Survey of Operating Systems 6th edition Holcombe Solutions Manual

SKU: 9781260096002-SOLUTIONS

Survey of Operating Systems - Sixth Edition

Instructor Manual

Chapter 2

Computer Security Basics

Learning Outcomes

In this lesson you will provide students with an overview of security basics for computer users. At the end of the lesson students should be able to:

LO 2.1 Describe security threats and vulnerabilities to computers and users.

LO 2.2 Identify methods for protecting against security threats.

LO 2.3 Troubleshoot common security problems.

Estimated time for lesson: 3 to 4 hours

Preparing for Class

Technology moves fast, but nothing seems to change as fast as security threats and the technology developed in response to these evolving evils. At the time of this writing, all major software vendors even remotely affected by security threats were announcing plans for major updates to address threats, especially those in the form of viruses, spyware, and adware. There were also new concerns about threats accessing Bluetooth connections and vulnerabilities in the expanding area of the Internet of Things. Therefore, be prepared to bring the students up-to-date on both newly evolved threats (there seems to be no lack of creativity in that area) and newly evolved defenses against the threats.

Whenever possible, demonstrate new products—especially free products—that will aid them in their fight against such predation.

This chapter contains two Step-by-Step exercises and five *Try This* activities. Review them before the start of class so that you are prepared for any additional information the students may need to complete them, depending on the computers and time available.

Prerequisites for Class

Ensure that the students are:

- Comfortable with basic computer skills (mouse, keyboard, and touch screen use).
- Able to access a running lab computer either individually or in small groups.
- Able to browse the Internet and capable of using a Web browser from the available devices.

Class Preparation Notes

Ensure that all lab computers are returned to the default settings. If that is not possible, at least ensure that all lab systems are running the same version of Windows, or other selected OS, with the same components installed. If another person or department is responsible for the lab computers, make sure that you are personally familiar with any security measures implemented on the computers and whether OS components are used, or third-party security is in effect. Test all the hands-on activities so that you will know beforehand if there is any conflict with the computers as configured.

Take time to review these activities beforehand so that you can gauge how much time you should

Survey of Operating Systems 6th edition Holcombe Solutions Manual

devote to them, depending on the level of the students.

General Teaching Tips

Depending on the level of the students, this information on security threats can be intimidating. Therefore, as they move through the long list of threats, assure them that they will soon learn behaviors that will make them less vulnerable to threats, and they will learn about software that will protect them and/or remove the damage from other threats.

Key Terms

Teaching Tip:

We present many of these terms in a simplified form for the audience, with narrow definitions. You may choose to present broader definitions, depending on the level of the students.

administrator account type—A user account with permission to perform system-wide tasks.

adware—A form of spyware software that collects information about the user in order to display user-targeted advertisements.

authentication—Validation of a user account and password that occurs before the security components of an OS give a user access to the computer network.

authorization—The process of both authenticating a user and determining the permissions that the user has for a resource.

back door—A way to bypass security and gain access to a computer.

bitcoin—An online payment system.

black hat hacker—Someone with a great deal of computer programming skills who invades private computers and networks, exploring computer system weaknesses to take advantage of the system or systems, for illegal and possibly terroristic purposes.

Bluesnarfing—The act of covertly obtaining information broadcast from wireless devices using the Bluetooth standard, a short-range wireless standard used for data exchange between computers and mobile devices.

bot herder—A person who initiates and controls a botnet.

botnet—A group of networked computers that, usually unbeknown to their owners, have been infected with programs that forward information to other computers over the network. A bot, short for robot, is a program that acts as an agent for a user or master program, performing a variety of functions for good or evil.

browser hijacking—This occurs when malware alters a browser so that the home page points to a site other than the user's choice. This is often a site advertising some product, such adware removal software.

click bait—Click bait is content designed to lure you to click on it and its associated link in order to open a web page or run a video.

content filter—In an Internet browser, software that blocks content.

cookies—Very small text files an Internet browser saves on the local hard drive at the request of a web site. Cookies may contain user preferences for a specific site, information

Survey of Operating Systems 6th edition Holcombe Solutions Manual

entered into a form at a web site (including personal information), browsing activity, and shopping selections made at a web site.

cybercrime—Illegal activity performed using computer technology.

cybercriminal—A person who breaks laws using computer technology.

cyberterrorism—The use of computers to cause destruction without regard to its effect on humanity.

cyberterrorist—Someone who uses a computer to cause destruction without regard to its effect on humanity.

data wiping—The permanent removal of data from a storage device.

digital certificate—A special file stored on a computer that may hold a secret key for decrypting data.

DMZ—Named for a wartime demilitarized zone, a network between the internal network and the Internet with a firewall on both sides. This is where an organization puts any servers that it wishes to have offer services over the Internet.

drive-by download—A program downloaded to a user's computer without consent. Often the simple act of browsing to a web site or opening an HTML email message may result in such a surreptitious download. A drive-by download may also occur when installing another application.

email spoofing—The act of forging an email address by modifying the sender's address in the email message's header (the information that accompanies a message but does not appear in the message).

