Information Communication Technologies

Lecture 13. **Computer Security**

Kassymova Aizhan Bakhytzhanovna
PhD, Associate professor
a.kassymova@satbayev.university

Agenda

1 Security Threats

2 Intruders: Who, Why, and How?

3 Identity Theft and Privacy Violation

4 Malicious Software

5 Denial of Service

Security Threats

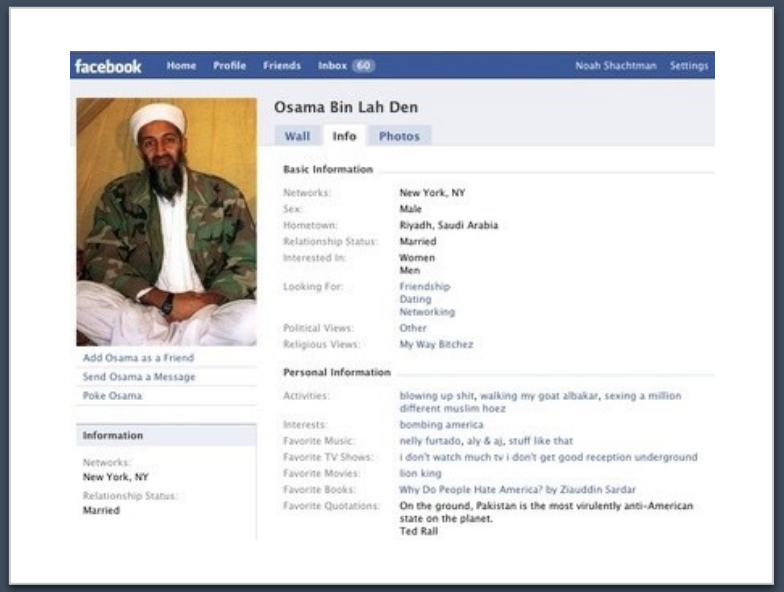
- **Data confidentiality**- data access is restricted to authorized personnel
- **Data integrity**- data is not altered unintentionally
- **Data availability**- services that enable data access are operational

Who are the Intruders?

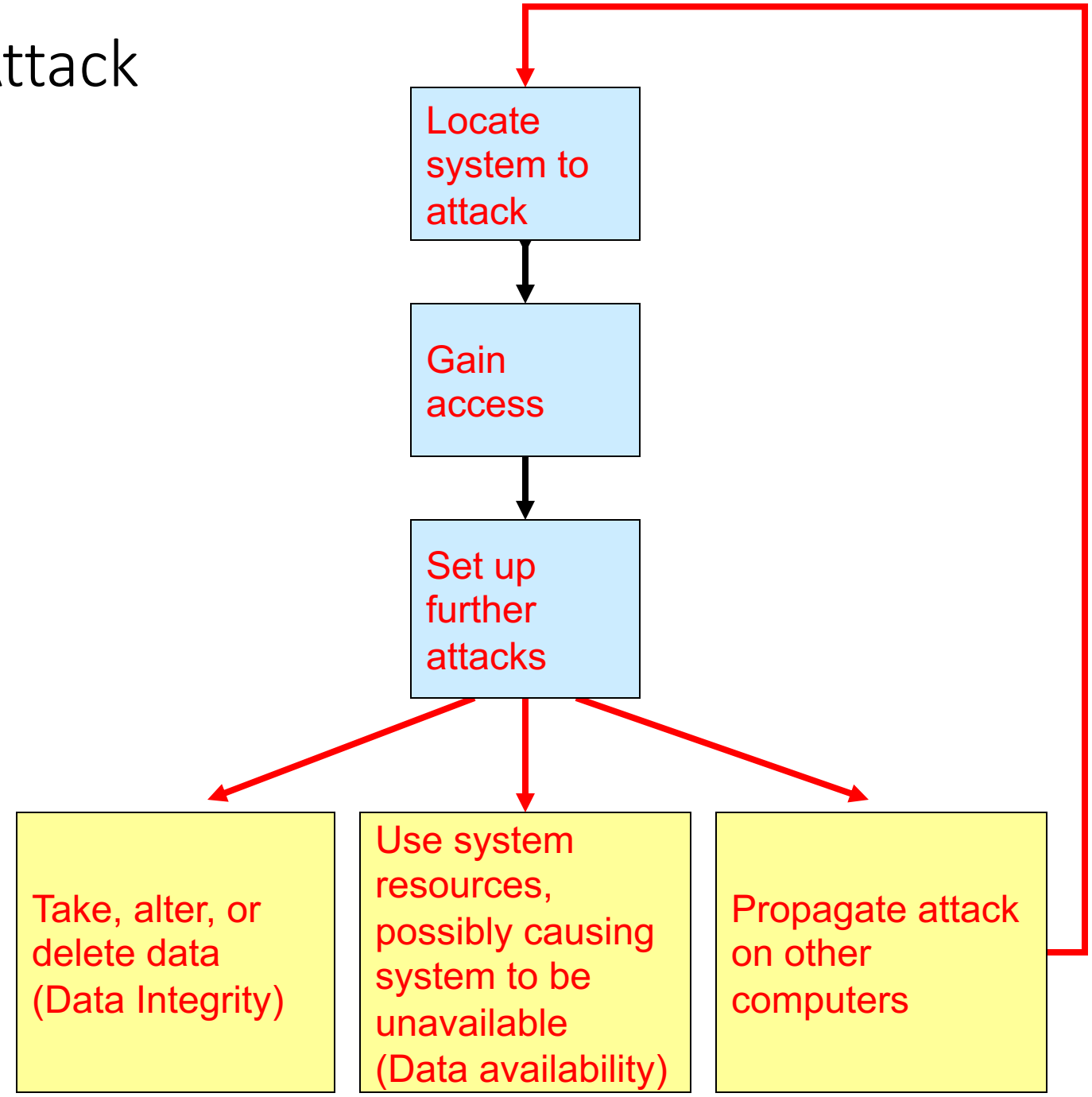
- **People who hack for fun**, curiosity, personal pride, or just for the sake of breaking into computer systems to see how far they can get
- Internal or external personnel who may be seeking **revenge on the targeted organization**
- **People who may want to make a profit** or gain other benefits using confidential data from the targeted system (for example, business advantage, military advantage)

