TT TEXTBOOK TESTBANKS

Solutions Manual for Computer Security Principles and Practice 5th Stallings

SOLUTIONS MANUAL SAMPLE PREVIEW

PUBLISHER
Pearson

COPYRIGHT
2024

RESOURCE TYPE
Solutions Manual

ISBN
9780138091439

SOLUTIONS MANUAL

COMPUTER SECURITY
FIFTH EDITION

CHAPTERS 1–12

WILLIAM STALLINGS
LAWRIE BROWN

Copyright 2024: William Stallings &
Lawrie Brown

© Copyright 2024 by William Stallings & Lawrie Brown

All rights reserved. No part of this document may be reproduced, in any form or by any means, or posted on the Internet, without permission in writing from the author. Selected solutions may be shared with students, provided that they are not available, unsecured, on the Web.

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

NOTICE

This manual contains solutions to the review questions and homework problems in *Computer Security, Fifth 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:

https://pearsonhighered.com/stallings

File name is S-CompSec5e-mmyy.

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

TABLE OF CONTENTS

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

CHAPTER 1 OVERVIEW

ANSWERS TO QUESTIONS

1.1 Computer security refers to protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

1.2 **Passive threats** 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 threats** 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 Fundamental security design principles include:

- **Economy of mechanism**: means that the design of security measures embodied in both hardware and software should be as simple and small as possible.
- **Fail-safe defaults**: means that access decisions should be based on permission rather than exclusion.
- **Complete mediation**: means that every access must be checked against the access control mechanism.
- **Open design**: means that the design of a security mechanism should be open rather than secret.
- **Separation of privilege**: means the practice in which multiple privilege attributes are required to achieve access to a restricted resource
- **Least privilege**: means that every process and every user of the system should operate using the least set of privileges necessary to perform the task.
- **Least common mechanism**: means that the design should minimize the functions shared by different users, providing mutual security.

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

- **Psychological acceptability**: implies the security mechanisms should not interfere unduly with the work of users and at the same time should meet the needs of those who authorize access.
- **Isolation**: is a principle that applies in three contexts. First, public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering. Second, the processes and files of individual users should be isolated from one another except where it is explicitly desired. And finally, security mechanisms should be isolated in the sense of preventing access to those mechanisms.
- **Encapsulation**: is a specific form of isolation based on object-oriented functionality. Protection is provided by encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points.
- **Modularity**: in the context of security 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**: refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
- **Least astonishment**: means a program or user interface should always respond in the way that is least likely to astonish the user.

1.5 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

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

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

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

a low potential impact from a loss of availability. Examples from FIPS 199.

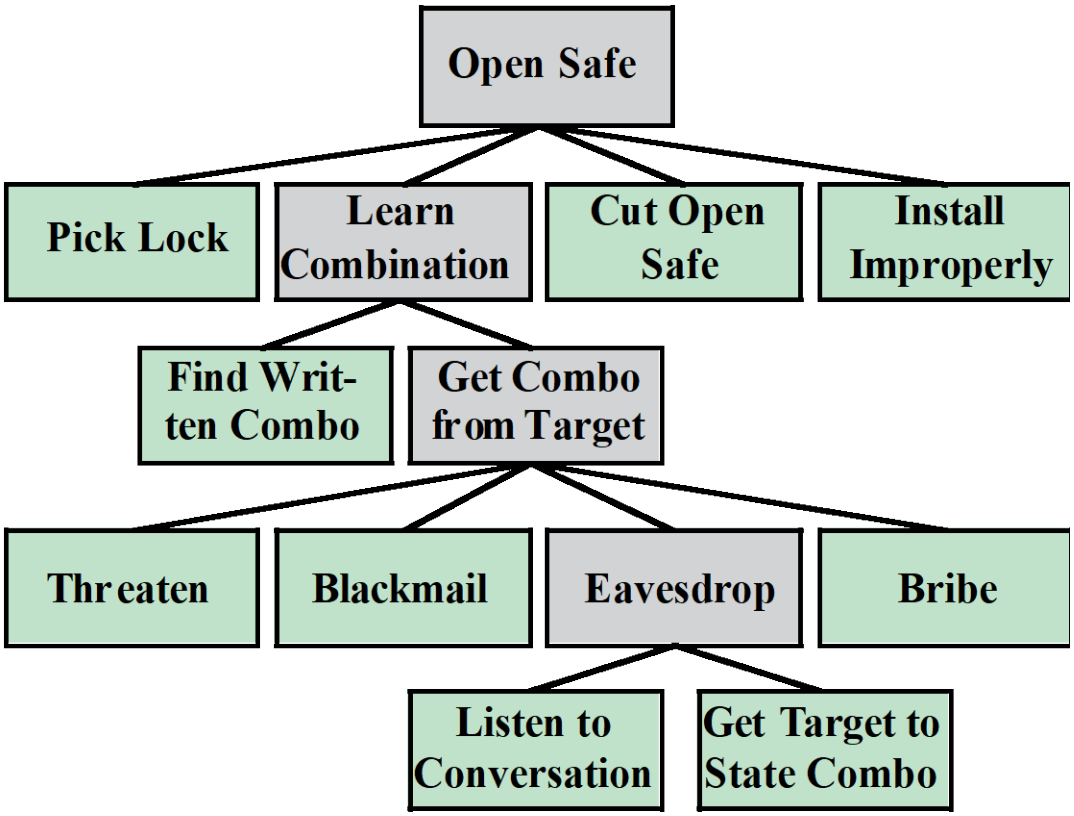
1.5 a. At first glance, this code looks fine, but what happens if IsAccessAllowed fails? For example, what happens if the system runs out of memory, or object handles, when this function is called? The user can execute the privileged task because the function might return an error such as ERROR NOT ENOUGH MEMORY.

