



Objectives

- ❑ Describe several types of computer crime and discuss possible crime prevention techniques.
- ❑ Describe the major security issues facing computer users, computer system administrators, and law enforcement officials
- ❑ Describe the ways in which computer security relates to personal privacy issues.
- ❑ Explain the ways in which security and computer reliability are related.



© 2008 Prentice-Hall, Inc.

Online Outlaws: Computer Crime

- ❑ Computers are used to break laws as well as to uphold them.
- ❑ Computer crime involves:
 - Theft by computer
 - Software piracy
 - Software sabotage
 - Hacking and electronic trespassing



© 2008 Prentice-Hall, Inc.

Online Outlaws: Computer Crime

The Computer Crime Dossier

- ❑ Computer crime is any crime accomplished through knowledge or use of computer technology.
- ❑ Businesses and government institutions lose billions of dollars every year to computer criminals.
- ❑ The majority of crimes committed by company insiders.
 - These crimes are typically covered up or not reported to authorities to avoid embarrassment.



© 2008 Prentice-Hall, Inc.

Online Outlaws: Computer Crime

- ❑ According to a 2001 survey of over 500 companies and government agencies:
 - 85% detected computer security breaches in the preceding 12 months.
 - Financial losses due to security breaches topped \$377 million.
 - 70% reported that Internet connections were frequent points of attack.
 - Only 31% said that internal systems were frequent points of attack.



© 2008 Prentice-Hall, Inc.

Online Outlaws: Computer Crime

Theft by Computer

- ❑ Theft is the most common form of computer crime.
- ❑ Computers are used to steal:
 - Money
 - Goods
 - Information
 - Computer resources



© 2008 Prentice-Hall, Inc.

Online Outlaws: Computer Crime

Theft by Computer

- ❑ Common types of computer crime:
 - **Spoofing:** the use of a computer for stealing passwords
 - **Identity theft:** the use of computers and other tools to steal whole identities
 - Involves **social engineering:** slang for the use of deception to get individuals to reveal sensitive information
 - **Online fraud**
 - 87% related to online auctions
 - Average cost per victim: \$600



© 2008 Prentice-Hall, Inc.

Online Outlaws: Computer Crime

Protect Yourself from Identity Theft:

- ❑ **Make all your online purchases using a credit card.**
 - Get a separate credit card with a low credit limit for your online transactions.
- ❑ **Make sure a secure Web site is managing your transaction.**
- ❑ **Don't disclose personal information over the phone.**
 - Don't give social security or driver's license numbers over the phone; don't print it on checks; and use encryption when sending it in email.
- ❑ **Shred sensitive information.**



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware

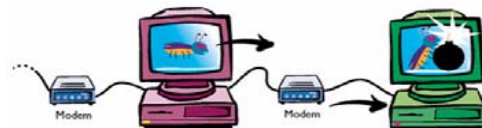
- ❑ Sabotage of software can include:
 - **Trojan horse:** performs a useful task while also being secretly destructive
 - Examples: Logic and time bombs
 - **Virus:** spreads by making copies of itself from program to program or disk to disk
 - Examples: Macro viruses and email viruses



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware



Origination
A programmer writes a tiny program—the virus—that has destructive power and can reproduce itself.

Transmission
Most often, the virus is attached to a normal program; unknown to the user, the virus spreads to other software.

Reproduction
The virus is passed by disk or network to other users who use other computers. The virus remains dormant as it is passed on.

Infection
Depending on how it is programmed, a virus may display an unexpected message, gobble up memory, destroy data files or cause serious system errors.

How a Virus Works



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware

- ❑ **Worm:** program that travels independently over computer networks, seeking uninfected sites
 - The first headline-making worm was created as an experiment by a Cornell graduate student in 1988.
 - In the summer of 2001, a worm called Code Red made worldwide headlines.
- **Virus War**
 - Researchers have identified more than 18,000 virus strains, with 200 new strains appearing each month.
 - At any given time, about 250 virus strains are in circulation.



