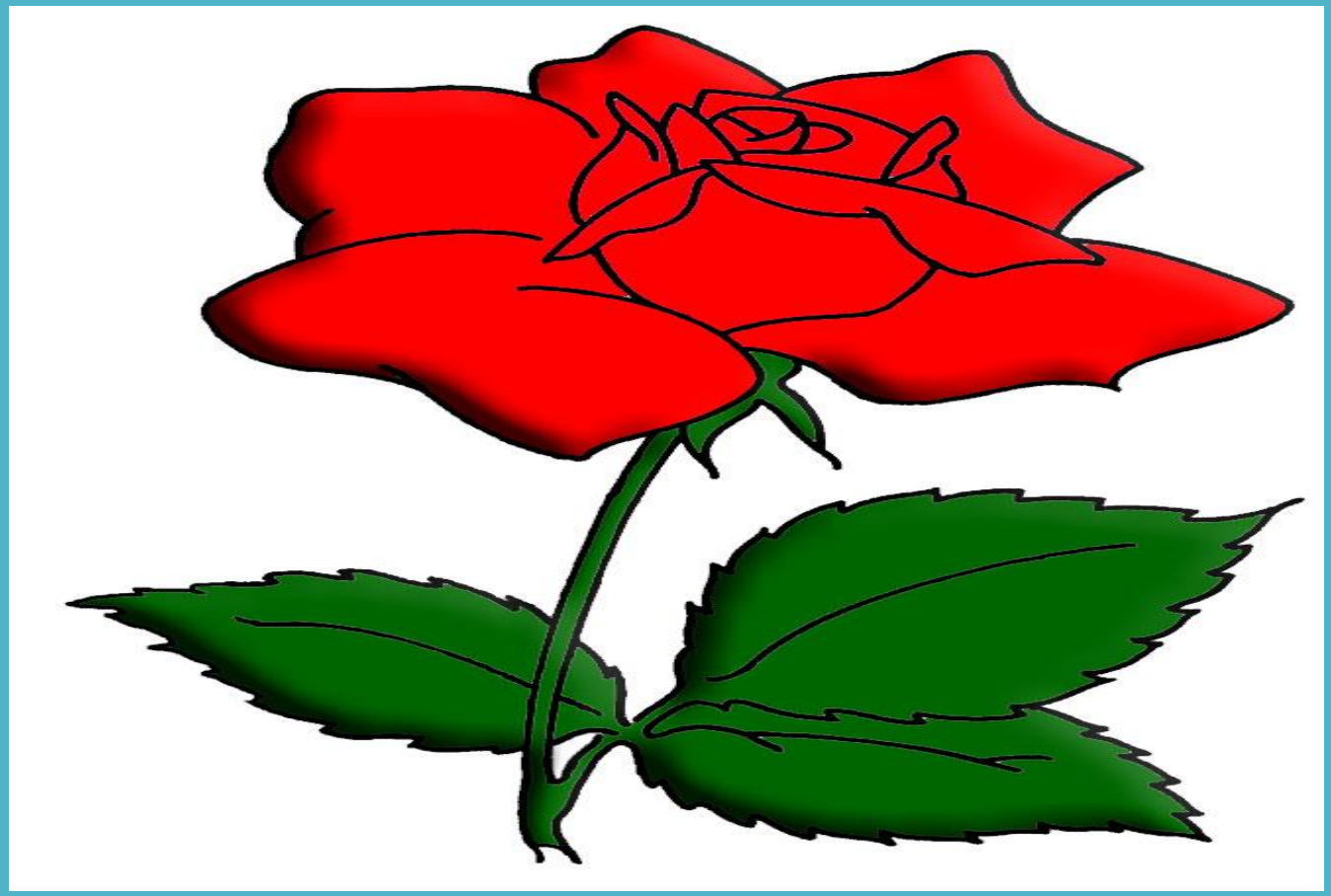
welcome



Shantonu Roy
Junior Instructor (Computer)
Sylhet Polytechnic Institute, Sylhet
Computer Technology(66)
Semester: 7th

Cyber Security & Ethics (66675)

Chapter-1: Understand Cyber Security

Introduction

- The term cyber security is used to refer to the security offered through on-line services to protect your online information.

- With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also.

To Understand

What is the meaning of the word CYBER

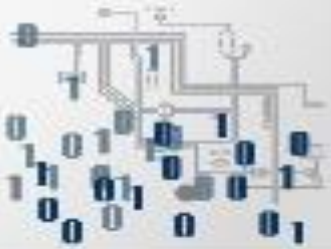
What is the need of Cyber Security

What are the security problems in Cyber field

How to implement and maintain Security of a Cyber field around us.

Meaning of the Word CYBER

- It is a combining form relating to information technology, the Internet, and virtual reality.



Need of cyber security

- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.


CIA Triad
Availability
Confidentiality
Integrity

Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability, known as the CIA triad (Figure 1), is a guideline for information security for an organization. Confidentiality ensures the privacy of data by restricting access through authentication encryption. Integrity assures that the information is accurate and trustworthy. Availability ensures that the information is accessible to authorized people.

