MAHENDRA ARTS & SCIENCE COLLEGE

(Autonomous)

Department of Computer Science & Applications

CLASS: III BCA

SUBJECT: CYBER SECURITY

PAPER CODE: M16UCA16

SEMESTER: V

Presented by
G.Vidhya M.Sc.,M.Phil.,
AP/CSA, MASC

UNIT-I

Introduction - History of internet – Introduction to cyber crime – Malware and its types – Kinds of cyber crime – Authentication – Encryption– Digital Signatures – Antivirus – Firewalls – Steganography – Computer forensics – Why Should we report cyber crime – Some recent cyber crime incidents –Cyber security initiatives in India – Generating secure password – Using password manager – Enabling two step verification – Securing computer using free antivirus – Configuring on MAC computer.

Today Topics

- Introduction
- History of internet
- Introduction to cyber crime
- Malware and its types

Introduction

- Internet is among the most important inventions of the 21st century.
- We use to talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, greet your friend on his birthday/ anniversary, etc.
- The technology have reached to an extent that we don't even require a computer for using internet.
- Now we have internet enabled Smartphone, palmtops, etc
- We can connected to our friends, family and office 24x7.

- Not only internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost effective.
- ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was a relatively very cheap.
- Now internet have made it possible to not only talk but use video conference using popular applications like skype, gtalk etc.
- We can remain connected to everyone, no matter what our location is.
- Working parents from office can keep eye on their children at home and help them in their homework.

History of Internet

- Russia Launched the world's first satellite, SPUTNIK into the space on 4th October, 1957.
- The research arm of Department of Defense, United States, declared the launch of ARPANET(Advanced Research Projects Agency NETwork) in early 1960's.
- The major task that ARPANET have to play is to develop rules for communication (i.e) protocols for communicating over ARPANET.
- In internetworking, Multiple separate networks could be joined into a network of networks.
- TCP/IP specifies the rules for joining and communicating over APRANET.

- In 1965, National Physical Laboratory(NPL) proposed a packing switching network.
- National Science Foundation (NSF). France also developed a packet switching network, know as CYCLADES in 1973.
- In 1981, the integration of two large networks took place. NFS developed Computer Science Network(CSNET) and was connected to ARPANET using TCP/IP protocol .
- Initially NFS supported speed of 56 kbit/s. It was upgraded to 1.5 Mbit/s
- NFSNET was expended and was upgraded to 45Mbit/s
- in 1991 National Research and Education Network (NREN) was founded and the World Wide Web was released

Internet Addresses

- We require some mechanism to uniquely identify every device that is connected to the internet.
- A centralized authority known as Internet Assigned Numbers Authority (IANA), which is responsible for assigning a unique number known as IP (Internet Protocol) address.
- An IP address is a 32-bit binary number which is divided into four octets and each octet consists of 8 binary digits and these octet are separated by a dot(.)
- An example of an IP address is

Binary = 10101100.00010000.11111110.00000001

Decimal = 172.16.254.1

- An IP address consists of two parts . Network and Host.
- Network part identifies the different network.
- The host part identifies a device of a particular network.

Five Regional Internet Registries (RIRs)

1) APNIC- This RIR is responsible for serving the Asia Pacific region
2) AfriNIC- This RIR is responsible for serving the African region
3) ARIN- This RIR is responsible for serving North America and several Caribbean and North Atlantic islands
4) LACNIC- This RIR is responsible for serving Latin America and the Caribbean, and
5) RIPE NCC- This RIR is responsible for serving Europe, the Middle East, and parts of Central Asia

For liaison and coordinating between these five RIRs, there is an organization called Number Resource Organization(NRO)

IP Address Classes

CLASS	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes

DNS

- Transfer the data over internet is only possible using IP addresses because the routing of the packet of data sent over internet is done using IP address. There is a server called Domain Name System(DNS).
- The computer keeps the track of recently visited sites and locally maintains a database in DNS cache.
- The root zone file describes where the authoritative servers for the DNS top-level domains (TLD) are located.

Internet Infrastructure

- Network - collection of several small, medium and large networks.
- ISP- The Internet Service Provider is the link between the internet backbone, through which the entire data route, and the user.
- NAP- The ISP connects to the internet backbone at Network Access Points(NAP).

World wide web

WWW is an information sharing model which is developed to exchange information over the internet. There are plenty of public websites, which is a collection of web pages, available over the internet.

What is cyber crime?

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Two main catagories

- Criminal activity that *targets*
- Criminal activity that *uses* computers to commit other crimes.

Introduction to cyber crime

- Cyber crime is used to describe a unlawful activity in which computer or computing devices such as smart phones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity.
- It is often committed by the people of destructive and criminal mindset either for revenge, greed or adventure
- Every second around 25 computer became victim to cyber attack and around 800 million individuals are affected by it till 2013.
- CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013.
- It is also estimated that around $160 million are lost per year due to cyber crime.
- Most of the cases are never reported.

Classification of Cyber Crimes

Two types

1. Insider Attack:

An attack to the network or the computer system by some person with authorized system access is known as insider attack.

2. External Attack:

When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack.

The cyber attacks can also be classified as structure attacks and unstructured attacks

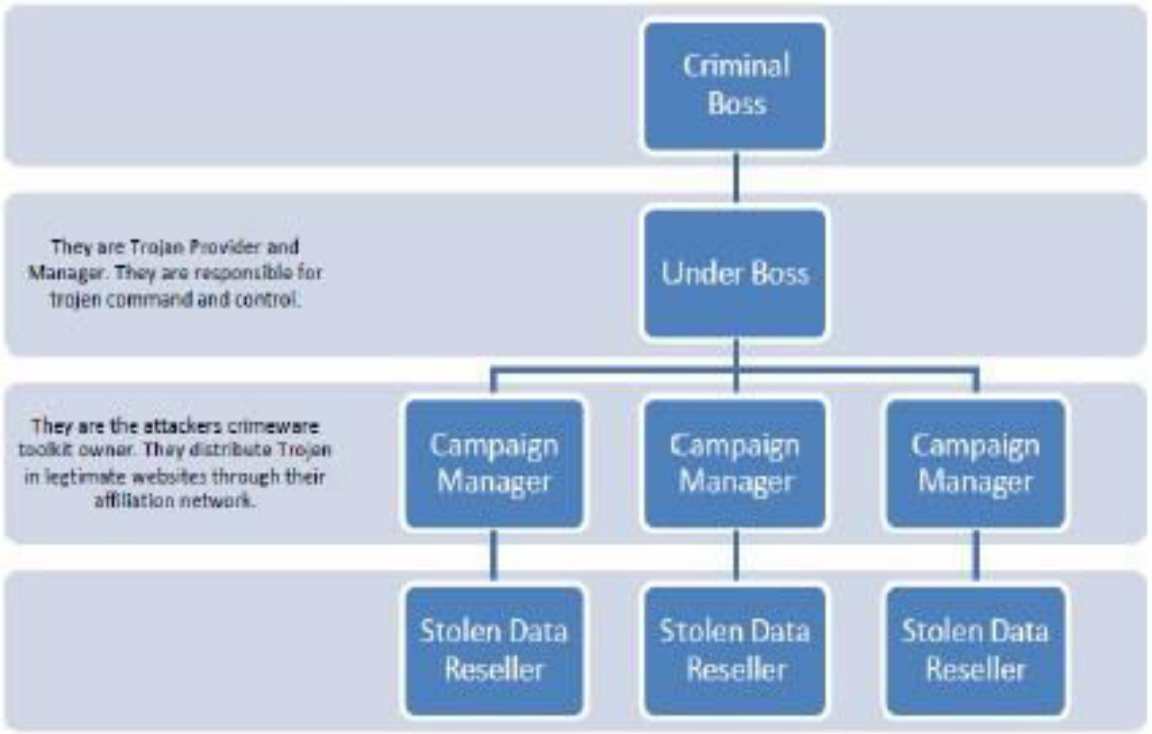
1. Unstructured attacks:

