# 1
# Introduction

Today alone, Dell Computer will sell more than $18 million worth of computer equipment through the Internet. In 1999, nine million Americans traded stocks online, accounting for one-third of all retail stock trades. And more than 200,000 Web sites worldwide (including sites belonging to 98 of the Fortune 100) can accept e-commerce transactions. Commercial use of the Web continues to grow at an astonishing pace, and securing Web transactions has become increasingly critical to businesses, organizations, and individual users.

Fortunately, an extremely effective and widely deployed communications protocol provides exactly that security. It is the Secure Sockets Layer protocol, more commonly known simply as ssl. The ssl protocol—along with its successor, the Transport Layer Security (tls) protocol—is the subject of this book.

This chapter introduces ssl and tls, and provides the essential context for both. It begins with a very brief look at Web security and electronic commerce, focusing on the issues that led to the creation of ssl. The next section follows up with a quick history of ssl and its transformation into tls. The relationship of ssl to other network security technologies is the subject of the third section. The forth section, "Protocol Limitations," is an important one. Especially with security technologies, it is critical to understand what they *cannot* do. The chapter closes with an overview of the rest of this book.