Confidentiality

Another term for confidentiality would be privacy. Company policies should restrict access to the information to authorized personnel and ensure that only those authorized individuals view this data. The data may be compartmentalized according to the security or sensitivity level of the information. For example, a Java program developer should not have to access to the personal information of all employees. Furthermore, employees should receive training to understand the best practices in safeguarding sensitive information to protect themselves and the company from attacks. Methods to ensure confidentiality include data encryption, username ID and password, two factor authentication, and minimizing exposure of sensitive information.

Integrity

Integrity is accuracy, consistency, and trustworthiness of the data during its entire life cycle. Data must be unaltered during transit and not changed by unauthorized entities. File permissions and user access control can prevent unauthorized access. Version control can be used to prevent accidental changes by authorized users. Backups must be available to restore any corrupted data, and checksum hashing can be used to verify integrity of the data during transfer.

Availability

Maintaining equipment, performing hardware repairs, keeping operating systems and software up to date, and creating backups ensure the availability of the network and data to the authorized users. Plans should be in place to recover quickly from natural or man-made disasters. Security equipment or software, such as firewalls, guard against downtime due to attacks such as denial of service (DoS). Denial of service occurs when an attacker attempts to overwhelm resources so the services are not available to the users.

Major security problems

- Virus
- Hacker
- Malware
- Trojan horses
- Password cracking

Viruses and Worms

- A Virus is a “program that is loaded onto your computer without your knowledge and runs against your wishes

Solution

- **Install a security suite that protects the computer against threats such as viruses and worms.**

Malware

- The word "malware" comes from the term "**MAL**icious soft**WARE**."
- Malware is any software that infects and damages a computer system without the owner's knowledge or permission.

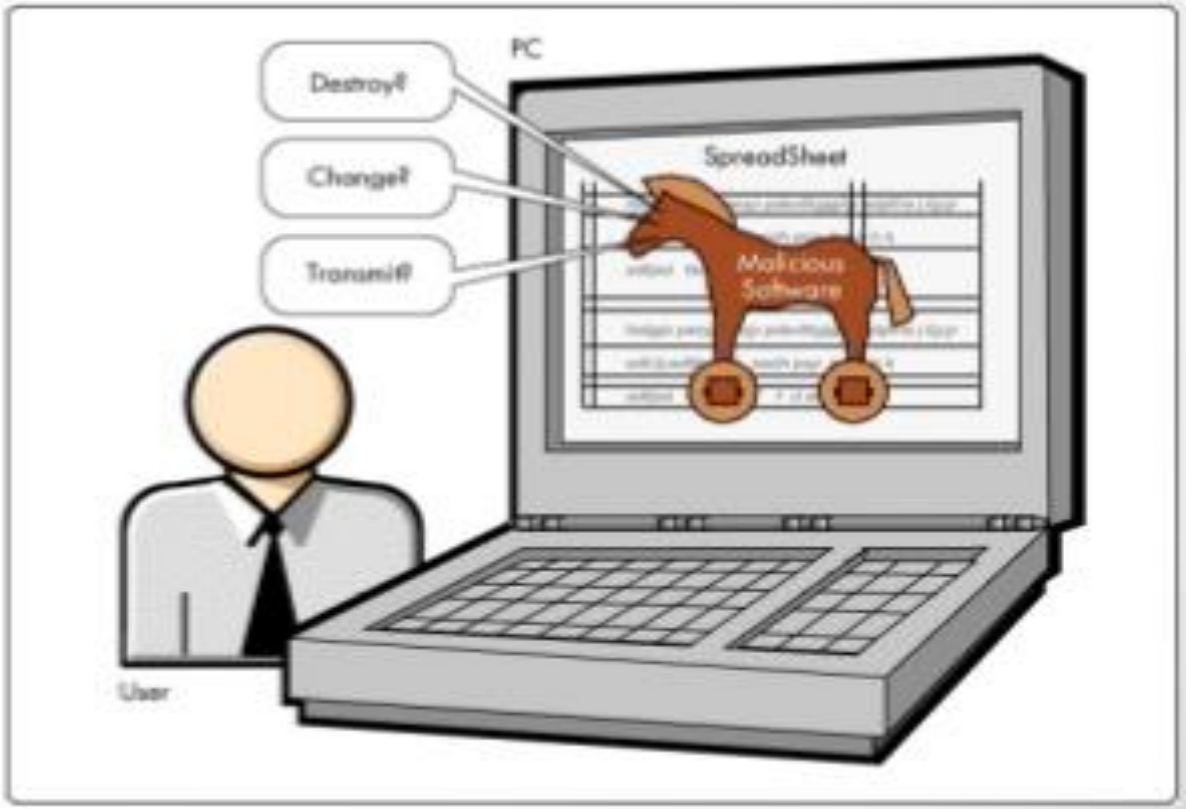
To Stop Malware

- Download an anti-malware program that also helps prevent infections.

- Activate Network Threat Protection, Firewall, Antivirus.

