Chapter 2
Computing Security and Ethics
Objectives

• In this chapter you will:
  – Learn about the origins of computer hacking
  – Learn about some of the motivations for hackers and crackers
  – Learn about technologies that system intruders use
  – Learn about malicious code
  – Learn what social engineering is and how it works
  – Learn how security experts categorize types of system attacks
  – Learn about physical and technical safeguards
Objectives (cont’d.)

• In this chapter you will (cont’d.):
  – Learn how to create a good password
  – Learn about antivirus software
  – Learn about encryption
  – Learn about preventive system setup, including firewalls and routers
  – Learn about laws to protect intellectual property and prosecute cracking
  – Learn about ethical behavior in computing
  – Learn about privacy in computing and ways to ensure it
Why You Need to Know About…
Computing Security and Ethics

• Good computer security
  – Requires looking beyond Hollywood characterization
  – Based on prevention
    • Accidental and natural events

• Security affects everyone, and everyone can affect it
  – Business computers are better protected than home computers
    • Mainly because corporations make a conscious effort to secure them
The Intruder

- **Hacker**
  - Technically proficient individual who breaks into a computer system
  - Originally connoted good intent
- **Cracker**
  - Unwelcome system intruder with malicious intent
- **Phreaking**
  - Illegally manipulating the AT&T phone system
- **Script kiddie**
  - Amateur hacker using available hacking tools
The Intruder (cont’d.)

- Intentional intruder types
  - Undirected hacker
    - Motivated by challenge of breaking into a system
  - Directed hacker
    - Motivated by greed and/or politics

- Hacktivism
  - Cracking into a system as a political act
  - The Hacker’s Manifesto
    - Anonymous document justifying cracking into systems as an ethical exercise
How Do They Get In?

• Failure to follow sound security practices
  – System configuration, programming, security
• Malicious software programs
  – Viruses
• Social engineering
  – Taking advantage of the innocent human tendency to be helpful
    • One of the most effective tools for hackers
Holes in the System

• Open nature of the Internet and networks
  – Remote access and mounting drives on other machines
• Backdoors
  – Shortcuts into programs created by system designers
• Sloppy programming
  – Leaving sensitive information in a URL string
• Buffer overflow
  – Placing more information into a memory location than that location can handle
Viruses, Worms, and Other Nasty Things

• Malicious code
  – Designed to breach system security and threaten digital information

• Viruses
  – Uninvited guest programs on a computer
    • Potential to damage files and the operating system
  – May be silent for a while
  – Sharing files may transmit viruses
  – E-mail attachments can host a virus
    • Activate when opened
Viruses, Worms, and Other Nasty Things (cont’d.)

Figure 2-1, A typical virus e-mail warning
Viruses, Worms, and Other Nasty Things (cont’d.)

- **Worm**
  - Program that actively reproduces itself across a network
    - A bot is a program that can roam the Internet anonymously and works on its own

- **Trojan program**
  - Program posing as an innocent program
    - Worst possible is an antivirus program
The Human Factor: Social Engineering

• Preys on human gullibility, sympathy, or fear to take advantage of the target
  – Posing as an insider at a company
  – Dumpster diving
  – Browsing a company Web site for intranet information
  – Using cracker techniques
  – Sending spam
Types of Attacks

• Access attacks include snooping, eavesdropping, and interception
  – Snooping: browsing a person’s files
  – Eavesdropping: using a sniffer program
    • Allows the user to listen in on network traffic
  – Intercepting: determines whether the information continues on to its intended receiver

• Modification attacks
  – Alter information illicitly
Types of Attacks (cont’d.)