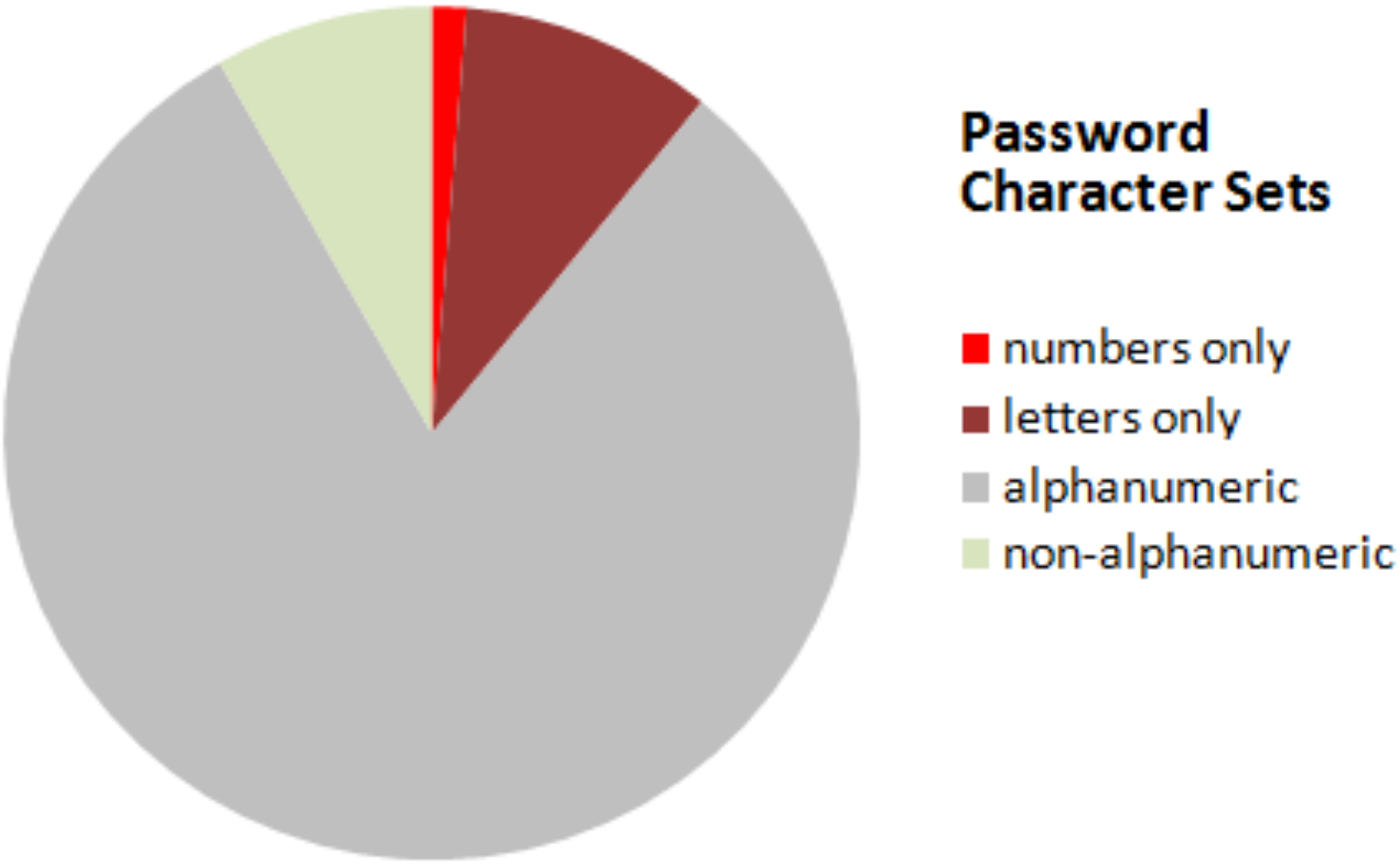
Who are the Intruders? (continued)

- **Criminals** or organizations whose objective is to **corrupt the security** of the targeted system for unethical purposes including blackmail and industrial espionage
- **Terrorists** who want to promote political aims and demoralize the victim country



Process of Attack




Password
Character Sets
numbers only
letters only
alphanumeric
non-alphanumeric

Identity Theft: Password Cracking

- Password Cracking
  - ***Dumpster diving,*** rummaging through trash to find passwords
  - ***Brute force method***, trying all different alphanumeric combinations until the password is cracked
  - ***Dictionary attack***, matching every word in the dictionary against the password to decrease the search space

