Answers are in blue.

# For Exercises 1–27, mark the answers true or false as follows:



**Computer Science Illuminated, Seventh Edition**

Nell Dale, PhD; John Lewis, PhD

**CHAPTER 17**

EXERCISES AND ANSWERS

1. **True**
2. **False**
   1. Information integrity ensures that data can be modified only by appropriate mechanisms.

A

* 1. Pairing threats with vulnerabilities is a part of risk analysis. A
  2. Smart cards are the most popular form of authentication cre- dentials currently used.

B

* 1. Biometrics is a type of user authentication that relies on the user having a smart card or a card with a readable magnetic strip.

B

* 1. A password should not resemble anything that looks like a word or phrase in a language that humans speak.

A

* 1. CAPTCHA is a software mechanism that authenticates a par- ticular user before allowing him or her to post a comment to a blog.

B

* 1. The reCAPTCHA project serves a secondary purpose—to help digitize books.

A

* 1. The cost of fingerprint analysis has dropped significantly in recent years, and fingerprint analysis is now regularly built into laptop computers.

A

* 1. The Touch ID biometric system uses retinal scans for user validation.

B

* 1. A computer virus “infects” another program by embedding itself into that program.

A

* 1. The terms “Trojan horse” and “worm” are used interchange- ably to describe a particular category of malicious code.

A

* 1. A logic bomb is set to go off when a particular system event occurs, such as a particular date and time.

A

* 1. Antivirus software is not effective against non-virus types of malware.

B

* 1. A password-guessing program uses dictionaries to try thou- sands of potential passwords each second.

A

* 1. Phishing is a technique that uses deceptive emails and web sites to obtain user information such as usernames and passwords. A
  2. A back-door threat is implemented by a programmer of the system under attack.

A

* 1. A denial-of-service attack does not directly corrupt data. A
  2. Decryption is the process of converting plaintext into ciphertext.

B

* 1. A cipher is an algorithm used to encrypt and decrypt text. A
  2. A transposition cipher is an example of modern cryptography. B
  3. In public-key cryptography, each user has two related keys, one public and one private.

A

* 1. A digital signature allows the recipient to verify that the mes- sage truly originates from the stated sender.

A

* 1. The Internet can create a false sense of anonymity. A
  2. Users of social media sites make good use of the controls available to protect their information online.

B

* 1. A website’s security policy describes the constraints and behaviors that an organization embraces regarding informa- tion management.

A

* 1. Many mobile phones collect and store location data that can then be read and used by third parties, such as law enforcement.

A

* 1. WikiLeaks founder Julian Assange is currently in prison in the United States.

B

# Exercises 28–55 are short answer.

* 1. What is the CIA triad of information security?

The CIA triad represents the three core aspects of informa- tion security: confidentiality (protection from unauthorized access), integrity (ensuring data can only be modified appro- priately), and availability (the degree to which valid users can access data).

* 1. Other than those presented in this chapter, give three exam- ples of data integrity violations.

Data integrity ensures that data can only be modified by appropriate mechanisms. For example, even though a per- son who works at Facebook might be able to access your posts, you wouldn’t want him or her to change them. You wouldn’t want a backup to be restored so that improper information is made available. And you wouldn’t want the software to inappropriately put the wrong privacy settings on a post.

* 1. What are the three general approaches to presenting autho- rization credentials?

Authorization credentials can be presented using something the user knows, like a password; something the user has, like a smart card; or something the user is physiologically, like fingerprints.

* 1. List at least four guidelines related to password creation and management.

Some guidelines for password management: (1) easy to remember, but difficult for others to guess, (2) don’t write passwords down, (3) use combinations of character types in passwords (upper and lowercase letters, digits, etc.), (4) don’t send your password in an email. There are several other guidelines that could be included.

* 1. Is “diningroom” a good password? Why or why not?

The word “diningroom” is not a good password because it is made up of simple words, without special characters, that can be easily guessed by a password guessing program.

* 1. Is “fatTony99” a good password? Why or why not?

The word “fatTony99” is a moderately good password in that it has a combination of uppercase and lowercase letters and includes digits. It could be improved by making it even less easy to map to real words.

* 1. What is password management software?

Password management software are applications that track your authentication information in a secure manner.

* 1. What is the goal of a CAPTCHA interaction?

The goal of a CAPTCHA interaction is to verify that the per- son filling out a web form is indeed a human being and not an automated program. It does not identify a particular user.

* 1. What are the dual purposes of the reCAPTCHA system?

The dual purposes of the reCAPTCHA system are to verify that the user is human and to help digitize books (or other- wise augment OCR projects).

* 1. What is Apple’s Touch ID technology used for?

Apple’s Touch ID technology is used to authenticate users on recent versions of the iPhone using fingerprint recognition technology. In particular, users can choose to be able unlock their phones by gently placing their finger on the button.