These attacks are generally performed by armatures that don't have any predefined motives to perform the cyber attack.

2. Structure Attack:

These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind.

Hierarchical Organizational Structure

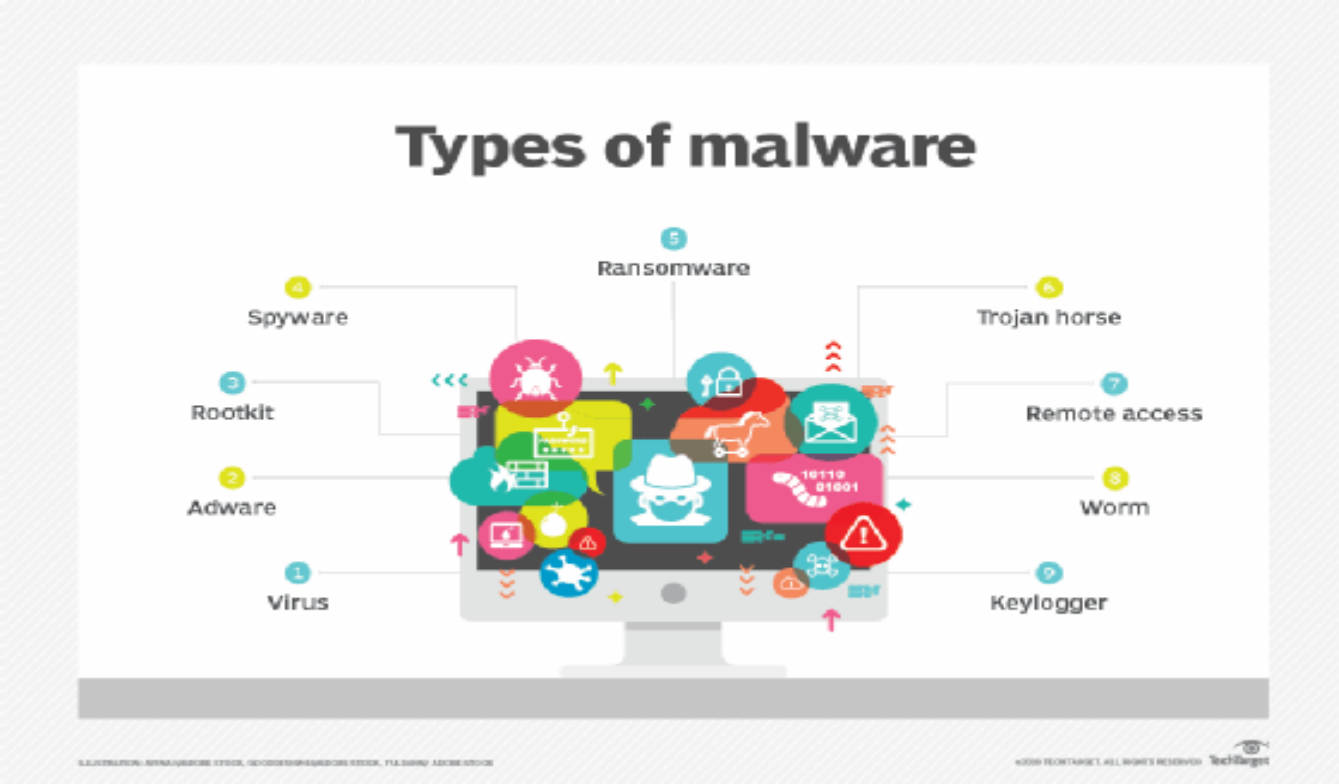


Reasons for Commission of Cyber Crimes

- *Money:* People are motivated towards committing cyber crime is to make quick and easy money.
- *Revenge:* Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
- *Fun:* The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.
- *Recognition:* It is considered to be pride if someone hack the highly secured networks like defense sites or networks.
- *Anonymity:* Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world.
- *Cyber Espionage:* At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

Malware and Its Types

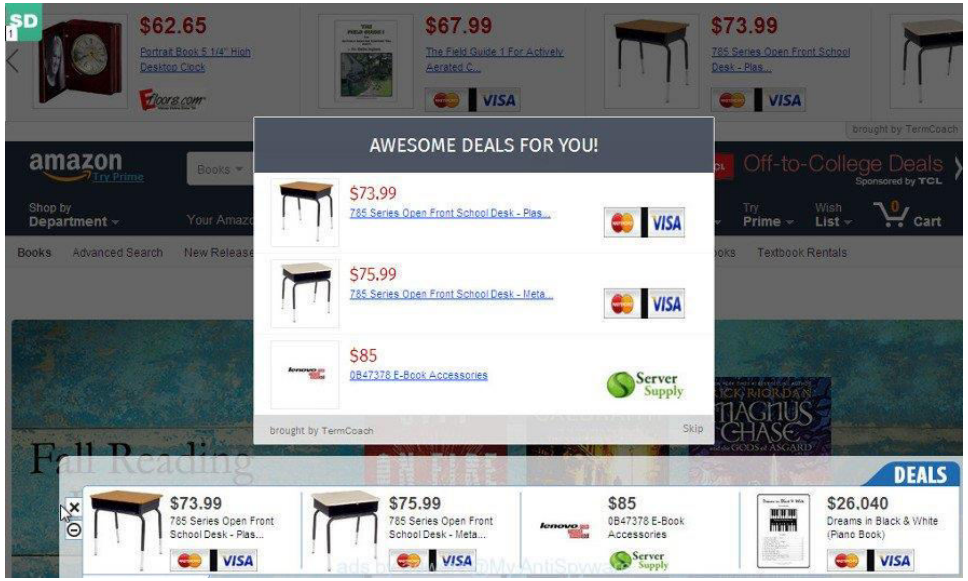
- Malware stands for "Malicious Software' and it is designed to gain access or installed into the computer without the consent of the user.
- It degrade the performance of the host machine.