Dumpster diving

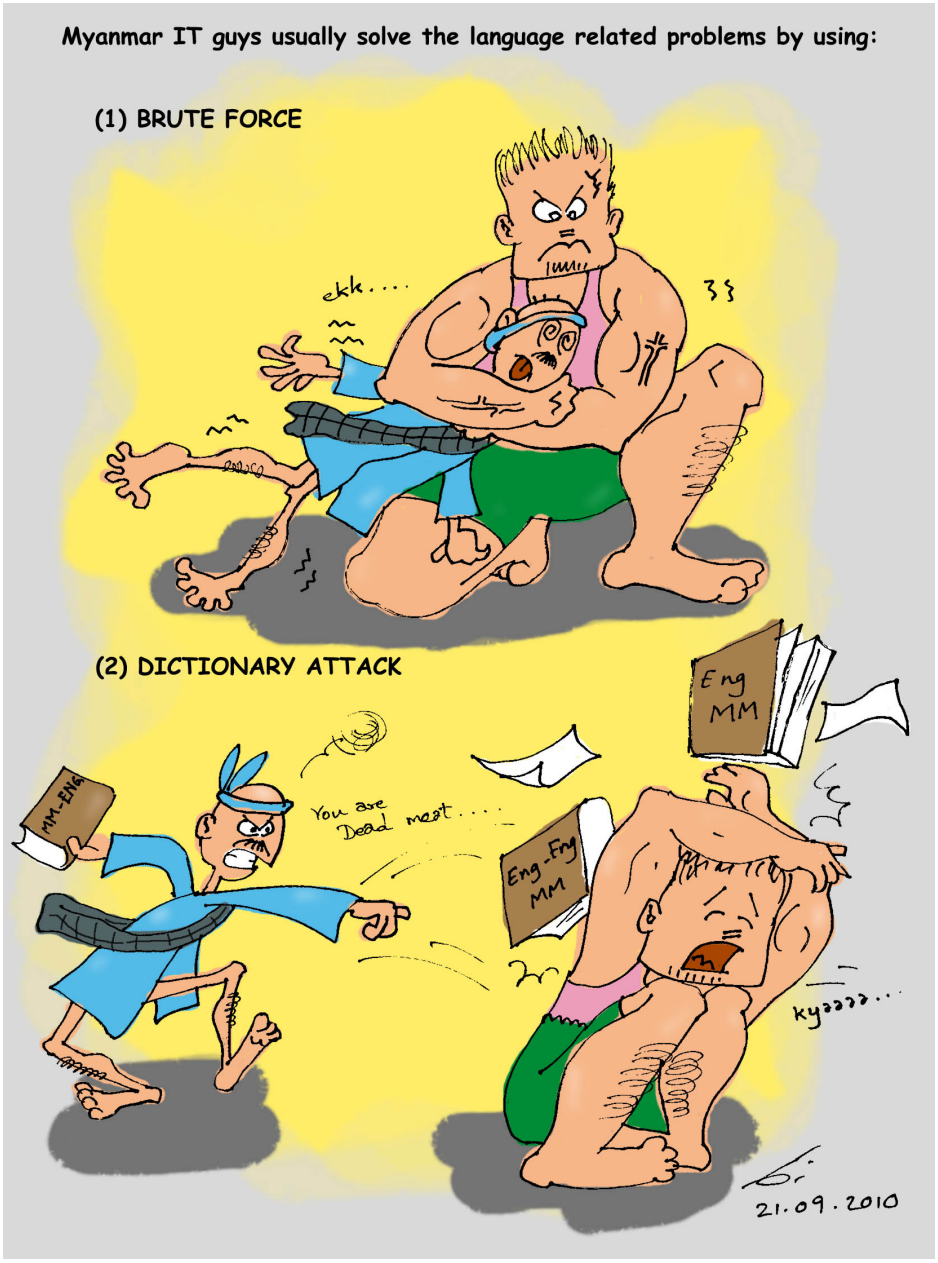
Dictionary Attack

- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

Brute Force

- Guess every possible password
- Depending on the length and complexity of your password, this can take time
- If it takes an infeasibly long time to find your password, you may be safe

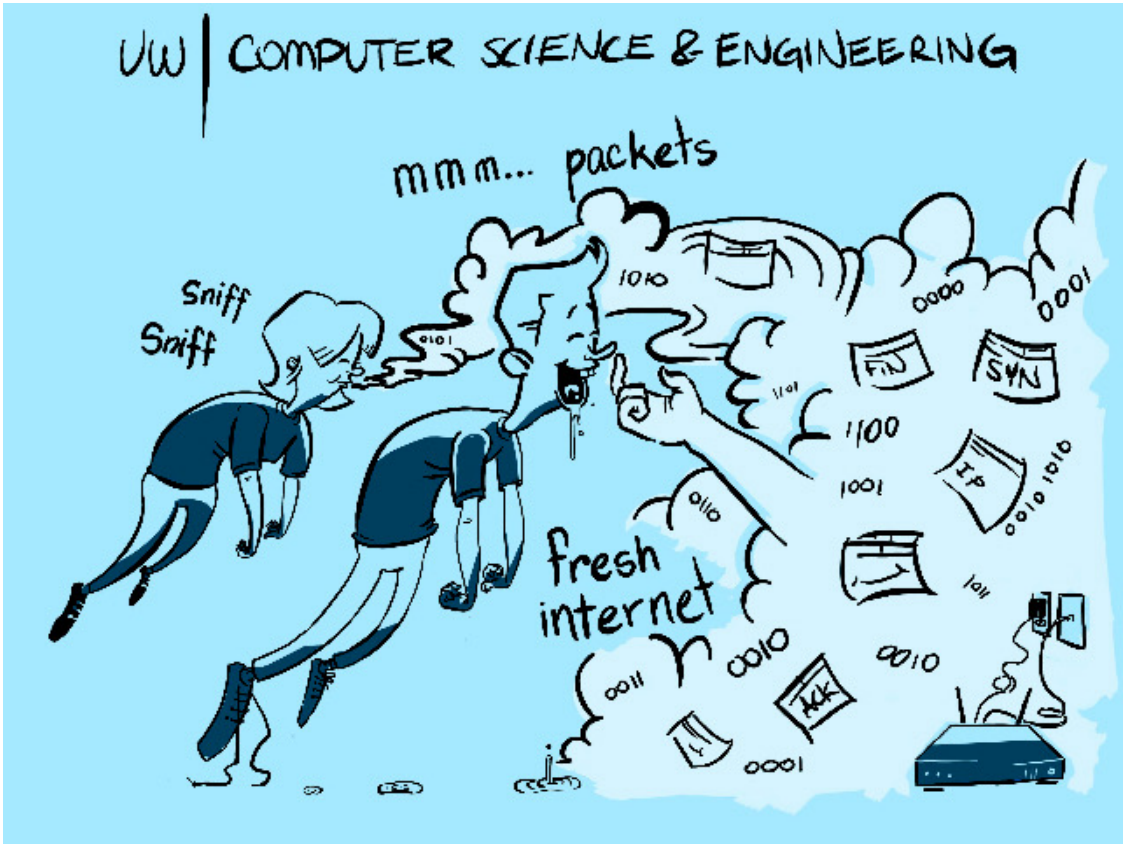
Myanmar IT guys usually solve the language related problems by using:



Identity Theft: Password Cracking (continued)

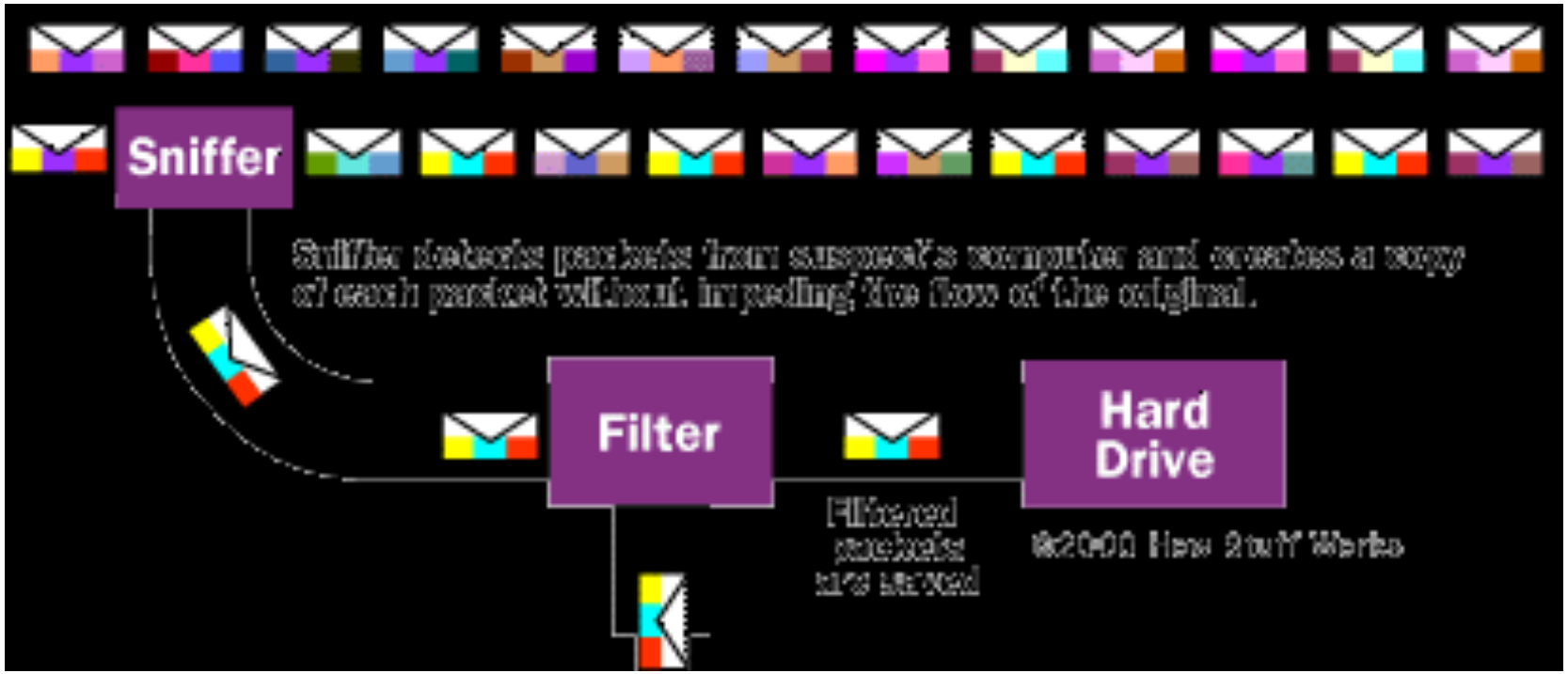
- Prevention
  - **Do not throw away legible password information in the trash** or leave your passwords at obvious places
  - **Destroy or lock up sensitive information**
  - **Use difficult to guess passwords** that are resistant to brute force or dictionary attacks
  - **Change passwords frequently**
  - **Limit physical access to computer** areas, especially central servers