Encrypting File System (EFS)—An NTFS file encryption feature introduced with Windows 2000 and NTFS5.

encryption—The transformation of data into a code that can only be decrypted using a secret key or password.

exploit—A malware attack that takes advantage of some vulnerability in our computers or networks.

FileVault—A feature of macOS that will encrypt all the files in the Home folder.

firewall—A hardware device or software that protects a network or computer by examining traffic and rejecting certain traffic based on a set of rules.

first-party cookie—A cookie that originates with the domain name of the URL to which you directly connect.

forged email address—An address that may appear but is in reality fake or forged.

fraud—The use of deceit and trickery to persuade someone to hand over money or other valuables.

group account—A security account that may contain one or more individual accounts. Some security accounts databases may contain other groups.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

guest account—A special account used when someone connects to a computer over a network but is not a member of a security account recognized on that computer. That person connects as a guest (if the guest account is enabled) and will only have the permissions assigned to the guest account.

hacker—Someone with a great deal of computer programming skills who invades private computers and networks.

header—The information that accompanies a message but does not appear in the message.

honeypot—A server created as a decoy to draw malware attacks and gather information about attackers.

hotspot—A Wi-Fi network that connects to the Internet through a router.

identity theft—This occurs when someone collects personal information belonging to another person and uses that information to fraudulently make purchases, open new credit accounts, or even obtain new driver's licenses and other forms of identification in the victim's name.

keylogger—Another name for a keystroke logger.

keystroke logger—Software or a hardware device that monitors and records every keystroke entered at a computer.

malware—Malicious software. Any software security threat.

Microsoft family—A service in which a Microsoft account holder can create new accounts for family members or invite a relative with a Microsoft account to join the family. It also offers security tools for family members.

Parental Controls—A feature of Windows 7 that allows parents to protect their children from harm while surfing the Internet. Replaced by Family Safety.

password—A confidential string of characters that a user enters (along with a user name) to be authenticated.

password cracker—A program used to discover a password.

password manager—Software used to create strong passwords, storing credentials for many sites, and automatically filling in these credentials when needed.

permission—An action that may be performed on an object, such as a computer, file, or folder.

phishing—A fraudulent method of obtaining personal financial information through web page pop-ups, email, and even via letters mailed via the postal service.

pop-up—An ad that runs in a separate browser window that you must close before you can continue with your present task.

pop-up blocker—A program that works against pop-ups.

pop-up download—A program that is downloaded to a user's computer through the use of a pop-up page that appears while surfing the Web.

ransomware—Malware that threatens to do damage or lock the victim out of a computer unless he or she pays a fee.

rootkit—Malware that hides itself from detection by anti-malware programs by concealing

Survey of Operating Systems 6th edition Holcombe Solutions Manual

itself within the OS code or in any other program running on the computer.

scareware—Similar to a Trojan Horse (see below), an advertisement that appears to be something harmless and that offers to take some action, such as pretending to scan your computer for problems, but the results will be bogus. It offers to fix the problems it claims to find and asks for payment to support charities. Scareware threats state that you must donate or it will delete critical files.

secret key—A special code that can be used to decrypt encrypted data.

Secure HTTP (HTTPS)—An enhancement to the HTTP protocol that encrypts communications using the Secure Sockets Layer (SSL) security protocol.

Secure Sockets Layer (SSL)—A protocol used to encrypt messages.

security account—In a security accounts database, a security account is a listing of information about a user, group, or computer. A user or computer account is used for authentication; both user and group accounts are used for authorization with assigned permissions.

shoulder surfing—The act of reading information off a screen over the shoulder of the victim.

social engineering—The use of persuasion techniques to gain the confidence of individuals.

social media—Any service (Internet-based or other) that provides a place where people can interact in online communities, sharing information in various forms. Community members generate social-media content.

social networking—The use of social media.

spam—Unsolicited email, (most often seeking financial gain for the sender). This includes email from a legitimate source selling a real service or product, but if you did not give them permission to send such information to you, it is considered spam.

spam filter—Software designed to combat spam by examining incoming email messages and filtering out those that have characteristics of span, including certain identified keywords.

spear phishing—A targeted phishing attack where the target is usually one that has a high probability of delivering a very valuable return.

spim—An acronym for "Spam over Instant Messaging;" the perpetrators are called spimmers.

spyware—A category of software that runs surreptitiously on a user's computer, gathers information without permission from the user, and then sends that information to the people or organizations that requested the information.

standard user account—An ordinary user account without administrator status.

third-party cookie—A cookie that originates with a domain name beyond the one shown in your URL.

token—A physical device that can be used in authentication, either alone or together with a

Survey of Operating Systems 6th edition Holcombe Solutions Manual

user name and password.