Types of malware

1)Adware:

- It used for forced advertising.
- It redirect the page to some advertising page or pop-up an additional page.
- It financially supported by the organizations whose products are advertised.



2) Spyware:

- Installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine.
- It gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer.
- It can act as a key loggers to sniff the banking passwords and sensitive information, etc.

3) Browser hijacking software:

- It downloaded along with the free software offered over the internet and installed in the host computer.
- This software modifies the browsers setting and redirect links to other unintentional sites.

4)Virus

- A virus is a malicious code written to damage/harm the host computer

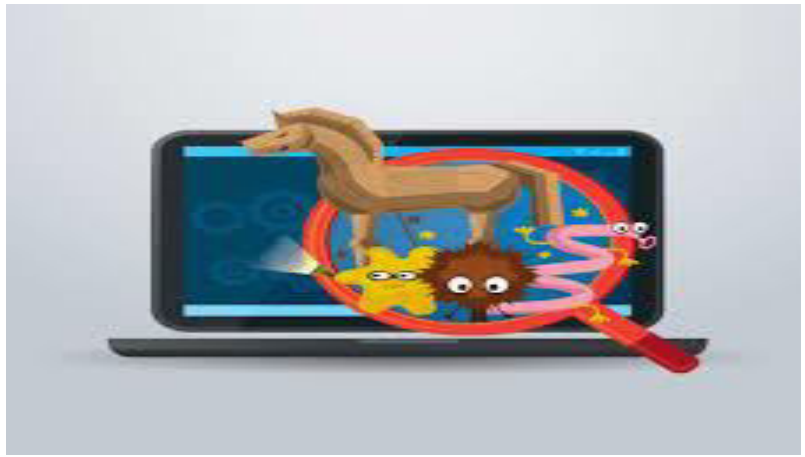
- It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc.
- A virus may be present in a computer but it cannot activate itself without the human intervention.

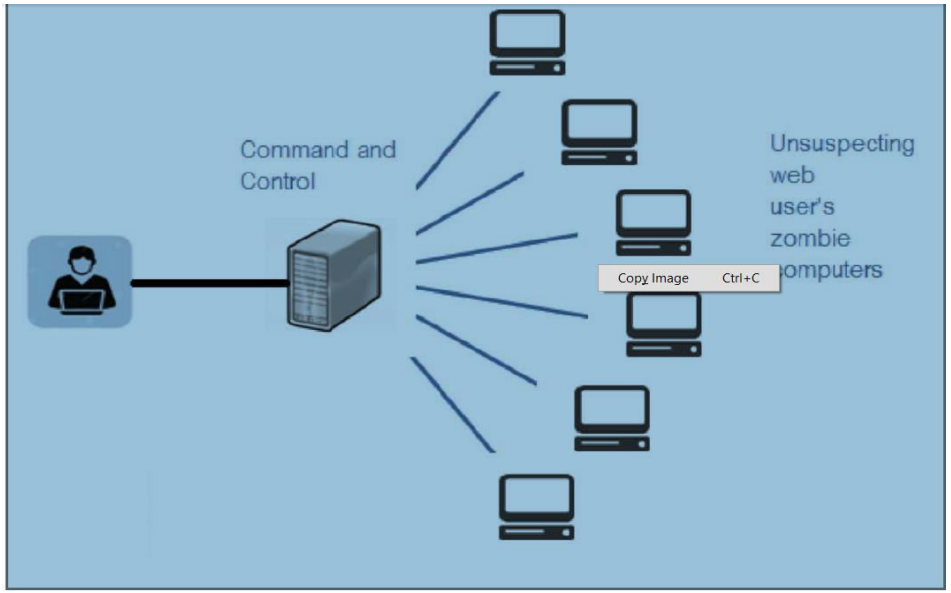
5)Worm

- Worms can spread either through network, using the loopholes of the Operating System or via email.

6) Trojan Horse

- Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software.
- It can become a part of botnet(robot-network), a network of computers which are infected by malicious code and controlled by central controller.
- The computers of this network which are infected by malicious code are known as zombies.





A typical Botnet

Scareware

- While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user's computer.
- As a remedial measure, the message suggests the used download the full paid version of the software.
- As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer.

UNIT-I

Introduction - History of internet – Introduction to cyber crime – Malware and its types – Kinds of cyber crime – Authentication – Encryption– Digital Signatures – Antivirus – Firewalls – Steganography – Computer forensics – Why Should we report cyber crime – Some recent cyber crime incidents –Cyber security initiatives in India – Generating secure password – Using password manager – Enabling two step verification – Securing computer using free antivirus – Configuring on MAC computer.

Previous topics

- Introduction
- History of internet
- Introduction to cyber crime
- Malware and its types

Topics discuss to…

- Kinds of cyber crime
- Authentication
- Encryption
- Digital signatures
- Antivirus
- Firewalls

Kinds of Cyber Crime

1)Cyber Stalking

- It is an act of stalking, harassing or threatening someone using Internet/computer as a medium.
- It done to defame a person and use email, social network, instant messenger, web-posting, etc.

2) Forgery and Counterfeiting

- It is a use of computer to forgery and counterfeiting is a document.
- It is possible to produce counterfeit which matches the original document.
- it is not possible to judge the authenticity of the document without expert judgment

3) Software Piracy and Crime related to IPRs

- Software piracy is an illegal reproduction and distribution for personal use or business.
  IPR(**Intellectual Property Right**) infringement are:

  download of songs, downloading movies, etc.

4) Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives

5)Phishing

It is a process of acquiring personal and sensitive information.

If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which sms is used to lure customers.

6) Computer Vandalism

It is an act of physical destroying computing resources using physical force or malicious code.

7) Computer Hacking

- It modifying computer hardware and software .

Types of hackers

1)White hat: Paid employee of an organization who is employed to find the security loop-holes.

2)Black hat: They hack the system for social, political or economically motivated intentions.

3)Gray hat: Find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.

4)Blue hat:They used to bug-test a system prior to its launch, looking for exploits

8)Creating and distributing viruses over internet

The spreading of an virus can cause business and financial loss to an organization

i) Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming

criterias

a. Mass mailing: - the email is not targeted to one particular person but to a large number of peoples.
b. Anonymity: - The real identify of the person not known
c. Unsolicited:- the email is neither expected nor requested for the recipient.

9) Cross Site Scripting:

It is an activity which involves injecting a malicious client side script into a trusted website.

The malicious script gets access to the cookies and other sensitive information and sent to remote servers.

10) Online Auction Fraud

It lead to either overpayment of the product or the item is never delivered once the payment is made.

11) Cyber Squatting

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

a)Logic Bombs

These are malicious code inserted into legitimate software. The malicious action is triggered by some specific condition.

