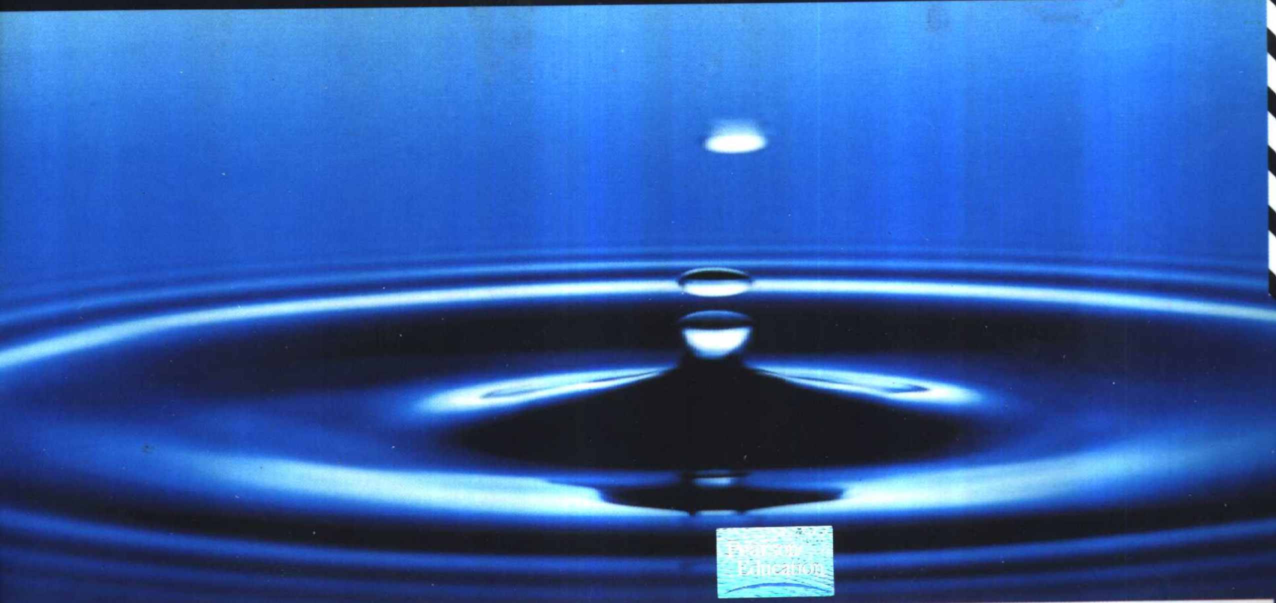
大学计算机教育国外著名教材、教参系列（影印版）

Network Security Essentials: Applications and Standards

William Stallings

Winner of the 1999 TEXTY award for the best computer science and engineering textbook

网络安全基础教程：应用与标准



Pearson Education

清华大学出版社
http://www.tup.tsinghua.edu.cn

Prentice Hall

培生教育出版集团
http://www.pearsoned.com

Network Security Essentials:

Applications and Standards

网络安全基础教程:

应用与标准

William Stallings

清华大学出版社　　培生教育出版集团

（京）新登字 158 号

Network Security Essentials: Applications and Standards
William Stallings

图书在版编目(CIP)数据

网络安全基础教程：应用与标准/(美)斯托林斯著．影印本．—北京：清华大学出版社，2002
（大学计算机教育国外著名教材、教参系列）
ISBN 7-302-05536-X

Ⅰ.网…　Ⅱ.斯…　Ⅲ.计算机网络－安全技术－高等学校－教材－英文　Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 037390 号

出版者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
　　　　http:// www.tup.tsinghua.edu.cn
印刷者：北京牛山世兴印刷厂
发行者：新华书店总店北京发行所
开　本：787×960 1/16　印张：24
版　次：2002 年 6 月第 1 版　2002 年 6 月第 1 次印刷
书　号：ISBN 7-302-05536-X/TP・3259
印　数：0001～4000
定　价：35.00 元