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware

- **Antivirus** programs are designed to search for viruses, notify users when they're found, and remove them from infected disks or files.
 - Antivirus programs continually monitor system activity, watching for and reporting suspicious virus-like actions.
 - Programs need to be frequently revised to combat new viruses as they appear.
 - Most can automatically download new virus-fighting code from the Web as new virus strains appear.
 - It can take several days for companies to develop and distribute patches for new viruses.



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware

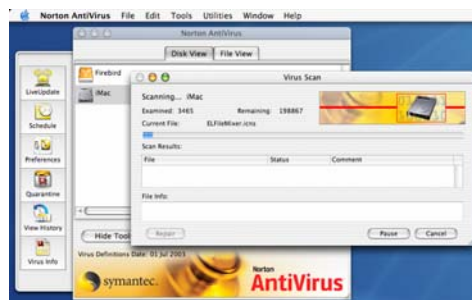
- **Spyware** is technology that collects information from computer users without their knowledge or consent.
 - Also called: *Tracking software* or *Spybot*
 - Information is gathered and shared with others via the Internet.
 - Your keystrokes could be monitored.
 - Web sites you visit are recorded.
 - Snapshots of your screen are taken.
 - Spyware can be the cause of pop-ups appearing on your screen.
 - 91% of PC users have spyware on their computers.
 - In **drive-by downloads** just visiting a Web site can cause a download.



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware



Norton Antivirus Software's Interface



© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware

Hacking and Electronic Trespassing

- **Hacker** (or cracker) refers to people who break into computer systems.
- **Webjackers** hijack Web pages and redirect users to other sites.
- **Denial of Service (DOS) attacks** bombard servers and Web sites with traffic that shuts down networks.



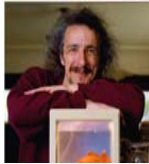
© 2008 Prentice-Hall, Inc.

Software Sabotage

Viruses and Other Malware

Hacking and Electronic Trespassing

- ❑ Breaking into other computer systems is called **electronic trespassing**.
- ❑ Electronic crime rings focus on stealing credit card numbers and other valuable information.



Cliff Stoll discovered an international computer espionage ring because of a \$.75 accounting error.



© 2008 Prentice-Hall, Inc.

Reducing Risks

Physical Access Restrictions

- ❑ Computer crime has led to a need to protect computer systems.
- ❑ Computer security attempts to protect computers and the information they contain.
- ❑ Computer security protects against unwanted access, damage, modification, or destruction.



© 2008 Prentice-Hall, Inc.

Reducing Risks

- ❑ Depending on the security system, you might be granted access to a computer based on:
 - Something you have
 - A key, an ID card with a photo, or a **smart card** containing digitally encoded identification in a built-in memory chip
 - Something you know
 - A password, an ID number, a lock combination, or a piece of personal history, such as your mother's maiden name
 - Something you do
 - Your signature or your typing speed and error patterns
 - Something about you
 - A voice print, fingerprint, retinal scan, facial feature scan, or other measurement of individual body characteristics—collectively called **biometrics**



© 2008 Prentice-Hall, Inc.

Reducing Risks

Passwords

- ❑ Passwords are the most common tool for restricting access to a computer system.
- ❑ Effective passwords are:
 - Not real words
 - Not names
 - Changed frequently
 - Kept secret
 - A combination of letters and numbers



© 2008 Prentice-Hall, Inc.

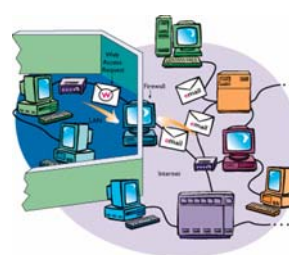
Reducing Risks Firewalls, Encryption and Audits

- These security systems reduce or prohibit the interception of messages between computers.
 - A firewall is like a gateway with a lock.
 - Encryption is where codes protect transmitted information and a recipient needs a special key to decode the message.
 - Shields are specially developed machines that prevent unwanted interception.



© 2008 Prentice-Hall, Inc.