12) Web Jacking

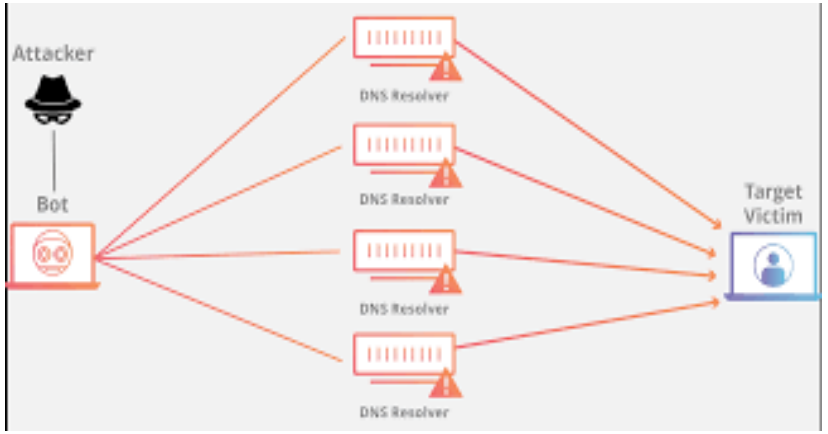
The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest.

13) Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

14) Denial of Service Attack

It is a cyber attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.



15) Salami Attack

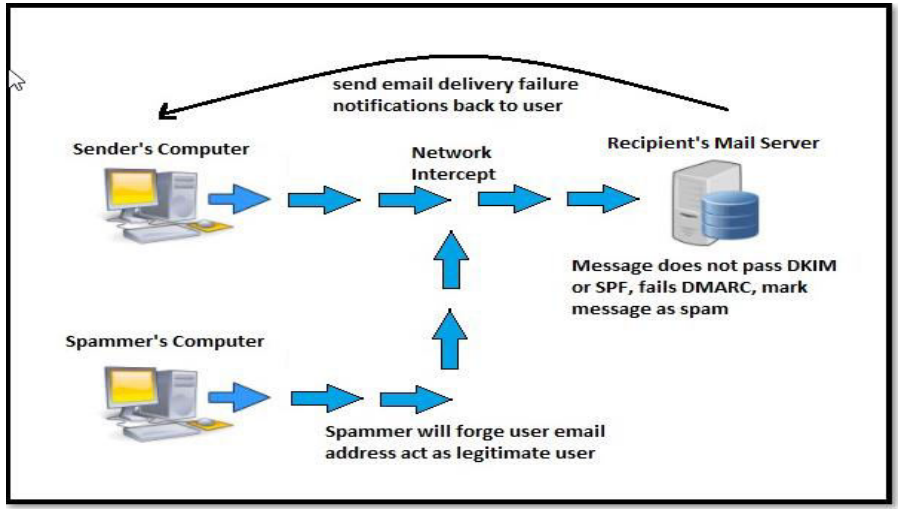
It is an attack which proceeds with small increments and final add up to lead to a major attack

16)Data Diddling

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done

17) Email Spoofing

It is a process of changing the header information of an e-mail so that its original source is not identified

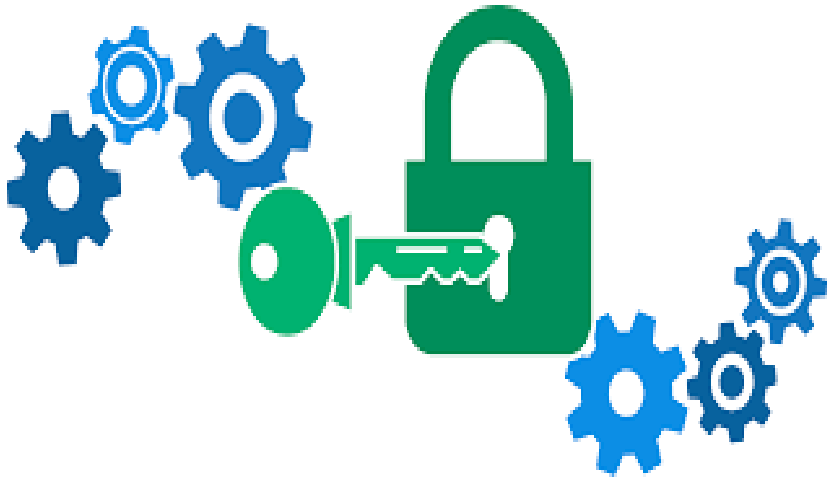


Authentication

- It is a process of identifying an individual.
- A typical method for authentication over internet is via username and password.
- The organizations have made some additional arrangements for authentication like One Time Password(OTP).
- Two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication.
- The process of giving access to an individual to certain resources based on the credentials of an individual is known as Authorization.

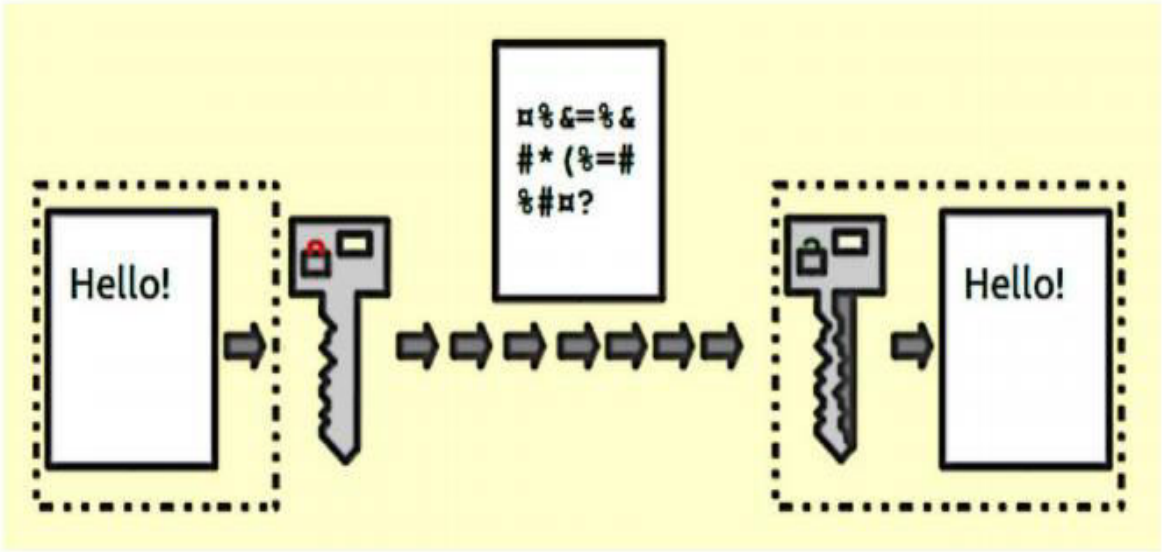
Encryption

- It is a technique to convert the data in unreadable form before transmitting it over the internet.
- Only the person who have the access to the key and convert it in the readable form and read it.
- Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms.



