction to the enduring solution to our real-world security problems. The column starts out,

> I remember being excited when I was asked to use a sledgehammer to tear down a covered garage that wasn't approved by the city. It had been standing beside my girlfriend's house for years. You could tell it was built intelligently and with love. The supporting beams were twice as thick as required by code, and every nail and screw was driven straight. The lumber itself was top shelf, not a knot or bend in it.
>
> I have a hard time driving a nail straight -- yet it took me less than an hour to turn the structure into a crumpled pile of lumber. In the security world, something similar happens every day when hackers tear down whole networks and systems.

The fundamentally flawed set of assumptions about information systems comes from the same place as the notion of the Information Highway. A highway, physical or online, is an outdoor public transport system. The assumptions underlying our information systems are outdoor assumptions.

The answer lies in moving things indoors.

In the physical world we solved the outdoor problem with the concept of buildings. These indoor spaces are built using construction materials that meet building codes issued by public authority, designed by architects with licenses issued by public authority, built and inspected by contractors and building inspectors with licenses issued by public authority. Their resulting habitability is attested to by occupancy permits.

Buildings in the developed world tend to be reliable. While you use highways to get to them, the buildings are separate from the highways. Buildings provide indoor spaces that deliver what real estate lawyers call "quiet enjoyment."

The assumptions upon which highways are built, managed, and used are very different from the assumptions upon which buildings are built, managed, and used. If we build information facilities that are based upon indoor assumptions we will not only solve the security problem. As a bonus those facilities will be immensely more manageable and useful, in business, government, schools, other organizations, and homes.

7

You Know More Than The Experts

People who have been in any type of environment for a little while know too much for their own good. ***It boxes them in. They know what's not possible.***

David Marcus, who became president of PayPal in April 2012

Assumptions from the 1970s and '80s guided the fundamental design of our computers and networks. When applied in today's information environment, they are fatally flawed.

If you are not involved in information security then you probably do not have those assumptions. Your assumptions about security are better than those of the security experts.

Therefore, if you were to design an information infrastructure without consulting information security expertise, it would likely be more secure than the information infrastructures that are designed by security experts.

You Don't Believe Me, Do You?

That's understandable. It sounds preposterous.

But it is true.

Let me demonstrate that your assumptions make you better prepared to design a secure space than the security experts.

Picture a Space

Mentally picture a physical space for a branch office of a company. The space includes cubicles, a private office, a meeting room, some file cabinets, and a day-care facility for employees' children. Your mental picture is probably in an office building.

Now let's have some people from out of town visit the facility. Picture the process.

The visitors arrive by car, turning from the public roadway into the building's parking lot. They leave the car, leave the outdoor space, enter the building's lobby and approach the main reception desk, where the receptionist asks them to sign in, perhaps checks ID, and issues name tags. They are directed to the floor where the company has its offices. There, the visitors approach another receptionist, who greets them and politely asks who is expecting them. Perhaps they're there for a sales meeting, or perhaps they're state inspectors there to evaluate the day care facility. The appropriate employee is notified, and escorts the visitors to the proper location.

The design of the facility, then, is generally based upon common sense.

Something you probably left out of the picture in your mind is a framed document on some nondescript wall somewhere in the building: the occupancy permit. We'll give you credit for having it there because while no one thinks about it much, you probably know that an office building must have one.

The signature of a professionally licensed architect, contractor, and building inspector on that piece of paper or on the paperwork leading to its issuance is the assurance that the building is a habitable indoor space, fit for its intended purposes. If that turns out not to be – if the building starts to lean or develop cracks, or if undocumented secret passageways are discovered – then the individuals who signed the document stand to lose their professional licenses, their livelihoods, their reputations.

Picture the Space Again

Now let's look at how the facility for the same workgroup and its day care operation would be designed and built using existing assumptions and methods for non-physical facilities.

Picture a commando outpost with a razor wire perimeter constructed in a paved outdoor rest area alongside a busy highway. Instead of a reception desk, we see guards toting automatic weapons. On the backs of the guards' uniforms are stenciled the words FIREWALL, INTRUSION DETECTION, INTRUSION PREVENTION, DATA LOSS PREVENTION, SECURITY EVENT ANALYSIS, and MALWARE DETECTION. Inside the razor wire perimeter are markings on the pavement: painted yellow lines subdividing the outpost into rectangles marked "Collaboration Space," "User File Area," "Chroot Jail," and "Kids' Chat Room." The table and file cabinets and child care space are in their designated areas.

Everything is on the pavement, outdoors. There are no walls, only guards standing on the lines delimiting the spaces. Trucks and cars and their drivers come and go right alongside the office and child care area. Since it is an outdoor space, it of course does not carry an occupancy permit with signatures of licensed architect, contractor, and building inspector. After all, it's a commando outpost, architected not for individual accountability but for "security."

Every item in the whole space, including each and every document in each file folder in each drawer in each file cabinet has a label marked "-rwxr-xr-x" and "-rw-r--r–" and "-rwxrwxr—." These strange markings designate which members of which groups are allowed to do what with each document. Next to the labels are more guards.

Again, let's bring in the visitors. They arrive, parking their car in one of the spaces on the same pavement the facility is built upon. The visitors wear badges identifying their roles and the group they belong to, but not their names.

They approach the guards, who scrutinize them thoroughly, examining the contents of their briefcases, their appearance, the language they're speaking, every little detail. They peek into the visitors' car, checking out the GPS to see where they came from. The collected data about the visitors is fed into a powerful computer, which issues a judgment of the intentions and character of the visitors. They appear to be legit, so they're ushered past the razor wire.

Inside the Space

Once inside, the painted boundaries of this outdoor facility alongside the highway allow the visitors to enter any area whose permissions encoded in the -rwxr-xr-x and -rw-r--r and -rwxrwxr are appropriate to their badges. If a badge doesn't allow them to go where they want to go, they approach a person wearing a badge labeled "Administrator of -rwxr-xr-x and -rw-r--r— and -rwxrwxr — Services" and request a new badge.

The Administrator, having so many combinations and permutations of groups and privileges and protectable things to keep track of, is a very busy person, and so new badges are either fairly easily obtained or not obtainable at all. The truth of the matter is that the job description of the Administrator of -rwxr-xr-x and -rw-r--r — and -rwxrwxr — Services defines an impossibility.

Sounds crazy, right? No reasonable person would design a facility for a company's workgroup that way. Who would set up a meeting table, file cabinets, and day care facilities in an outdoor space alongside a busy highway? And who would set up access controls that way?

In every workplace, whoever is responsible for what goes on in a room also is responsible for managing and distributing the keys to the room; the operator of the key-cutting machine simply cuts the keys to the specifications. It's not about who is good and who is bad; it's about who is accountable for what. It's all common knowledge based upon common sense.

But when it comes to information facilities, we struggle to get our heads around the outdoor assumptions of the information technology industry. After all, they're the experts. They've been dealing with security challenges for years; they must know what they're doing, right?

History is replete with examples of professions that have gone off in strange directions as a consequence of flawed sets of assumptions that underlie “best practices.” For how many centuries physicians were draining blood from patients in an effort to remove “bad humors” while victims and their families assured themselves that “they must know what they’re doing.”

