Introduction

One of the lessons I learned early in life is to never confess the stupid things that I have done in public—unless there's a good punch line at the end of the story. Well, there is really no punch line at the end of the story I am about to tell you, but I am going to tell it anyway, because it helps introduce some of the key issues and concepts involved when securing e-mail clients and servers.

In 1994, I was browsing the Web with my trusty version of Netscape Navigator (version 1.0—yes, the one that ran just great on a Windows 3.11 machine that screamed along on top of an ultra-fast 486 processor). While browsing, I found a Web page that was selling a really nifty Telnet client. This piece of software had everything: I could use Kermit, Xmodem, and Zmodem to transfer files, and it even allowed automatic redial in case of a dropped connection. I just *had* to have it, and I had to have it right away; there was no waiting for it to arrive via "snail mail." I wanted to download it immediately.

Things being the way they were in 1994, the site's Web page invited me to either call their 800 number, or e-mail my Visa information for quicker processing. I'm something of a night owl, and it was about 2:30 a.m., and no one was manning the phones at the time. Rather than wait, I naïvely decided to use my Eudora e-mail client and send my Visa card number and expiration date to the site.

Two things happened as a result of this choice: I received an e-mail message response right away, complete with an access code that allowed me to download the software. With my new purchase, I was able to use Telnet as no one had ever used it before. That was the good part. The second thing happened two days after I began Telnetting my way across the world: I received a phone call from my Visa card company, asking me if I had authorized the use of this card for $250.00 in telephone charges, and around $375.00 for shoes. I hadn't. Someone

was using my Visa card to make telephone calls to Hawaii and purchase really expensive Nike's.

Before I had a chance to say anything to the Visa customer service representative (my profound response to her was a long "uuuhhh…"), she informed me that my charges were nearly identical to several others, all of which belonged to users who had sent e-mail messages to a certain site on the Internet. I remember the way she said the words "e-mail" and "Internet," because she said them as if she had never seen nor heard the words before. I told her that yes, I had visited the site on the Internet, and that I had sent an e-mail message containing my Visa information. I also told her that I had not made any purchases on the card lately. She quickly reversed the charges, cancelled the card, and issued me a new one. As I hung up the phone, I remember feeling both grateful and frightened: I had just been the victim of an Internet hacker who had obtained my Visa information via e-mail, presumably by "sniffing" it as it passed across the Internet, or by breaking into the site itself.

Now, alas, you have probably lost all confidence in me, the technical editor for this book. You may feel just like a person who is about to embark on a three-day journey through the great woods of the Pacific Northwest with no one else but a thin, nervous Forest Service guide who has poison ivy rashes all over his face. After all, I have helped write this book, and yet I have fallen victim to a hacker. Some expert I must be, right? Well, in some ways, I don't blame you if you feel a bit nervous about this book, at least at first. I still sometimes ask myself what was I thinking when I clicked the Send button. How could I be so foolish? What was I thinking? How could I be so lucky that my credit card company contacted me about this incident, rather than the other way around? Do you have any idea about the kind of runaround I would get in trying to reverse these illicit charges if it was only my idea?

And that's just the beginning of the questions I asked myself on the day I found out I had been "hacked." Trust me: Most of the remaining questions I ask myself are pretty harsh. After all, sending important information without first encrypting it is, to put it bluntly, pretty silly. But one thing that helps me regain some sort of self-confidence is the knowledge that I learn quickly from my mistakes.

Nowadays, I congratulate myself by knowing exactly how I got hacked, and, even more important, how I can use today's cutting-edge technologies to help keep anything like this from ever happening again. I now understand how an e-mail message is passed from the end user's

client machine through e-mail servers across the Internet. I have, in essence, empowered myself with knowledge concerning how e-mail messages are sent, processed, and received. I didn't learn these things as a direct result of getting hacked. Still, it has been very helpful for me to think back to that incident as I subsequently learned about arcane bits of knowledge relevant to e-mail (the Simple Mail Transfer Protocol (SMTP), the Domain Name System (DNS), packet sniffing applications, and encryption, etc.).

