WEEK 3

COMPUTER AND INTERNET CRIME

IT SECURITY INCIDENTS: A WORSENING PROBLEM

- Security of information technology is of utmost importance
  - Protect confidential data
    - Safeguard private customer and employee data
  - Protect against malicious acts of theft or disruption
- Number of IT-related security incidents is increasing around the world

IT SECURITY INCIDENTS: A WORSENING PROBLEM (CONTINUED)

- Computer Emergency Response Team Coordination Center (CERT/CC)
  - – Established in 1988 at the Software Engineering Institute (SEI)
  - -Charged with
    - Coordinating communication among experts during computer security emergencies
    - Helping to prevent future incidents

INCREASING COMPLEXITY INCREASES VULNERABILITY

- Computing environment is enormously complex
  - – Continues to increase in complexity
  - – Number of possible entry points to a network expands continuously

HIGHER COMPUTER USER EXPECTATIONS

- Computer help desks
  - Under intense pressure to provide fast responses to users' questions
  - Sometimes forget to
    - Verify users' identities
    - Check whether users are authorized to perform the requested action
- Computer users share login IDs and password

EXPANDING AND CHANGING SYSTEMS INTRODUCE NEW RISKS

- Network era
  - Personal computers connect to networks with millions of other computers
  - All capable of sharing information
- Information technology
  - Ubiquitous
  - Necessary tool for organizations to achieve goals
  - Increasingly difficult to keep up with the pace of technological change

INCREASED RELIANCE ON COMMERCIAL SOFTWARE WITH KNOWN VULNERABILITIES

- Exploit
  - Attack on information system
  - Takes advantage of a particular system vulnerability
  - Due to poor system design or implementation
- Patch
  - "Fix" to eliminate the problem
  - Users are responsible for obtaining and installing patches
  - Delays in installing patches expose users to security breaches

INCREASED RELIANCE ON COMMERCIAL SOFTWARE WITH KNOWN VULNERABILITIES (CONTINUED)

- Zero-day attack
  - Takes place before a vulnerability is discovered or fixed
- U.S. companies rely on commercial software with known vulnerabilities

TYPES OF ATTACKS

- Most frequent attack is on a networked computer from an outside source
- Types of attacks
  - Virus
  - Worm
  - Trojan horse
  - Denial of service

VIRUSES

- Pieces of programming code
- Usually disguised as something else
- Cause unexpected and usually undesirable events
- Often attached to files
- Deliver a “payload”

VIRUSES (CONTINUED)

- Does not spread itself from computer to computer
- Must be passed on to other users through
  - Infected e-mail document attachments
  - Programs on diskettes
  - Shared files
- Macro viruses
  - Most common and easily created viruses
  - Created in an application macro language
  - Infect documents and templates

WORMS

- Harmful programs
  - Reside in active memory of a computer
- Duplicate themselves
  - Can propagate without human intervention
- Negative impact of virus or worm attack
  - Lost data and programs
  - Lost productivity
  - Effort for IT workers

TROJAN HORSES

- Program that a hacker secretly installs
- Users are tricked into installing it
- Logic bomb
  - Executes under specific conditions

DENIAL-OF-SERVICE (DOS) ATTACKS

- Malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks
  - The computers that are taken over are called zombies
- Does not involve a break-in at the target computer
  - Target machine is busy responding to a stream of automated requests
  - Legitimate users cannot get in
- Spoofing generates a false return address on packets

DENIAL-OF-SERVICE (DOS) ATTACKS (CONTINUED)

- Ingress filtering
  - When Internet service providers (ISPs) prevent incoming packets with false IP addresses from being passed on

- Egress filtering
  - Ensuring spoofed packets don’t leave a network

PERPETRATORS

- Motives are the same as other criminals
- Different objectives and access to varying resources
- Different levels of risk to accomplish an objective

HACKERS AND CRACKERS

- Hackers
  - Test limitations of systems out of intellectual curiosity
- Crackers
  - Cracking is a form of hacking
  - Clearly criminal activity

MALICIOUS INSIDERS

- Top security concern for companies
- Estimated 85 percent of all fraud is committed by employees
- Usually due to weaknesses in internal control procedures
- Collusion is cooperation between an employee and an outsider

MALICIOUS INSIDERS (CONTINUED)