b.

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == NO_ERROR) {
    // Secure check OK.
    // Perform task.
} else {
    // Security check failed.
    // Inform user that access is denied.
}
```

In this case, if the call to IsAccessAllowed fails for any reason, the user is denied access to the privileged operation.

1.6



Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

1.7 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

1.8 No general answer, as will depend on papers chosen and quality of summary.

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

CHAPTER 2 CRYPTOGRAPHIC TOOLS

ANSWERS TO QUESTIONS

2.1 **Plaintext:** This is the original message or data that is fed into the algorithm as input. **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext. **Secret key:** The secret key is also input into the encryption algorithm. The exact substitutions and transformations performed by the algorithm depends on the key. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

2.2 One secret key.

2.3 (1) a strong encryption algorithm; (2) Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

2.4 Message encryption, message authentication code, hash function.

2.5 A **message authentication code** (MAC) is a complex function of both the message or data to be authenticated and a secret key. The message plus code are transmitted to the intended recipient.

2.6 **(a)** A hash code is computed from the source message, encrypted using symmetric encryption and a secret key, and appended to the message. At the receiver, the same hash code is computed. The incoming code is decrypted using the same key and compared with the computed hash code. **(b)** This is the same procedure as in (a) except that public-key encryption is used; the sender encrypts the hash code with the sender's private key, and the receiver decrypts the hash code with the sender's

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

SOLUTIONS TO PRACTICE PROBLEMS

COMPUTER SECURITY
PRINCIPLES AND PRACTICE
FIFTH EDITION

WILLIAM STALLINGS
LAWRIE BROWN

Copyright 2024: William Stallings & Lawrie Brown

TABLE OF CONTENTS

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.

CHAPTER 1 OVERVIEW

1.1 All of these activities could create the right conditions to threaten the network.

a. The regular daily courier is familiar to employees, so they may not notice anything is wrong should that person walk into the server room.

b. Even with good severance packages and benefits, employees who lost their jobs due to downsizing may be disgruntled.

c. An employee's traveling to another location may not create a threat, but if the employee has a laptop computer that contains private information or the Web browser has saved passwords, then if the laptop is stolen, a hacker has gained valuable information.

d. If the sprinkler system went off, it could damage the company's servers and other computing equipment.

1.2 With reference to the Security Concepts and Relationships shown in Figure 1.2 in the text.

a. **asset** (or system resource) - something of value to the organisation; eg. Data; a service provided by a system; a system capability; an item of system equipment; a facility housing operations and equipment.

attack - An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate the security policy of a system.

risk - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

The relationship between them is that a risk is the likelihood of loss caused by some asset vulnerability being realised in an attack.

b. In this example: the asset is the users internet banking credentials; the attack is the use of "drive-by-download" to compromise browser to reveal the users banking credentials; the risk is the likelihood that the user will lose their credentials via this attack and hence that the attacker is able to steal money from their account.

Copyright © 2024, 2018, 2015 by Pearson Education, Inc. or its affiliates.