SOLUTIONS MANUAL

NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS SIXTH EDITION

WILLIAM STALLINGS

NOTICE

This manual contains solutions to the review questions and homework problems in *Cryptography and Network Security, Sixth Edition*. If you spot an error in a solution or in the wording of a problem, I would greatly appreciate it if you would forward the information via email to wllmst@me.net. An errata sheet for this manual, if needed, is available at http://www.box.net/shared/nh8hti5167 . File name is S-NetSec6e-mmyy

W.S.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

ANSWERS TO QUESTIONS

1.1 The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

1.2 **Passive attacks** have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. **Active attacks** include the modification of transmitted data and attempts to gain unauthorized access to computer systems.

1.3 **Passive attacks:** release of message contents and traffic analysis.
Active attacks: masquerade, replay, modification of messages, and denial of service.

1.4 **Authentication:** The assurance that the communicating entity is the one that it claims to be.
Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
Data confidentiality: The protection of data from unauthorized disclosure.
Data integrity: The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Availability service: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

1.5 See Table 1.3.

1.6 Economy of mechanism: the design of security measures embodied in both hardware and software should be as simple and small as possible.

Fail-safe defaults: access decisions should be based on permission rather than exclusion.

Complete mediation: every access must be checked against the access control mechanism.

Open Design: the design of a security mechanism should be open rather than secret.

Separation of privilege: a practice in which multiple privilege attributes are required to achieve access to a restricted resource.

Least Privilege: every process and every user of the system should operate using the least set of privileges necessary to perform the task.

Least common mechanism: the design should minimize the functions shared by different users, providing mutual security.

Psychological acceptability: the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.

Isolation: a principle that applies in three contexts. (1) public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering. (2) the processes and files of individual users should be isolated from one another except where it is explicitly desired. (3) security mechanisms should be isolated in the sense of preventing access to those mechanisms.

Encapsulation: a specific form of isolation based on object-oriented functionality.

Modularity: refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation.

Layering: the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.

Least Astonishment: means that a program or user interface should always respond in the way that is least likely to astonish the user.

1.7 An attack surface consists of the reachable and exploitable vulnerabilities in a system. An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

ANSWERS TO PROBLEMS

1.1 The system must keep personal identification numbers confidential, both in the host system and during transmission for a transaction. It must protect the integrity of account records and of individual transactions. Availability of the host system is important to the economic well being of the bank, but not to its fiduciary responsibility. The availability of individual teller machines is of less concern.

1.2 The system does not have high requirements for integrity on individual transactions, as lasting damage will not be incurred by occasionally losing a call or billing record. The integrity of control programs and configuration records, however, is critical. Without these, the switching function would be defeated and the most important attribute of all - availability - would be compromised. A telephone switching system must also preserve the confidentiality of individual calls, preventing one caller from overhearing another.

1.3 **a.** The system will have to assure confidentiality if it is being used to publish corporate proprietary material.
b. The system will have to assure integrity if it is being used to laws or regulations.
c. The system will have to assure availability if it is being used to publish a daily paper.

1.4 **a.** An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability.
b. A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate.
c. A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.
d. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