- Insiders are not necessarily employees
  - Can also be consultants and contractors
- Extremely difficult to detect or stop
  - Authorized to access the very systems they abuse

INDUSTRIAL SPIES

- Illegally obtain trade secrets from competitors
- Trade secrets are protected by the Economic Espionage Act of 1996
- Competitive intelligence
  - Uses legal techniques
  - Gathers information available to the public

INDUSTRIAL SPIES (CONTINUED)

- Industrial espionage
  - Uses illegal means
  - Obtains information not available to the public

CYBERCRIMINALS

- Hack into corporate computers and steal
- Engage in all forms of computer fraud
- Chargebacks are disputed transactions
- Loss of customer trust has more impact than fraud
- To reduce the potential for online credit card fraud sites:
  - Use encryption technology
  - Verify the address submitted online against the issuing bank
  - Request a card verification value (CVV)
  - Use transaction-risk scoring software

CYBERCRIMINALS (CONTINUED)

- Smart cards
  - – Contain a memory chip
  - – Are updated with encrypted data every time the card is used
  - – Used widely in Europe
  - – Not widely used in the U.S

CYBER-TERRORISTS

- Intimidate or coerce governments to advance political or social objectives
- Launch computer-based attacks
- Seek to cause harm
  - Rather than gather information
- Many experts believe terrorist groups pose only a limited threat to information systems

REDUCING VULNERABILITIES

- Security
  - Combination of technology, policy, and people
  - Requires a wide range of activities to be effective
- Assess threats to an organization's computers and network
- Identify actions that address the most serious vulnerabilities
- Educate users
- Monitor to detect a possible intrusion
- Create a clear reaction plan

CERTIFICATION (CONTINUED)