Trojan Horses

- Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
- These viruses are the most serious threats to computers



How to Avoid Trojans

- **Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.**

Password Cracking

- **Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.**

Securing Password

- Use always Strong password.
- Never use same password for two different sites.

Cyber Security Is Everyone's Responsibility

Chapter-2: Data and Evidence Recovery

Overview

- ✓ What is Data Recovery?
- ✓ How can it be used?
- ✓ Techniques
- ✓ *Recovery Methods*
- ✓ *Secure Deletion*
- ✓ *Private vs. Government services*
- ✓ *Software vs. Hardware Solutions*
- ✓ What can you do?

What is data recovery?

Retrieving deleted/inaccessible data from electronic storage media (hard drives, removable media, optical devices, etc...)

Typical causes of loss include:

- Electro-mechanical Failure
- Natural Disaster
- Computer Virus
- Data Corruption
- Computer Crime
- Human Error

Cases of Recovery

FIRE

Found after a fire destroyed a 100 year old home – All data Recovered

CRUSHED

A bus runs over a laptop – All data recovered

SOAKED

PowerBook trapped underwater for two days – All data recovered

Uses of data recovery

Average User:

- Recover important lost files
- Keep your private information private

Law enforcement:

- Locate illegal data
- Restore deleted/overwritten information.
- Prosecute criminals based on discovered data

Software Recovery of data

Generally only restore data not yet overwritten.

Do not work on physically damaged drives

Undelete Pro, EasyRecovery, Proliant, Novanet, etc.

Prices range from Free-1000

Example: dd on linux used on corrupt floppies

Recovery Methods

- Hidden files
- Recycle bin
- Unerase wizards
- Assorted commercial programs
- Ferrofluid
  - Coat surface of disk
  - Check with optical microscope
  - Does not work for more recent hard drives
- More recently...

Recovery Methods

When data is written – the head sets the polarity of most, but not all, of the magnetic domains

The actual effect of overwriting a bit is closer to obtaining a 0.95 when a zero is overwritten by a one, and a 1.05 when a one is overwritten with a one.

- Normal equipment will read both these values as ones
- However, using specialized equipment, it is possible to work out what the previous "layers" contained

Steps include

- Reading the signal from the analog head electronic with a high-quality digital oscilloscope
- Downloading the sampled waveform to a PC
- Analyzing it in software to recover the previously recorded signal.

Recovery Methods

Scanning Probe Microscopy (SPM)

- Uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface to be analyzed, where it interacts with the stray field emanating from the sample to produce a topographic view of the surface
- Reasonably capable SPM can be built for about US$1400, using a PC as a controller
- Thousands in use today

