Professional Ethics for Computer Science

Lecture 3: Computer and Internet Crime

Klaus Mueller

Computer Science Department

Stony Brook University

IT Security Incidents: A Worsening Problem

Security of information technology is critical

- *protect confidential business data*, including customer and employee data
- protect against malicious acts of theft or disruption

Security concerns must be balanced against other business needs (*ethical decision regarding IT security*):

- pursue prosecution at all costs or maintain low profile
  - to avoid negative publicity?
- how much effort and money should be devoted to security?
- if firm produces SW with security flaws, what actions should it take?
- what if security safeguards make life more difficult for customers and employees
  - will it result in lost sales and increased costs?

Number Of IT Security Incidents Are Increasing

Computer Emergency Response Team Coordination Center (CERT/CC)

- established in 1988 at the Software Engineering Institute (SEI)
  - SEI: federally funded R&D center at CMU
- charged with
  - coordinating communication among experts during computer security emergencies
  - helping to prevent future incidents
  - study Internet security vulnerabilities
  - publish security alerts
  - develop information and training for organizations

Increasing Complexity Increases Vulnerability

Computing environment is enormously complex

Continues to increase in complexity:

- networks, computers, OSes
- apps, Web sites
- switches, routers, gateways
- all interconnected and driven by 100s of millions of LoC (Lines of Code).

Number of possible entry points to a network expands continuously as more devices added,

- this increases possibility of security breaches

Increased Reliance on Commercial Software with Known Vulnerabilities

***Exploit*:**

- an attack on an information system that takes advantage of a particular system vulnerability

Typically due to poor system design or implementation

SW developers quickly create and issue ***patch:***

- a “fix” to eliminate the problem
- users are responsible for obtaining and installing patches
  - which they can download from the Web
- 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
- blaster worm released to Internet a month after Microsoft released patch (2004)

U.S. companies rely on commercial software with known vulnerabilities.

- why is that?

IT orgs continue to use installed SW “as is” (e.g. IE, RealPlayer, JRE)

- since security fixes could make SW harder to use or eliminate “nice to have” features.