• Denial-of-service attacks
  – Prevent legitimate users from using the system or accessing information
    • Pure vandalism
• Repudiation attacks
  – Injure the reliability of information by creating a false impression about an event
    • Sending an e-mail to someone as if it were from someone else
Managing Security: The Threat Matrix

- Managed risk
  - Basis of security
- Risk
  - Relationship between vulnerability and threat
- Vulnerability
  - Sensitivity of the information and the skill level needed by the attacker to threaten that information
    - Open ports and Internet connections
- Threat
  - Characterized by targets, agents, and events
Vulnerabilities

• Examples:
  – Internet connections
  – Hard or soft connections to partner organizations
  – Open ports
  – Physical access to the facilities
  – Phone modem access

• Evaluating vulnerabilities is essential
Threat: Agents

• Examples:
  – Crackers
  – Employees and ex-employees
  – Terrorists and criminals
  – Commercial rivals, partners, customers, visitors
  – Natural disasters
  – General public

• Items to examine regarding agents:
  – Access capability to information, knowledge, and motivation
Threat: Targets and Events

• Confidentiality
  – Ensures that only those authorized to access information can do so

• Encryption
  – Used for information with a high level of confidentiality
  – Transforms original text into coded or encrypted data

• Integrity
  – Assures that information is correct
    • Digital certificates and encryption
Threat: Targets and Events (cont’d.)

• Availability
  – Making information and services accessible on a normal basis
    • Backup copies and disaster recovery plans

• Accountability
  – Ensures system is as secure as feasible and an activity record exists for reconstructing a break-in
  – Identification and authentication (I&A)
    • Identification: knowing who someone is
    • Authentication: verifying that someone is who they claim to be
Measuring Total Risk

• Risk is measured in terms of cost
• Risk is difficult to calculate until the event occurs
  – Time the event might take to fix if a key system down
  – Physical resources needed to be brought to bear
  – Damage to organization’s reputation
  – Opportunity cost of lost business during the crisis
Managing Security: Countermeasures

• Topics:
  – Clean living
  – Passwords
  – Antivirus software
  – Encryption
  – Proper system setup
Clean Living (or Only the Paranoid Survive)

- Create and enforce a security policy
- Use physical safeguards
  - Computers, trash, visitors
- Use passwords to protect everything
  - Startup, e-mail, router, phone, PDA, screen saver
- Destroy old copies of sensitive material
  - Shred, overwrite, use a software degausser
- Back up everything of value
  - Copies kept off-site or in a bombproof lockbox
Clean Living (cont’d.)

**Figure 2-2, A computer lock as a physical safeguard**

**Figure 2-3, Two technologies that help back up your system: a surge suppressor and a UPS**
Clean Living (cont’d.)

- Protect against system failure
  - Surge protector, uninterruptible power supply
- Create an acceptable use policy (AUP)
  - Defines who can use company computers and networks, when, and how
    - Callbacks and virtual private networks
- Protect against viruses
  - Antivirus, antispam, and anticookie software
Clean Living (cont’d.)

• Create a disaster recovery plan (DRP)
  – Written plan for responding to natural or other disasters
    • Minimizes downtime and damage to systems and data
  – Key items to address
    • Data storage and recovery, centralized and distributed systems recovery, end-user recovery, network backup, internal and external data and voice communication restoration, emergency management and decision making, customer services restoration
  – May require off-site storage and communication considerations
Passwords

• Good passwords characteristics
  – At least eight characters
  – No real words
  – Include as many different characters as possible

• Use a combination of something you:
  – Know (password)
  – Have (an ID)
  – Are (biometrics)
Table 2-1, Password protection using combinations of the letters A through Z

<table>
<thead>
<tr>
<th>number of characters (A through Z)</th>
<th>possible combinations</th>
<th>human avg. time to discovery (max time/2)</th>
<th>computer avg. time to discovery (max time/2)</th>
<th>tries per second: 1</th>
<th>tries per second: 1 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>26</td>
<td>13 seconds</td>
<td>.000013 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$26 \times 26 = 676$</td>
<td>6 minutes</td>
<td>.000338 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$26$ raised to 8 = $208,827,064,576$</td>
<td>6640 years</td>
<td>58 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$26$ raised to 10 = $1.4 \times 10$ raised to 14</td>
<td>4.5 million years</td>
<td>4.5 years</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Passwords (cont’d.)