Let’s Turn Some Bad Guys Loose

Now let’s test the two facilities by turning loose two bunches of bad guys intent on doing harm.

The first group of bad guys looks the part, their seedy appearance giving them away to the armed guards in the outdoor version of the facility. One of the guards steps forward and prevents entry into the outdoor facility.

By contrast, no one prevents members of the first group from entering the building where the indoor version of the facility exists. In fact, their low-quality fake IDs are accepted by the building’s receptionist, allowing them to take the elevator right to the offices containing our indoor meeting room, filing cabinet, and child care facility.

There, the receptionist, politely pretending to ignore their rough appearance and demeanor, asks who is expecting them. “Some guy named Joe just told us to go ahead into the meeting room to get some files he left for us in the file cabinet, then play with his children in the child care area.” Dubious but still polite, the office receptionist checks the access control list for the meeting room and explains that there has apparently been some mistake.

Both the outdoor security guards and the receptionists will be effective in stopping this first group of bad guys, which is composed of would-be intruders who lack the skills, intelligence, energy, and resources to effectively disguise themselves and to carry convincing fake IDs.

Now let’s bring in a new set of predators, fraudsters, and thieves who have taken the trouble to look and act respectable, and carry high-quality fake IDs.

How do we defend the outdoor facility from this second bunch of intruders? Do we add more razor wire and more highly trained commandos toting more deadly automatic weapons? Kinda costly, and not at all effective. But in the indoor facility, this second group of bad guys will breeze right by the building receptionist. At the office suite reception desk, though, they’ll be greeted by the question: “Who is expecting you?” That is, “It’s not my business to judge intentions or character. It’s up to the person you’re visiting to know your business with us.” And of course those people are accountable for the actions of their guests while they’re in the office.

The information security technology we all depend upon is all about determining the intentions and character of the sender of a stream of bits. As with a commando outpost, the approach is to distinguish friend from enemy.

Do You Think That Is Possible?

We said that you know more than the experts, so let's test that claim. Do you think it is possible to determine the intentions and character of the sender of a stream of bits? If so, you must be an expert.

Because it is impossible to determine the intentions and character of the sender of a stream of bits. Therefore, security schemes that depend upon such a determination will fail.

And if it is possible in some cases and not in others, which would-be intruders are most likely to get through? The amateurs with limited skills and resources, or the highly-skilled attackers who know what they're doing and what they're looking for?

When information security technology does work, it tends to keep out the least threatening attackers, leaving the more professional thieves free to steal intellectual property, credit card numbers, money, internal relationships, confidential plans, identities.

Shouldn't it be the other way around?

The information facilities that we depend upon are merely extensions of what used to be called the information highway. That is, they are extensions of an outdoor public transport facility. A very good outdoor public transport facility to be sure, but no more suitable for our files, meetings, and kids than a paved rest area alongside a busy highway.

Information security built upon outdoor assumptions does not work in real-world environments.

How Did It Get That Way?

If we step back we can see that the problem that information security technology is trying to address, and failing to solve, is the same problem that buildings were invented to solve.

In addition to the obvious benefit of comfort, buildings exist to provide accountability. You want to know who is in the room with you and why they are there. Buildings make regular occupants and their visitors accountable for their actions.

Buildings exist to provide a space in which things get done, or in which to socialize or be entertained. By contrast, a commando outpost's function is to hold embattled territory. Just being there is its purpose. When we move our information facilities from commando outposts to indoors, things will be easier and more productive.

In the next chapter we'll see why in fact the design of information facilities is better left in the hands of laymen who rely upon their common sense understanding of how facilities work.

8

The Frog Test

Failure is simply the opportunity to begin again, this time more intelligently.

Henry Ford

Experiments performed in 1872 and 1875[4], and thankfully not since then, appear to show that if you drop a frog into hot water it will immediately jump out. But if you put a frog into a pot of cold water and then gradually heat it, the frog will sit there until it boils to death.

The boiling frog metaphor is often applied to information security. We frogs sit in the water as it gets hotter, doing nothing meaningful to mitigate the steadily worsening disaster that is the security of the world's information infrastructure.

The first edition of this book sounded the alarm and offered the solution: the Quiet Enjoyment Infrastructure.

The Quiet Enjoyment Infrastructure does indeed solve security problems, as well as problems of loss of privacy and loss of manageability. But QEI does not come in a shrink-wrapped package you can go out and buy. It's not a downloadable "thing." Rather, QEI is a new approach to designing and managing information infrastructures, thoroughly inspired by the way we build and manage buildings.

Before you can have a building you need construction materials that meet building codes, which of course means that you need building codes. You need architects and contractors and building inspectors who put their professional licenses and livelihoods and reputations on the line with each structure. And you need occupancy permits.

When you have an infrastructure that includes those elements, you can have secure and manageable and private online indoor spaces, shared with others. Until then, nothing you can purchase will make your computer or phone secure.

[4] William Sedgwick, *Studies From the Biological Laboratory*, by N. Murray, Baltimore, MD, Johns Hopkins University, 1888.

Hello?

My appearances on a series of talk shows to promote the first edition of this book evoked a bit of the boiling-frog syndrome. Before each show I would ask the producer to let the host know that a particular question would inevitably arise:

"Wes, can you tell our listeners what they can buy to make their computers secure?"

...and that the only answer I would be able to offer would be,

"There is nothing your listeners can buy or download that will make their computers secure."

...and so I suggested that the host avoid asking the question.

In spite of that conversation, almost every host would ask at some point,

"Wes, can you tell our listeners what they can buy to make their computers secure?"

Perhaps it's understandable that seven years ago people were skeptical when I suggested that information security technology was built upon flawed assumptions; that frankly, it was not working. Back then, Bill Gates was promising the imminent end of spam, and with it, spam-borne malware. No one had heard about botnets, so when I spoke and wrote about them, it didn't ring a bell with anyone. Certainly no one suspected that the security protecting their information would get steadily worse. Surely, went the general assumption, the computer companies would make steady progress against the threats to their technology.

About two-thirds of the way through that promotional campaign it occurred to me that if people were not yet ready to hear me say that no software would make their computers secure, then they certainly weren't ready to spend weeks reading my 500-page tome on online security. I stopped promoting the book and went back to work to turn my ideas into working systems.

Two things have happened since then.

First, it's become clear that the computer and software makers are not going to be able to fulfill their promise of making information infrastructures secure. Things have only gotten worse. Just pick up today's newspaper, or read any information security newswire, for stories of routine disasters.

Second, the Quiet Enjoyment Infrastructure has become more than an ideal. We have made considerable progress in making it into practical reality.

Seven years may seem a long time, but this infrastructure is very much like the internet itself. It doesn't fit into a box. You can't go out and buy it and install it in your computer. As the internet was a collaborative effort among the groups that would use it, so is our Quiet Enjoyment Infrastructure.

Security technologists, meanwhile, have kept their own hope alive. Information security technology has in fact improved. Malware profiling techniques, firewall rule sets, and intrusion detection/prevention technology have gotten much better.