2 keys

1.Public key – Every User
2.private key – Particular user



Encryption

Digital Signatures

- It is a technique for validation of data.
- Validation is a process of certifying the content of a document.
- The digital signatures not only validate the data but also used for authentication.
- The digital signature is created by encrypting the data with the private key of the sender.
- The encrypted data is attached along with the original message and sent over the internet to the destination.
- The receiver can decrypt the signature with the public key of the sender.
- Now the decrypted message is compared with the original message.
- As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition.

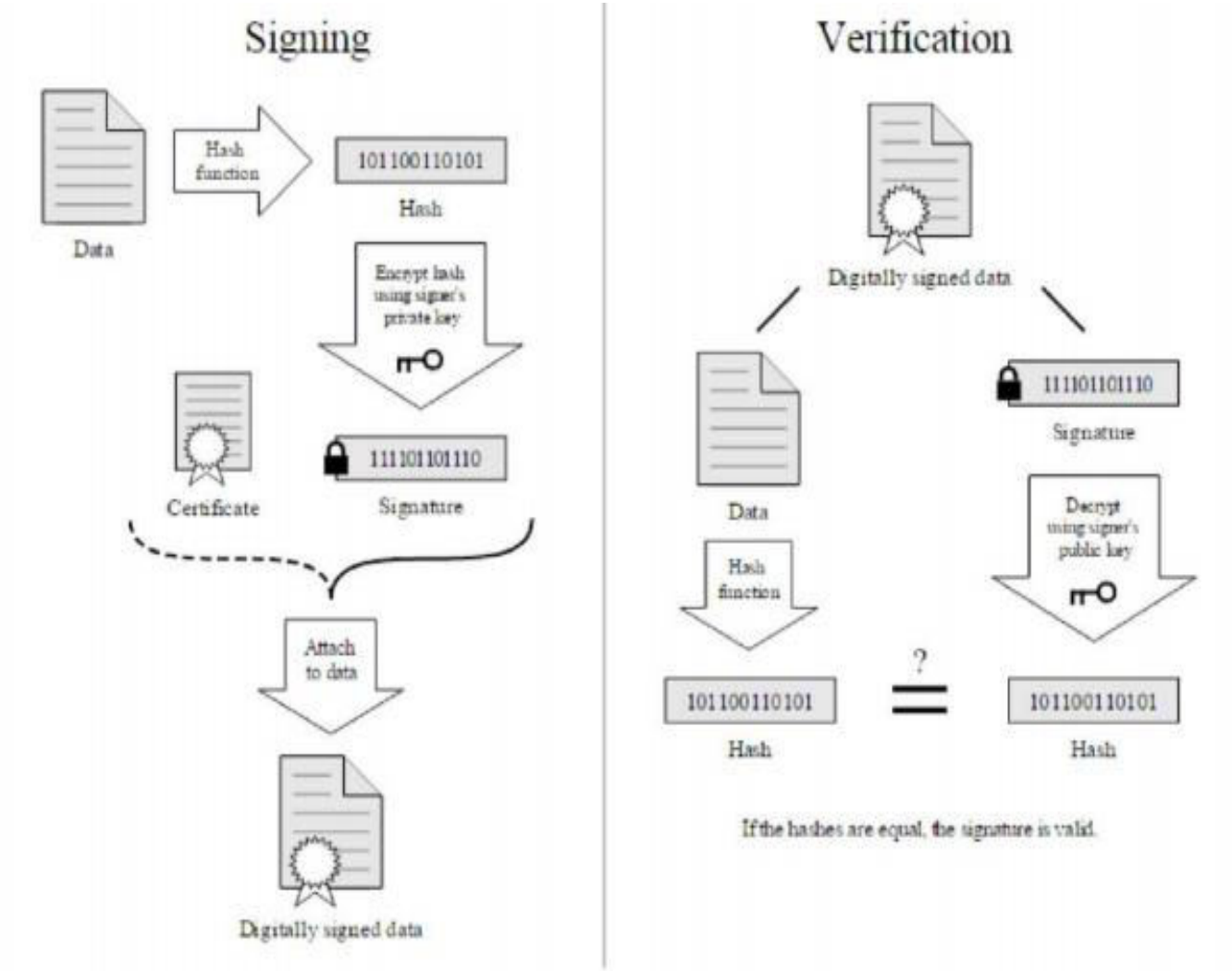


Figure 5: Digital signature[3]

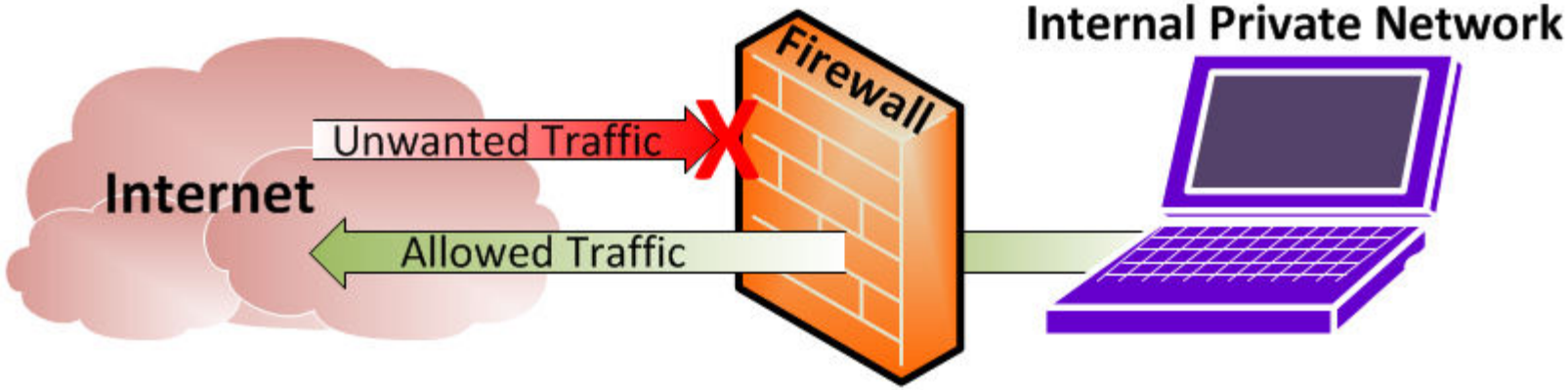
Antivirus

- There are verities of malicious programs like virus, worms, trojan horse, etc.
- It destroy data and stored into the computer or gain financial benefits by sniffing passwords etc.
- To prevent these malicious codes to enter to your system, a special program called an anti-virus
- The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc.