Number of Vulnerabilities Reported to CERT/CC

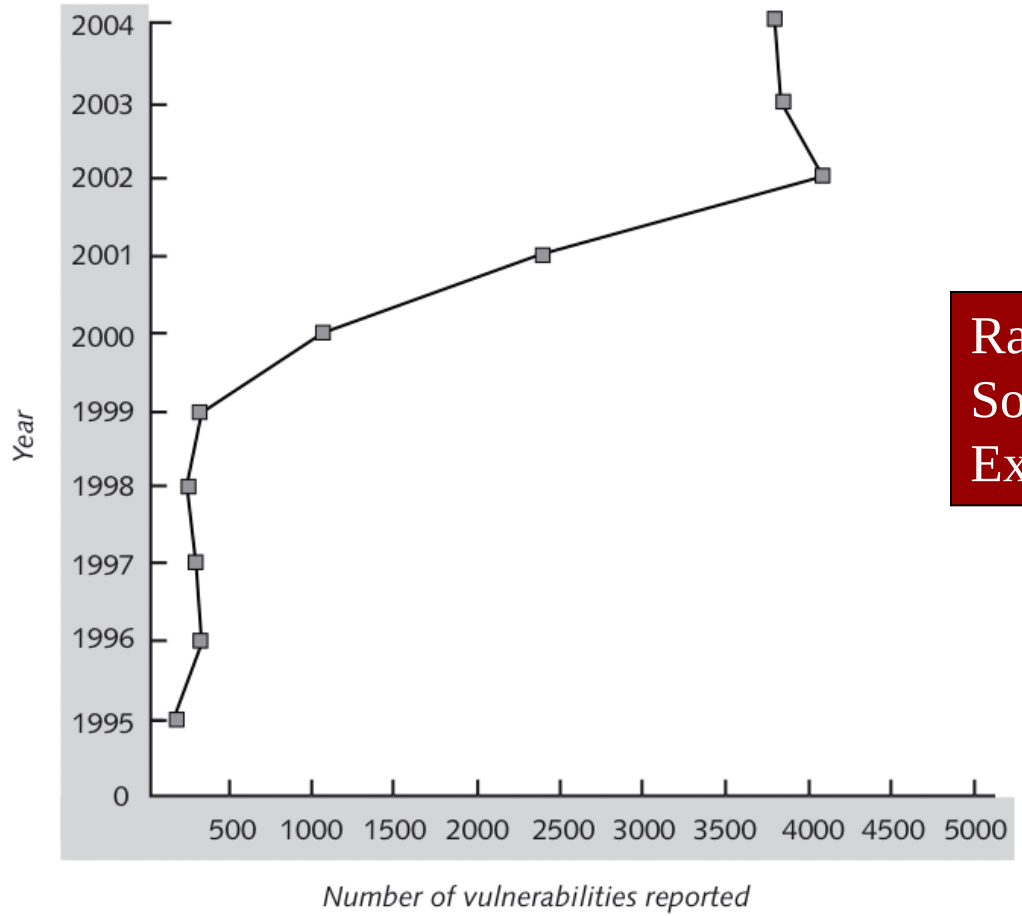

FIGURE 3-1 Number of vulnerabilities reported to CERT/CC

Rate of discovering Software vulnerabilities Exceeds 10/day

Types of Attacks

Most frequent attack:

- on a *networked* computer from an *outside* source

Types of attacks are many

Virus:

- malicious piece of code; requires users to spread infected files

Worm:

- harmful programs that reside in active memory and duplicate themselves

Trojan horse:

- a program a hacker secretly installs on a computer

Denial of service:

- malicious hacker takes over computers on Internet and causes them to flood a target site with demands for data and other small tasks

Viruses

Pieces of programming code

Usually disguised as something else

Cause unexpected and usually undesirable events

Often attached to files

- when file is opened, virus executes

Deliver a “payload”

- e.g. display a message
- delete or modify a document
- reformat hard drive

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
  - e.g. Visual Basic or VBScript
- infect documents
  - insert unwanted words, numbers or phrases
- infect application templates
  - thereby embedding itself in all future docs

Famous Virus: Melissa

Melissa attacked computers in March 1999, infecting machines when users opened a Word document attachment.

Though the effect the virus had on individuals' computers was minimal, users of Outlook Express unintentionally sent virus on to first 50 people who were in their Global Address Book.

For companies, however, the virus had a larger impact.

The virus was sent to users with the subject, "Important message from [name]."

More than a million users were affected, the BBC reported.

Also caused $80 million in damage, and was first virus to travel through e-mail.

Worms

Harmful programs that reside in active memory of a computer

Duplicate themselves

- can propagate *without* human intervention (unlike viruses)

Send copies of themselves to other computers via

- email (e.g. zip file attachment)
- Internet Relay Chat (IRC)

Negative impact of virus or worm attack

- lost data and programs
- lost productivity
  - as workers attempt to recover data & programs
- effort for IT workers
  - to clean up mess

Cost Impact of Worms

TABLE 3-1 Cost impact of worms

Name	Year released	Worldwide economic impact
ILOVEYOU	2000	$8.75 billion
Code Red	2001	$2.62 billion
SirCam	2001	$1.15 billion
Melissa	1999	$1.10 billion

The Love Bug worm flooded Internet with e-mails in May 2000 with subject, ILOVEYOU.

Body of deceptive e-mail read, "Kindly check attached love letter coming from me."

When opened, wreaked havoc on computers, replicating automatically, sending copies to everyone in user's address book, & damaging computer files, e.g. MP3s.

First detected in Asia, Love Bug spread across the world, infecting U.S. government computers at Congress, the White House and the Pentagon.

Estimated that the worm affected 80 percent of businesses in Australia, and a similar percentage in the United States.