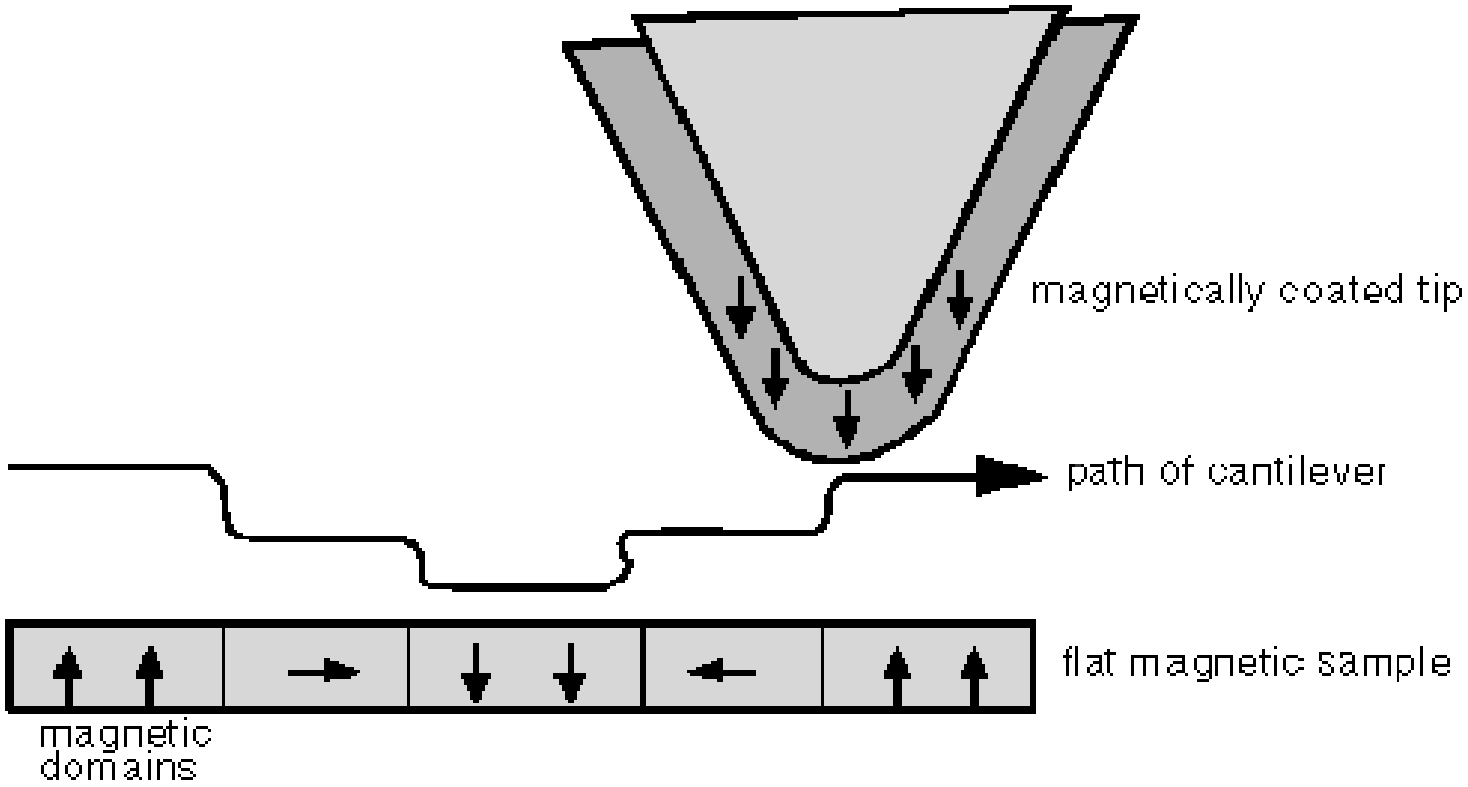
Recovery Methods

Magnetic force microscopy (MFM)

- Recent technique for imaging magnetization patterns with high resolution and minimal sample preparation.
- Derived from scanning probe microscopy (SPM)
- Uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface to be analyzed where it interacts with the stray magnetic field
- An image of the field at the surface is formed by moving the tip across the surface and measuring the force (or force gradient) as a function of position. The strength of the interaction is measured by monitoring the position of the cantilever using an optical interferometer.

Recovery Methods

Magnetic force microscopy (MFM)



Recovery Methods

Using MFM:

Techniques can detect data by looking at the minute sampling region to distinctly detect the remnant magnetization at the track edges.

Detectable old data will still be present beside the new data on the track which is usually ignored

In conjunction with software, MFM can be calibrated to see past various kinds of data loss/removal. Can also do automated data recovery.

It turns out that each track contains an image of everything ever written to it, but that the contribution from each "layer" gets progressively smaller the further back it was made.

Chapter-3: Cyber Crimes

What Is Cyber Crime?

When an offence is committed, in full or in part, via a computer, network or other computer enabled device.
-Warwickshire Police

Types of Cyber Crime

Fraud
Identity Theft
Phishing Scams
Viruses
Revenge Porn
Online Hate Crime
Grooming
Stalking

Holiday Fraud
Dating Fraud
Bullying
Pension Fraud
Hacking
Online Extremism
Child Sexual Exploitation

...and this is just the tip of the iceberg

Stats

As age increases, knowledge of online risks reduces slightly while the feeling of being at risk increases significantly

56.4% of those surveyed in Warwickshire had received a phishing email

1 in 10 fell victim to the phishing scam

Under 18s are the age group most targeted for online harassment or bullying with females targeted twice as much as males

Nearly one third of parents have neither applied online restrictions nor spoken to their children about internet safety

Real Or No Real: Emails

Real Or No Real: Emails

Phishing- The Warning Signs

The offer seems too good to be true

Links do not go to the place you would expect them to

Spelling mistakes throughout the email or in the subject line

The sender's address is not a genuine email (e.g. instead of halifax.co.uk, it is halifab.co.uk, or even fiodnusgbi.hfx

There is a sense of urgency to respond to the email's request

Be aware for calls & texts too!

Viruses

1.4 million cases of computer viruses in the UK (ONS 2016 Crime Data)

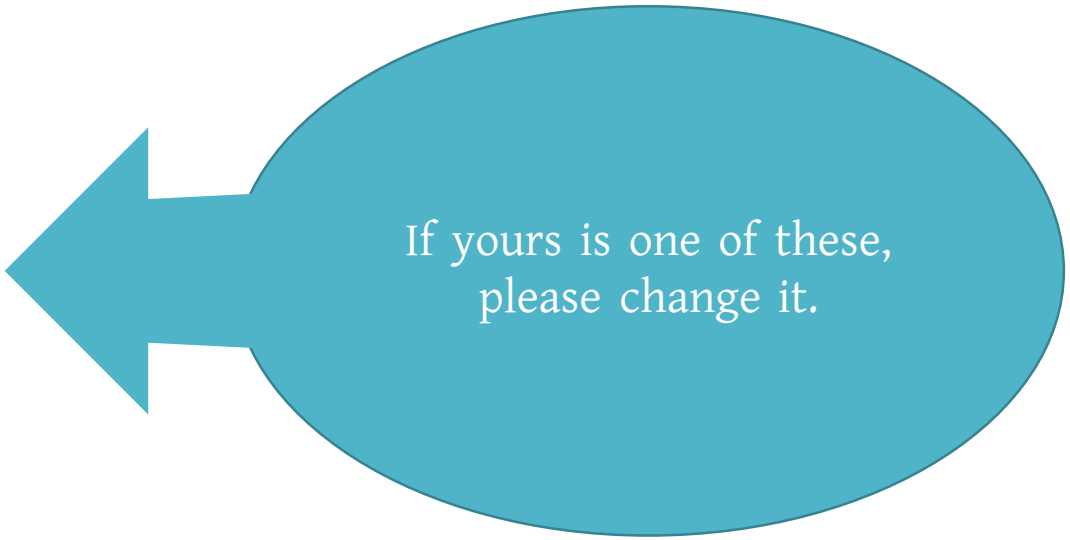
Malware can have harmful effects such as:

- displaying irritating messages
- stealing data
- giving hackers control over your computer
- certain malware can lock your computer until you pay a ‘ransom fee’

Passwords

Pitfall for a great amount of cyber security

Most common passwords globally:
1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball



Passwords

Need a new password?
- think of your favourite book/film/song/poem

- choose a line from it

- take the first letters of each word

- change some of the letters for CAPITALS, numb3r5 and punctuat!on

Top Tips For Online Safety

Be careful of links and attachments in e-mails.

Use different passwords for online accounts.

Check websites security.

If you are ever unsure about something online, do your research.

Anti-virus software.

Top Tips For Online Safety

Keep computer software updated.

Keep all devices safe.

Limit use of public Wi-Fi for work.

Update social media privacy settings.

Report it

Cyber Act in Bangladesh

তথ্য ও যোগাযোগপ্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০১৩)

৫৪ ধারা অনুযায়ী, কম্পিউটার বা কম্পিউটার সিস্টেম ইত্যাদির ক্ষতি, অনিষ্ট সাধন যেমন ই-মেইল পাঠানো, ভাইরাস ছড়ানো, সিস্টেমে অনধিকার প্রবেশ বা সিস্টেমের ক্ষতি করা ইত্যাদি অপরাধ। এর শাস্তি সর্বোচ্চ ১৪ বছর কারাদণ্ড এবং সর্বনিম্ন ৭ বছর কারাদণ্ড বা ১০ লাখ টাকা পর্যন্ত জরিমানা।

৫৬ ধারায় বলা হয়েছে, কেউ যদি ক্ষতি করার উদ্দেশ্যে এমন কোনো কাজ করেন, যার ফলে কোনো কম্পিউটার রিসোর্সের কোনো তথ্য বিনাশ, বাতিল বা পরিবর্তিত হয় বা এর উপযোগিতা হ্রাস পায় অথবা কোনো কম্পিউটার, সার্ভার, নেটওয়ার্ক বা কোনো ইলেকট্রনিক সিস্টেমে অবৈধভাবে প্রবেশ করেন, তবে এটি হবে হ্যাকিং অপরাধ, যার শাস্তি সর্বোচ্চ ১৪ বছর কারাদণ্ড এবং সর্বনিম্ন ৭ বছর কারাদণ্ড বা ১ কোটি টাকা পর্যন্ত জরিমানা।

৫৭ ধারায় বলা হয়েছে, কোনো ব্যক্তি যদি ইচ্ছাকৃতভাবে ওয়েবসাইটে বা অন্য কোনো ইলেকট্রনিক বিন্যাসে কোনো মিথ্যা বা অশ্লীল কিছু প্রকাশ বা সম্প্রচার করে, যার দ্বারা মানহানি ঘটে, আইনশৃঙ্খলার অবনতি হয় অথবা রাষ্ট্র বা ব্যক্তির ভাবমূর্তি ক্ষুণ্ন হয়, তাহলে এগুলো হবে অপরাধ। এর শাস্তি সর্বোচ্চ ১৪ বছর কারাদণ্ড এবং সর্বনিম্ন ৭ বছর কারাদণ্ড এবং ১ কোটি টাকা পর্যন্ত জরিমানা।

Chapter-4: Hacking

Hackers

- In common a **hacker** is a person who breaks into computers, usually by gaining access to administrative controls.

Types of Hackers

- White Hat Hacker
- Grey Hat Hacker
- Black Hat Hacker

Social Engineering

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. For example, an attacker could call an authorized employee with an urgent problem that requires immediate network access. The attacker could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

These are some types of social engineering attacks:

Pretexting - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

Tailgating - This is when an attacker quickly follows an authorized person into a secure location.