Trojan horse—A program that is installed and activated on a computer by appearing to be something harmless, which the user innocently installs. This is a common way that a virus or a worm can infect a computer.

user account—A security account that is assigned to a single person and contains, at minimum, a user name and password used to authenticate a user.

User Account Control (UAC)—Beginning in Windows Vista, a feature that prompts a user (even an administrator type account) when the user or any software attempts to perform a function requiring administrator permissions.

user right—In Windows, the privilege to perform a system wide function, such as access the computer from the network, log on locally, log onto a computer from the network, back up files, change the system time, or load and unload device drivers.

vector—A mode by which malware infects a computer.

virus—A program that is installed and activated on a computer without the knowledge or permission of the user. At the least the intent is mischief, but most often it intends to be genuinely damaging in one way or another.

war driving—The act of moving through a neighborhood in a vehicle or on foot, using either a laptop equipped with Wi-Fi wireless network capability or a simple Wi-Fi sensor available for a few dollars from many sources. War drivers seek to exploit open hotspots, areas where a Wi-Fi network connects to the Internet without the use of security to keep out intruders.

white hat hacker—Someone with a great deal of computer programming skills who invades private computers and networks, exploring computer system weaknesses for the purpose of making systems more secure.

worm—A self-replicating computer virus.

zero-day exploit—A software vulnerability unknown to the publisher of the targeted software. When someone devises a way to exploit that vulnerability (often with a virus), it is often very difficult to protect against such a threat.

zombie—An individual computer in a botnet, so-called because it mindlessly serves the person who originated the botnet.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

Survey of Operating Systems - Sixth Edition

Instructor Manual

Chapter 2

Lecture Outline

I. LO 2.1 Threats to Computers and Users

Teaching Tip:

This section consists of several pages of information on threats to computers and users. Students will have heard of many of these concepts, but this may be the first time they are being formally presented to them. This text is broken up with three Try This activities that will encourage them to research the latest information on spam, phishing frauds, and identity theft. They can even take a phishing IQ test. Allow time for these activities because they will help the students assimilate all this information.

Discussion Point:

Try to avoid going into detail on actions to take to protect against these threats until you move on to the next major section, Defense Against Threats.

A. Introduction to LO 2.1

Risks of insecure computer or mobile devices.

Identity

Work you created

Employer's integrity

Your job

Government regulations require organizations to protect certain personal information.

Cybercrime is illegal activity using computer technology.

B. Malicious Tools and Methods

Survey of Operating Systems 6th edition Holcombe Solutions Manual

Malware=malicious software

Malware development a large industry

Targets all computing devices

Great growth in malware targeting mobile devices

1. Vectors

Discussion Point:

To introduce vectors, ask the students if they have ever heard the term vector used outside of computer malware? They may have heard of vectors in reference to human viruses. Talk about the similarity between human viruses and malware.

i) **Click bait** is content designed to lure the user to click on it to open a web page or run a video.

ii) **Social networking**

a) Using **social media**, such as a social networking site, to communicate with others.

b) Social networking is a vector for malware and **social engineering** because it's a rich source of personal information that many who use social networks seem willing to share.

Teaching Tip:

Take a moment to allow students to do the Try This! Activity titled More About Social Media.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

iii) Email

iv) Malicious Code on Web sites

v) **Trojan Horse**—malware disguised as a harmless program.

vi) **Scareware** is a threat that causes to you act out of fear.

vii) Searching for unprotected computers

viii) Sneakernet—the oldest vector

ix) **Back Door**—a method for gaining access to a computer, bypassing authentication security.

x) **Rootkits**—malware that hides within OS or other program.

xi) **Pop-up Download** – malware installed through a **pop-up** on a web page.

xii) **Drive-By Download** – a program installed without consent; often by browsing to a website, opening an HTML email message, or during a program installation.

xiii) War Driving

a) The act of moving through a neighborhood using either a laptop equipped with Wi-Fi wireless network capability, or a simple Wi-Fi sensor searching for open **hotspots**.

b) War drivers may also leave a sign of an open hotspot by "war chalking"

c) Web sites and videos show how to war drive

xiv) **Bluesnarfing**

a) Like war driving with Bluetooth signals

2. Password theft

i) **Password** is a string of characters entered, along with an identifier.

ii) Stealing passwords through websites

iii) Stealing passwords with **password crackers**

Survey of Operating Systems 6th edition Holcombe Solutions Manual

iv) Stealing passwords with **keystroke logger** (**keylogger**)

3. Zero-Day Exploits

i) Used as both a noun and verb. An **exploit** is something that takes advantage of an opportunity as well as the action of doing so. Not

Survey of Operating Systems 6th edition Holcombe Solutions Manual

in itself a bad thing. A malware attack is called an exploit because it takes advantage of a vulnerability in computers or networks.

ii) A **zero-day exploit** occurs when someone devises a way to exploit a previously unknown vulnerability.