Packet Sniffing



Identity Theft: Packet Sniffing

- ***A packet sniffer*** is **a software program or a hardware device that captures data packets as they are transmitted through the network**.



Packet Sniffing

- Can be installed on communication channels that are shared by a LAN (e.g. wireless network or cable modem)
- Prevention:
  - **Employ data encryption to use encrypted protocols (more about encryption will be discussed later)**
  - **Limit physical access to network connections**
  - **Monitor network usage and investigate abnormal or suspicious activities**

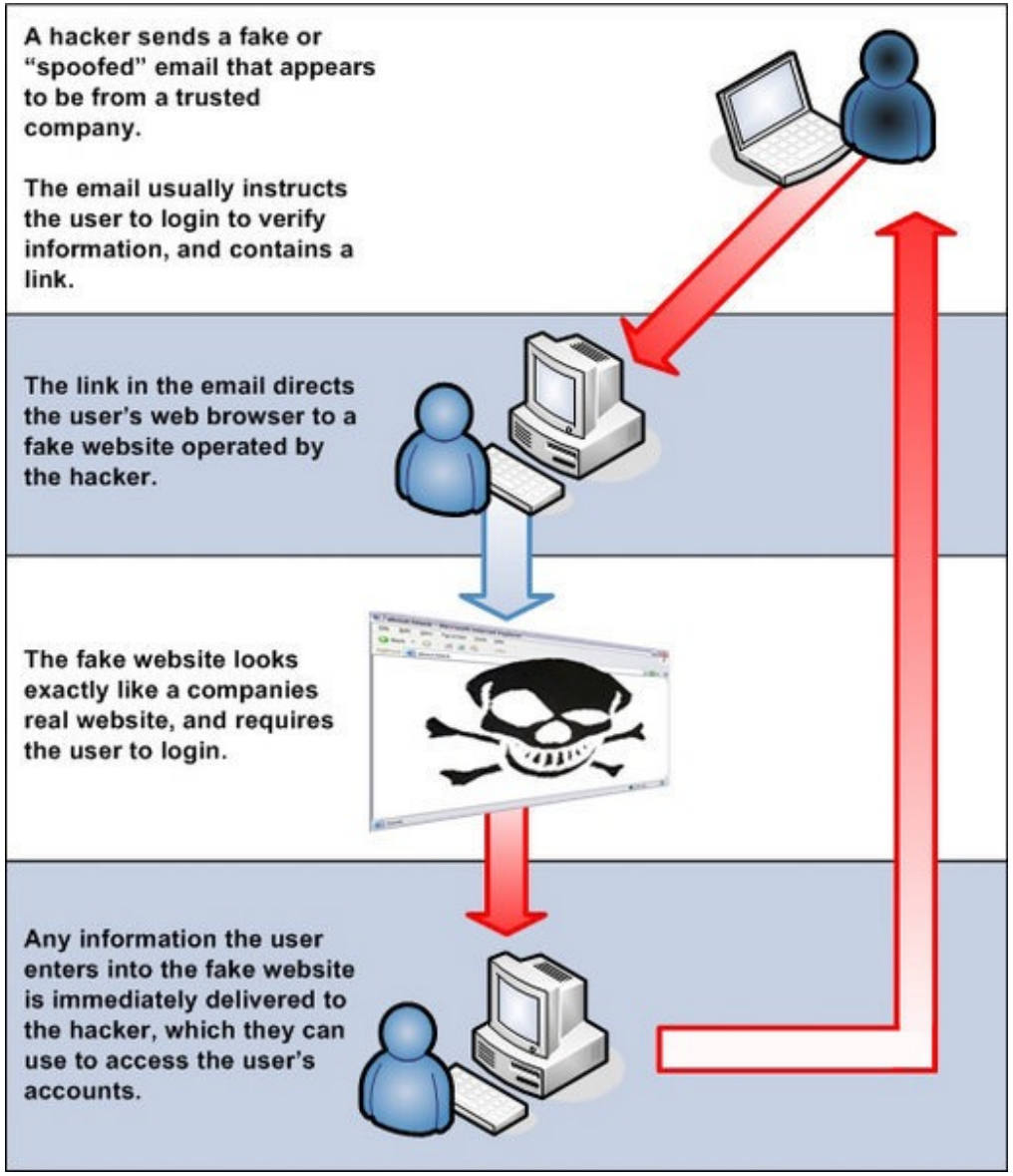
Packet Sniffing

- Which Web sites you visit
- What you look at on the site
- Whom you send e-mail to
- What's in the e-mail you send
- What you download from a site
- What streaming events you use, such as audio, video and Internet telephony
- Who visits your site (if you have a Web site)

Social Engineering

- ***Social engineering*** **refers to the action of tricking people into providing information needed to gain access to systems**.
  - Does not involve a software tool
  - Manipulation of the network administrator or other authorized user (account name and password information)
  - Achieved over the phone, via email or even in person pretending to be someone important in an organization (**Quid pro quo)**

Social Engineering: Phishing



Social Engineering (continued)

- Prevention:
  - Verify identities of people requesting sensitive information
  - Become aware of social engineering schemes and educate others of security policies and their importance

Spoofing

- ***Spoofing* is the act of using one machine to impersonate another**.
- Intruder can mask the identity of a machine with special access privileges to obtain control of other computers on the network.
- Intruder can use spoofed machines to attack other machines causing the spoofed machines to become liable for the attack

Spoofing (continued)

