

## CHAPTER

## 1

# Introduction

In the early days of the Internet, no one worried about security. Those days are long gone. Today, everyone uses the Internet, and electronic mail is used for both business communication and personal communication. Much of it is sensitive, making security necessary. Secure electronic mail is available, yet very few people use it.

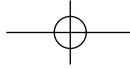
Many people are under the mistaken impression that email is point-to-point communication protocol. It is not. Many servers are involved, and each one of them can mess with the messages — unless you protect them. You do not want the messages read by anyone other than the intended recipient. You do not want anyone to change the message content. And, you do not want others to masquerade as you. Luckily, the tools are all readily available for providing these protections.

In this book, we explain security tools, including cryptography, security protocols, tokens, and hardware security modules to protect your email. You do not need to be an expert in these technologies to secure your email. Products are available that can help you. This book provides the information needed to first select wisely from these security offerings and then successfully deploy them. The case studies at the end of the book allow you to emulate the successes and avoid the potholes found by others.

## How This Book Is Organized

---

We organized this book in to six sections. The later sections build on material presented in the earlier ones. A person familiar with email and who understands fundamental security services may be able to skip the earlier parts, but most readers will want to read the book from beginning to end.



## 4 **Part I ■ Email and Security Background**

---

We start by introducing Internet email, which is what we want to secure. Next, we provide motivation for why you should want to secure your email from prying eyes and then show you how to do it. Finally, we discuss the mechanism necessary to secure email. Three case studies give you hands-on lessons concerning these programs that will prove invaluable to you. Finally, we provide our Magic 8 Ball predictions for the future. Obviously, only time will tell if our Magic 8 Ball was lying.

### **Part I: Email and Security Background**

Part I contains four chapters, including this one. Chapter 2, “Understanding Email,” explains the Internet electronic mail transport and content standards. We use postal service analogies, hoping to make it easier to understand by leveraging things that you already know about the postal service (sometimes called snail mail). Chapter 3, “Security Fundamentals,” explains who might want to read your email, how they might try to do it, and what you can do to stop them. Chapter 4, “Cryptography Primer,” introduces the basics of cryptography, which is one of the key arrows in your quiver for thwarting the attackers introduced in Chapter 3.

### **Part II: PKI Basics**

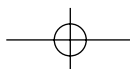
Part II contains only one chapter, dealing with Public Key Infrastructure (PKI). Chapter 5, “Understanding PKI,” explains who should be trusted to properly perform specific activities in a PKI. It describes the most common PKI architectures, explains the public key certificates, and elucidates the certificate revocation lists structures produced by a PKI.

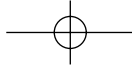
### **Part III: Secure Email**

Part III contains two chapters, both detailing the ins and outs of email security. Chapter 6, “Protecting Email Message Contents,” provides a history of email security mechanisms and explains the most common mechanism to protect your emails’ contents, whereas Chapter 7, “Protecting Email Passwords, Message Headers, and Commands,” explains how to make sure that your passwords aren’t disclosed to attackers and how to protect the email message headers and commands.

### **Part IV: Tokens**

Part IV also contains a single chapter. Chapter 8, “Tokens and Hardware Security Modules,” describes the different types of devices that can be used to store and protect your private keys. We also discuss the ways that these devices are evaluated by professionals in certified laboratories.





## **Part V: Case Studies**

Part V contains three chapters, one for each case study. Each chapter describes an implementation that includes secure email, PKI, and tokens. Chapter 9, “Signatures and Authentication For Everyone,” describes the SAFE program in the pharmaceutical community, which interconnects the PKIs from many members of that community to support secure email, as well as other applications that make use of digitally signed documents. Chapter 10, “Department of Defense Public Key Infrastructure, Medium Grade Service, and Common Access Cards” describes PKI, Medium Grade Service (MGS), and Common Access Card (CAC) programs of the U.S. Department of Defense. Chapter 11, “National Institute of Standards and Technology Personal Identity and Verification,” describes the smart-card-based standard developed by the National Institute of Standards and Technology (NIST) and the way that it is being used to fulfill the requirements in HSPD12.

## **Part VI: Expectations for the Future**

Part VI contains a single chapter. Chapter 12, “Future Developments,” offers predictions for developments in each of the areas discussed in this book.

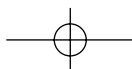
## **Appendices**

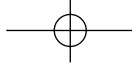
We provide supplemental information in four appendices. Appendix A, “ABNF Primer,” provides an introduction to Augmented Backus-Noir Form, which is the formal language used to describe the syntax for character-based protocols, such as electronic mail. Appendix B, “ASN.1 Primer,” provides an introduction to Abstract Syntax Notation One, which is the formal language used to describe the syntax in many binary-oriented protocols. Appendix C, “MIME Primer,” explains how arbitrary data is included in character-based email messages using Multipurpose Internet Mail Extensions. We provide sufficient detail for reading and understanding the structures used in this book, but you’ll need to look elsewhere for a complete coverage of these topics. Appendix D, “RFC Summaries,” provides a summary of the Requests for Comments (RFCs) that are referenced in this book.

## **Who Should Read This Book**

---

This book is intended for the chief technology officer (CTO) or perhaps the person whom the CTO assigns to implement an enterprise secure email solution, including PKI and tokens. It will also help people who want to buy the various components of such a system, but who may not have the expertise to do so confidently.





## 6 Part I ■ Email and Security Background

---

Keep in mind that this is not a guide for developers. However, developers of one component within an overall email security system will find it useful to understand how their component interacts with the rest of the system. It is not possible to include every detail of every component in this book. Therefore, we recommend that developers refer to the Internet Engineering Task Force (IETF) standards for details on the syntax and semantics of email-related protocols and PKI-related protocols.

You are presented with many choices when implementing an email security system. We hope that this book will help you wade through these options and achieve the benefits of secure email.