Trojan Horses

Program that a hacker secretly installs

Used to steal passwords, SSNs or spy on users by recording keystrokes

Users are tricked into installing it

- e.g. disguised as iTunes file or malicious web site

Logic bomb – another type of Trojan Horse

- executes under specific conditions
- triggered e.g. by
  - change in a particular file
  - typing a specific series of keystrokes
  - specific date/time

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

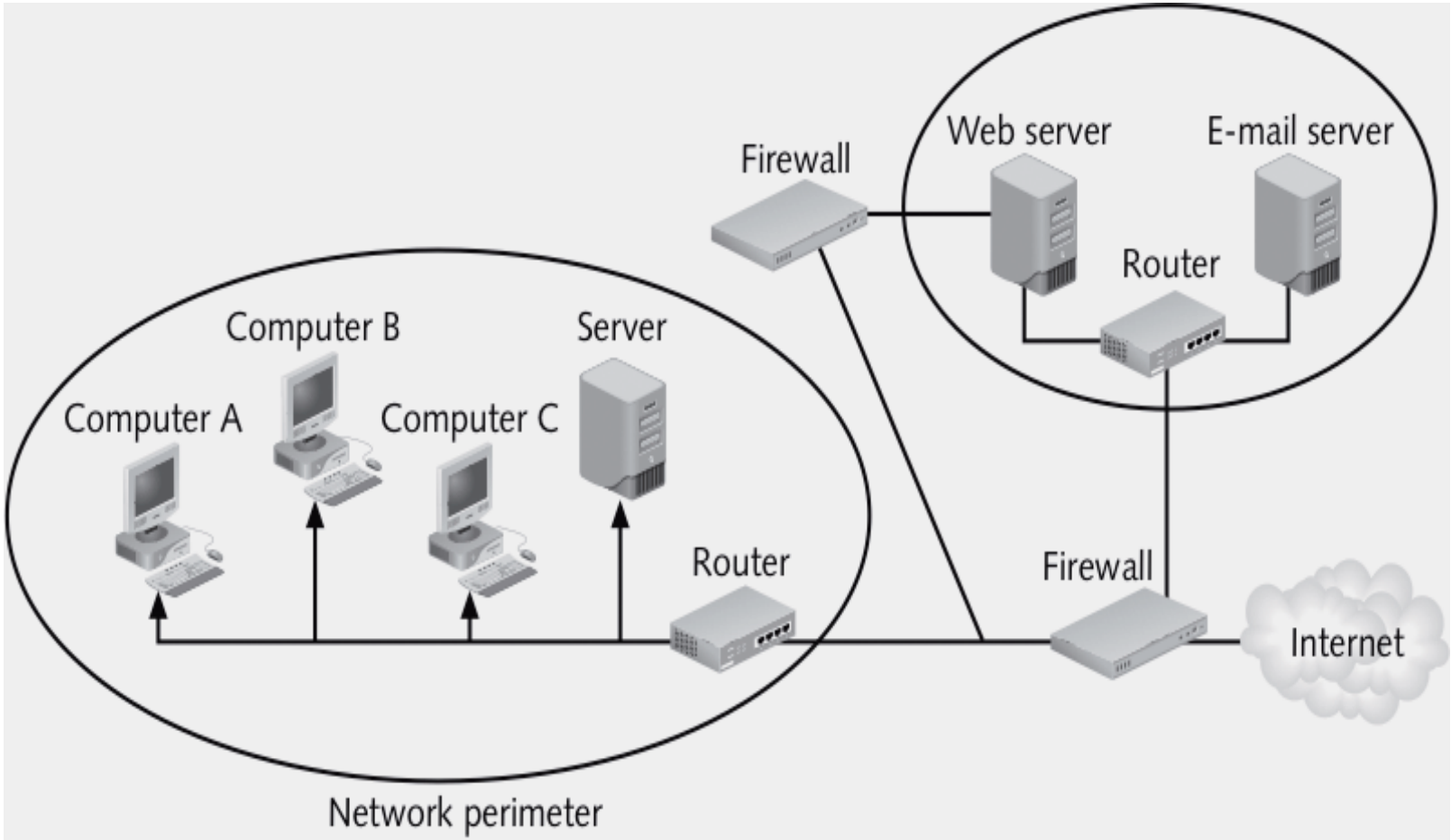

FIGURE 3-3 Firewall protection

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