4. **Viruses**

i) A program installed and activated without the knowledge or permission of the user

ii) Mischief or damaging results

5. **Worms**

i) A virus that self-replicates

ii) Travel between computers via many vectors

iii) Netsky and MyDoom worms generated disabling amounts of network traffic

iv) Nimda inserted its code into other executable files on the local drive of each machine

6. Botnets and Zombies

i) **Botnet** is a group of network computers

ii) Infected with programs that forward information to other computers

iii) Bot (short for robot) program acts as an agent

iv) Can be used for good or evil

v) **Zombie** is a computer working mindlessly as part of the botnet

vi) **Bot herder** is someone who initiates and controls a botnet

7. **Spyware**

i) Gathers information and sends it to the people who requested it

ii) Tracks surfing or buying patterns for marketing

iii) Used for industrial espionage

Survey of Operating Systems 6th edition Holcombe Solutions Manual

iv) Law enforcement uses spyware to track sexual predators or other criminals

v) Governments use spyware to investigate terrorism

8. Adware

i) A form of spyware that collects information about the user in order to display advertisements targeted to the user, either in the form of inline banners or pop-ups

ii) Pop-ups run in a separate browser window that you must close before continuing

iii) Clicking to accept an offer presented in an inline banner or pop-up may trigger a pop-up download installing a virus or worm

9. Browser Hijacking

i) When your home page points to a site you didn't select

ii) Remedy by changing default home page in options unless the browser was modified so that options are not available

10. Spam and Spim

i) **Spam**

a) Unsolicited email

b) May be from legitimate sources selling real services or products

c) May involve a scam.

d) Perpetrators of spam are called spammers

Teaching Tip:

Take a moment to allow students to do the Try This! Activity titled Research Spam Statistics.

Discussion Point:

When a new Domain Naming System top-level domain (TLD) becomes available the authors have seen a flood of new spam originating from newly-created domains. For instance, the ninja and work TLDs are fairly new additions. Not everyone who acquired a second-level domain within one of these TLDs is a spammer, but there are enough new spams generated from these domains that we have blocked each entire TLD with our spam filters.

We have yet another experience with this scenario from a different point of view. In 2001 a new generic TLD (.biz) became available and the authors decided to register a domain name in this TLD. At that time, Jane managed mail and file-and-print servers in small businesses. She was surprised to receive an advisory recommending blocking all incoming mail from .biz

Survey of Operating Systems 6th edition Holcombe Solutions Manual

sources. This didn't last long, and the authors only recall one of their own emails that was rejected. That was remedied by a conversation with the email administrator at the recipient's company, Read the Wikipedia article on .biz to learn other interesting facts, like what "biz" means in Turkish (It's a good thing.)

ii) **Spim**

a) An acronym for Spam over Instant Messaging

b) Bots (or spimbots) collect instant messaging screen names

c) Typical spim message contains links to product web sites

d) Perpetrators are called spimmers

11. **Social Engineering**

Discussion Point:

When introducing this section, bring up some real world examples you may have experienced or learned about, and then ask if students have ever received a message they thought suspicious or that they discovered was not from the source it appeared to be from?

Survey of Operating Systems 6th edition Holcombe Solutions Manual

i) Uses persuasion techniques to gain the confidence of individuals.

ii) **Fraud**: The use of deceit and trickery to obtain money or other valuables.

a) One form of fraud, **ransomware**, is malware that threatens to do damage or lock out a user who doesn't pay them. Some ransomware claims to have proof that the victim committed an illegal act and threatens to report this to the authorities unless paid a ransom.

b) Online payment system, such as **bitcoin**, used for ransomware payments.

iii) **Phishing**: Fraudulent method of obtaining personal financial information through using pop-ups or email appearing to be from legitimate organizations.

a) Enticing bait in a message or pop-up.

b) **Spear phishing** is targeted.

c) **Forged email address** of someone you know and trust.

d) Message **header** contains sender's address.

e) **Email spooking.**

iv) Hoaxes

a) Take many forms

b) Example: an email message claiming to be from Microsoft and including a link to a web site for downloading a fix. Microsoft never sends out updates through email

v) Enticements to Open Attachments that may install malware on your computer

Teaching Tip:

Have the students do Step-by-Step 2.01, "Take a Phishing IQ Test!" This will take them a while to perform but it leads to a very rich discussion session on the subtleties that phishers use to fool victims.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

12. **Identity Theft**

    i) Personal information stolen in order to commit fraud

    ii) Obtaining a social security number and other key personal information is all that is needed to steal someone's identity

Teaching Tip:

Take a moment to allow students to do the Try This! Activity titled Learn More About Identity Theft.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

13. Exposure to Inappropriate or Distasteful Content

14. Invasion of Privacy

    i) Protect all personal information at banks and elsewhere.

    ii) **Shoulder surfing** is surreptitiously reading information from someone else's screen.