Firewall

It is a hardware/software which acts as a shield between an organization's network and the internet

- and protects it from the threats like virus, malware, hackers, etc.
- It can be used to limit the persons who can have access to your network and send information to you.



Two types of traffic

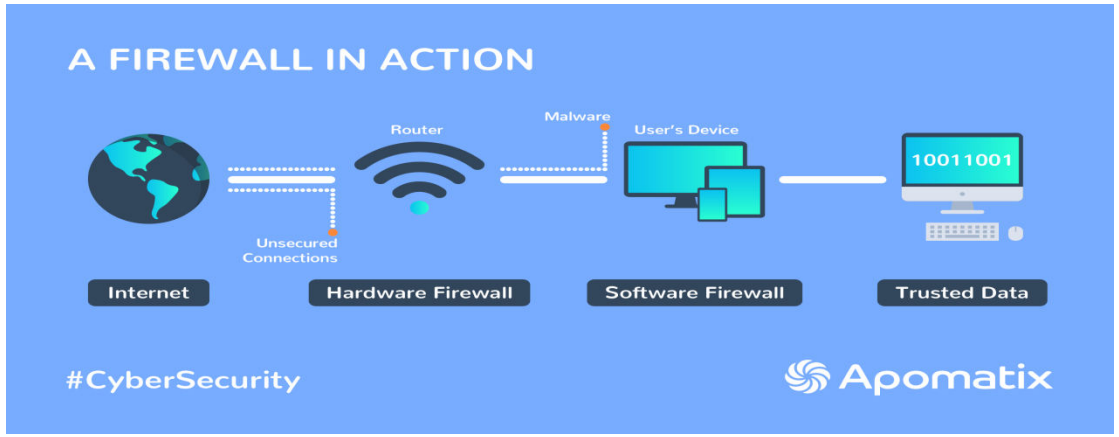
1)inbound traffic 2)outbound traffic

Firewall types
1)Hardware Firewalls

Hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet

2)Software Firewalls

These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations' network.



Firewall mechanisms

1)Proxy

All the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.

2)Packet filtering

Each packet is filtered by their type, port information, and source & destination information. The example of such characteristics is IP address, Domain names, port numbers, protocols etc. Basic packet filtering can be performed by routers

3)Stateful Inspection

All the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only

UNIT-I

Introduction - History of internet – Introduction to cyber crime – Malware and its types – Kinds of cyber crime – Authentication – Encryption– Digital Signatures – Antivirus – Firewalls – Steganography – Computer forensics – Why Should we report cyber crime – Some recent cyber crime incidents –Cyber security initiatives in India – Generating secure password – Using password manager – Enabling two step verification – Securing computer using free antivirus – Configuring on MAC computer.

Previous class

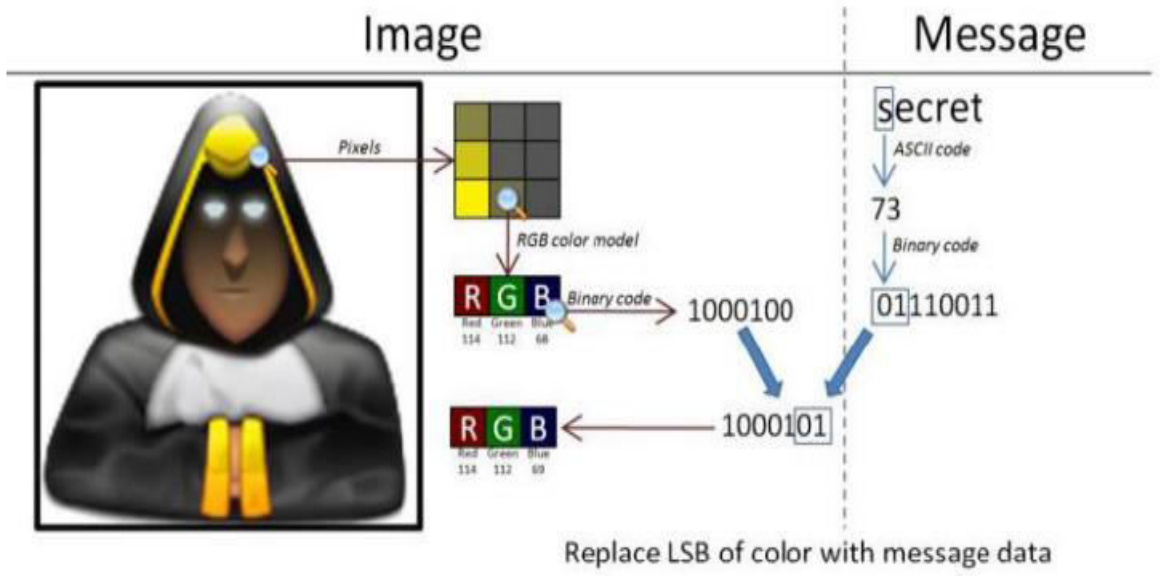
- Kinds of cyber crime
- Authentication
- Encryption
- Digital signatures
- Antivirus
- Firewalls

Topics

- Steganography
- Computer forensics
- Why Should we report cyber crime
- Some recent cyber crime incidents
- Cyber security initiatives in India

Steganography

- ✓ Steganography It is a technique of hiding secret messages in a document file, image file, and program or protocol etc.
- ✓ The embedded message is invisible and can be retrieved using special software.
- ✓ Only the sender and the receiver know about the existence of the secret message in the image.
- ✓ The advantage of this technique is that these files are not easily suspected.



Types of steganography

- Text Steganography
- Image Steganography
- Video Steganography
- Audio Steganography

Text Steganography

- **Text steganography** is a mechanism of hiding secret **text** message inside another **text** as a covering message or generating a cover message related with the original secret message