* 1. What do we mean when we say a computer virus is self- replicating?

A computer virus is self-replicating in that it copies itself into another program, “infecting” it.

* 1. Describe the two techniques used by antivirus software to identify malware.

The two general techniques that antivirus software uses to identify malware are (1) signature detection, which looks for recognizable patterns of specific, known malware programs, and (2) the use of heuristics, which look for more general pat- terns (based on know malware but not exactly like it) in order to find mutated versions of the original malware.

* 1. Describe a hypothetical scenario, other than the one described in this chapter, of a phishing attack.

Sample phishing attack: You’re sent an email, supposedly from your bank, that tells you to log onto their website and update your account for some important reason. In the email is a link that looks like it will open a page on your bank’s website. In reality, the link opens a website that is made to look like your bank’s site, but isn’t. When you attempt to log in, your credentials are secretly stored or sent to the phishing author, and you receive an error message to try again later. Now the malware creators have your login information and you may not ever realize it.

* 1. Describe how a Trojan horse attacks a computer system.

A Trojan horse is a program that appears to be helpful in some way, but actually causes a problem when executed. It’s simply malicious code disguised as a program you want to run.

* 1. Describe a buffer overflow and how it might make a com- puter system vulnerable.

A buffer overflow occurs when too much data is provided and cannot fit into it’s designated area in memory. In some systems, this could cause a program to crash and leave the user in a state with inappropriate (high) authority levels. Some attacks deliberately try to exploit a buffer overflow problem to gain such access.

* 1. How does a man-in-the-middle attack work?

A man-in-the-middle attack occurs when information being transferred across a network is intercepted at some network communication point. The information may then be for- warded to its destination so that the sender or receiver is not even aware it was intercepted.

* 1. Using a Caesar cipher, shifting three letters to the right, encrypt the message “WE ESCAPE TONIGHT.”

Using a three-shift Caesar cipher, the message “WE ESCAPE TONIGHT” would be encrypted as “ZH HVFDSH WRQLJKW”.

* 1. Using the Caesar cipher described in this chapter, decrypt the message “WJNSKTWHJRJSYX FWWNAJ RTSIFD.” Using the Caesar cipher described in this chapter, the mes- sage “WJNSKTWHJRJSYX FWWNAJ RTSIFD” is decoded into the message “REINFORCEMENTS ARRIVE MONDAY”.
  2. Using the transposition cipher technique used in this chapter, encrypt the message “WHO IS THE TRAITOR.”

Using the transposition cipher technique in this chapter the message “WHO IS THE TRAITOR” is encrypted as “TORITTOHWIHRAES.”

* 1. Describe how Claire would send a message to David using public-key encryption.

Claire sends a message to David using public-key encryption by first obtaining David’s public key and using it to encrypt the message. Then she sends the encrypted message to David, who decrypts it with his private key.

* 1. What is a digital signature?

A digital signature is a way to “sign” a document to verify the identity of the sender. The signature is created by com- pressing the message into a digest and encrypting it with the sender’s private key. The receiver uses the sender’s public key to decrypt the digest and compare it to the message itself.

* 1. What does a website’s security policy describe?

A website’s security policy describes the constraints or behav- ior of an organization in terms of how it uses the information that is provided by the users of the site.

* 1. What is GPS? How is it used to support cell phone applications?

GPS stands for Global Positioning System, which allows satellites to pinpoint the location of any GPS receiver. Cell phones often have these receivers allowing applications that run on the phones to identify their location and present maps and directions in context.

* 1. What abuses are possible given the current state of cell phone data collection?

Currently, cell phone companies are logging and collecting information from your phone, including GPS data and WiFi hotspot locations. Some law enforcement agencies have

been using this data to track a person’s detailed movements. There have been reports of police gathering this information without a warrant during routine traffic stops.

* 1. What is a wiki?

A wiki is a website that allows its content to be created and edited by multiple users. For example, the articles at Wikipe- dia, the online encyclopedia, can be updated by any regis- tered users.

* 1. What is WikiLeaks? Is it a wiki?

WikiLeaks is an organization and website whose goal is to disseminate classified data to the public. Although the WikiLeaks website was originally set up as a wiki, it no longer is. Its entries are only updated by the WikiLeaks managers.

* 1. Who is Julian Assange?

From the text: “The founder of WikiLeaks, Julian Assange, is a former hacker and programmer. For many years he was constantly on the move, living for only a brief time in one of dozens of countries before moving on. In 2012, Ecuador granted Assange political asylum, which has been his base of operations since.”

* 1. Describe the recent security issues regarding the WikiLeaks archives.

In September of 2011, it became known that a large set of unredacted U.S. government documents had been available for download for months from the WikiLeaks site, and that the encryption key to decrypt them was available as well. Then, in 2016, WikiLeaks released emails that had been sto- len from presidential candidate Hilary Clinton.