出 版 说 明

进入 21 世纪，世界各国的经济、科技以及综合国力的竞争将更加激烈。竞争的中心无疑是对人才的争夺。谁拥有大量高素质的人才，谁就能在竞争中取得优势。高等教育，作为培养高素质人才的事业，必然受到高度重视。目前我国高等教育的教材更新较慢，为了加快教材的更新频率，教育部正在大力促进我国高校采用国外原版教材。

清华大学出版社从 1996 年开始，与国外著名出版公司合作，影印出版了“大学计算机教育丛书（影印版）”等一系列引进图书，受到了国内读者的欢迎和支持。跨入 21 世纪，我们本着为我国高等教育教材建设服务的初衷，在已有的基础上，进一步扩大选题内容，改变图书开本尺寸，一如既往地请有关专家挑选适用于我国高校本科及研究生计算机教育的国外经典教材或著名教材以及教学参考书，组成本套“大学计算机教育国外著名教材、教参系列（影印版）”，以飨读者。深切期盼读者及时将使用本系列教材、教参的效果和意见反馈给我们。更希望国内专家、教授积极向我们推荐国外计算机教育的优秀教材，以利我们把“大学计算机教育国外著名教材、教参系列（影印版）”做得更好，更适合高校师生的需要。

计算机引进版图书编辑室
2002.3

For my loving wife ATS
and her loving companions
Geoffroi and Kate Lan Kinetic

PREFACE

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, network security has assumed increasing importance. Two trends have come together to make the topic of this book of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.

OBJECTIVES

It is the purpose of this book to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards, especially Internet standards, that have been widely deployed.

INTENDED AUDIENCE

The book is intended for both an academic and a professional audience. As a textbook, it is intended as a one-semester undergraduate course on network security for computer science, computer engineering, and electrical engineering majors. The book also serves as a basic reference volume and is suitable for self-study.

PLAN OF THE BOOK

The book is organized in three parts:

I. **Cryptography:** A concise survey of the cryptographic algorithms and protocols underlying network security applications, including encryption, hash functions, digital signatures, and key exchange.

II. **Network Security Applications:** Covers important network security tools and applications, including Kerberos, X.509v3 certificates, PGP, S/MIME, IP Security, SSL/TLS, SET, and SNMPv3.

III. **System Security:** Looks at system-level security issues, including the threat of and countermeasures for intruders and viruses, and the use of firewalls and trusted systems.

A more detailed, chapter-by-chapter summary appears at the end of Chapter 1. In addition, the book includes an extensive glossary, a list of frequently used acronyms, and a bibliography. There are also end-of-chapter problems and suggestions for further reading.

INTERNET SERVICES FOR INSTRUCTORS AND STUDENTS

There is a Web page for this book that provides support for students and instructors. The page includes links to relevant sites, transparency masters of figures in the book in PDF (Adobe Acrobat) format, and sign-up information for the book's Internet mailing list. The Web page is at http://www.shore.net/~ws/NetSec.html. An Internet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and with the author. As soon as typos or other errors are discovered, an errata list for this book will be available at http://www.shore.net/~ws.

PROJECTS FOR TEACHING NETWORK SECURITY

For many instructors, an important component of a cryptography or security course is a project or set of projects by which the student gets hands-on experience to reinforce concepts from the text. This book provides an unparalleled degree of support for including a projects component in the course. The instructor's manual not only includes guidance on how to assign and structure the projects, but also includes a set of suggested projects that covers a broad range of topics from the text:

- **Research Projects:** A series of research assignments that instruct the student to research a particular topic on the Internet and write a report.

- **Programming Projects:** A series of programming projects that cover a broad range of topics and that can be implemented in any suitable language on any platform.
- **Reading/Report Assignments:** A list of papers in the literature, one for each chapter, that can be assigned for the student to read and then write a short report.

See Appendix B for details.