15. Misuse of Cookies

    i) **Cookies** may contain:

        a) User preferences from visiting a specific site

        b) Information you may have entered into a form at the Web site, including personal information

        c) Browsing activity

        d) Shopping selections on a web site

    ii) Cookies can be a convenience to a user

    iii) Most good web sites describe how they use cookies and what they use them for in a privacy statement.

    iv) **First-party cookies** originate with the domain name of the URL to which you connect.

    v) **Third-party cookies** originate with a domain name beyond the one shown in your URL. Source can be an ad embedded in a Web page.

16. Computer Hardware Theft

    i) Physical security best protection.

    ii) Mobile devices more vulnerable to theft.

C. Accidents, Mistakes, and Disasters

1. Accidents, mistakes, and disasters happen.

2. Prepare with frequent backups.

D. Keeping Track of New Threats

1. Federal Trade Commission (FTC) Bureau of Consumer Protection (www.ftc.gov/bcp)

E. The People behind the Threats (Cybercriminals)

Survey of Operating Systems 6th edition Holcombe Solutions Manual

1. Organized Crime
2. **Cyberterrorists** and **cyberterrorism**
3. **Hackers**
4. Crackers—**black hat hackers** vs **white hat hacker**
5. Script Kiddies
6. Click Kiddies
7. Packet Monkeys

II. LO 2.2 Defense Against Threats

A. Education

1. Computer symptoms to watch for:
   - i) Strange screen messages
   - ii) Sudden computer slowdown
   - iii) Missing data
   - iv) Inability to access the hard drive
2. Non-computer activities of concern:
   - i) Charges on credit accounts that you are sure you or your family did not make
   - ii) Calls from creditors about overdue payments on accounts you never opened
   - iii) A turndown when applying for new credit, for reasons you know are not true
   - iv) A credit bureau report of existing credit accounts you never opened

B. Paranoia 101: Don't Be a Victim

Survey of Operating Systems 6th edition Holcombe Solutions Manual

1. Nothing is Free
    i) Example: Free email accounts
        a) Some use metadata from email messages
        b) Others also scan email content
    ii) Configure security and privacy settings for all accounts
2. What Can You do to Protect Yourself?
    i) Security and Privacy controls for all accounts.
    ii) Do you really need free services?
    iii) Consider your own domain name and email service.
3. What Are You Revealing about Yourself?
    i) Your online behavior reveals personal information
        a) Playing games
        b) Enabling apps within social media
        c) Responding to online surveys
    ii) Responses to simple questions adds to the store of data on you
4. Resist Click Bait
5. Government regulations slowly coming.
    i) European Commission's General Data Protection Regulation (GDPR)
    ii) Some legislation in process in the United States Congress.

C. Security Policies

Survey of Operating Systems 6th edition Holcombe Solutions Manual

1. Define data sensitivity and data security practices

2. Exist in both document form and software form

   i) Administrators configure computer security to enforce written policy

   ii) Password policy should require strong passwords and state the complexity requirements that are enforced on computers

D. Firewalls—hardware device or software that examines network traffic.

1. Network-based Firewalls

   i) Firewall Technology

      a) IP packet filter

      b) Proxy service

      c) Encrypted authentication

      d) Virtual private network (VPN)

   ii) DMZ

      a) A network between private and public network.

      b) Servers accessed from public side are in DMZ.

      c) Protects private side.

      d) **Honey pot**: a decoy server for drawing malware attacks. May be placed with other servers in DMZ.

Teaching Tip:

Inform the students that the professionals who work with dedicated firewalls for large organizations must be highly-trained and are usually well-compensated for a job that carries a great deal of responsibility.

1. Personal Firewalls

   i) Come with most OSs

   ii) Come with third-party security software

Discussion Point:

Survey of Operating Systems 6th edition Holcombe Solutions Manual

The margin Note on page 56 mentions honey pot, *a decoy server used to attract malicious attackers. Consider discussing the use of such methods to catch criminals of all sort. For instance, sexual predators are lured by law enforcement officers posing as potential victims.*

Survey of Operating Systems 6th edition Holcombe Solutions Manual

E. Security Software

1. Antispam Software—Spam Filter
    i) On email clients.
    ii) On central mail servers.
    iii) Internet-based.
2. Antivirus Software
    i) Examine contents of storage and RAM.
    ii) Require frequent updating
3. Pop-Up Blockers
    i) In free and commercial security programs
    ii) Feature of browsers
    iii) Configure to exclude or include (as exceptions) sites
4. Privacy Protection and Cookies
    i) Privacy settings include several features
    ii) Individual settings for first-part and third-party cookies
5. Parental Controls and Microsoft Family
    i) **Parental Controls** in macOS
        a) System Preferences window or
        b) Users and Groups dialog
    ii) Microsoft Family in Windows
        a) Service for Microsoft accounts
            1) Activity report
            2) Screen time limits
            3) Content restrictions
6. **Content Filtering**

Survey of Operating Systems 6th edition Holcombe Solutions Manual

i) Blocks or allows certain sites

ii) May be part of a multifunction package

iii) May be included in browser

iv) Services on Internet give ratings to web sites

v) Configure filter to allow or disallow unrated sites

7. Software Updates

i) Keep software updated with security patches

ii) Very old versions of Windows may not be supported by updates

Teaching Tip:

Allow time for students to do the Try This! Activity titled View the Windows Update History.