But the technology used by the intruders has gotten better, too.

Existing Systems Favor Advances Made by the Intruders

Here's the thing: The fundamental architecture of our information systems strongly favors advances in the intruders' technology over advances in security technology.

Let's use a sports analogy to compare the efforts to intrude and efforts to prevent intrusion. Professional athletes' salaries are proportional to their ability to contribute to success, Carl Crawford notwithstanding. So let's take a great big leap and allege that an effort to intrude, and an effort to prevent intrusion, are both quantifiable functions of (money spent + skills applied + attention paid). After all, such quantification of effort is precisely what is expected of security managers at budget time.

This book will demonstrate that information infrastructures are built upon one of two models, which we will call the outdoor model and the indoor model. As long as we use the outdoor commando outpost model of security, owners of a resource will have to increase their security efforts fourfold to match a doubling of efforts by intruders. That is, in an "outdoor" infrastructure, **an effort to intrude is equal in effectiveness to the square of an effort to prevent intrusion**. I'll call it Kussmaul's theory of outdoor security.

Its corollary is Kussmaul's theory of indoor security, where an information facility is built upon indoor assumptions. In an indoor facility, **an effort to prevent intrusion is equal in effectiveness to the square of an effort to intrude**.

Both the outdoor and indoor theories are based solely on personal anecdotal observation; the complete proof will involve gathering data points to test them. But the thought model in Chapter 4 as well as anecdotal information, as found in the standard security vendor white paper such as the following Splunk App for Enterprise Security[5] [6], will help you judge whether they reflect reality.

They start with a common refrain: Information security is getting more difficult to achieve even as the intruders get more efficient.

[5] "Saying It's Disbanding, Hacker Group Urges New Cyberattacks," *The New York Times*, June 27, 2011.

[6] *Splunk App for Enterprise Security*, Copyright © 2012 Splunk Inc. All rights reserved. Splunk is a registered trademark or trademark of Splunk Inc. in the United States and/or other jurisdictions.

> **The Challenges of Providing Security Intelligence**
>
> There is a widening asymmetry between the mindset and methodology of the attacker and the security professional and their detection tool set. Current tools have the security team monitoring a more mobile workforce and in constant cleanup mode reacting to infected hosts. Attackers have the time, expertise and resources to create attack scenarios that bypass detection by security point products and downstream security and event management (SIEM) systems hiding their activities in the terabytes of data generated through normal user activities. Though small in number, these highly targeted attacks can take place over years siphoning off the most sensitive and highly valued enterprise data. The same can be said of individuals bent on crimes of fraud, abuse or corruption. Both the persistent attacker and the 'criminal-on-the-inside' can be classified as unknown threats. These criminals have realized that many security teams can't see their attacks in the context of operations data due to organizational data silos, data collection issues, scalability challenges or a lack of analytics capabilities.
>
> Monitoring for known threats as reported by traditional security systems and unknown threats are now part of a revised security charter. How does the security team meet this new challenge? What enterprise solution can meet the goal of providing security Intelligence aligned with business risk?

Standard security white paper language gets initial buy-in by touching the known pain button: Making information systems secure gets harder and harder while the intruders find it easier and easier to defeat the efforts of the security engineers. The situation looks desperate.

One can imagine the same PR agency writing pain-button copy for an audience of overweight people, or people with financial problems, or people with a persistent health problem. These white papers offer the same answer for any seeker of a miracle: Buy our miracle product and your pain will disappear.

> **The Splunk App for Enterprise Security**
>
> The Splunk App for Enterprise Security has been created to take full advantage of all of the Splunk Enterprise platform's big-data analytics

> and visualization capabilities. In addition, it provides key functionality supporting the search for and processing of 'known' and 'unknown threats.' Equally suitable for a small security team or an enterprise security operations center, the App is the primary data interface for the security professional faced with a growing list of challenges.

When that doesn't work, there's always another white paper offering another miracle cure. Irrational hope is a reliably persistent money-maker.

Are we doing the same thing, promising a solution to the problem of deteriorating information security?

Well, yes. But our solution, the Quiet Enjoyment Infrastructure, is no quick plug-in miracle cure. It asks you to think about how surprisingly similar problems have been solved in the world of physical spaces, and to step back, think, and not expect an easy solution. This will take time.

But it will solve the problems.

Why This Is Important

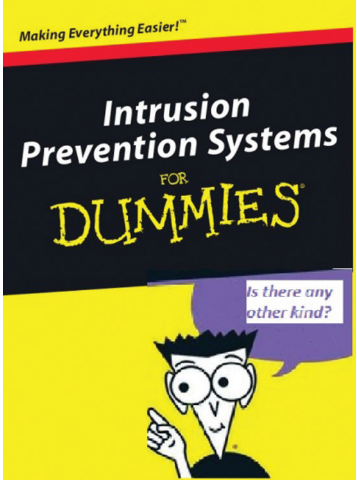
The introductory chapter in the first edition of this book included a set of warnings about the vulnerability of financial information, children in social networks (then called chat rooms and bulletin boards), identity information, critical infrastructure, and privacy. It went on to warn about a likely convergence of botnets that I called Arpanet II.

The original Arpanet of the 70s was an attempt by the U.S. Department of Defense to build a resilient network that could operate even if an enemy succeeded in taking out a large number of its servers. Arpanet II, now renamed Arpanet III, will provide such a network for its sponsors.

One of our videos described how Arpanet II will resemble the development of monarchy in the earliest history of civilization. The first kings got their crowns by being the smartest leaders of the toughest gang of thugs in the countryside, squeezing out the other gangs in the protection rackets where farmers handed over geese and pigs and sons in order to be (temporarily) left alone.

Back then of course there was this limiting condition called "turf." Arpanet III knows nothing about physical turf. It's actually easier to extract tribute from a Minnesota computer user if you're in Nigeria or Estonia than in Minnesota. Troublesome things like laws and jurisdictions and all that, you know.

Stepping back means stepping back all the way. The laws of nations grow steadily more meaningless against criminals who understand that the internet does not respect geographic boundaries and legal jurisdictions. The solution must be global, not national. It cannot come from legislatures. The shrinking of the planet will continue whether we like it or not, so there's no sense demonstrating in the streets against globalization. The challenge is to find a way to make globalization work in favor of security and privacy, rather than against them.



The Size of the Solution

In fact, these apparently contradictory goals — globalization, plus security and privacy — can be achieved. There is a way to make the effect of globalization as constructive to personal security and privacy and individual well-being as it has been constructive to big business. And, fortunately, this new approach does not require that people and nations suddenly embrace and enforce international law with new enthusiasm, which of course people and nations are unwilling to do (often with good reason).

The problem is not the internet itself. The internet does its job well. The foundation of the solution to our problem is not to transform the internet but to build facilities on top of it, and to move our important activities into those facilities. Really, it's nothing more than recognizing that the outdoor space in rest stops along the information highway is no place in which to conduct business. It's time to move indoors.

The solution to a problem this big must itself be big.

