# Ethics and the Law

- Following the requirements of the law provides protection from prosecution
- Since engineering work utilizes new technology before experience and laws can catch up, ethics seeks to go beyond the dictates of current law
- Ethical behavior provides protection from civil suits, from damage to reputation, or from loss of professional licensure and encompasses ways engineers should conduct themselves in their practice
- Legal acts are not necessarily ethical; Acts which are ethical are not necessarily legal.
- Not legally binding – an engineer cannot be arrested for violating an ethical code, but may be expelled from or censured by the engineering society

# Ethical Values

- Integrity
- Honesty
- Fidelity
- Responsibility

# Ethical Issues in Engineering Design

Philosophical and practical ethics
Codes of Ethics

- Health and welfare of humans and nature
- Informing client/employers of consequences
- Statements and information in truthful manner
- Treating people fairly (avoiding conflict of interest)
- Limits of professional competence
- Building professional reputations according to merits
- Continuing professional development
- Issues with intellectual property.

**[ SSL (2004) ]**

**Issues**

Life systems preservation
Maintenance of quality of life
Maintaining high standards of personal and professional conduct
Managing intra-professional customs, identifiers, habits, and limits.

# Codes of Ethics Commonly Hold

- Engineers and technologists have a duty to hold the heath and safety of the public as a primary concern.  Usually the first cannon of any code.
- Other duties are summarized in order of importance with most important first e.g. Safety is more important than conflict of interest.

# Fundamental Canons

1. Engineers shall hold paramount the safety, health and welfare of the public and shall strive to comply with the principles of sustainable development in the performance of their professional duties.
2. Engineers shall perform services only in areas of their competence.
3. Engineers shall issue public statements only in an objective and truthful manner.
4. Engineers shall act in professional matters for each employer or client as faithful agents or trustees, and shall avoid conflicts of interest.
5. Engineers shall build their professional reputation on the merit of their services and shall not compete unfairly with others.
6. Engineers shall act in such a manner as to uphold and enhance the honor, integrity, and dignity of the engineering profession and shall act with zero-tolerance for bribery, fraud, and corruption.
7. Engineers shall continue their professional development throughout their careers, and shall provide opportunities for the professional development of those engineers under their supervision.

# Resolving Ethical Dilemmas

- Obtain the facts of the situation
- List the stakeholders
- Consider the motivations of the stakeholders
- Formulate alternative solutions using code of ethics or basic ethical values
- Evaluate the alternatives, reject unethical solutions
- Seek assistance from co-workers, supervisors, and ombudsmen
- Select the alternative that satisfies the highest ethical values
- Implement the selected solution through the chain of command
- Monitor the outcome
- If unsatisfactory, contact legal counsel, professional society, and the media.

# Whistleblowing

- Definition: The act by an employee which informs the public or higher management of unethical or illegal behavior by an employer or supervisor
- **Always the LAST RESORT, it indicates serious corporate culture problems**

# Examples of problems that might warrant whistle-blowing

- Incompetence
- Criminal Behavior
- Unethical Policies
- Threat to Public Safety
- Injustices to Workers

# 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 client-server 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
- thus legitimate users cannot get in

***Spoofing*** generates false return address on packets

- therefore, sources of attack cannot be identified and turned off

DoS has become a means to extortion $$$ from companies

- do not respond, but report to police

# Denial-of-Service (DoS) Attacks Defense

## 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

## Overhead:

- may prevent legitimate users from getting in
- companies need to deploy faster and more powerful routers and switches to check IP addess on each packet

# Classifying Perpetrators

| Type of perpetrator | Objectives | Resources available to perpetrator | Level of risk acceptable to perpetrator | Frequency of attack |
|---|---|---|---|---|
| Hacker | Test limits of system and gain publicity | Limited | Minimal | High |
| Cracker | Cause problems, steal data, and corrupt systems | Limited | Moderate | Medium |
| Insider | Make money and disrupt company's information systems | Knowledge of systems and passwords | Moderate | Low |
| Industrial spy | Capture trade secrets and gain competitive advantage | Well funded and well trained | Minimal | Low |
| Cyber-criminal | Make money | Well funded and well trained | Moderate | Low |
| Cyber-terrorist | Destroy key infrastructure components | Not necessarily well funded or well trained | Very high | Low |

# Prevention

Implement a ***layered security solution***

- make computer break-ins harder
  - if hacker breaks through one layer, there is another layer to overcome

Firewall

- any Internet traffic not explicitly permitted into intranet denied entry; can also block access to certain Web sites, IM, etc.