Reducing Risks Firewalls, Encryption and Audits



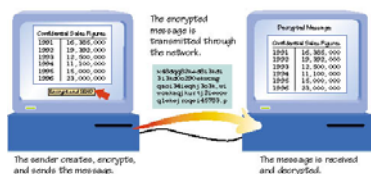
Software and Hardware Firewalls



© 2008 Prentice-Hall, Inc.

Reducing Risks

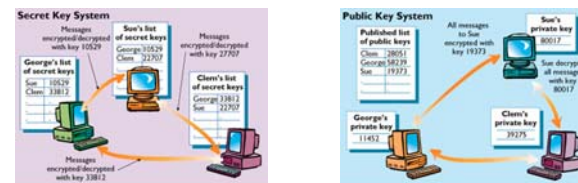
- Making a message secure from outsiders requires **encryption software**.
 - Encryption software scrambles the sent message using a key.
 - A different key is needed to unscramble the received message.



© 2008 Prentice-Hall, Inc.

Reducing Risks

- **Cryptography** is the process of encrypting messages.



Audit-control software monitors and records computer activity.

- Effective audit-control software forces every user to leave a trail of electronic footprints.



© 2008 Prentice-Hall, Inc.

Reducing Risks

Backups and Other Precautions

- ❑ An **uninterruptible power supply (UPS)** can protect computers from data loss during power failures.
- ❑ **Surge protectors** shield electronic equipment from power spikes.
- ❑ Have a routine for making regular backups.
 - Many systems are backed up at the end of each work day.



© 2008 Prentice-Hall, Inc.

Human Security Controls

Law, Management and Ethics

- ❑ Security measures prevent crime, but can also pose threats to personal privacy.
- ❑ Managers must make employees aware of security issues and risks.
- ❑ Systems Administrators play a key role in security and back-up.
- ❑ In 2003, Microsoft launched a “Trustworthy Computing” initiative:
 - Long-term goal: to make its software as secure as possible when released
 - Will lessen the need for security patches



© 2008 Prentice-Hall, Inc.

The Delicate Balance

Security, Privacy, Freedom and Ethics

When Security Threatens Privacy

- ❑ **Active badges** can simultaneously improve security and threaten privacy by:
 - Identifying who enters a door or logs onto a machine
 - Finding an employee’s current or earlier location
 - Remembering: At the end of the day, an active-badge wearer can get a minute-by-minute printout listing exactly where and with whom he or she has been.

“In this age of advanced technology, thick walls and locked doors cannot guard our privacy or safeguard our personal freedom.”
—Lyndon B. Johnson.



© 2008 Prentice-Hall, Inc.

Rules of Thumb

Safe Computing

- Share with care.
- Beware of BBS risks.
- Don’t pirate software.
- Disinfect regularly.
- Treat diskettes with care.
- Take your password seriously.
- Lock sensitive data.
- Use backup systems.
- Consider encryption for Internet activities.
- Prepare for the worst.



© 2008 Prentice-Hall, Inc.

The Delicate Balance Security, Privacy, Freedom and Ethics

Justice on the Electronic Frontier

- Dozens of hackers have been arrested for unauthorized entry into computer systems and for the release of destructive viruses and worms.

Through our scientific genius, we have made this world a neighborhood, now through our moral and spiritual development, we must make of it a brotherhood.
—The Rev. Martin Luther King, Jr.



© 2008 Prentice-Hall, Inc.

The Delicate Balance Security, Privacy, Freedom and Ethics

- Federal and state governments have responded to the growing computer crime problem by creating new laws against electronic trespassing and by escalating enforcement efforts:
 - Telecommunications Act of 1996
 - Digital Millennium Copyright Act of 1998
- Each of these laws introduced new problems by threatening rights of citizens—problems that have to be solved by courts and by future lawmakers.



© 2008 Prentice-Hall, Inc.

Security and Reliability

- Computer security involves more than protection from trespassing, sabotage, and other crimes.
- Software errors and hardware glitches account for some of the most important security issues, such as:

Bugs and Breakdowns



- Software bugs do more damage than viruses and computer burglars combined.



© 2008 Prentice-Hall, Inc.