The new-economy people have come up with a term for a big change. People who use charts to measure how things change call it an "inflection point." But this is different. It is too big even to be called an inflection point. We — all of us — are at a point of decision. Either we will quickly deploy the elements that will bring about a dramatic reduction in terror, contain rapidly proliferating crimes and general online anarchy, and markedly improve the general quality of life, or we are headed for another Dark Age.

So, where do you sit on the frog scale? Do you believe that the purveyors of security technology will gain the upper hand, that improvements in their methods will come faster than the improvements in the methods used by the intruders? If so, you needn't read further.

9

Meet The New Boss

Meet the new boss / Same as the old boss

The Who, “Won’t Get Fooled Again”

Writers about security often cite the transition of the cracker/hacker community from pranksters to money-motivated thieves. That’s accurate, but it omits an important detail. Those who break into networks and develop and distribute malware are driven by a number of motives: pranking, proving their prowess, stealing money. But there’s also a fourth motivator that has received too little attention.

If you’re involved in gaming, particularly multiplayer online games, you know all about this motivator. Even if you’re not, you know about it from history class.

The verb “to pwn” means roughly the same as “to own,” and is often misquoted as the latter by those who believe that a word should have at least one vowel. Pwning someone is exerting control over them. Avid online multiplayer gamers seek to pwn their opponents, and the most megalomaniacal of them seek to pwn as many other gamers as possible. Pwning the gaming network itself, say perhaps the Sony Playstation network, is a triumph of the first order.

In fact, the desire to pwn is older than civilization itself.

A Very Short History of the World

Once upon a time, smart people learned that living in houses and raising food on farms was better than living in caves and eating whatever you could find that looked like food.

Some, however, never got the hang of farming. Instead, they joined with other non-farmers in gangs that offered to protect the farmer if he handed over a couple of geese and pigs.

“Protect from whom?” asked the farmer.

“From me, of course,” said the leader of the gang as he carried off the livestock.

The farmers could put up with one gang of thugs, but with many competing gangs, each demanding more geese and pigs, life became very difficult.

Then the smartest leader of the toughest gang came up with a solution. “I’ll protect you not only from myself but also from the other gangs. Just hand over geese, pigs, a few goats, and a son to join my protection enterprise. And toss in that shiny trinket so I can add it to this fancy thing I want to wear on my head. And oh yes, refer to me as ‘highness.’ ”

And so the toughest and smartest gang leader became king.

If he had been even smarter, he would have filed a business method patent on his invention, which came to be known as the protection racket.

The earliest monarchs pwned their subjects. They exerted total control.

Stories of the pursuit of conquest at great cost, stories of intrigue, treachery, fratricide, matricide, and patricide in royal families over the next few thousand years show just how strong is the desire to dominate others, to pwn them. When domination of large populations appears to be a possibility, that little psychopath on an egotist’s shoulder becomes energized.

Making pwnership of others even more appealing is the fact that it is usually accompanied by wealth. In gaming circles, that wealth takes the form of digital objects, virtual swords and grails. In the great game of conquest of servers and personal computers in the non-virtual world, the accumulated wealth takes a more material form, typically U.S. dollars.

However, those dollars are not as fungible as the ones in your wallet. Before they can be used, they must be skillfully laundered by enlisting the help of innocent housewives responding to work-at-home schemes. The more dollars sent to be laundered, the more conspicuous the laundry.

To really liberate that cash, the other reward, power, must be accumulated as well. Really, one who sets out to satisfy one of the hacker motives on a really large scale must in fact satisfy them all. Power, wealth, and the admiration of peers for having masterfully pulled off a global prank — you’ll need them all if you are to truly have any of them.

The King of the World’s Information Infrastructure

To keep our world history short, let’s fast forward a few millennia. The Arpanet, the precursor of the internet, was designed in the 1970s largely by my customer, Bolt Beranek & Newman Inc., for the Advanced Research Projects Agency of the U.S. Defense Department. Arpanet was to be a network that would continue to function even after a significant number of nodes was disabled, presumably by an enemy[7].

In the first edition of this book we identified a nefarious worldwide network-in-the-works, a network of botnets, being assembled by parties unknown. They were injecting malware of increasingly advanced design into conscripted home

[7] A disproven myth held that the Arpanet was designed to withstand the attack of an enemy using nuclear weapons, e.g., the Soviet Union. In reality the enemy’s name is Murphy.

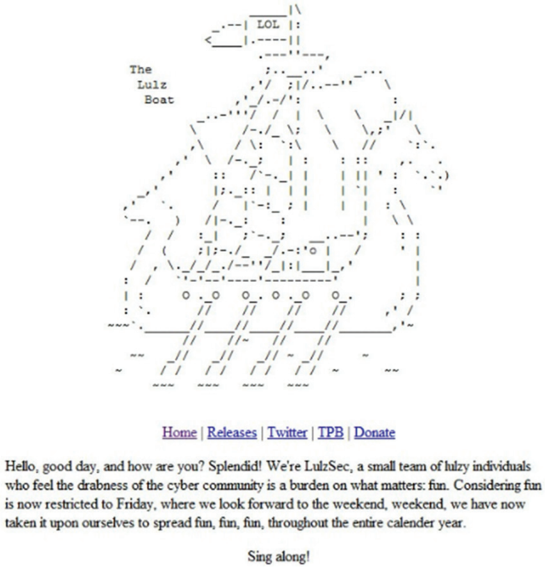
computers. Since it's designed to survive attempts of its enemies to shut it down, we named the new network Arpanet III.

The enemy of Arpanet III is you and me and everyone else who would like to have a reliable global information infrastructure.

Have the prankster hackers set their sights on domination of the world's information infrastructure? Who knows.

But human nature says that eventually they certainly will.

Where Are You off to, LulzSec?



Home | Releases | Twitter | TPB | Donate

Hello, good day, and how are you? Splendid! We're LulzSec, a small team of lulzy individuals who feel the drabness of the cyber community is a burden on what matters: fun. Considering fun is now restricted to Friday, where we look forward to the weekend, weekend, we have now taken it upon ourselves to spread fun, fun, fun, throughout the entire calender year.

Sing along!

For the time being, the pranker networks Anonymous, the "disbanded" Lulz Security, TeaMp0isoN, and others seem to be unconnected to the botnets, whose modi operandi are all about cultivating fields of personal file systems, harvesting credit card numbers, names, and national ID numbers, and selling those crops at auction.

When will the smartest botnet builder or prankster take advantage of the obvious synergy between the two pwnification strategies?

My guess is that has already happened.

After a spectacular run of intrusions against major institutions, Lulz Security announced that it was disbanding on June 26, 2011.

What does it mean when an amorphous group of unidentified individuals "disbands"? The efforts of journalists and law enforcement to impute form and structure to such blobs resembles earlier efforts with crime "families." There are groups and there are bosses, and eventually one boss becomes more powerful than the other bosses. But it's not as though they have articles of organization and boards of directors or trustees and stockholders. There are no stock certificates or membership cards. The lack of formal structure, it seems, is difficult for analysts who relentlessly and futilely try to draw org charts of criminal organizations.