Antivirus software

- scans for a specific sequence of bytes known as ***virus signature***
  - may clean, delete or quarantine affected files
- two of most widely used are Norton Antivirus and Dr. Solomon's Antivirus from McAfee

# Firewall Protection

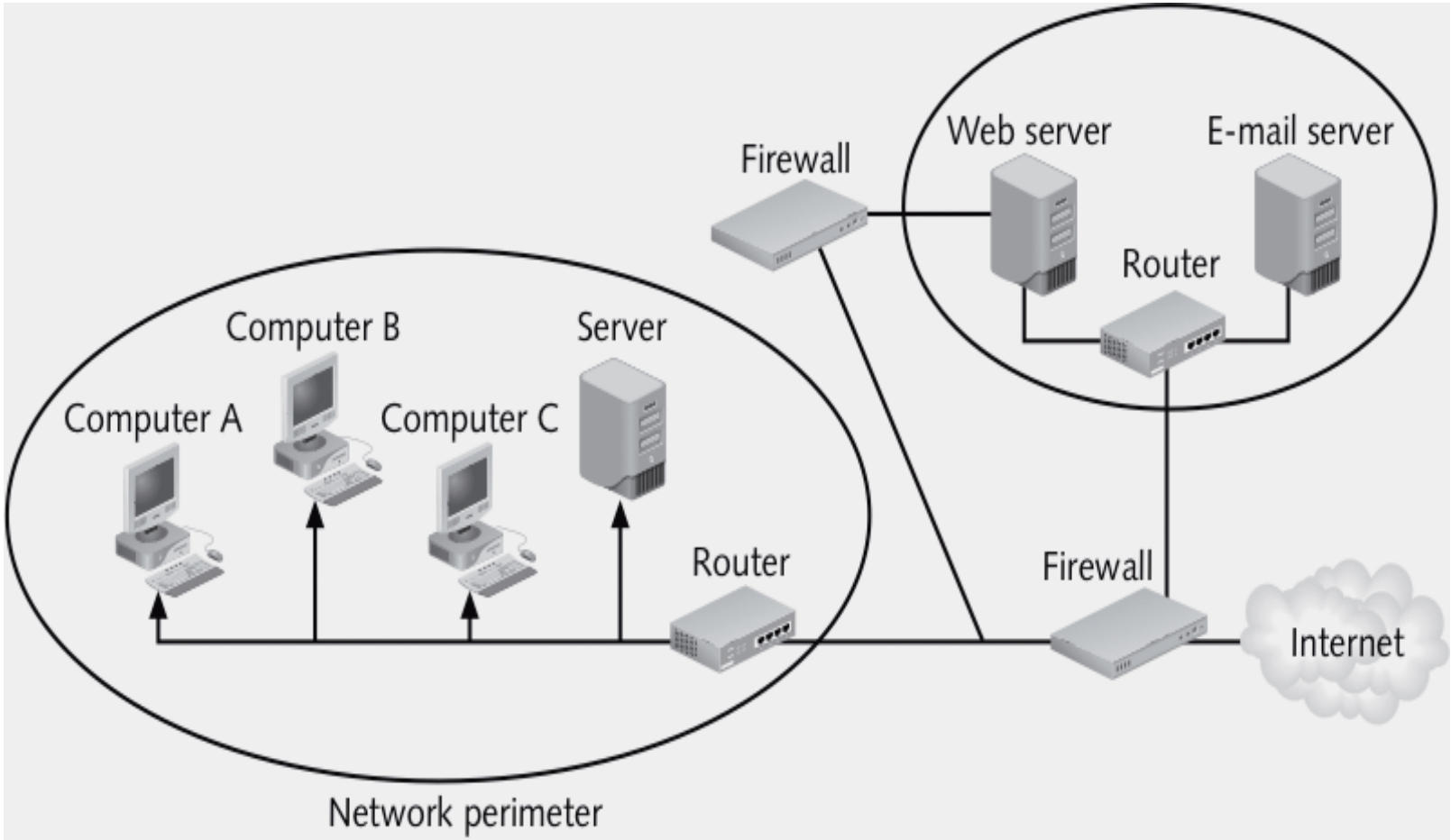


**FIGURE 3-3** Firewall protection

# Popular Firewall Software for Personal Computers

**TABLE 3-4** Popular firewall software for personal computers

| Software | Vendor |
|---|---|
| Norton Personal Firewall | Symantec |
| Tiny Personal Firewall | Tiny Software |
| BlackICE Defender | Network Ice Corporation |
| ZoneAlarm Pro | Zone Labs |
| Personal Firewall | McAfee |