Security and Reliability

- Facts about software engineering:
 - It is impossible to eliminate all bugs.
 - Even programs that appear to work can contain dangerous bugs.
 - The bigger the system, the bigger the problem.
 - Computer breakdowns pose a risk to the public, and the incidence rate doubles every two years.
 - Hardware problems are rare when compared with software failures.



© 2008 Prentice-Hall, Inc.

Security and Reliability

Computers at War

- ❑ **Smart weapons** are missiles that use computerized guidance systems to locate their targets.
- ❑ An **autonomous system** is a complex system that can assume almost complete responsibility for a task without human input.



© 2008 Prentice-Hall, Inc.

Security and Reliability

Warfare in the Digital Domain

- ❑ The front lines of the future may be in cyberspace.
- ❑ By attacking computer networks an enemy could conceivably cripple:
 - Telecommunications systems
 - Power grids
 - Banking and financial systems
 - Hospitals and medical systems
 - Water and gas supplies
 - Oil pipelines
 - Emergency government services



© 2008 Prentice-Hall, Inc.

Human Questions

for a Computer Age

- ❑ **Will Computers Be Democratic?**
 - “The higher the technology, the higher the freedom. Technology enforces certain solutions: satellite dishes, computers, videos, international telephone lines force pluralism and freedom onto a society.”—**Lech Walesa**
 - “When machines and computers, profit motives, and property rights are considered more important than people, the giant triplets of racism, materialism, and militarism are incapable of being conquered.”
— **Rev. Martin Luther King, Jr.**



© 2008 Prentice-Hall, Inc.

Human Questions

for a Computer Age

- ❑ **Will the Global Village Be a Community?**
 - “Progress in commercial information technologies will improve productivity, bring the world closer together, and enhance the quality of life.”
—**Stan Davis and Bill Davidson, in 2020 Vision**
 - “The real question before us lies here: do these instruments further life and its values or not?”—
Lewis Mumford



© 2008 Prentice-Hall, Inc.

Human Questions for a Computer Age

- ❑ Will We Become Information Slaves?
 - “Our inventions are wont to be **pretty toys** which distract our attention from serious things. They are but improved means to an **unimproved end.**”—**Henry David Thoreau**
 - “**Computers are useless.** They can only give you answers.”
—**Pablo Picasso**
- ❑ Standing on the Shoulders of Giants
 - “If I have seen farther than other men, it is because I stood on the shoulders of giants.”—**Isaac Newton**



© 2008 Prentice-Hall, Inc.

Inventing the Future The Future of Internet Security

- ❑ **Layered Defenses**
 - Organizations will place sophisticated pattern-recognition software and special hardware on the perimeter of their networks.
 - Special-purpose hardware, called security processors, will allow every message to be encrypted.
- ❑ **The People Problem**
 - This is the weak link in the system.
- ❑ **How Open?**
 - Will the onslaught of malware and spam place the openness of the Internet in peril?



© 2008 Prentice-Hall, Inc.

Lesson Summary

- ❑ Computers play an ever-increasing role in fighting crime.
- ❑ At the same time, law enforcement organizations are facing an increase in computer crime—crimes accomplished through special knowledge of computer technology.
- ❑ Some computer criminals use computers, modems, and other equipment to steal goods, money, information, software, and services.
- ❑ Because of rising computer crime and other risks, organizations have developed a number of computer security techniques to protect their systems and data.




© 2008 Prentice-Hall, Inc.

Lesson Summary

- ❑ Normally, security measures serve to protect our privacy and other individual rights, but occasionally security procedures threaten those rights.
- ❑ The trade-offs between computer security and freedom raise important legal and ethical questions.
- ❑ Computer systems aren't just threatened by people, they're also threatened by software bugs and hardware glitches.
- ❑ An important part of security is protecting systems—and the people affected by those systems—from the consequences of those bugs and glitches.



© 2008 Prentice-Hall, Inc.



Daftar Pustaka

Williams, Brian K, 2007, *Using Information Technology: Pengenalan Praktis Dunia Komputer dan Komunikasi Edisi 7*, Penerbit Andi. (Bab 2,7,9)

Beekman George, 2009, *Tomorrows's Technology and You 9th Edition*, Prentice Hall. (Chapter 10)