Indeed, the "disbanding" of LulzSec was accompanied by its anonymous leadership's call to carry on with the "revolution." Asked about the development, Dino A. Dai Zovi, a prominent security consultant, noted that, "It looks like these sorts of 'hacktivist' ideas are spreading and gaining popularity."[8]

[8] "Saying It's Disbanding, Hacker Group Urges New Cyberattacks," *The New York Times*, June 27, 2011.

In an effort that is probably independent of the various botnets, the Sony Playstation network was hacked. After a humiliating week's outage, Sony allowed it to re-open, only to be hacked again. Sony was compelled to advise its vast global network of gamers that their personal information had been compromised, with possible financial consequences to each of them. More hacks followed.

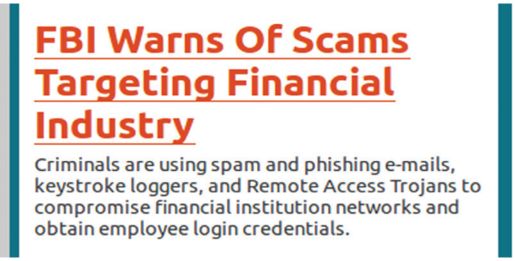
Sony Corporation's stockholders can take comfort that their company has merely been pwned, not owned. At least for the moment.

A little conjecture here will give you an opportunity to judge my attempt at prophecy, for things will keep unfolding in the rapidly developing Arpanet III.

Some aspiring and savvy lieutenants in either the botnet or hacktivist world are right now sizing up their prospects for a "promotion." Surely there are power struggles and coups being planned and executed.

Hacktivists will scoff at this notion. "You completely miss the point, d00d. We're in it to have fun while we shake up things that need to be shaken up."

Nature, Power, and Vacuums



FBI Warns Of Scams Targeting Financial Industry

Criminals are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans to compromise financial institution networks and obtain employee login credentials.

In other words, they're out to shake up power structures, creating power vacuums. And we all know how nature feels about a vacuum.

Most of us also understand that there's at least one latent power-hungry misanthrope in any gathering of more than a few dozen people, their tendencies becoming overt when opportunity arises. The opportunity becomes most prominent in groups whose governance is by the rules of the jungle, as with hactivists, botnet builders, and organized crime families.

Put a number of such groups-in-formation together and you have a perfect Petri dish for the smartest leader of the toughest gang of thugs to take charge of the formation of Arpanet III. His or her, no his, first goal will probably be to pwn and own a few small banks in Third World countries. We know that national governments — and by extension their bank regulators — vary greatly in their attitudes toward cybercrime. It seems that some view phishing attacks and online theft as a growth industry, a boost to the balance of payments. With half a dozen small banks in those countries in their pocket, money laundering would be a much less formidable job for our would-be leader of Arpanet III.

Quickly after that, while the scattered patchwork of law enforcement agencies in the 200+ nations of the world tries to figure out how to isolate transactions involving those institutions, other banks and other organizations and companies will be pwned and owned.

Suddenly the most difficult job of the serious cybercriminal, that is, rendering his plunder usable, becomes much, much easier. After all, with undisclosed ownership of banking facilities, he's got control of nodes on the world's financial transaction network.

Easier money laundering will in turn enable more effective theft, generating more easily-laundered cash, with which some more reputable institutions could be controlled, much in the manner of mafia bust-out schemes of reputable companies in the 20th century. At some point a full-blown bust-out of some richly capitalized institution, such as the one perpetrated in 1991 against Mutual Benefit Life Insurance Company, will be pulled off.

At that point the assets available to the boss of Arpanet III will rival those of some sovereign nations. Certainly they will be sufficient to buy up stock of companies that sell security technology products, or otherwise infiltrate them.

And perhaps just for old time's sake he'll take an interest in the devalued shares of Sony Corporation.

Meet the New Boss

That's when the boss of Arpanet III becomes king of the world's information infrastructure. When that happens you will not be able to communicate with anyone in a way that is not discoverable by the big boss, except in face-to-face meetings in the physical outdoors. We'll then all reminisce about similar scenarios in novels we all were assigned to read in middle school.

The designers and builders of Arpanet III continue to show their skill. We have botnets with millions of personal computers acting as zombie nodes; we also have rampant breaches of the networks and servers of Citibank, Lockheed Martin, and others. What happens when the smartest, most megalomaniacal leader of the most aggressive bunch of hackers in the botnet/Anonymous/LulzSec/ TeaMp0isoN/ phishing/SQLinjection/online-human-trafficking community decides that he wants to control the world's information infrastructure? Could that be pulled off today?

The first one to have a go at it is likely to come up short. After all, it's an ambitious goal. But it will surely inspire others. Before there was a Lenin there had to be a Trotsky. Major power grabs seem to start with a pattern set by a visionary whose work gets co-opted by a series of progressively more vicious psychopathic megalomaniacs. Trotsky → Lenin → Stalin; von Bismarck → von Hindenburg → Ludendorff → Lenk → Hitler.

How many more attempts will be required before one of these psychopaths actually succeeds? Will there be massive casualties from wars of succession?

Stay tuned.

As long as we're all outdoors, keeping our files, holding our meetings, and letting our kids hang out outdoors in cardboard boxes by the side of the information highway, we're fair game for the gangs of thugs and their ambitious leaders. This time they won't ask us to hand over geese and pigs. If we're lucky they'll just demand money to allow us to continue to use information and communication.

Or Will It Be the PRISM Boss?

Edward Snowden famously revealed details about the U.S. National Security Agency's PRISM, its surveillance of all the world's communications. Never mind the fact that *Wired* magazine had done a story[9] about the whole PRISM program a year earlier.

Which is scarier: governments taking control of all our communications or a global mafia extorting money and obedience from all of us in its protection racket? At least Arpanet III will (perhaps) never have armies and missiles and police forces with arrest powers and missile-equipped drones and all those things that make pervasive government surveillance more threatening.

PRISM attempts to intercept all communication, not just that which happens to traverse optical fiber and wires that cross U.S. borders. But it's still a U.S. Government initiative. Of the 206 sovereign nations of the world, how many have their own PRISMs? Certainly Russia has one, and the UK's version is apparently very closely tied in to that of the USA. While the EU government was busy crafting its indignant response to revelations of PRISM snooping into the private communications of Europeans, *Le Monde* rained on their parade by reporting[10] that France's Directorate-General for External Security has been illegally intercepting e-mails, texts, phone calls, and Web activity in a manner very similar to PRISM.

Older functions of government tend to deal with the one thing that has historically made government relevant. That thing is territory. Turf. The space inside geographic boundaries.

Geographic territory is utterly irrelevant to a stream of packets on the internet. Bits know nothing about national boundaries. The obvious implication is that governance of information and communication on the one hand, and governance of territory on the other, are largely incompatible.

Governments simply don't know what to do about that. They create multinational super-PRISMs, while at the same time they build national citizen identity systems, oblivious to the fact that the people using the networks to be protected are very likely to be outside their jurisdiction.

Third Possible Boss: Silibandia

Governments and global organized crime aren't the only ones who want to control the world's information and communications infrastructure. We'll call the third contender "Silibandia," for the confluence of Silicon Valley, the broadband+wireless industry, and the media industry.