F. Authentication and Authorization

Survey of Operating Systems 6th edition Holcombe Solutions Manual

1. Authentication

i) Verification of who you are.

ii) One-factor authentication based on something you know, such as user name and password

iii) Two-factor authentication based on something you know plus something you have (a **token**)

a) ATM cash card is a token.

b) Online services send a one-time code.

c) Authenticator apps.

iv) Three-factor authentication may add biometric data such as a retinal scan, voiceprint, or fingerprint.

2. Automatic Login

i) All modern OSs require login

ii) If automatic login configured, no login box appears.

iii) Still authenticated with preconfigured name and password.

iv) Same credentials; same privileges

3. Authorization

i) Determines the level of access to a computer or a resource

ii) Includes both authentication, plus verification of access level (permissions and/or rights)

iii) **Permission** describes an action that can be performed on an object

iv) **User right** is a system-wide action a user or group may perform

G. Passwords

1. A password is a string of characters entered for authentication

2. Don't take passwords for granted

3. Do not use the same password everywhere

Survey of Operating Systems 6th edition Holcombe Solutions Manual

4. Basic defense against invasion of privacy/identify theft

5. Use long and complex passwords

6. Do not use common words

7. Use a **password manager** to create strong passwords and store all your credentials for all devices.

8. Best Practices with Passwords and Accounts

   i) You are at risk if you answer "yes" to any of the following:

      a) Do you have too many passwords to remember?

      b) Do you use the same password everywhere?

      c) Do you have your password written on sticky notes or your desk calendar?

      d) Have you used the same password for more than a few months?

      e) Reusing the same user name also puts user at risk

   ii) Create Strong Passwords

      a) A strong password is one that meets certain criteria, which change over time as hackers create more techniques and tools for discovering passwords

      b) Always use strong passwords for the following types of accounts:

         1) Banks, investments, credit cards, and online payment providers

         2) Email

         3) Work-related accounts

         4) Online auction sites and retailers

         5) Sites where you have provided personal information

   iii) Avoid Creating Unnecessary Online Accounts

      a) When a web site requests that you "join," question the benefits of joining

      b) Question why a web site needs information about you

Survey of Operating Systems 6th edition Holcombe Solutions Manual

iv) Don't Provide More Information than Necessary

a) Avoid creating accounts with web sites that request your social security number and other personal and financial information

b) Avoid having your credit card numbers and bank account information stored on a web site

c) Although it's not easy to do online, in person you can ask the following questions:

1) Why do you need it?

2) How will you protect it?

3) How will you use it?

4) What happens if I don't give it to you?

Teaching Tip:

Allow time for students to do the Try This! Activity titled Get Help Creating Passwords.

H. Security Account Basics

1. **Security account**: An account that can be assigned permission to take action on an object (such as a file, folder, or printer) or the right to take some action on an entire system, such as install device drivers into an

Survey of Operating Systems 6th edition Holcombe Solutions Manual

operating system on a computer. Or simply to log on to a computer or web site.

i) User Accounts

a) Assigned to a single person—can be created by administrator user

b) Contains (at minimum)

1) User name

2) Password

ii) Built-in User Accounts

a) Administrator (Windows)

b) Root (macOS and Linux)

c) Guest account

iii) Standard versus Administrator Accounts

a) **Standard user account** (previously *limited account* in Windows XP)

b) Administrator account type

Teaching Tip:

Point out that they can view the Windows Administrator account in the Local Users and Groups node of Computer Management. Show students that the Administrator account is disabled by opening the Administrator Properties in Local Users and Groups. Then (only if your computer does not belong to a Windows Domain) restart the computer in Safe Mode and sign in with the Administrator account.

iv) Group Accounts

a) Security account that contains one or more individual accounts

b) May contain other groups

c) Some built-in (Windows Administrators, Users, Guests)

d) Some software will create a special group account for use by the software

Teaching Tip:

Survey of Operating Systems 6th edition Holcombe Solutions Manual

This last point may be confusing. Point out that at one time, many programs ran with "System" privileges, which are all-powerful. Therefore, this practice was a huge security hole. Now, software that requires a special account to run will have an individual account with lesser privileges than those given to System.

e) Administrators can create others

v) Computer Accounts

a) Computers may have security accounts

b) Windows computers join an Active Directory Domain where an account is created for the computer

Discussion Point:

Tell students that if their school or work has a Windows Active Directory domain, Windows computers log on to the domain when they start up each day. Ask if they can think of why this would be true. See if they understand that this guarantees that the computers are not "rogue" computers. Of course, each user must also log on.