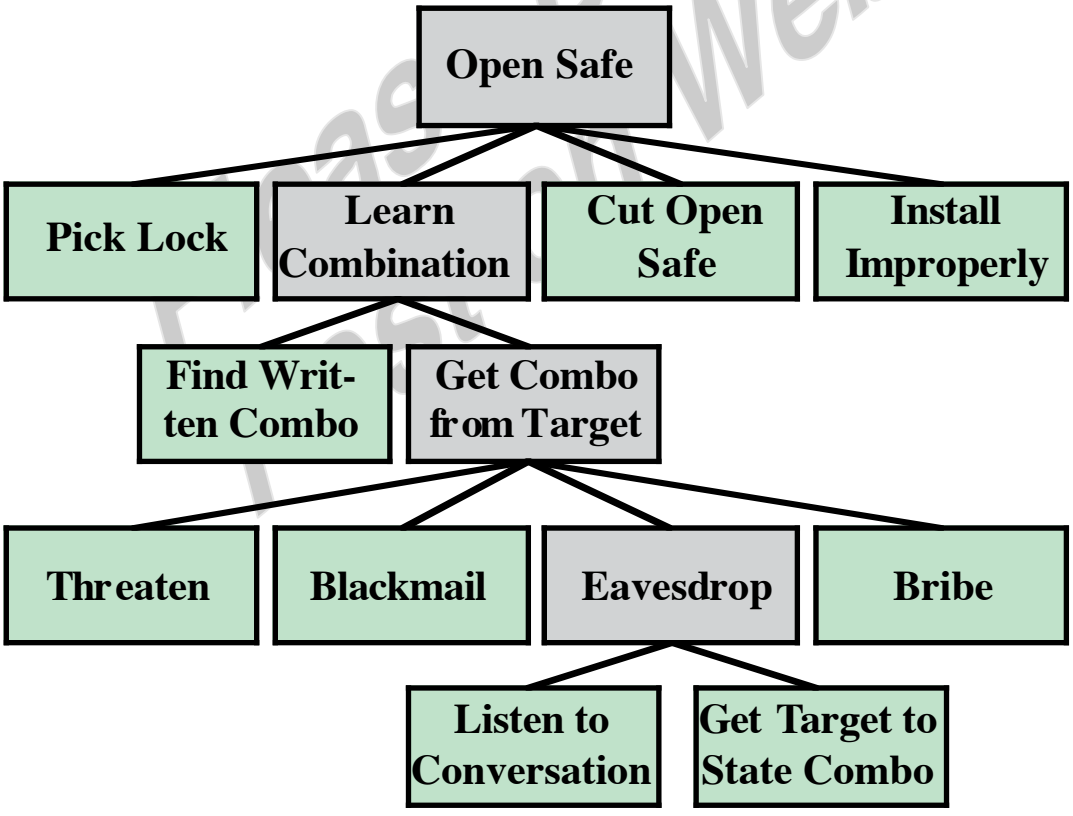
e. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. Examples from FIPS 199.

1.5	**Release of message contents**	**Traffic analysis**	**Masquerade**	**Replay**	**Modification of messages**	**Denial of service**
Peer entity authentication			**Y**			
Data origin authentication			**Y**			
Access control			**Y**			
Confidentiality	**Y**					
Traffic flow confidentiality		**Y**				
Data integrity				**Y**	**Y**	
Non-repudiation			**Y**			
Availability						**Y**

1.6

	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Encipherment	Y					
Digital signature			Y	Y	Y	
Access control	Y	Y	Y	Y		Y
Data integrity				Y	Y	
Authentication exchange	Y		Y	Y		Y
Traffic padding		Y				
Routing control	Y	Y				Y
Notarization			Y	Y	Y	

1.7



1.8 We present the tree in text form; call the company X:

Survivability Compromise: Disclosure of X proprietary secrets

OR 1. Physically scavenge discarded items from X
- OR 1. Inspect dumpster content on-site
- 2. Inspect refuse after removal from site

2. Monitor emanations from X machines
- AND 1. Survey physical perimeter to determine optimal monitoring position
- 2. Acquire necessary monitoring equipment
- 3. Setup monitoring site
- 4. Monitor emanations from site

3. Recruit help of trusted X insider
- OR 1. Plant spy as trusted insider
- 2. Use existing trusted insider

4. Physically access X networks or machines
- OR 1. Get physical, on-site access to Intranet
- 2. Get physical access to external machines

5. Attack X intranet using its connections with Internet
- OR 1. Monitor communications over Internet for leakage
- 2. Get trusted process to send sensitive information to attacker over Internet
- 3. Gain privileged access to Web server

6. Attack X intranet using its connections with public telephone network (PTN)
- OR 1. Monitor communications over PTN for leakage of sensitive information
- 2. Gain privileged access to machines on intranet connected via Internet