Preface

For more than a decade, surveys of Internet users, administrators, and developers have consistently ranked "security" as their top concern. Despite the advances in Internet security technology, the problem of criminal activity on the Internet has only become worse.

As Nicholas Negroponte, founder of the MIT Media Lab and the One Laptop Per Child association observed: *bits not atoms*. As the world goes digital, so does crime. Only the venue is new in Internet crime. Every one of the crimes described in this book is a new twist on an ancient story. Willie Horton robbed banks because, "That's where the money is." Today, the money is on the Internet, and so are the criminals trying to steal it.

People not bits: Internet crime is about people. Money is the means; technology is merely an end. Some Internet criminals are world-class technology experts, but rather fewer than you might expect. Most Internet criminals are experts in manipulating and exploiting the behavior of people rather than machines.

Internet crime is caused by the criminals, but certain limitations of the original design of the Internet and the Web have encouraged its growth. To change the behavior of people, we must change the environment in which they interact. Paradoxically, understanding the *problem* of Internet crime as a social process leads us to *solutions* that are primarily expressed as technical proposals.

If we are going to beat the Internet criminals, we are going to need both strategy and tactics. In the short term, we must respond tactically—foiling attacks in progress even if doing so costs more than accepting the loss. In the longer term, we must change the infrastructure of the Internet so that it is no longer a lawless frontier but do so in a way that does not compromise the privacy and liberties that have attracted people to the Internet in the first place.

We must pursue both courses. Unless we can bring Internet crime under short-term control through a tactical response, it will be too late for strategy. If we don't use the time bought by the tactical approach to advance a long-term strategy, we will eventually run out of tactical options.

The Internet has more than a billion users. It is a complex and expensive infrastructure. Changing the Internet is difficult, particularly when success requires many changes to be made at the same

time and the people who must bear the cost are not always the ones who will see the benefit.

I am currently a participant in six different working groups tasked with changing a small part of the Internet. I have interactions with and occasionally appear at 20 more. Taken individually, none of the groups are likely to have a significant effect on the level of Internet crime. The best that can be hoped for is to move the problem from one place to another. Secure the e-mail system, and the criminals will start infiltrating Instant Messaging; secure Instant Messaging, and they will attack blogs or voice communications.

Taken together, the groups are working toward something that is much larger: a new Internet infrastructure that is a friendlier place for the honest person and a less advantageous environment for criminals.

The purpose of this book is to show how these pieces come together. In particular, it is an argument for a particular approach to Internet security based on *accountability*.

This book is arranged in four sections providing a rough narrative from problem to solution and from people issues to technology issues.

Section One: People Not Bits

Before we start to look at solutions, we need to understand both the problem we want to solve and the reasons it has not been solved before. What might surprise some readers is that technology only plays a minor role. *Money is the motive; people are the cause*. You don't need to be a technology expert to understand how these crimes work; the typical Internet criminal is not a technology expert.

The first two chapters deal with the problem. Chapter 1, "Motive," looks at the crimes themselves, every one a new twist on an ages-old scam, and Chapter 2, "Famous for Fifteen Mouse Clicks," looks at the criminals behind the scams. The common theme running through both chapters is that these crimes are due to the lack of accountability in the design of the Internet and the Web. To combat Internet crime, we must establish an accountable Web.

The next three chapters consider the problem of changing the Internet infrastructure to make it a less crime-friendly environment, and how to make the changes necessary to establish accountability. Chapter 3, "Learning from Mistakes," looks back at the reasons that the Internet is the way that it is. Chapter 4, "Making Change

Happen," looks forward and sets out a strategy for changing the Internet that is driven by pain and opportunity. Chapter 5, "Design for Deployment," describes an engineering approach based on that strategy: design for deployment.

Section Two: Stopping the Cycle

Having looked at the problem, we can begin to look at solutions to specific types of Internet crime, such as phishing and measures to limit the use of the criminal infrastructures that support them.

At this point, we are looking at measures that can be deployed in the short term with minimal changes to the existing Internet infrastructure. As a result, the measures tend to offer tactical rather than strategic advantage. Although tactical measures are valuable in the short run, we must accept that the respite they offer is temporary and use the time that they provide to deploy strategic changes to the Internet infrastructure that bring lasting benefits that the criminals find much harder to circumvent and make a profit from their activities.