Figure 2-4, Three potentially combined authentication methods, from left to right: what you know, what you have, what you are
Antivirus Software

- Program designed to detect, block, and deal with computer viruses
  - Virus signature: code uniquely identifying a virus
  - Honeypot: trap to catch and track numbers
  - Heuristics: rule set to predict how a virus might act
  - Checksum: mathematical means to check the content of a file or value
Using Encryption to Secure Transmissions and Data

• Encryption uses an encryption key
  – Scrambles transmissions
    • Only receiver with appropriate decoding key can read it
  – The longer the key, the more secure the encryption
    • 128-bit encryption used for online banking

• Web pages
  – Use S-HTTP, SET, or SSL to send secure transactions
    • S-HTTP and SSL use digital certificates issued by a certification authority (CA)
Using Encryption to Secure Transmissions and Data (cont’d.)

- Encryption standards today: key-based
  - Data Encryption Standard (DES)
  - RSA (named after Rivest, Shamir, and Adelman)
  - Advanced Encryption Standard (AES)

- Symmetric encryption
  - Uses a private key to both encrypt and decrypt

- Asymmetric encryption
  - Uses both a public key and a private key
Using Encryption to Secure Transmissions and Data (cont’d.)

Figure 2-5, Using a public and private key (asymmetric encryption)
Securing Systems with Firewalls

• Firewall
  – Software or hardware
  – Acts as a protective filter between an internal computer system and an external network
  – Only allows authorized entrants

• Two main types of firewalls
  – A proxy firewall establishes new link between each information packet and its destination
  – A packet-filtering firewall inspects each packet and moves it along an established link
    • Faster but less secure than a proxy firewall
Protecting a System with Routers

• **Router**
  – Moves packets as quickly as possible toward their intended destination

• **Router filtering software**
  – Front line of defense against certain service requests
  – Closes unauthorized ports
  – Determines where servers are located on the network
  – Determines what services are available outside a firewall
    • Internal and external DNS servers
Protecting a System with Routers (cont’d.)

<table>
<thead>
<tr>
<th>service</th>
<th>port</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>21, 22</td>
<td>File transfer</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>Access the Web</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>Create a remote session</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
<td>Create a remote session</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>Access remote e-mail accounts</td>
</tr>
</tbody>
</table>

Table 2-4, Some of the many ports available on a router and what they do
The DMZ

- Demilitarized zone
  - Location outside the firewalls (or between firewalls)
  - More vulnerable to attack from outside
  - Separates services offered internally from those offered externally
  - Protected by router filters
  - Allows each server a particular service
  - Another firewall exists on the other side
The DMZ (cont’d.)

Figure 2-6, System configuration of a network that includes a firewall, a DMZ, and a router
Protecting Systems with Machine Addressing

- Organizations usually have more machines than IP addresses
  - Handled by dynamically allocating IP addresses
- Organizations also use private class addressing
  - Nodes on the internal network have a different address than what is seen on the outside
  - Network Address Translation (NAT)
    - Conversion of internal to external IP addresses (and vice versa)
    - Usually provided by the firewall
Putting It All Together

• A comprehensive security effort includes:
  – Security policy
    • Well defined, clearly understood, and seriously enforced
  – Properly configured firewalls and antivirus software
  – Restricting physical access to buildings and hardware
  – Reminders and training about security dangers
  – Continual updates and patches
  – Appropriate access controls
Computer Crime

• Topics covered:
  – Types of computer crime
  – Legal safeguards
  – Avenues for prosecuting and punishing computer intruders
Defining Computer Crime

• Intellectual property protections
  – Copyright
    • Protects the expression of the idea, not the idea itself
  – Patent
    • Government grant giving sole right to make, use, and sell an invention for a specified period of time
  – Trade secrets
    • Methods, formulas, or devices providing companies a competitive advantage
    • Kept secret
Prosecuting Computer Crime

• U.S. laws to protect against computer crime
  – Differ widely (both in the U.S. and in other countries)
  – Are open to interpretation