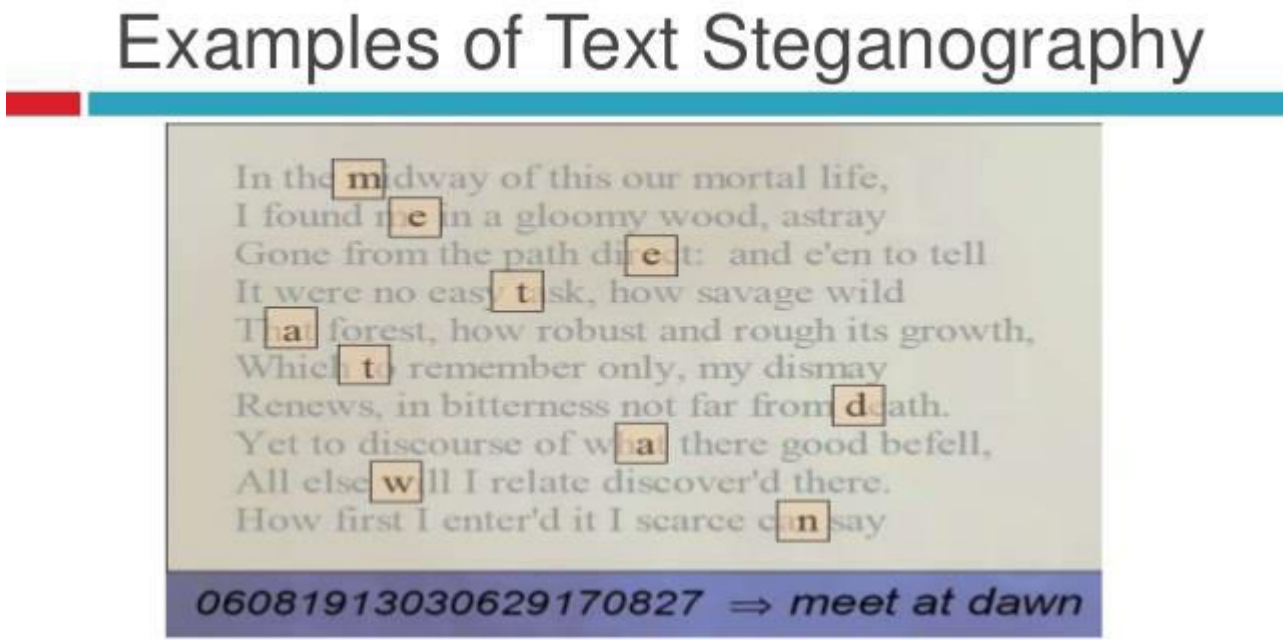
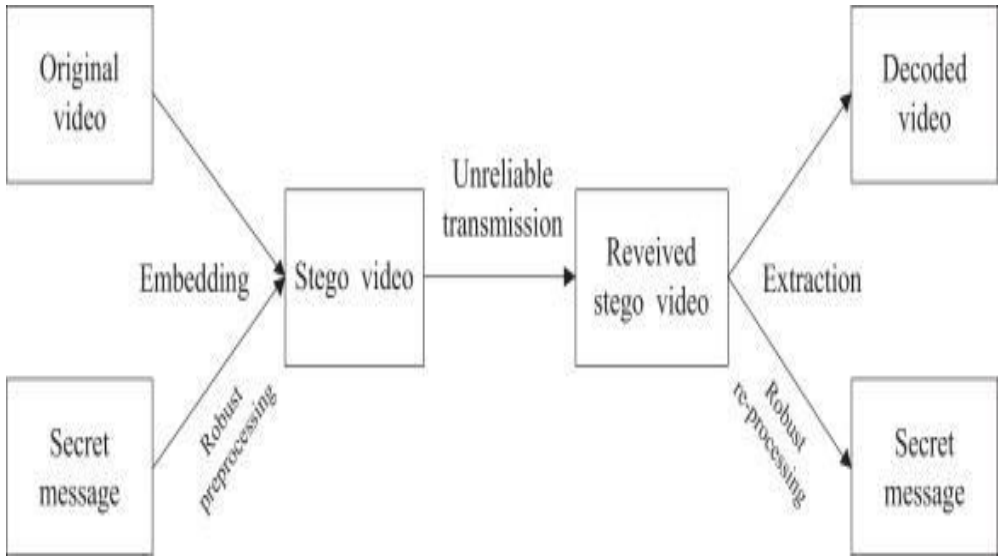


Image Steganography

- An image is a collection of numbers that constitute different light intensities in different areas of the image .
- This numeric representation forms a grid and the individual points are referred to as pixels.
- Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour .
- These pixels are displayed horizontally row by row.

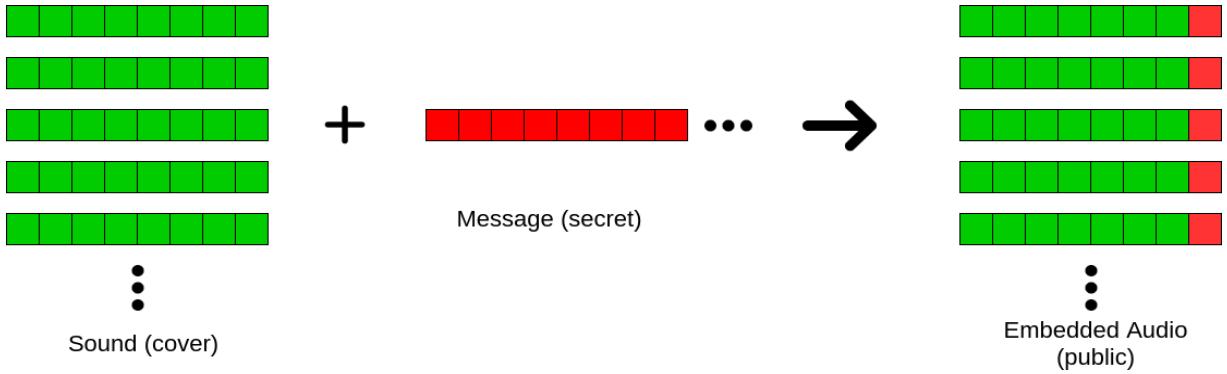
Video Steganography

It is a technique to hide any kind of files into a cover **Video** file. The use of the **video** based **Steganography** can be more secure than other multimedia files, because of its size and complexity.



Audio Steganography

- It is a technique used to transmit hidden information by modifying an **audio** signal in an imperceptible manner. It is the science of hiding some secret text or **audio** information in a host message



Computer Forensics

- It’s a techniques for investigation of digital data to find evidences against a crime.
- It is a practice of preserving, extracting, analyzing and documenting evidance from digital devices such as computers, digital storage media, smartphones, etc.
- 2 types

  1)Intentional use

  2) unintentional use

Management process

1) Preparation: prepares guidelines.
2) Identification: examining the logs.
3) Containment: based on the feedback from the assessment team the action to respond to the incident
4) Eradication: the eradication or mitigate of the cause of the threat is planned and executed.
5) Recovery: it is the process of returning to the normal operational state after eradication of the problem.
6) Lesson Learned: incident can be documented.

The computer forensic investigation involves following steps:

1) Identify incident and evidence
2) Collect and preserve evidence
3) Investigate
4) Summarize and Presentation

Why should we report cyber crime?

- Cyber crime incident is not reported, the cyber criminals will never be crabbed by the law enforcement agencies.
- This will further worsen the conditions and encourage the criminals to repeat these types of incidents with the same or the other organizations.
- So it is very important to identify and prosecute them.
- The cyber crime should be reported to nearest cyber cell of your locality, state cyber cell, central investigating agencies like CBI, IB or the international bodies like Interpol.

Some Recent Cyber Crime Incidents

1. PayPal, an international online money transfer service, which allows you to safely transfer money through an Internet using various encryption techniques and provides an alternative to other traditional payment methods like cherubs, money orders, etc.