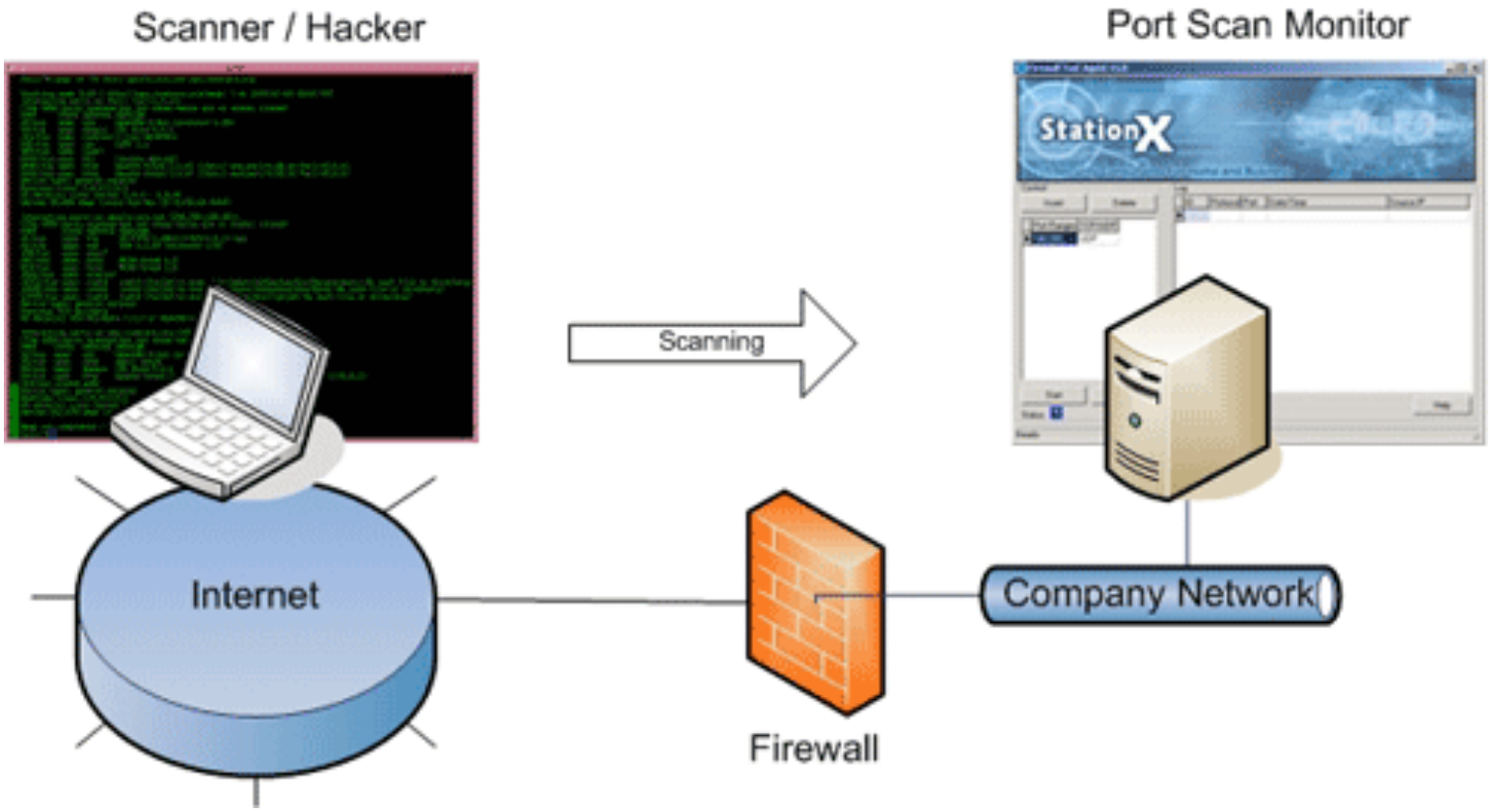
- ***IP spoofing*** is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- ***Email spoofing*** is where an attacker **fakes an email header** to make it appear as if it came from somewhere or someone other than the actual source.

Spoofing (continued)

- Prevention:
  - Monitor transaction logs of servers such as email server, Web server, and scan for unusual behaviors (monitoring should be done off-line to avoid attacks during the process)
  - Minimize system privileges of servers
  - Limit user access to network or administrator command functions

Port Scanning

- ***Port scanning*** **is used to detect security weaknesses in a remote or local host**
  - Usually a precursor to an attack on a target system.
- A ***port scanner*** is a program that scans TCP/IP ports and services (for example, TELNET or FTP) and reports responses from the target system.
  - Can be used to find information about the target host such as which port is open and whether an anonymous user can log in.
- Prevention:
  - Close unused ports & monitor suspicious network activities.



Port Scanning

Brain.a – first virus for PC

- Welcome to the Dungeon © 1986 **Basit** * **Amjad** Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Contact us for vaccination...

Viruses

- Programs or pieces of code that are loaded onto your computer without your knowledge
- They can attach themselves to files, reproduce, and spread to other files.
- Viruses can:
  - corrupt or destroy data
  - display irritating messages
  - disrupt other computer tasks

Viruses

- An infected computer can become a host computer to infect other computers.
- Computer viruses can infect .exe files, system files and word processor or spreadsheet applications containing macros.
- When a computer executes an infected program, it also executes the attached virus instructions.

Types of Viruses

- ***File virus*** - attaches itself to an application program
  - Chernobyl - designed to lurk in computer until April 26
- ***Boot sector virus*** - infects the system files that your computer uses every time you turn it on
- ***Macro virus*** - infects the word processor or spread sheet files by creating a destructive ***macro***, a miniature program that usually contains legitimate instructions to automate document and worksheet production
  - Infected files can be sent via e-mail as an attachment
  - When the infected attachment is opened, the virus enters the general pool of macros and spread to other documents that pick up the macros