Chapter 6, "Spam Whack-a-Mole," looks at previous efforts to control spam and the reasons that they have failed. Chapter 7, "Stopping Spam," describes more recent efforts to control spam by establishing an accountability infrastructure for e-mail use.

Chapter 8, "Stopping Phishing," examines the problem of phishing. Although phishing is not the only form of bank fraud on the Internet, it is currently the one that causes the most widespread concern.

Spam is one of the two principle engines of Internet crime. Chapter 9, "Stopping Botnets," looks at ways to disrupt the use of the other principle engine of Internet crime: networks of captured computers known as **botnets**.

Section Three: Tools of the Trade

Before looking at how to change the Internet infrastructure to make strategic changes, it is necessary to describe the technical tools available, in particular the use of cryptography.

Chapter 10, "Cryptography," presents a brief introduction to modern cryptography. Cryptography is a powerful tool but must be used with care. Security is a property of a system. A program can

employ the most advanced cryptographic techniques known and still fail to control real risks and thus provide security in the real world.

Chapter 11, "Establishing Trust," describes mechanisms that are used to establish trust in the online world today and some of the recent developments in the state of the art that will help us to establish the infrastructure we need to meet our future needs.

Section Four: The Accountable Web

The final section of this book presents the actual technical architecture of the accountable Web. Each chapter focuses on a particular layer of security infrastructure, beginning with those where work is already well advanced.

Chapters 12, "Secure Transport," and 13, "Secure Messaging," describe work that is currently underway to create the next-generation transport and messaging layer security infrastructures. In particular, the design of Extended Validation certificates and Secure Internet Letterhead are examined.

Chapters 14, "Secure Identity," and 15, "Secure Names," address the issues of identity and naming. This area is currently hotly contested with OpenID, CardSpace, and SAML all competing for position. I believe that in the long run, all of these technologies will develop complementary niches within a common Identity 2.0 ecology.

Chapter 16, "Secure Networks," looks at the network layer and describes Default Deny Infrastructure, an architecture designed to meet the challenge of deperimeterization. Chapter 17, "Secure Platforms," describes some of the work currently underway to develop a secure operating system and the use of next-generation code signing.

Chapter 18, "Law," examines the use of the legal system to reduce Internet crime, ensuring that law enforcement and prosecutors have the tools they need to do their job. Chapter 19, "The dotCrime Manifesto," sets out a plan of action for stopping Internet crime.

A Note on Jargon

Most technologists (sometimes including me) use rather too much jargon. After 25 years in the technology business, I have come to the conclusion that the more jargon a person uses, the less he is likely to know what he is talking about.

While preparing to edit this book, I reread a book on a related topic that was also aimed at a general audience written some years ago. I was somewhat surprised to find it somewhat heavy going even though I had found it a light read at the time. The field has moved on in the years since the book was first published, and so has the language. Will anyone remember what a "Joe job" is in ten years' time? I hope not. I hope we have made both the attack and the jargon name for it obsolete.

To avoid this problem, I have adopted the following principles.

- Where a term has been used as a term of art for many years in the field, I use it. The term **social engineering** has been used in the security field to describe obtaining information from a person through some form of confidence trick.
- Where a jargon term is widely used in the establishment media, I use it. The term **phishing** is widely used to describe the theft of credentials through a social engineering attack.
- Where a term has been recently introduced and is either self-explanatory or readily remembered after explanation, I use that term after giving an explanation. The term **capture site** is used to refer to a Web site used to collect credentials stolen in a phishing attack.
- Where a term is used with different meanings inside and outside the field or is otherwise ambiguous, I avoid it. Even though the term **hacker** is commonly used to refer to computer criminals, it is often used in the field in the original sense of an expert trickster.
- Where a term is not widely used outside a specialist clique and is not self-explanatory without reference to other jargon terms, I avoid it. In particular, I make a point of avoiding the hacker jargon **leet speak**. The point of leet speak is that it allows cliques to show each other how clever they are through use of a private code.

Word games can be fun, but we won't beat the criminals if we allow them to choose the rules and the game. I was recently in a meeting where a speaker had a cute term for every Internet crime imaginable. The next morning they were all forgotten.