2. User Account Control (UAC)

Discussion Point:

Ensure that students understand the reason for UAC. The text explains the scenario, but students may miss the significance of the protection UAC gives you.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

i) Began in Windows Vista

ii) Prompts a user (even an administrator type account) when the user or any software attempts to perform a function requiring administrator permissions

iii) Two scenarios

a) A user logged on with an administrator type account only has privileges of a standard account until the user (or malware) attempts to do something privileged

1) UAC dims the desktop and displays the Consent Prompt

2) User must respond in order to continue.

b) User logged on as a standard type account

1) UAC dims the desktop and displays the Credentials Prompt

2) User must enter both a username and password of an administrator type account.

iv) UAC-type function in macOS

a) Certain dialog boxes have a lock symbol

1) If the lock is turned on, only "safe" actions can be completed

2) Unlocking a dialog box requires credentials; then you will see advanced settings

I. Best Practices When Assigning Permissions

1. Principle of least privilege

i) Assign permissions that allow each user only the level of access required to complete assigned tasks

ii) Do not give users more access than necessary

J. Encryption

1. The transformation of data into a code that you can decrypt only with a secret key or password

2. **Secret key** is a special code used to decrypt encrypted data

Survey of Operating Systems 6th edition Holcombe Solutions Manual

3. You can encrypt data before sending it over a network

   i) Most online methods use **digital certificate**:

   ii) A secret key in the form of a file stored on a computer

4. You can encrypt stored data files

5. Encrypting Network Traffic

   i) **Secure HTTP (HTTPS)** encrypts communications using **Secure Sockets Layer (SSL)** security protocol

Discussion Point:

Ask how many students do online banking or purchase items online. Ask if they know to look for the HTTPS protocol in the address box of the browser? Some browsers (Chrome, etc.) block sites without HTTPS or issue a warning to you.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

6. Windows Encrypting File System

   i) Windows NTFS file system includes **Encrypting File System (EFS)** for encrypting locally stored files.

7. Encrypting with Window BitLocker

   i) Windows BitLocker Drive Encryption a feature of some editions of Windows

   ii) BitLocker to Go encrypts external hard drives and flash drives.

8. Encrypting with macOS **FileVault**

   i) Enable in Security and Privacy Settings.

   ii) Encrypted files only available to user signed in with same credentials as the user who encrypted.

K. Data Wiping

1. Remove data from old computers before disposing of them

2. **Data wiping** is the permanent removal of data from storage

   i) Reformat of hard drive does not truly remove data

   ii) Data wiping software writes over data many times to completely erase it

   iii) Can wipe data on any rewritable storage device

   iv) On newer hard drives wiping programs use built-in Secure Erase

L. Physical Security

1. Limit access to building or room

2. Laptops and other mobile devices are more vulnerable

M. Security for Mobile Computing

   i) Be extra wary of the danger of theft

   ii) Encrypt sensitive and confidential data

III. LO 2.3 Troubleshooting Common Security Problems

A. Troubleshooting Log-on Problems

1. Caps lock key turned on

Survey of Operating Systems 6th edition Holcombe Solutions Manual

2. Too many log-on attempts

   i) Account locked out

   ii) Must wait for the lockout duration to expire or have administrator unlock.

Teaching Tip:

Please point out that they will probably only encounter the problem of being locked out after too many wrong passwords if they are logging on to a network. Setting the account lock out and other password policy settings is an advanced task, not usually applied to a computer unless it is logging on to a network server, as in the case of a desktop computer that is a member of a Windows Active Directory domain.

B. Using the Administrator Account in Troubleshooting

1. The local built-in Administrator account in Windows is disabled by default and does not have a password.

2. If a computer is not a member of a Windows Active Directory domain when starting in Safe Mode, you can log on with an Administrator account and attempt to troubleshoot.

Teaching Tip:

Please point out that they can view the Windows Administrator account in the Local Users and Groups node of Computer Management.

C. Troubleshooting a Suspected Malware Attack

1. Run a scan of all drives and memory

2. If no malware is found, try a reputable online scanner, such as Housecall by Trend Micro

Teaching Tip:

Step-by-Step 2.02—Perform an Online Virus Scan on a PC or Mac.

Extra Project One

After completing Lab Project 2.3 take the job titles you discovered through your research of a security certification and look online for a salary survey that includes one or more of the job titles. Then report on the job titles and salaries you find.