• Prosecuting a computer crime is a complex matter
  – Systems must be replicated entirely or put out of use
  – Perpetrators are very difficult to find
I Fought the Law and the Law Won

- Crackers are being caught and persecuted more than ever
- Corporations are willing to pursue copyright violations much more aggressively
- Legal ways to use software today
  - Purchase the right to use a copy with a EULA agreement
  - Purchase time on a program and connect to it through a network
Ethics in Computing

• Ethics
  – Principles for judging right and wrong
  – Held by an individual or a group

• Ethical systems (along with laws)
  – Help create a stable platform from which to live life comfortably with other people and benefit all

• Organizations of computer professionals
  – Outline ethical standards or codes of ethics
    • IEEE, ACM, Computer Ethics Institute
Ethics in Computing (cont’d.)

• Approach ethical reasoning from different perspectives
  – Orientation toward consequences versus orientation toward rules
  – Orientation toward the individual versus orientation toward the universal
  – Terms
    • Egoism
    • Deontology
    • Utilitarianism
    • Rule-deontology
Software Piracy

• Software piracy
  – Illegal copying of software
  – Detrimental to everyone
    • Spread of viruses
    • Takes away resources for new program development
    • Increases software cost for everyone

• Consequences of piracy
  – May get a virus
  – May lose job
  – May lose share value on stock holdings
Viruses and Virus Hoaxes

• It is unethical to:
  – Write a virus
  – Knowingly pass a virus along

• Advice
  – Use antivirus software
  – Be aware of virus hoaxes
    • Do not pass along
Weak Passwords

- Using weak passwords
  - Could be considered unethical
  - They give online vandals access to systems
  - They might take advantage of any other system weaknesses and cause further damage
Plagiarism

• Academically
  – Enforced through honor codes
  – Results from pressure to perform
  – Long-term consequences
    • Student does not learn information or skills developed by doing the assignment

• Contradicts many ethical standards and rules of conduct

• Avoiding plagiarism
  – Cite the work
Cracking

• Equivalent to virtual trespassing
• Intentional or unintentional
  – Can cause a tremendous amount of economic damage
• Cracker justifications
  – Stupidity should be punished
  – Society is better off for their actions
Health Issues

• Ethics reaches into computer design, particularly ergonomics
  – Poorly designed user interfaces
    • May lead to repetitive strain injuries
  – Computer components or peripherals may be made of toxic materials

• Computers should not harm human beings
  – Rules in ACM, IEEE, and the Computer Ethics Institute
  – OSHA has guidelines addressing these problems
Privacy

- Internet and computerized databases
  - Invasion of privacy easier
  - Spam
    - Unsolicited e-mail
  - Spyware
    - Software to track, collect, and transmit certain information about a user’s computer habits to a third party
  - Cookies
    - Programs used to gather information about a user
    - Stored on the user’s machine
One Last Thought

• Operators of computer systems
  – Part of an overall vulnerability

• Steps to reduce vulnerability
  – Install and update antivirus software, firewalls, and operating system patches
  – Guard against communicating information
  – Reassess balance between ease of use, customer service, time, and cost on one hand, and system security on the other
Summary

• “Hacking” and “hacker”
  – Did not originally have a negative connotation
• Intruders classifications
  – Directed or undirected
• Crackers find holes in systems
  – Intentionally or unintentionally
• How crackers infiltrate systems
  – Viruses, worms, and Trojan programs
  – Social engineering
  – Human manipulation
Summary (cont’d.)

• Total risk to an organization
  – Vulnerability, threat, existing countermeasures

• Intruder targets
  – Confidentiality, integrity, availability, or accountability of information

• Countermeasures in managing security
  – Antivirus software, system updates, physical restrictions, and backup systems

• Users support cracking by using weak passwords
  – Encrypt information to secure communications
Summary (cont’d.)

• Use firewalls and routers
• It is difficult to prosecute computer attackers
• Many issues must be viewed from an ethical perspective
• Privacy is protected by law
  – Many tools available to protect privacy
• Computer and network security
  – Everyone’s responsibility