# Prevention (continued)

Antivirus software

- continually updated with the latest virus detection information, called ***definitions***

Do not leave accounts active after employees leave company

- promptly delete computer accounts, login IDs, and passwords

Carefully define employee roles

- e.g. do not allow a single employee to initiate a PO and approve invoice for its payment

Create roles and user accounts

- so employees have authority to perform their responsibilities and no more

# Prevention (continued)

Keep track of well-known vulnerabilities and patch them!

- SANS (System Administration, Networking, and Security) Institute
- CERT/CC

Back up critical applications and data regularly

Perform a ***security audit*** to ensure organization has well-considered ***security policy*** in place and that it is being followed

- e.g. users much change password every 30 days

# Detection

Detection systems

- catch intruders in the act

But note: preventive measures are not fail-proof

***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
- two fundamental approaches:
  - *Knowledge-based* and
  - *Behavior-based*

# More on Intrusion Detection Systems

## Knowledge-based approaches

- utilize information about *specific attacks and system vulnerabilities* and watch for attempts to exploit these
- examples include repeated failed login attempts, attempts to download a program to a server, or other symptoms of possible mischief

## Behavior-based approaches

- *model normal behavior* of a system and its users from reference source
- compare current activity to this model and generate alarm if deviation found
- examples include *unusual traffic* at odd hours or a user in HR department who accesses accounting program he never used before

# Detection (continued)

## ***Intrusion Prevention Systems*** (IPSs)

- prevent attacks by *blocking*
  - viruses
  - malformed packets
  - other threats
- sits directly behind the firewall and examines all traffic passed by it
- firewall and network IPS are complementary:
  - firewall blocks everything except what you explicitly allow through;
  - IPS lets everything through except what it is told to block

# Detection (continued)

## *Honeypot*

- provides would-be hackers with *fake information* about the network
- decoy server
  - goal is to confuse hackers, trace them or keep a record for prosecution
- keeps hackers well-isolated from the rest of the network
- can extensively log activities of intruders
- honeypot can identify attacker *reconnaissance probes*
  - used by attackers to obtain info about network resources he wants to attack

# Response

## Response plan

- prepare for the worst
- develop well in advance of any incident
- should be approved by
  - legal department
  - senior management

## Primary goals

- regain control
  - technical and emotional
- limit damage
- restore data and information systems to normal
  - don’t worry about catching intruder at this point

# Response (continued)

*Incident notification* defines

- who to notify
  - within company, customers, suppliers?
- who *not* to notify

Security experts recommend *against* releasing specific information about a security compromise in public forums

- such as news reports, conferences, online discussion groups

Document all details of a security incident

- do this for future prosecution and to help with incident eradication and follow-up
- all system events
- specific actions taken
- all external conversations

# Response (continued)

Act quickly to ***contain*** an attack

- may need to shut down or disconnect critical system from network

***Eradication*** effort

- collect and log all possible criminal evidence from the system
- verify necessary backups are current and complete
  - create disk image of all compromised systems for later study and as evidence
- create new backups
  - after virus has been eradicated

Follow-up (the ‘aftermath’)

- determine how security was compromised
  - prevent it from happening again
  - was a software fix not installed?

# Response (continued)

## Review

- determine exactly what happened
- evaluate how the organization responded
- write *formal incident report*

## Capture the perpetrator

- how much effort will this take?

## But consider the potential for negative publicity

- brokerage firm might lose customers who think their money or records not secure

## Legal precedent

- hold organizations accountable for their own IT security weaknesses
  - particularly true for ISPs
  - e.g., Verizon forced to issue customer rebates during outbreak of Slammer worm

# Summary

Ethical decisions regarding IT security include determining which information systems and data most need protection

65-fold increase in the number of reported IT security incidents from 1997 to 2003

Most incidents involve a:

- virus
- worm
- trojan horse
- denial-of-service

# Summary (continued)

Key elements of a multilayer process for managing security vulnerabilities include:

- threat assessment
  - to organization's computers and network
- user education
  - of risks and preventative actions
- response plan