[9] "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," James Bamford, *Wired*, March 2012.

[10] "Révélations sur le Big Brother Français," *Le Monde*, July 5, 2013.

What makes Silibandia scary is its ability to control perceptions. Silibandia can get you and me to believe what they want us to believe, aided greatly by the tendency of you and me to believe we're too smart to be have our perceptions manipulated. Among other fairy tales, they have us believing that PRISM is Evil Big Brother Right On Our Doorstep, while their own much more powerful data-mining tools merely serve to offer us products and services in which we've shown interest. All their little manipulations of perceptions work to serve the big manipulation, the Big Lie, the message that Silibandia is your friend. As their friend, they would like you to support them as they work to limit the unwarranted and invasive schemes of governments — you know, those bad PRISM guys — to interfere with their earnest work to provide you what you need, while at the same time providing jobs and boosting the economy. "We're committed to 'do no evil.' Please 'like' us on Facebook." And please don't ask about what happens behind the scenes when you do that. You are getting drowsy… sleep… sleep…

Can't We All Get Along?

We all know that big industries such as Silibandia tend to have their way with legislatures, and that too many laws are made by lobbyists. Industry and government "work closely together in the spirit of cooperation in ensuring that [insert name of industry] continues to contribute to [insert some good thing], creating new jobs and new opportunities yadayada…" Translation: We bought your senator.

But the collusion at the centers of power isn't just between industry and government. History is replete with stories of governments cooperating with that first group, organized crime. While the story of James Whitey Bulger's cozy relationship with the FBI is fresh on peoples' minds, it shouldn't shock people as much as it appears to. From the intrigues of European governments and monarchies to the American police forces described in *The Autobiography of Lincoln Steffens*, the Venn circles of government and organized crime often significantly overlap.

Example: For centuries, the dynasty of Thurn und Taxis gathered wealth and power largely through its operation of the European postal system. Most communication, whether between governments or individuals, organized crime bosses or business people, leaders of Protestants or Catholics, was monitored by the Thurn und Taxis version of PRISM. Theirs involved the twin technologies of managing a (handwritten) database of who was communicating with whom, and the technology of discerning the contents of private correspondence in an undetectable fashion, by holding letters up to the sunlight and, when that failed, steaming envelopes and melting seals. To the princes of Thurn und Taxis, distinctions between government and media and business and criminal activity was a source of amusement. Those were all random labels for various instances of one unified thing called power. And the real power was theirs. Europe was largely owned by the House of Thurn und Taxis.

Conspiracy theorists, I have news for you: Collusion between government and organized crime is not news. It's been going on since, well, since "government" meant the smartest leader of the toughest gang of thugs in the countryside.

So let's not argue over whether government or the technology industries or the new global organized crime pose the biggest threat to our freedom and autonomy and survival. Probably one of the three will play a bigger role than the other two, but who knows which one or how it will all play out. We used to call it "the establishment." The bottom line is that if we don't do something to engineer a solution to this aggregation of information and communication power — all power these days — well, we're all back in the role of peasants, living at the mercy of the smartest leader of the toughest band of thugs in the countryside. Be prepared to hand over your geese and pigs and sons and daughters and any digital gold or jewels you might happen to have accumulated. Most of your dollars or pounds or yen or euros or bitcoins exist on some disk drive whose location is unknown to you, right? If we don't fix this problem with an engineered solution, prepare to yield them to the new despot. Who knows, he may be a robot.

Engineered Authority

The last big attempt at engineered authority was led by Hamilton, Madison, Jay, Adams, Franklin, Jefferson, Washington, et al and was remarkably productive. Building upon and refining the mostly English principle of due process, it made for an effective means of applying authority where needed, while keeping the bearers of that authority from letting power do what unchecked power does to people.

Now we need an engineered source of authority that fits communities that are not defined by geography. The new engineered means of governance will reach the old and elusive goal of direct participation by the governed, without intermediaries. It will allow people to participate directly in governance from the comfort of their homes. And it can be greatly more accountable and participatory than that provided for in the Federalist Papers and its descendant, the United States Constitution.

Our goal is to allow any member of a community to participate in its governance, provided they are measurably active in that governance. And with the tools of QEI we can have just that.

One caveat, however: While QEI delivers accountable anonymity to everyone, serving a role in public governance requires partially piercing the veil of anonymity. To serve, you'll need to disclose your natural name. Not your location or other identifying information, but as a public official your natural name must be disclosed along with the name of the office(s) in which you serve.

Come Indoors

Our solution is an impervious, secure worldwide infrastructure assembled through the use of open and consensual processes inspired by those developed over centuries by the real estate, vital records, and professional licensing professions.

It all starts with a process of establishing the identity of users of online facilities, while at the same time keeping those identities confidential. Accountable anonymity. It can be done. Stay tuned.

Our goal is not just better networks. It is not even a world that is better protected from terrorist threats. The goal is a world of “Quiet Enjoyment,” a world that offers a better quality of life for all people.

That kind of assertion risks being labeled as Utopian. But really, things don’t have to be as bad as they are now, and they certainly don’t have to get worse. We needn’t be so openly vulnerable. The foundation of the solution is right in our hands. When we deploy it widely, it will help us achieve rampant Quiet Enjoyment.

A new industry is in the works.

The new industry will thoroughly resemble the real estate industry: the design, construction, and management of commercial and residential buildings.

Security and manageability go hand in hand. You can’t have one without the other.

10

Another New Boss?

Will humanity be replaced by unhuman intelligence?

Elon Musk has said that artificial intelligence is one of the most pressing threats to the survival of the human race. "AI is the rare case where I think we need to be proactive in regulation instead of reactive. Because I think by the time we are reactive in AI regulation, it'll be too late. AI is a fundamental risk to the existence of human civilization."

Then there are Stephen Hawking's thoughts on the subject: "I fear that AI may replace humans altogether," he told *Wired* magazine. "If people design computer viruses, someone will design AI that improves and replicates itself. This will be a new form of life that outperforms humans. The development of full artificial intelligence could spell the end of the human race."

Another notable, Bill Joy, has the kind of résumé that would get the attention of Benjamin Franklin's headhunter. Cofounder and, until early 2004, Chief Scientist of Sun Microsystems, Co-chair of the Presidential Commission on the Future of IT Research, coauthor of the Java language specification, and creator of the Jini pervasive computing technology, Joy is a renowned thinker about the effects of technology upon people and a very practical and successful person. I mention all this so that you'll keep in mind that the following notions do not come from some space shot.

In April of 2000 *Wired* magazine published a much-noted article by Bill Joy entitled, "Why The Future Doesn't Need Us." The subhead to the article warned, "Our most powerful 21st century technologies – robotics, genetic engineering, and nanotech – are threatening to make humans an endangered species."[11]

The article made a big impact because of its very scary premise: there may be no place for our species in a future that is dominated by our creations. Most notable of those creations will be something called an "assembler," a device that springs from the intersection of nanotechnology, biotechnology, and information technology. The article cited other works with similar messages. All of them reflect

[11] *Wired*, April 2000.

an understanding that if we create things that have the *capacity* to rule us, then we will *let* them rule us.