Project Solution

It will depend on the certification and job title.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

One example: Security+ is a certification that people have who hold the following job titles and salaries:

Job Title	Annual salary range
Information Technology Specialist	$44,636-66,711
Security Engineer, Information Systems	$59,212-83,868
Systems Administrator	$45,612 – 63,770
System Administrator, Computer/Network	$42,180 – 63,141
Senior Systems Administrator	$65,396 – 80,539

A high-end example: Certified Information Systems Security Professional (CISSP) can lead to the following job titles and median salary ranges:

Job Title	Annual salary range
Security Engineer, Information Systems	$75,171 – 102,417
Security Consultant, (Computing/Networking/Information Technology)	$74,075 – 107,213
Security Manager, IT	$83,030 – 112,344
Senior Network Engineer	$79,145 – 110,859
Information Technology (IT) Director	$85,519 – 129,590

Discussion Point:

Point out that the salary surveys often show several job titles with a range of salary. Just because a job title is associated with a certification does not mean that the certification is all that is required for the job. Many security-related jobs require on-the-job experience and additional certifications. Someone aiming for one of the higher-paid job titles related to security may need to start at a lower level, such as systems administrator (with qualifications for that role) before acquiring the experience to apply for the desired job.

Extra Project Two

You may decide to limit your exposure online, but you already have a history of using social media and eCommerce sites. There is a growing service industry centered on removing your online history. Can you do this yourself, without using an app? Research the steps for removing data from various online sites.

Project Solution

Answers will vary. An article published by ZDNet on September 20, 2018 describes this process. Briefly the tasks they recommend are:

- Use Google to search for information about you. Document what you find, including the

Survey of Operating Systems 6th edition Holcombe Solutions Manual

sites associated with the data.

- If you are an EU citizen, you have the right to be forgotten, but you must request this directly from such sites as Google, and they may not act.
- Use the HaveIBeenPwned service to see if any of your account information has been compromised.
- Tighten your Google Account settings, especially *Sign-in & Security* and *Personal Info & Privacy*.
- If you have social media accounts, explore the security settings and ensure that they will protect you.
- Delete & Deactivate Old Accounts.
- Remove old posts you may have made on social media or other places, such as a blogs.
- Sometimes, we want to make a single purchase from a site, and do not intend to be a regular customer. Consider having an extra email account for use with such sites.
- Use a Virtual Private network (VPN) to hide your IP address form the public.

Assessment Quiz

This extra quiz, not included in the text book, will test the knowledge students have gained during the lesson.

Questions

1. Logging on with something you know (username and password) plus something you have (fingerprint or a one-time authentication code) is known as _____ authentication.
2. A/an _____ is one that originates from a domain name beyond the one shown in the URL for the current web page, and it may be used by an ad embedded in a Web page to track your Web surfing habits.
3. The term "brute force" is used to describe one category of _____.
4. While browsing the Internet, Celine answered survey questions that appeared in a pop-up window and inadvertently became the recipient of a/an _____.
5. Harry's smartphone became the target of _____ via a wireless technology he normally uses for his headphones. Using this method, a stranger acquired Harry's address book.
6. No matter how you connect to the Internet, it is important for you to turn on and configure a/an _____ on the computer or device to monitor traffic to and from the network.
7. Configure _____ in macOS System Preferences to set specific restrictions on a child's Internet browsing.

Survey of Operating Systems 6th edition Holcombe Solutions Manual

8. A user and a group are examples of types of _____,
9. A very frustrated user complains that he has correctly entered his password several times, but was rejected each time. Experience has shown that leaving the _____ turned on is a frequent cause of failure to log on.
10. The oldest malware vector is called _____because malware moves from computer-to-computer by being carried by a person with a flash drive or other portable storage device.

Answers

1. Logging on with something you know (username and password) plus something you have (fingerprint or a one-time authentication code) is known as *two-factor* authentication.
2. A *third-party cookie* is one that originates from a domain name beyond the one shown in in the URL for the current Web page, and it may be to track your Web surfing habits.
3. The term "brute force" is used to describe one category of *password cracker*.
4. While browsing the Internet, Celine answered survey questions that appeared in a pop-up window and inadvertently became the recipient of a *pop-up download*.
5. Harry's smartphone became the target of *Bluesnarfing* via a wireless technology he normally uses for his headphones. Using this method, a stranger acquired Harry's address book.
6. No matter how you connect to the Internet, it is important for you to turn on and configure a *personal firewall* on the computer or device to monitor traffic to and from the network.
7. Configure *Parental Controls* in macOS System Preferences to set specific restrictions on a child’s Internet browsing.
8. A user and a group are examples of types of *security accounts*,
9. A very frustrated user complains that he has correctly entered his password several times, but was rejected each time. Experience has shown that leaving the *Caps Lock key* turned on is a frequent cause of failure to log on.
10. The oldest malware vector is called *sneakernet* because malware moves from computer-to-computer by being carried by a person with a flash drive or other portable storage device.

Survey of Operating Systems 6th edition Holcombe Solutions Manual