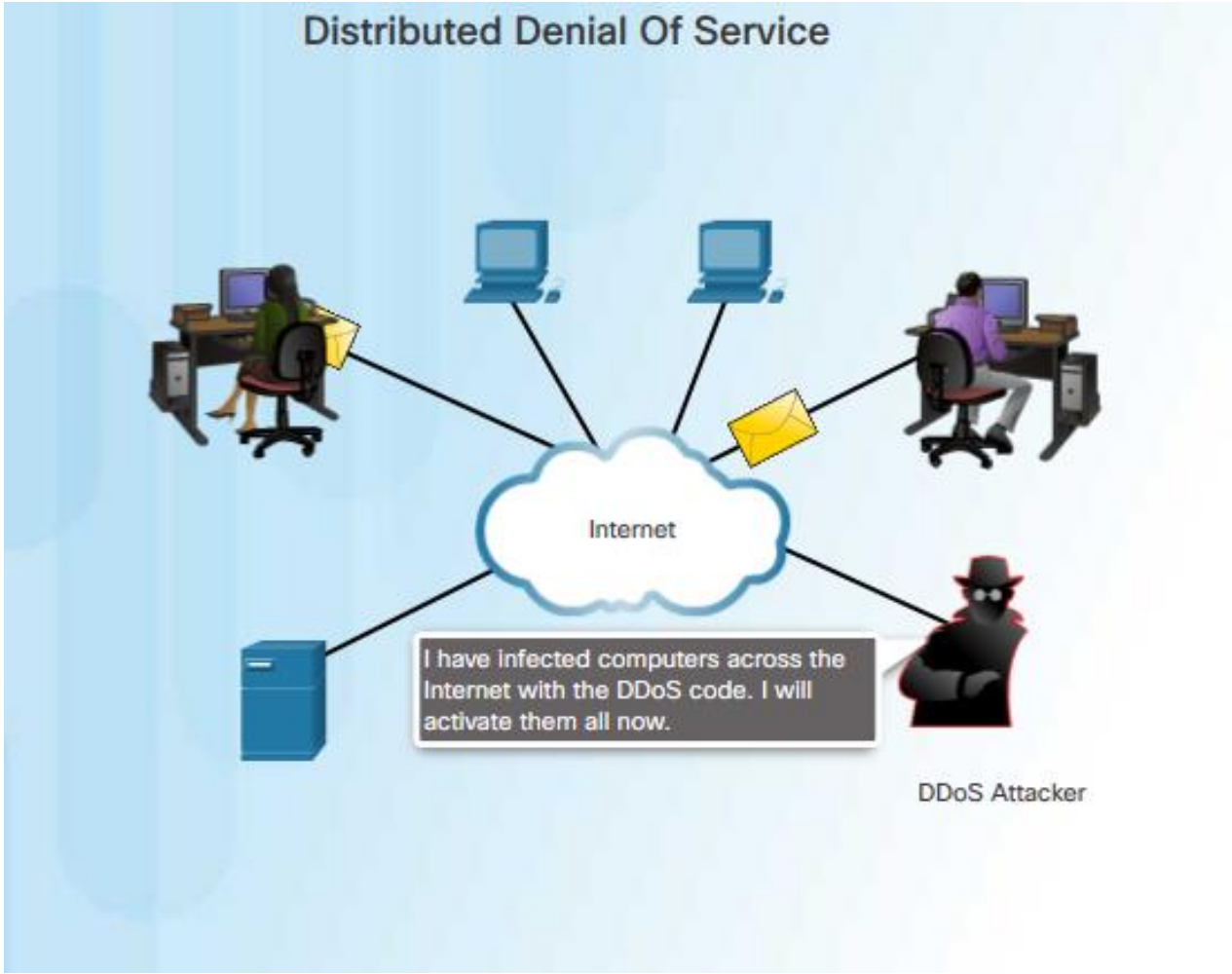
Something for Something (Quid pro quo) - This is when an attacker requests personal information from a party in exchange for something, like a free gift.

This illustration displays a person controlling two puppets.

Phishing

Phishing is when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on their device, or into sharing personal or financial information. An example of phishing is an email forged to look like it was sent by a retail store asking the user to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing emails are customized to a specific person. The attacker researches the target's interests before sending the email. For example, an attacker learns the target is interested in cars, and has been looking to buy a specific model of car. The attacker joins the same car discussion forum where the target is a member, forges a car sale offering and sends email to the target. The email contains a link for pictures of the car. When the target clicks on the link, malware is installed on the target's computer.


Distributed Denial Of Service
Internet
I have infected computers across the Internet with the DDoS code. I will activate them all now.
DDoS Attacker

DDoS

A Distributed DoS Attack (DDoS) is similar to a DoS attack but originates from multiple, coordinated sources. As an example, a DDoS attack could proceed as follows:

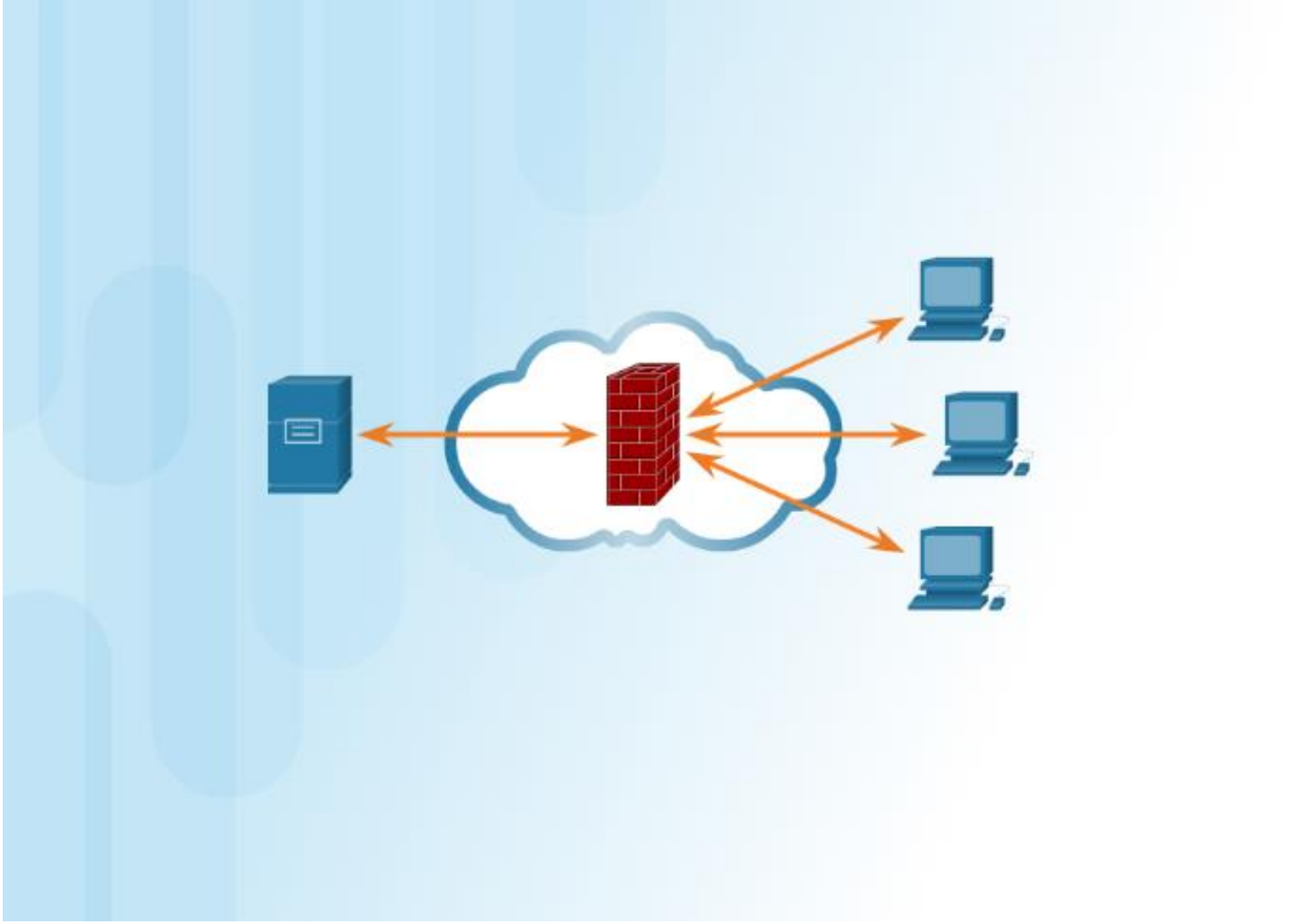
An attacker builds a network of infected hosts, called a botnet. The infected hosts are called zombies. The zombies are controlled by handler systems.

The zombie computers constantly scan and infect more hosts, creating more zombies. When ready, the hacker instructs handler systems to make the botnet of zombies carry out a DDoS attack.

How To prevent hacking

- It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.

Chapter-5: Understand the basics of security



Firewall Types

A **firewall** is a wall or partition that is designed to prevent fire from spreading from one part of a building to another. In computer networking, a firewall is designed to control, or filter, which communications are allowed in and which are allowed out of a device or network, as shown in the figure. A firewall can be installed on a single computer with the purpose of protecting that one computer (host-based firewall), or it can be a stand-alone network device that protects an entire network of computers and all of the host devices on that network (network-based firewall).

Over the years, as computer and network attacks have become more sophisticated, new types of firewalls have been developed which serve different purposes in protecting a network. Here is a list of common firewall types:

- ✓ **Network Layer Firewall** – filtering based on source and destination IP addresses
- ✓ **Transport Layer Firewall** –filtering based on source and destination data ports, and filtering based on connection states
- ✓ **Application Layer Firewall** –filtering based on application, program or service

- ✓ **Context Aware Application Firewall** – filtering based on the user, device, role, application type, and threat profile

- ✓ **Proxy Server** – filtering of web content requests like URL, domain, media, etc.

- ✓ **Reverse Proxy Server** – placed in front of web servers, reverse proxy servers protect, hide, offload, and distribute access to web servers

- ✓ **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts

- ✓ **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system

Security Appliances

Today there is no single security appliance or piece of technology that will solve all network security needs. Because there is a variety of security appliances and tools that need to be implemented, it is important that they all work together. Security appliances are most effective when they are part of a system.

Security appliances can be stand-alone devices, like a router or firewall, a card that can be installed into a network device, or a module with its own processor and cached memory. Security appliances can also be software tools that are run on a network device. **Security appliances fall into these general categories:**

Routers - Cisco Integrated Services Router (ISR) routers, shown in Figure 1, have many firewall capabilities besides just routing functions, including traffic filtering, the ability to run an Intrusion Prevention System (IPS), encryption, and VPN capabilities for secure encrypted tunneling.