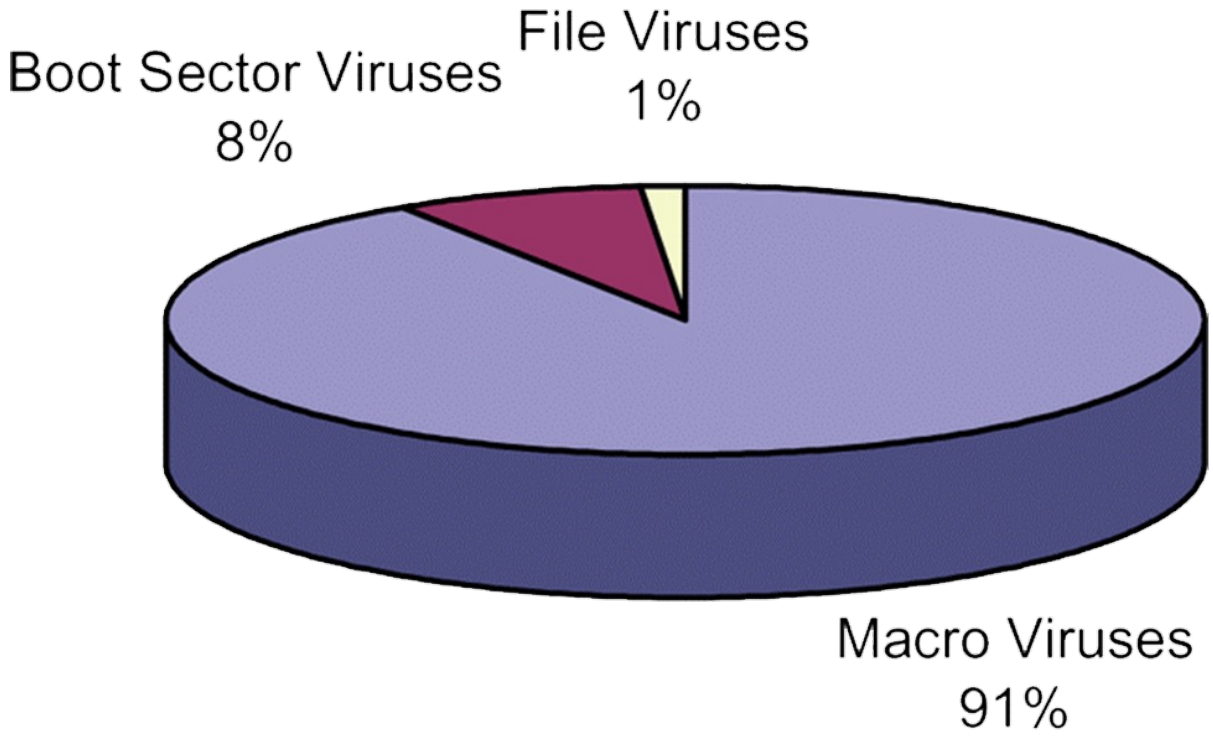
Melissa Macro Virus

- Arrives as an email message with **"list.doc"** attached.
- The subject line of the email usually contains, **"important message from"**.
- It affects Microsoft Outlook client
- When opened, Melissa alter the macro security setting to allow other macros to execute.
- Opens Outlook address book and sends copies of itself along with the document that contains it to other users without the original user's knowledge.
- It can infect other Word files.

Love Bug

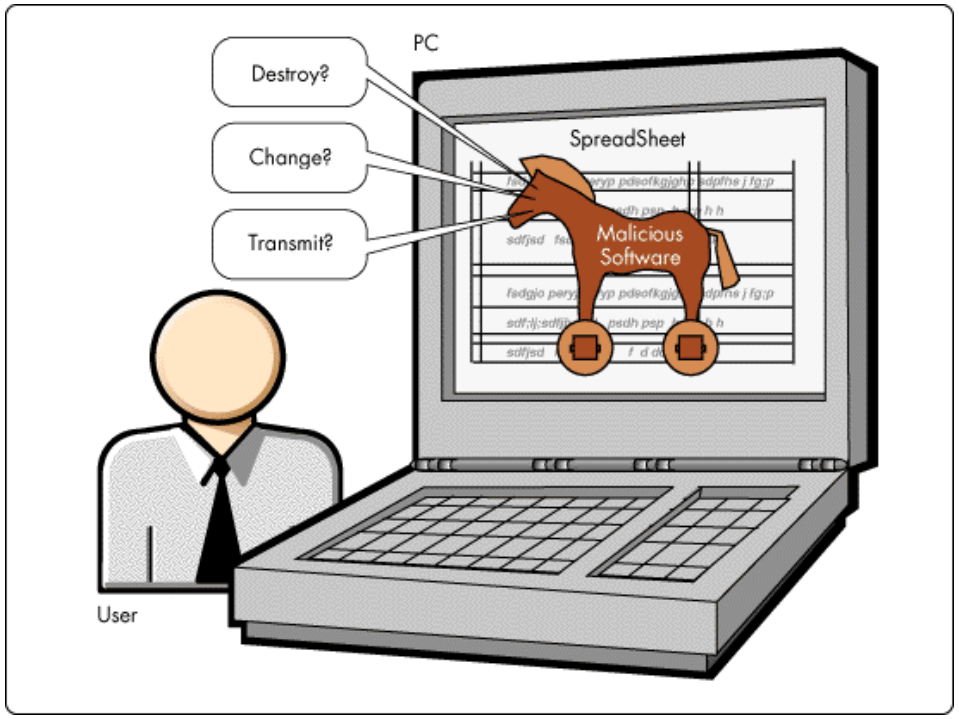
- LOVE-LETTER-FOR-YOU.TXT.vbs.
- Virus overwrites most of the music, graphics, document, spreadsheet, and Web files on your disk.
- Virus mails itself to everyone in your email address book.
- The damage due to the Love Bug cost up to US**$8.7 billion**

Macro Viruses are the Most Prolific



Trojan Horses

- **Programs that appears to be performing one task while executing a malicious task in the background.**
- May reach your computer as an email attachment, usually as amusing or seemingly useful software to entice you to open it.



Trojan Horses (continued)

- Once you open the attachment, the Trojan horse program can
  - Search for your user information
  - Steal your login names,
  - Copy your passwords
  - Delete, modify, or transmit files on your computer
  - May contain viruses, worms, or other Trojan horse programs
  - Use your account privileges to install other programs such as programs that provide unauthorized network access
  - Use your account to attack other systems and implicate your site as the source of an attack
  - Use your account to increase the level of access beyond that of the user running the program
  - Does not replicate itself

Trojan Horses (continued)

- Many Internet security problems are due to Java applets and ActiveX controls.
- ***Java applet*** - **program which adds interactive capabilities to Web pages.**
  - Can be downloaded automatically to a secure area of the computer called the ***sandbox***
    - Hackers can breach sandbox security
- **ActiveX controls also add interactivity to Web pages, but have full access to the entire computer.**
  - Hackers can use ActiveX controls to cause havoc

Trojan Horses (continued)

- Prevention:
  - ***Digital certificates*** (will be discussed later) can identify the author of an ActiveX control
    - Programs with digital certificates should be safe
  - Some companies implement a ***firewall*** (will be discussed later) to screen out potentially hostile programs.

Trojan Horses (continued)

- This type of virus does not harbor in the disk and do not replicate.
- Another type appears as a network password screen, it emails the id and password when entered to a hacker program which accesses the data from the computer by defeating the network security.

Worms

- A ***software worm*** **is a program designed to enter a computer system through security holes.**
  - Usually through a network (TCP/IP packets)
  - Does not need to be attached to a document to reproduce
  - Can replicate itself and use memory resources, but cannot attach itself to other programs
  - Can be stored on the computer, and then email itself to other computers

Worms (continued)

- Worm can affect the PC systems and network servers.
- They affect LAN and internet users by disrupting their access to files, web pages, and other service provided by the network.