RELATIONSHIP TO *CRYPTOGRAPHY AND NETWORK SECURITY, SECOND EDITION*

This book is on spin-off from *Cryptography and Network Security, Second Edition* (CNS2e). CNS2e provides a substantial treatment of cryptography, including detailed analysis of algorithms and a significant mathematical component, the whole of which covers over 300 pages. *Network Security Essentials: Applications and Standards* (NSE1e) provides instead a concise overview of these topics in Chapters 2 and 3. NSE1e includes all of the remaining material of CNS2e, with updates. NSE1e also covers SNMP security, which is not covered in CNS2e. Thus, NSE1e is intended for college courses and professional readers where the interest is primarily in the application of network security, without the need or desire to delve deeply in to cryptographic theory and principles.

CONTENTS

CHAPTER 1

INTRODUCTION

The requirements of **information security** within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. An example of the former is the use of rugged filing cabinets with a combination lock for storing sensitive documents. An example of the latter is personnel screening procedures used during the hiring process.

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, such as a time-sharing system, and the need is even more acute for systems that can be accessed over a public telephone or data network. The generic name for the collection of tools designed to protect data and to thwart hackers is **computer security**.

The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. In fact, the term **network security** is somewhat misleading, because virtually all business, government, and academic organizations interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet.[1]

There are no clear boundaries between these two forms of security. For example, one of the most publicized types of attack on information systems is the computer virus. A virus may be introduced into a system physically when it arrives on a diskette and is subsequently loaded onto a computer. Viruses may also arrive over an internet. In either case, once the virus is resident on a computer system, internal computer security tools are needed to detect and recover from the virus.

This book focuses on internet security, which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information. That is a broad statement that covers a host of possibilities. To give you a feel for the areas covered in this book, consider the following examples of security violations:

1. User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that are to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.
2. A network management application, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its con-

[1] We use the term *internet*, with a lowercase "i," to refer to any interconnected collection of network. A corporate intranet is an example of an internet. The Internet with a capital "I" may be one of the facilities used by an organization to construct its internet.

tents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

3. Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.
4. An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee's action may go unnoticed for some considerable time.
5. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

Although this list by no means exhausts the possible types of security violations, it illustrates the range of concerns of network security.

Internetwork security is both fascinating and complex. Some of the reasons follow:

1. Security involving communications and networks is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory one-word labels: confidentiality, authentication, nonrepudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.
2. In developing a particular security mechanism or algorithm, one must always consider potential countermeasures. In many cases, countermeasures are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
3. Because of point 2, the procedures used to provide particular services are often counterintuitive: It is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various countermeasures are considered that the measures used make sense.
4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed).
5. Security mechanisms usually involve more than a particular algorithm or protocol. They usually also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There is also a reliance

on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

Thus, there is much to consider. This chapter provides a general overview of the subject matter that structures the material in the remainder of the book. We begin with a discussion of the types of attacks that create the need for network security services and mechanisms. Then we develop a general overall model within which the security services and mechanisms can be viewed.

1.1 ATTACKS, SERVICES, AND MECHANISMS

To assess the security needs of an organization effectively and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. One approach is to consider three aspects of information security:

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Services

Let us consider these topics briefly, in reverse order. We can think of information security services as replicating the types of functions normally associated with physical documents. Much of the activity of humankind, in areas as diverse as commerce, foreign policy, military action, and personal interactions, depends on the use of documents and on both parties to a transaction having confidence in the integrity of those documents. Documents typically have signatures and dates; they may need to be protected from disclosure, tampering, or destruction; they may be notarized or witnessed; may be recorded or licensed, and so on.