Firewalls - Cisco Next Generation Firewalls have all the capabilities of an ISR router, as well as, advanced network management and analytics. Cisco Adaptive Security Appliance (ASA) with firewall capabilities are shown in Figure 2.

IPS - Cisco Next Generation IPS devices, shown in Figure 3, are dedicated to intrusion prevention.

VPN - Cisco security appliances are equipped with a Virtual Private Network (VPN) server and client technologies. It is designed for secure encrypted tunneling.

Malware/Antivirus - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.

Other Security Devices – This category includes web and email security appliances, decryption devices, client access control servers, and security management systems.

Chapter-6: Cyber Ethics

What is CyberEthics?

- In a nutshell, cyber ethics can be defined as responsible cyber behavior
- *Character is defined by doing what is right when no one is watching*

So What is Right when Surfing the Internet

- **DO** respect the privacy of other users on the Internet, just as you expect your privacy to be respected. How would you feel if someone read your private e-mail or your grades?
- **DO** use the Internet to help with schoolwork. The Internet is a source of great volumes of information. It's like having the world's largest library at your fingertips!
- **DO** keep your password's private. Giving away your password is like giving away the key to your house

Copyright? That's Just Books Right?

- Copyright respects the authors' or producers' ethical and legal ownership of their work
- Ownership of intellectual property includes books, articles, music, movies, artwork, photographs and the Internet
- You must acknowledge copyrighted information when you write a research paper, create a poster, post [illegible] do a presentation

What Counts as Plagiarsm/Academic Dishonesty?

- using an essay from another course/source
- copying a friend's homework or project
- using another person's ideas as your own
- copying and pasting from an electronic encyclopedia, online database, or the Internet

Why Do Students Plagiarize? They Tell us…

- **I didn't know I was plagiarizing**
  - I don't really understand the concepts of academic honesty and plagiarism
- **I didn't think I could do a good job on my own**
  - I'm not confident that my research and writing skills are as developed as they should be

Caught!

- Teachers know how it is done
- Teachers know you and your writing style
- Teachers are content experts and read widely
- Teachers, teacher-librarians and administrators work as a team to trace questionable information
- High-tech programs are available to detect plagiarism

Academic Honesty: Give Credit Where Credit is Due

- Acknowledge your sources of ideas and information when you write a research paper, create a poster, post a web site or do a presentation

Using Information in a Legal and Ethical Way

- Don't look for "short cuts".
- Give yourself time
- Be confident in the value of your own ideas
- Be yourself in your writing
- Develop strong research and literacy skills
- Ask for assistance

How To Protect Yourself From Computer Crime.

Tell a grown-up right away if you come across any information that makes you feel uncomfortable.

Do not give out any sensitive or personal information about you or your family in an Internet "chat room." Be sure that you are dealing with someone you and your parents know and trust before giving out any personal information about yourself via e-mail.

Never arrange a face-to-face meeting without telling your parents or guardians. If your parent or guardian agrees to the meeting, you should meet in a public place and have a parent or guardian go with you.

What is Your Privacy Worth?

What information about you or your parents do you think should be considered private? For example, medical information, a diary, your grades, how much money your parents owe, how much money your family has in a savings account or in a home safe, and your letters to a friend.

Would this kind of invasion of your privacy be any different than someone breaking into your school locker or your house to get this information about you and your family?

What is a Computer Pirate?

A Computer Pirate is someone who steals intellectual property.

Intellectual property is the physical expression of ideas contained in books, music, plays, movies, and computer software. Computer pirates steal valuable property when they copy software, music, graphics/pictures, movies, books (all available on the Internet).

So What are the Copyright Laws?

- **Copyright respects the authors' or producers' ethical and legal ownership of their work**
- **Ownership of intellectual property includes books, articles, music, movies, artwork, photographs and the Internet**
- **You must acknowledge copyrighted information when you write a research paper, create a poster, post a web site or do a presentation**

Seven ways to stay Safe

7

All computers connected to the Internet are vulnerable to attacks—at home, school, work, and the library. Regardless of the type of attack—virus, worm, Trojan, phishing, pharming, or others—there are ways for computer users to avoid them.

- Because many young people are more computer-savvy than their parents, they have a responsibility to help their families develop good cyber security practices.
- Children, teens, and adults are all targets for identity theft. Identity thieves collect, steal, and use private identity information—such as Social Security numbers—to pretend to be that person and then obtain driver's licenses or get credit cards in the stolen name.
- Private identity information includes a person's full name, postal address, e-mail address, phone numbers, credit and debit card numbers, and Social Security numbers.
- Passwords can get into the wrong hands when students willingly share them with their friends, when they can be guessed by someone who knows you, and when they are "cracked" by professional criminals.
- The most secure passwords are made up of combinations of eight or more letters, numbers, and symbols. They never use private information or information that can be easily guessed, and they do not contain words found in a dictionary.
- Don't open e-mails or accept instant messages from people you don't know. Don't reply to spam. Never click on links or download files unless you are sure they are safe.

Thank You