- Worm sample: 911 Worm
- C:\windows
  C:\windows\system
  C:\windows\command
  C:\

Time Bombs and Logic Bombs

- A virus can lurk in your computer system for days or months without discovery.
- A ***time bomb*** is a computer program that stays in your system undetected until it is triggered by a certain event in time.
  - usually carried by a virus or Trojan horse
  - For Example, **Michaelangelo virus affects the system on March 6, birth date of Michaelangelo.**
- ***Logic bomb*** - program triggered by appearance or disappearance of specific data.

Preventing Malicious Code Attacks

- Avoid opening unexpected email messages or attachments
- Be cautious and use only authorized media for loading data and software
- Do not run executable programs unless you trust the sender of the information and you confirmed with the sender that the message did originate from the sender.
- Avoid sending programs from an unknown source to others
- Be cautious when executing content such as Java applets, JavaScript, or Active X controls from web pages
- Disable macros and automatic execution of web page content if possible

Detecting Malicious Codes

- The following symptoms *might* indicate that your computer has caught a virus:
  - Unexpected changes in file sizes or date/time stamps
  - Slow starting or slow running because the virus is exhausting computer's resources
  - Unexpected or frequent system failures
  - Low computer memory on disks
  - Abnormal application behaviors
  - Displays a vulgar, embarrassing or annoying message
  - Develops unusual visual or sound effects
  - Difficulty saving files

Counter Measures

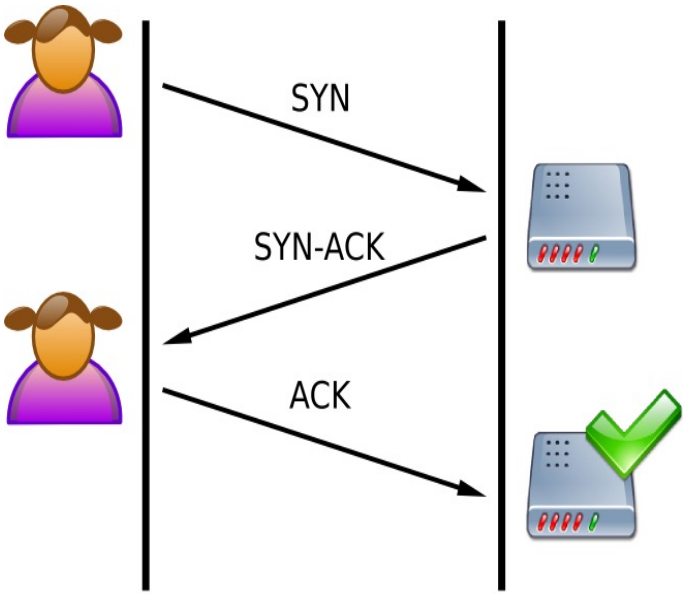
1. Try to contain the virus.
2. Try to identify the virus.
3. Try to recover corrupted data and files.
4. Once you have determined the source of infection, alert others of the virus.

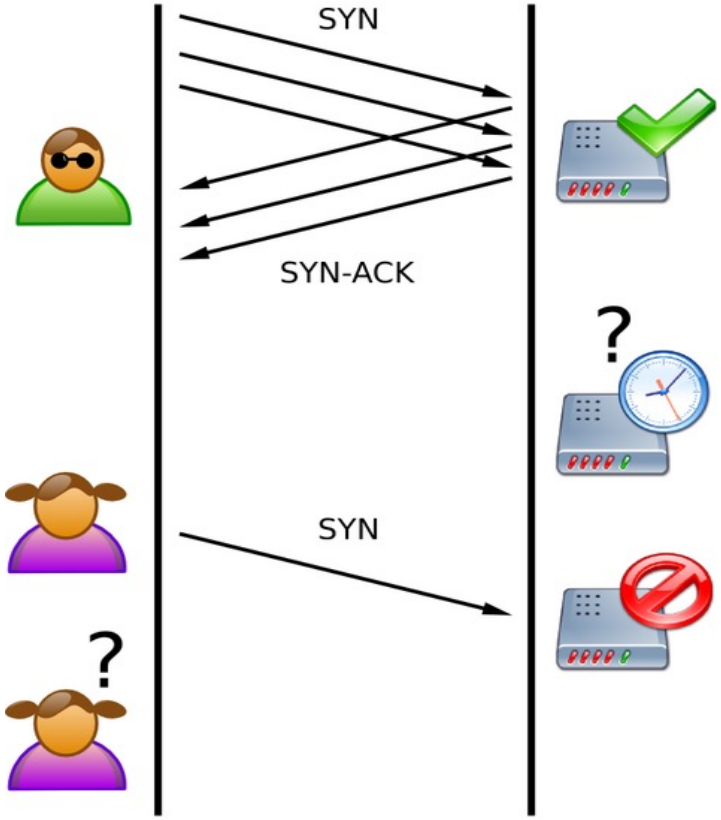
Denial of Service (DoS)

- Objectives of DoS attack:
  - Disruption of network connectivity and Internet services
  - Disruption of services to specific system(s) or person(s)
  - Consumption of other resources on a computer system

Methods of DoS attack

- **To tie up network connectivity of the target machine, an intruder can initiate a half-open connection to the target machine (e.g. SYN flood attack)**