As I think back to that incident, I consider another question that is really quite intriguing: What was it that made me almost immediately go back to my computer, fire up my e-mail client, and keep sending e-mail messages? After all, I had been hacked. Yet, as silly as I felt, I still needed to communicate via e-mail. The sheer speed, convenience, and usefulness of the medium made it far too important and compelling to stop using it.

End-users, power users, and systems administrators all use e-mail every day, in spite of the security problems found in current e-mail technologies. This book explains how to implement specific security measures for e-mail clients and servers that make communication via e-mail both secure and convenient. In this book, you will learn about the problems associated with e-mail, including specific attacks that malicious users, sometimes called hackers, can wage against e-mail servers. First, you will learn about how these attacks are waged, and why. Once you understand the hacker's perspective, you can then begin to approach your e-mail client and server software from a more informed perspective.

This book will show you how to encrypt e-mail messages using the freeware Pretty Good Privacy (PGP) application, one of the most successful software packages ever. You will also learn about problems associated with Web-based e-mail, and how to solve some of them by using more secure options. Later chapters discuss how to install and configure the latest anti-virus applications, and also how to install "personal firewall" software, which is designed to isolate your computer's operating system so that it is not as susceptible to attacks waged by malicious users.

Once this book has thoroughly discussed how to secure e-mail clients, it then turns to the server side. Remember, once you click the Send button, you then involve two types of e-mail servers: The first type is designed to send e-mail messages across the Internet. The second type is designed to store e-mail messages, then allow you to log in remotely in order to read and download them. In the second section,

you will learn how to harden the operating system so that it can properly house an e-mail server. You will then learn about how to protect your system against malicious code by invoking third-party software, which is designed to scan e-mail messages (and attachments) for malicious content.

This book is unique because it discusses the latest methods for securing both the e-mail client and the e-mail server from the most common threats. These threats include "sniffing" attacks that illicitly obtain e-mail message information, denial of service attacks, that attempt to crash e-mail clients and servers, and authentication-based attacks, that attempt to defeat the user names and passwords that we use every day to secure our systems. Time will not eliminate these threats. In fact, it is likely that these will become even more serious. As e-mail becomes even more central to business practice, you will find this book very handy as a desktop reference for installing the latest e-mail security software. Even after the software discussed in this book becomes outdated, you will find that the concepts and principles enacted in this book will remain timely and useful. This is the book that I wish I had back in 1994. With this book, I would have been able to use my nifty Telnet client with full peace of mind, because I would have waited until the proper technologies were available in order to send my confidential e-mail message.

The authors we have assembled for this book are all authorities in network security. They are a diverse group. Some of the authors are experts in creating public key encryption solutions and knowing how to harden an operating system so that it can safely house an e-mail server. Others are experienced software coders who have deep knowledge of just what malicious code can do. Some of the authors presented in this book are seasoned IT professionals, while others have had extensive contact with the very hackers that are currently lurking the Internet, looking for unwitting victims who have not yet bought and read this book (here's hoping you have bought this book, and have not checked it out from the library!).

As diverse as this group is, all have one thing in common: Each is sincere in the wish to teach you how to secure your system. Each has learned through extensive study and experience about the industry best practices to follow when deploying software solutions. What is more, each of these authors has taken the time to share insights. I hope you enjoy this book. I have enjoyed editing it, as well as contributing a chapter or two. After you have read this book, you will be able to encrypt your e-mails, scan for malicious code on both the client

and the server side, and thoroughly understand what happens when you click the Send button, or double-click an attachment.

So, as you read the Case Studies, all of which are provided as real-world examples from real-world companies, and as you thumb through the details provided in this book, consider that you are now able to take advantage of the shared wisdom of many different authors. It is even possible that some of them have made a few mistakes along the way, just so that you can benefit from the lessons they learned.