Could that happen?

Nobody has come up with a good argument to suggest that it can't.

Then again, it implies that human beings will voluntarily hand over their prerogatives to their creations. What sort of mentality accepts such an inevitability?

In fact, that mentality is commonplace among Internet technologists. It comes from an assumption underlying the writings of Joy and others that must be challenged. It's the fundamental assumption of something I call the *open Internet mindset*.

The assumption goes like this: since the information highway is essential to the deployment of new developments, and is the essential information and communication medium of the future, and since activity on that highway is ungovernable, then everything to which the highway connects is beyond the reach of governance.

That assumption is wholly without basis. The Internet is governable, as any highway is governable. Standards bodies decide what top-level domains and transport protocols may be used, just as the highway departments of municipalities, provinces and nations decide upon traffic signals, signage, and vehicle registration standards. As long as you are not carrying hazardous cargo, it is not the highway department's business what you use the highway for.

But obviously, governments *do* care if you are using a highway to transport illegal drugs. The highway department or the department of motor vehicles may not care but the law enforcement branches of government care very much and will make it their business to stop you.

And other authorities concern themselves with stopping non-criminal activities. If the highway takes you to a meeting where you are about to disclose company secrets to a competitor, the highway department will not care nor will the statutory government; but those who govern your company will care a lot. They will take steps to prevent the trip if they know about it. If necessary, they will appeal to judicial authorities (i.e., the statutory government) to issue an injunction to prevent the trip.

The highway system called the Internet is indeed open; it is owned by no one – just as the world's physical highway system is owned by no one. Even if you own equipment and communication lines that transport Internet traffic, you do not own equity in the Internet any more than ownership of the roadways in your office park gives you ownership interest in the world's system of highways.

Given the usefulness of the highway metaphor, let's consider a couple of things about the way highways work:

- The openness of the highway does not in the least change our right to govern activity that may involve that highway
- The openness of the highway does not prevent our using it for transport to spaces that are not so open

- The governance of those not-so-open spaces and the governance of activity that takes place on and off highways is not the business of the highway department, except as it affects the operation of the highway itself.

Many companies have their own networks that are built on top of the public Internet but at the same time are apart from it. The information and communication spaces they provide are not open to the rest of the Internet. Those networks are obviously owned by the companies that built them. They are bounded spaces – buildings, if you will – that are used for private communication among employees, suppliers, distributors, and whomever else the company invites in.

Such bounded, manageable networks are not now provided to affinity groups among Internet users. Instead, the Internet offers "communities" that present themselves as gathering points for people with common interests. But such spaces are no more bounded than the Internet itself – offering, in effect, roadside hangouts where anyone with time on their hands may drop in, hang out with others, and adopt any identity that suits their fancy. Is it any wonder that people are reluctant to communicate anything of substance in those spaces?

We will go into more detail about the construction of bounded spaces in Parts 3 and 4.

Mere Jelly

As Bill Joy sounds the alarm about our creations taking over, a truly scary book by Hans Moravec openly celebrates the possibility.[12] Moravec believes that if we manage to get all the information from a person's central nervous system into software and files, then the software and files are a complete substitute for the person. What is left behind is a useless carcass or, in Moravec's truly memorable expression, "mere jelly."

Moravec is a leading researcher in the field of robotics. But his vision of robots of the future is far removed from the quaint R2D2 kind of image most of us associate with robots:

> Some of us humans have quite egocentric world views. We anticipate the discovery, within our lifetimes, of methods to extend human life, and we look forward to a few eons of exploring the universe. The thought of being grandly upstaged by our artificial progeny is disappointing. Long life loses much of its point if we are fated to spend it staring stupidly at our ultra-intelligent machines as they try to describe their ever more spectacular discoveries in baby-talk that we can understand. We want to

[12] Hans Moravec, *Mind Children* (Cambridge: Harvard University Press, 1988).

become full, unfettered players in this new superintelligent game. What are the possibilities for doing that?

Genetic engineering may seem an easy option. Successive generations of human beings could be designed by mathematics, computer simulations, and experimentation, like airplanes, computers, and robots are now. They could have better brains and improved metabolisms that would allow them to live comfortably in space. But, presumably, they would still be made of protein, and their brains would be made of neurons. Away from earth, protein is not an ideal material. It is stable only in a narrow temperature and pressure range, is very sensitive to radiation, and rules out many construction techniques and components. And it is unlikely that neurons, which can now switch less than a thousand times per second, will ever be boosted to the billions-per-second speed of even today's computer components. Before long, conventional technologies, miniaturized down to the atomic scale, and biotechnology, its molecular interactions understood in detailed mechanical terms, will have merged into a seamless array of techniques encompassing all materials, sizes, and complexities. Robots will then be made of a mix of fabulous substances, including, where appropriate, living biological materials. At that time a genetically engineered superhuman would be just a second-rate kind of robot, designed under the handicap that its construction can only be by DNA-guided protein synthesis. Only in the eyes of human chauvinists would it have an advantage – because it retains more of the original human limitations than other roots.

Robots, first or second rate, leave our question unanswered. Is there any chance that we – you and I, personally – can fully share in the magical world to come? This would call for a process that endows an individual with all the advantages of the machines, without loss of personal identity. Many people today are alive because of a growing arsenal of artificial organs and other body parts. In time, especially as robotic techniques improve, such replacement parts will be better than any originals. So what about replacing everything, that is, transplanting a human brain into a specially designed robot body? Unfortunately, while this solution might overcome most of our physical limitations, it would leave untouched our biggest handicap, the limited and fixed intelligence of the human brain. This transplant scenario gets our brain out of our body. Is there a way to get our mind out of our brain?

You've just been wheeled into the operating room. A robot brain surgeon is in attendance. By your side is a computer waiting to become a human equivalent, lacking only a program to run. Your skull, but not your brain, is anaesthetized. You are fully conscious. The robot surgeon opens your brain case and places a hand on the brain's surface. This

> *unusual hand bristles with microscopic machinery, and a cable connects it to the mobile computer at your side. Instruments in the hand scan the first few millimeters of brain surface. High-resolution magnetic resonance measurements build a three-dimensional chemical map, while arrays of magnetic and electric antennas collect signals that are rapidly unraveled to reveal, moment to moment, the pulses flashing among the neurons . . .*
>
> *. . . to further assure you of the simulation's correctness, you are given a pushbutton that allows you to momentarily "test drive" the simulation, to compare it with the functioning of the original tissue . . .*
>
> *. . . As soon as you are satisfied, the simulation connection is established permanently. The brain tissue is now impotent – it receives inputs and reacts as before but its output is ignored. Microscopic manipulators on the hand's surface excise the cells in this superfluous tissue and pass them to an aspirator, where they are drawn away.*
>
> *The surgeon's hand sinks a fraction of a millimeter deeper into your brain, instantly compensating its measurements and signals for the changed position. The process is repeated for the next layer . . . Layer after layer the brain is simulated, then excavated. Eventually your skull is empty, and the surgeon's hand rests deep in your brainstem. Though you have not lost consciousness, or even your train of thought, your mind has been removed from the brain and transferred to a machine. In a final, disorienting step the surgeon lifts out his hand. Your suddenly abandoned body goes into spasms and dies. For a moment you experience only quiet and dark. Then, once again, you can open your eyes. Your perspective has shifted. The computer simulation has been disconnected from the cable leading to the surgeon's hand and reconnected to a shiny new body of the style, color, and material of your choice. Your metamorphosis is complete.*

Moravec then describes less invasive ways to do the same thing, "for the squeamish." The result is still the replacement of your body – "mere jelly" – with a robot of "your" choice. ("Your" is in quotes because the pronoun has just become ambiguous.)