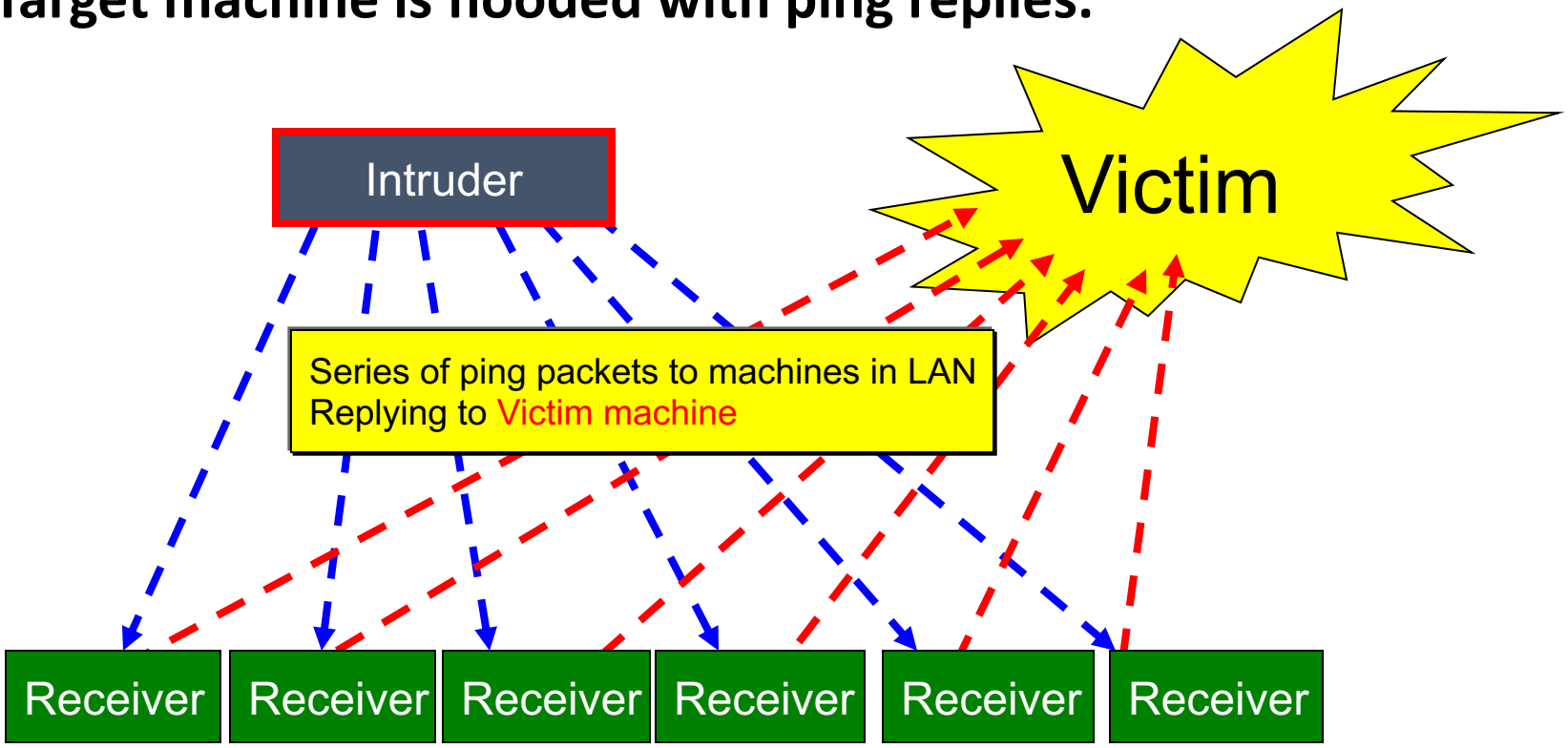


Methods of DoS attack

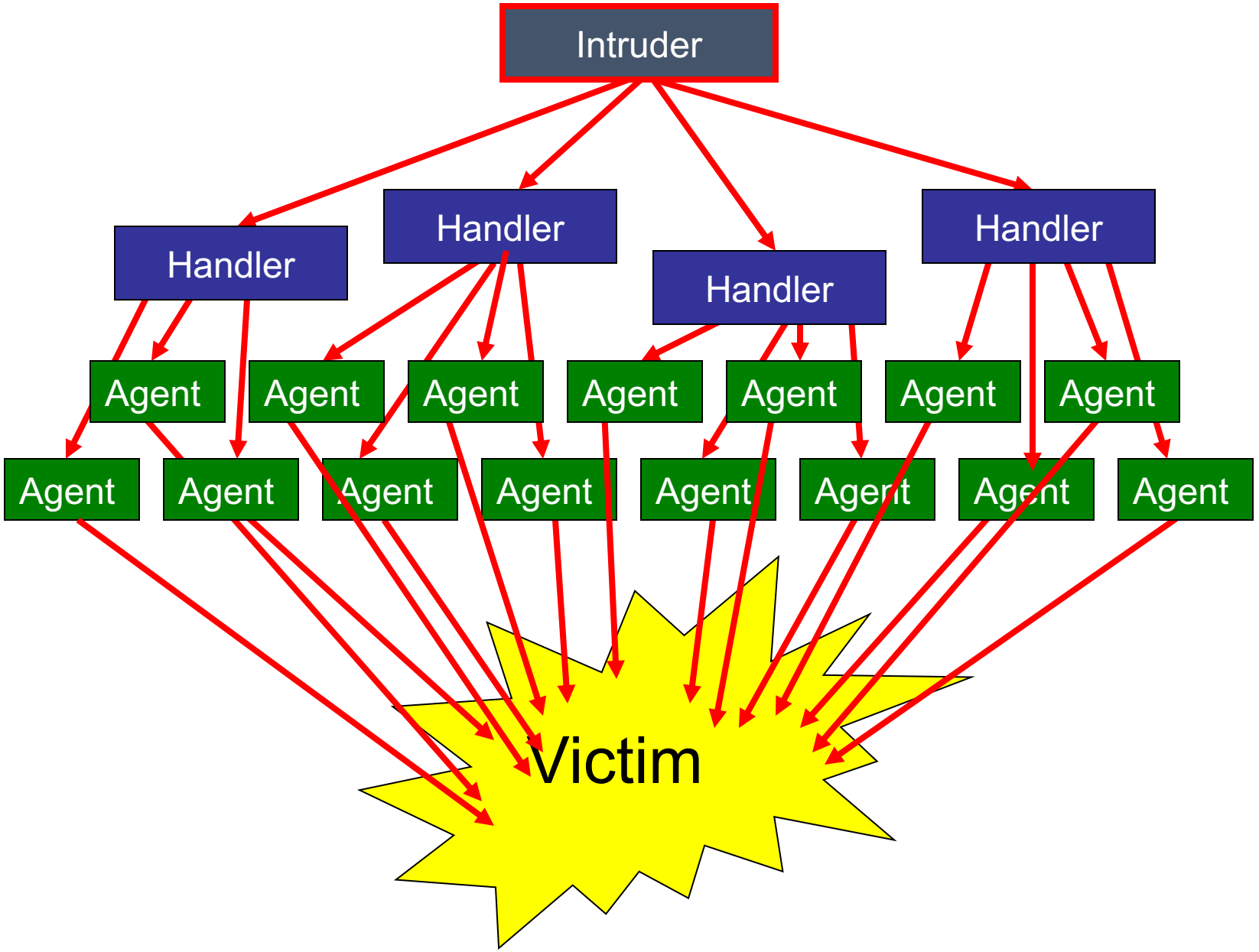
- Target system's network bandwidth to generate an excessive amount of traffic on that network
- Exhaust system resources such as CPU cycles, memory, and disk space
- Spam an email server by generating excessive numbers of email messages. For instance, when 80% of your email storage is filled with spam mails, disk space needed to store legitimate emails will be limited.
- Generate error messages that need to be written to disk continuously to exhaust disk space

Smurf Attack

- **Send ping commands repeatedly using the victim's address as the return address**
- **Receiver machines reply to the innocent, spoofed target system for each Ping command.**
- **Target machine is flooded with ping replies.**



Distributed Denial of Service Attacks



Preventing DoS Attacks

- Disable or block any unused network services.
- Observe your system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.
- Routinely examine your physical security with respect to your current needs (for example, servers, routers, unattended terminals, network access points).

End of Lecture 13