INTRODUCTION

A Few Words about Me

I seem to have been born a computer geek, but my adventure with network security began only by accident. I have always loved to experiment, explore new ideas, and solve seemingly well defined but still elusive challenges that require innovative and creative approaches—even if just to fail at solving them. When I was young, I spent most of my time pursuing sometimes risky and often silly attempts to explore the world of chemistry, mathematics, electronics, and finally computing rather than ride my bike around the block all day long. (I probably exaggerate a bit, but my mother always seemed to be worried.)

Shortly after my first encounter with the Internet (in the mid '90s, perhaps eight years after I coded my first "Hello world" program on a beloved 8-bit machine), I received an unusual request: a spam letter that, hard to believe, asked me (and a couple thousand other folks) to join an underground team of presumably malicious, black hat hackers. This did not drive me underground (perhaps due to my strong instinct for self-preservation, known in certain circles as cowardice) but somehow provided a good motivation to explore the field of computer security in more detail. Having done plenty of amateur programming, I found it captivating to look at code from a different perspective and to try to find a way for an algorithm to do something more than it was supposed to do. The Internet seemed a

great resource for the challenges I craved—a big and complex system with only one guiding principle: You cannot really trust anyone. And so it all began.

I do not have the background you might expect from the usual computer security specialist, a profession that is becoming commonplace today. I have never received any formal computer science education, nor do I hold an impressive-sounding set of certifications. Security has always been one of my primary passions (and is now my living). I am not the stereotypical computer geek—I do get up once in a while to look at my work from a sane distance or to get away from computers altogether.

For good or bad, all this has affected the shape of this book and its message. My goal is to show others how I view computer security, not how it is usually taught. For me, security is not a single problem to be solved nor a simple process to follow. It is not about expertise in a specific field. It is an exercise in seeing the entire ecosystem and understanding its every component.

About This Book

Even in the dim light of our monitors, we are still only humans. We were taught to trust others, and we do not want to be too paranoid. We need to find a sensible compromise between security and productivity to live comfortably.

The Internet is, nevertheless, different from a real-world society. There is no common benefit from conforming to the rules, and there is seldom any remorse for virtual misdeeds. We cannot simply trust the system, and our attempts to come up with a single rule that can be applied to all problems will fail miserably. We instinctively draw a straight line to separate "us" from "them" and call our own island safe. Then, we look out for rogue ships on the horizon. Soon, security problems start to appear as localized abnormalities that can be easily defined, diagnosed, and resolved. From that perspective, attackers appear to be driven by clear motives, and if we are vigilant, we can see them and stop them as they approach.

Yet, the virtual world is quite different: security is not the absence of bugs; safety does not lie in being beyond the reach of attackers. Just about any process involving information has inherent security implications, which are visible to us the moment we look beyond the scope of the goal the process tries to achieve. The art of understanding security is simply the art of being able to cross the line and look from a different perspective.

This is an unconventional book, or so I hope. It is not a compendium of problems or a guide to securing your systems. It begins with an attempt to follow the story of a piece of information, from the moment your hands touch the keyboard, all the way to the remote party on the other end of the wire. It covers the technology and its security implications, focusing on problems that cannot be qualified as bugs, with no attacker, no flaw to be analyzed and resolved, or no detectable attack (or at least not one that we can distinguish

from legitimate activity). The goal of this book is to demonstrate that the only way to understand the Internet is to have the courage to go beyond the specifications or read between the lines.

As the subtitle suggests, this book focuses on privacy and security problems inherent to everyday communications and computing. Some of them have profound implications, while others are simply interesting and stimulating. None will have an immediate damaging impact on your environment or destroy the data on your disk drive. The information here is useful and valuable to IT professionals and seasoned amateurs who want to be challenged to exercise their minds and who want to learn about the nonobvious consequences of design decisions. This is a book for those who want to learn how to use these subtleties to take control of their environment and gain an advantage over the world outside.

The book is divided into four sections. The first three cover stages of data flow and technologies deployed there. The last section focuses on the network as a whole. Every chapter covers relevant elements of the technology used to process the data at each stage, a discussion of security implications, a demonstration of its side-effects, suggestions on how to address the problems (if possible), and recommendations for how to further explore the subject. I do my best to avoid charts, tables, pages of specifications, and so forth (though you will find numerous footnotes). Since you can easily find plenty of good reference materials online, my focus is on making this book simply enjoyable.

Shall we begin?

PART I

THE SOURCE

On the problems that surface long before one sends any information over the network