Mind Children was recommended to me by my Delphi colleague, Kip Bryan, as we were implementing a means of providing artificial opponents for players of Delphi's games when no human opponent was available or desired. The idea had come from a legendary MIT computer program called Eliza, which simulated a psychotherapist – you would tell Eliza something and "she" would ask you a question in the context of your comment.

The question of disclosure had to be dealt with: how do we ensure that the Delphi game player knows that his or her opponent is not a human being? I wanted to make it clear, but humorous rather than pedantic – avoiding the style of those idiotic warnings that were starting to appear on wine bottles. We thought we had accomplished that, but then a competitor – General Electric's GEnie online service – started "revealing" to the market of online users that Delphi was conning them with fake game players. Our reaction: Oh please, is anyone so naïve that they can't tell? Answer: Yes indeed, there were a few. Perhaps there were many more, too embarrassed to admit they'd been fooled!

Effectively we had created robots that were participating in human society. When Kip Bryan suggested reading the Moravec book and thinking about the larger implications, I was thoroughly amused. I got a copy of the book not so much to humor him as to humor myself with some off-the-wall science fiction. Kip's concerns seemed to me to be in the same category as those of a compulsive conspiracy theorist.

In the intervening decade and a half, however, I have come to see that Kip's concerns were valid. What is more alarming than the scenarios offered by Bill Joy and Hans Moravec is the belief that at every step of the way we must yield our prerogatives to anything that seems to be an advancement in intelligence.

What is it that makes intelligence the highest ideal of our age? Which of the following intelligent minds is closest to the ideal of the intelligence supremacists:

Josef Goebbels
Slobodan Milosevic
Dennis Kozlowski
Ivan Boesky
Joseph Stalin
Saddam Hussein
Pol Pot
Osama bin Laden
Vladimir Putin

Is this what we're after, the pursuit of super intelligence to the exclusion of all other values? Is that really what will advance humanity toward Utopia 0.6?

If my children had a choice between living a fulfilling and responsible life and graduating from MIT at age 16, I would obviously encourage them to seek the former. Wouldn't you? I hope so, as long as we both inhabit the same planet. The position advocated here is that intelligence is a tool for implementation of something that's essentially a matter of arbitrary choice: the desire to improve the lives of everybody by providing a means for encouraging people to be more responsible to one another and to the world.

> It's ridiculous to live 100 years and only be able to remember 30 million bytes. You know less than a compact disc. The human condition is really becoming more obsolete every minute.
>
> *Marvin Minsky*

I am fortunate in having had to deal with real artificial intelligence early, in the encounter with game-bots. The real artificial intelligence question isn't about applying some neural network technique to solving a problem, it's about software participating in society. Soon it will become a real issue. It is essentially ideological and political; there is no "correct" answer to the question of whether a robot or program with superior intelligence should take over the prerogatives of humans. If you believe that an object with a superior ability to process incoming signals and act on them quickly in a manner that suggests intelligence should always assume control over slower carbon-based objects, then for you the Internet is as it should be. Human identities shouldn't get in the way of the progress of digital objects. Without such encumbrances the most intelligent objects on the Net will gain control, and any human casualties along the way are of not much consequence as the new order is built. The new collection of intelligent objects may coalesce into one big global or intergalactic organism or, who knows, they may form nations that go to war with each other. The outcome will be of no consequence to us. If we humans are permitted to live as flesh-and-blood physical specimens, it will be in zoos or alongside the squirrels in places like Colonial Williamsburg, where robots can take their children to see life as it used to be, complete with the now endangered human species.

Admiral Hyman Rickover, who developed the United States Navy's nuclear submarine fleet, was once asked[13] by a congressman "What do you think is the prospect, then, for nuclear war?", to which he replied "Well I think we'll probably destroy ourselves. So what difference will it make? Some new species will come up that might be wiser than we are. I do not believe in divine intercession. In the eyes of the Lord, we are not the most important thing in the universe."

Back to Elon Musk, who notes that "…you could sort of think of humanity as a biological boot loader for digital super intelligence[14]." A boot loader is the thing that starts up your computer.

If one who favors members of his own race is a racist, then is one who favors his own species a speciesist? If so – forgive me, but I am a speciesist. And I hope that the speciesists will always prevail.

Don't we humans want and need the digital identity tools that will allow us and those we care about to assert our humanness over the various non-human objects found in networks?

As we encounter other beings in our travels about the internet, we need to have confidence that those beings are human – or else that they are under the control of humans.

[13] CBS 60 Minutes, interview with Diane Sawyer, April 15, 2011

[14] Wired magazine, 09.01.2019, https://www.wired.com/story/elon-musk-humanity-biological-boot-loader-ai/

You, the notary public, are the key to the source of that confidence. As an Attestation Officer, you will be able to let your fellow human beings know, with measurable certainty, whether the entity that is directing them or communicating with them or judging them is another human being – or a member of an alien species.

The future needs you.

ABOUT THE AUTHOR

Wes Kussmaul was the sole founder of Delphi Internet Services Corporation, "The Company That Popularized The Internet." At the time it was sold to Rupert Murdoch's News Corporation in 1993, Delphi was among the four largest online services, along with AOL, CompuServe, and Prodigy, and the first to bring full internet access to mass audiences. Delphi began as the world's first commercially available computerized encyclopedia and was the first with online auctions, shopping carts, and many other features of the online medium which we now take for granted.

In 1986, while CEO of Delphi, Wes launched a spinoff, Global Villages, Inc., to serve magazine publishers and business clients with their own private-label online services. During the next 12 years Global provided business planning, design, engineering, hosting, management and promotion services for Digital Equipment Corporation, William F. Buckley's National Review, BioTechniques, Hardcopy, International Business, Business Digest, and many other companies and magazines. Wes sold Global's hosting business in 1998 and is now a part of NTT Verio.

Before becoming a pioneer of the online services industry, Wes managed sales of computer graphics hardware and software products for Tektronix, Benson and Gould. Prior to that, he worked for Liberty Mutual Insurance Company in database development projects.

Wes earned a BS in physics from Central Missouri State University while stationed at nearby Whiteman Air Force Base (Strategic Air Command). He is an individual adherent of the International Union of Latin Notariats (UINL) and has been appointed a Notary Ambassador by the National Notary Association (NNA).

When not promoting authenticity entrepreneurship, Wes enjoys hiking and skiing with his family. He lives with his wife Maria, one of his five children, and the memories of their late dog Kerberos in Boston, Massachusetts.