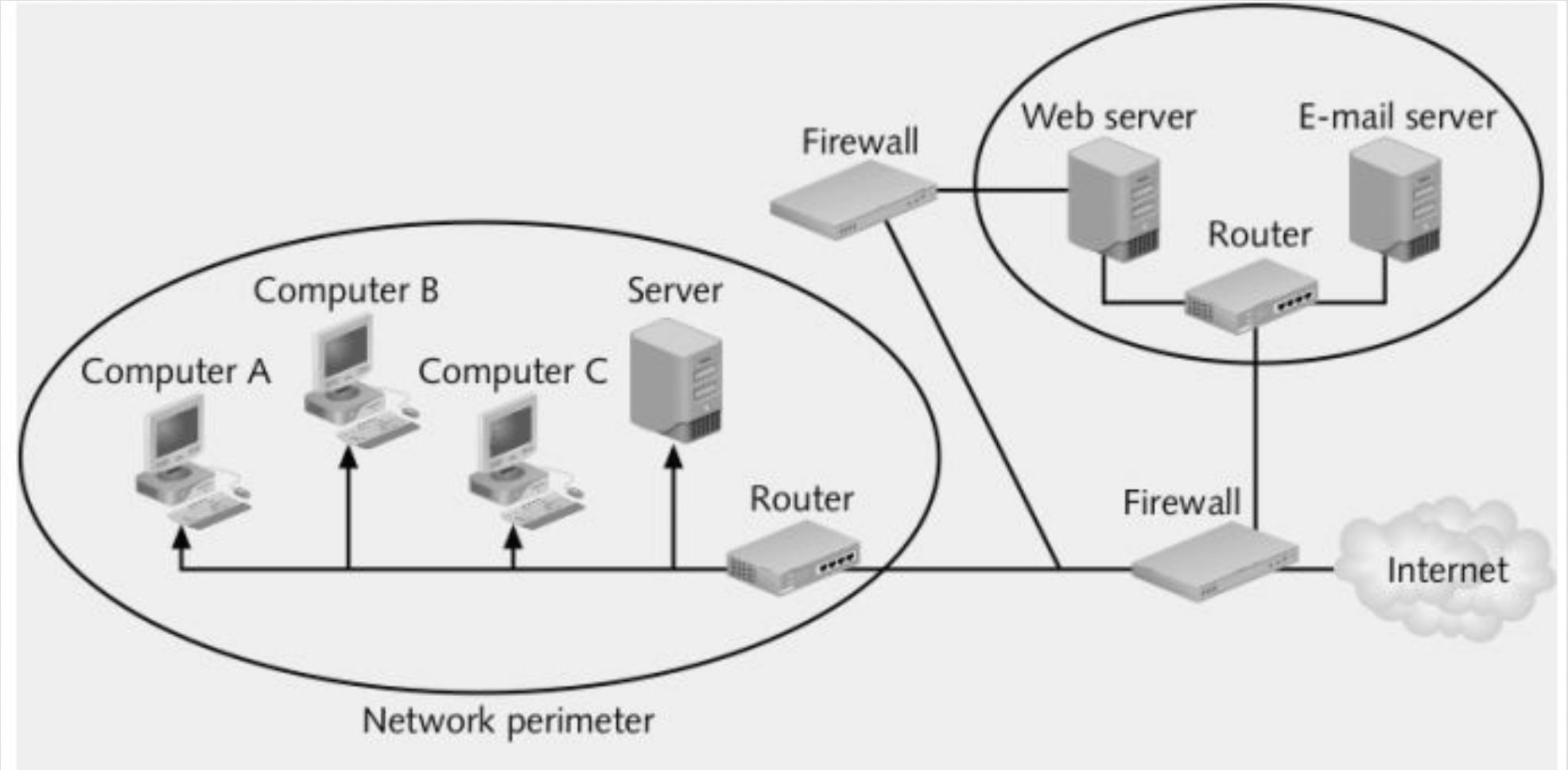
Risk Assessment

- Organization's review of:
  - Potential threats to computers and network
  - Probability of threats occurring
- Identify investments that can best protect an organization from the most likely and serious threats
- Reasonable assurance
- Improve security in areas with:
  - Highest estimated cost
  - Poorest level of protection

PREVENTION

- Implement a layered security solution
  - Make computer break-ins harder
- Firewall
  - Limits network access
- Antivirus software
  - Scans for a specific sequence of bytes
- Known as the virus signature
  - Norton Antivirus
  - Dr. Solomon’s Antivirus from McAfee

PROTECTION


Firewall
Web server
E-mail server
Router
Computer B
Server
Computer A
Computer C
Router
Firewall
Internet
Network perimeter

PREVENTION (CONTINUED)

- Antivirus software
  - Continually updated with the latest virus detection information
- Departing employees
  - Promptly delete computer accounts, login IDs, and passwords
- Carefully define employee roles • Create roles and user accounts

PREVENTION (CONTINUED)

- Keep track of well-known vulnerabilities
  - SANS (System Administration, Networking, and Security) Institute
  - CERT/CC
- Back up critical applications and data regularly
- Perform a security audit

DETECTION

- Detection systems
  - Catch intruders in the act
- Intrusion detection system
  - Monitors system and network resources and activities
  - Notifies the proper authority when it identifies
- Possible intrusions from outside the organization
- Misuse from within the organization
  - Knowledge-based approach
  - Behavior-based approach

DETECTION (CONTINUED)

- Intrusion prevention systems (IPSs)
  - Prevent attacks by blocking
- Viruses
- Malformed packets
- Other threats
  - Sits directly behind the firewall

DETECTION (CONTINUED)

- Honeypot
  - Provides would-be hackers with fake information about the network
  - Decoy server
  - Well-isolated from the rest of the network
  - Can extensively log activities of intruders

RESPONSE

- Response plan
  - Develop well in advance of any incident
  - Approved by
    - Legal department
    - Senior management
- Primary goals
  - Regain control
  - Limit damage

RESPONSE (CONTINUED)

- Incident notification defines
  - Who to notify
  - Who not to notify
- Security experts recommend against releasing specific information about a security compromise in public forums
- Document all details of a security incident
  - All system events
  - Specific actions taken
  - All external conversations

RESPONSE (CONTINUED)

- Act quickly to contain an attack
- Eradication effort
  - Collect and log all possible criminal evidence from the system
  - Verify necessary backups are current and complete
  - Create new backups
- Follow-up
  - Determine how security was compromised
    - Prevent it from happening again

RESPONSE (CONTINUED)

- Review
  - Determine exactly what happened
  - Evaluate how the organization responded
- Capture the perpetrator
- Consider the potential for negative publicity • Legal precedent
  - Hold organizations accountable for their own IT security weaknesses

THANK YOU!