As information systems become ever more pervasive and essential to the conduct of our affairs, electronic information takes on many of the roles traditionally performed by paper documents. Accordingly, the types of functions traditionally associated with paper documents must be performed on documents that exist in electronic form. Several aspects of electronic documents make the provision of such functions or services challenging:

Table 1.1 A Partial List of Common Information Integrity Functions [SIMM92b]

- Identification
- Authorization
- License and/or certification
- Signature
- Witnessing (notarization)
- Concurrence
- Liability
- Receipts
- Certification of origination and/or receipt
- Endorsement
- Access (egress)
- Validation
- Time of occurrence
- Authenticity-software and/or files
- Vote
- Ownership
- Registration
- Approval/disapproval
- Privacy (secrecy)

1. It is usually possible to discriminate between an original paper document and a xerographic copy. However, an electronic document is merely a sequence of bits; there is no difference whatsoever between the "original" and any number of copies.
2. An alteration to a paper document may leave some sort of physical evidence of the alteration. For example, an erasure can result in a thin spot or a roughness in the surface. Altering bits in a computer memory or in a signal leaves no physical trace.
3. Any "proof" process associated with a physical document typically depends on the physical characteristics of that document (e.g., the shape of a handwritten signature or an embossed notary seal). Any such proof of authenticity of an electronic document must be based on internal evidence present in the information itself.

Table 1.1 lists some of the common functions traditionally associated with documents and for which analogous functions for electronic documents and messages are required. We can think of these functions as requirements to be met by a security facility.

The list of Table 1.1 is lengthy and is not by itself a useful guide to organizing a security facility. Computer and network security research and development have instead focused on a few general security services that encompass the various functions required of an information security facility. We return to this topic after a consideration of security mechanisms and attacks.

Mechanisms

There is no single mechanism that will provide all the services just listed or perform all the functions listed in Table 1.1. As this book proceeds, we will see a variety of mechanisms that come into play. However, we can note at this point that there is one particular element that underlies most of the security mechanisms in use: cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Thus, this book focuses on the development, use, and management of such techniques.

Table 1.2 Reasons for Cheating [SIMM92b]

1. Gain unauthorized access to information (i.e., violate secrecy or privacy).
2. Impersonate another user either to shift responsibility (i.e., liability) or else to use the other's license for the purpose of:
   a. originating fraudulent information,
   b. modifying legitimate information,
   c. using fraudulent identity to gain unauthorized access,
   d. fraudulently authorizing transactions or endorsing them.
3. Disavow responsibility or liability for information the cheater did originate.
4. Claim to have received from some other user information that the cheater created (i.e., fraudulent attribution of responsibility or liability).
5. Claim to have sent to a receiver (at a specified time) information that was not sent (or was sent at a different time).
6. Either disavow receipt of information that was in fact received, or claim a false time of receipt.
7. Enlarge cheater's legitimate license (for access, origination, distribution, etc.).
8. Modify (without authority to do so) the license of others (fraudulently enroll others, restrict or enlarge existing licenses, etc.).
9. Conceal the presence of some information (a covert communication) in other information (the overt communication).
10. Insert self into a communications link between other users as an active (undetected) relay point.
11. Learn who accesses which information (sources, files, etc.) and when the accesses are made even if the information itself remains concealed (e.g., a generalization of traffic analysis from communications channels to databases, software, etc.).
12. Impeach an information integrity protocol by revealing information the cheater is supposed to (by the terms of the protocol) keep secret.
13. Pervert the function of software, typically by adding a covert function.
14. Cause others to violate a protocol by means of introducing incorrect information.
15. Undermine confidence in a protocol by causing apparent failures in the system.
16. Prevent communication among other users, in particular, surreptitious interference to cause authentic communication to be rejected as unauthentic.

Attacks

As G. J. Simmons perceptively points out, information security is about how to prevent cheating or, failing that, to detect cheating in information-based systems wherein the information itself has no meaningful physical existence [SIMM92a].

Table 1.2 lists some of the more obvious examples of cheating, each of which has arisen in a number of real-world cases. These are examples of specific attacks that an organization or an individual (or an organization on behalf of its employees) may need to counter. The nature of the attack that concerns an organization varies greatly from one set of circumstances to another. Fortunately, we can approach the problem from a different angle by looking at the generic types of attack that might be encountered. That is the subject of the next section.

1.2 SECURITY ATTACKS

Attacks on the security of a computer system or network are best characterized by viewing the function of the computer system as providing information. In general,