- It have an active user base of over 100 million active users in 190 countries and performs over 9 million payments daily.
- Romanion Hacker TinKode aka Razvan Cernaianu, explioted a loophole in the code of the chargeback process of PayPal.

2. In Australia, a website called MP3/WMA Land, which offers a large number of pirated songs, music video clips for free download to its users.

- This resulted in heavy financial losses to the artists and the producers of those songs.
- The complain was lodged by an organizations called Music Industry Piracy Investigations.
- The owners of the website, Ng, Tran and Le, who were the students of Australian University, were framed for Australia's largest copyright infrigement case

3. One of the interesting case of online stalking was registered by Mrs. Ritu Kohli at Delhi Police (Kaur, 2013).

- She reported that someone is using her identity over the Internet in the website www.mirc.com for chatting, and distributed her address and phone number.
- This caused a lot of mental frustration and she decided to report the case.
- Based on her complain, Delhi Police tracced the IP address and finally traced the address of accused, Manish Kathuria and arrested him.

4. Iran's necular facility at Natanz was attacked by virus, Stuxnet which is belived to be developed by US .

- The virus first infected the third party utility which is used by Natanz facility and gained assess to the network.
- The virus was designed to attack a specific system software which controls the operation of Siemens controllers.
- it hijacked the system and send false signals about the health and status of the nuclear plant.

5. A trojen mail was used to hack the user name and the password of the current account of Mumbai based firm RPG Group and siphoned off Rs. 2.41 crore by Real Time Gross Sattlement(RTGS) (Narayan, 2013).

- Th bank officials suspected when they notice the huge amount of money transfer.

6. Online degree fraud are very popular these days over internet where accredited online degrees are offered by fake Universities (Gollin, 2003).

- These diploma mills offer to turn your work experience into a degree in exchange of money.
- The transcripts are also issued to the students on the basis of self evaluation.
- Its only when the students is rejected on account of fake degree, he realize that he fell pray to online fraud

7, Recently a new virus, which infects the Point of Sale(POS) machines and steals the payment record of credit card of the customers.

- These confidential data like PIN codes, credit card numbers, expiration date, CCV number, etc. are tracked and sent to the hackers so that this information can be misused for committing financial frauds (US-CERT, 2014).

8. Recently, a Chinese mobile company, Xiaomi was found guilty for sending the sensitive data to Chinese servers (Kumar, 2014).

- This information includes sms, photographs, contact list, etc. without the knowledge of the users.
- It's not the first time that a Chinese company was help suspected for espionage and US government have banned the use of Chinese equipments in some of its major establishments.

Cyber Security Initiatives In India

1. National Counter Terrorism Center(NCTC):

The Indian government realized the importance of Counter terrorism initiatives and proposed National Counter Terrorism Center(NCTC) to provide intelligence inputs to the decision makers to plan for counter terrorist activities.

2. National Information Security Assurance Programme (NISAP):

To create the awareness among the people in the government and critical sector organization, CERT-In has taken an initiative called National Information Security Assurance Programme (NISAP).

3. Computer Emergency Response Team-India(CERT-In):

The Indian Computer Emergency Response Team was created in 2004 by Department of Information Technology. The purpose of creating CERT-In was to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices.

4.Indo US Cyber Security Forum (IUSCSF):

The India-US Cyber Security Forum was established in 2001 and is dedicated to protecting the critical infrastructure of the knowledge-based economy.

The Forum focuses on cyber-security, cyber-forensics and related research and works towards enhancing co-operation among law enforcement agencies on both sides in dealing with cyber crime.

5. National Critical Information Infrastructure Protection Centre (NCIPC) of India:

It is declared as a nodal agency for the protection of critical information infrastructure of India and is responsible for all measures including R&D for protection of critical information infrastructure.

6. National Intelligence Grid (Natgrid) project of India:

It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel

7. Crime and Criminal Tracking Networks and Systems (CCTNS) project of India:

It is a project under National e-Governance Plan(NeGP) covering all 28 States and 7 UTs which aims at creation of a nation-wide networking infrastructure for evolution of IT-enabled sophisticated tracking system around 'investigation of crime and detection of criminals.

8. National Cyber Coordination Centre (NCCC):

National Cyber Coordination Centre is a proposed cyber security and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies.

9. Botnet Cleaning Center:

As a part of the Digital India programme, the Government is setting up a centre that will detect malicious programmes like 'botnets' and help people remove such harmful softwares from their devices. "

10. E-mail policy of Government of India:

E-mail has become major mode of communications for the entire government. With the increasing use of Emails to communicate among different Govt. Agencies, the Email Policy was laid down by Government of India (GOI) in October 2013.

11. Ministry of Home Affairs (MHA):

The Ministry of Home Affairs (MHA) is a ministry of the Government of India. An interior ministry, it is mainly responsible for the maintenance of internal security and domestic policy. Readers are adviced to read annual report of the Ministry of Home Affairs.

12. National Crime Records Bureau (NCRB):

NCRB shall endeavour to empower Indian Police with Information Technology and Criminal Intelligence to enable them to effectively & efficiently enforce the law & improve public service delivery.

Previous class

- Steganography
- Computer forensics
- Why Should we report cyber crime
- Some recent cyber crime incidents
- Cyber security initiatives in India

Topics

- Generating secure password
- Using password manager
- Enabling two step verification
- Securing computer using free antivirus
- Configuring on MAC computer

Generating Secure Password
Guideline for setting secure Password

The simple tips below are intended to assist you in choosing a good password.

Basics

- Use at least eight characters
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.
- Never use the same password twice.
- Don't just add a single digit or symbol before or after a word.

Tips

- Choose a password that you can remember so that you don't need to keep looking it up.

  Choose a password that you can type quickly.

Bad Passwords

- Don't use passwords based on personal information such as: name, nickname, birthdate, phone number
- Don't use passwords based on things located near you. Ex: computer,keyboard
- Don't ever be tempted to use one of those oh so common passwords e.g. "password", "letmein".
- Never use a password based on your username, account name, computer name

Choosing a password

1. Use good password generator software.
2. Use the first letter of each word from a line of a song or poem.
3. Alternate between one consonant and one or two vowels to produce nonsense words.

   eg. "taupouti".

4. Choose two short words and concatenate them together with a punctuation or symbol character between the words. eg. "seat%tree" Changing your password
5. You should change your password regularly, I suggest once a month is reasonable for most purposes.
6. You should also change your password whenever you suspect that somebody knows it,
7. Even that they may guess it, perhaps they stood behind you while you typed it in.
8. Remember, don't re-use a password.

Protecting your password

- Never store your password on your computer except
- Don't tell anyone your password, not even your system administrator
- Never send your password via email or other unsecured channel
- Write your password down but don't leave the paper lying around, lock the paper
- Away somewhere, preferably off-site and definitely under lock and key.
- Be very careful when entering your password with somebody else in the same room.

Remembering your password

- Use a secure password manager, see the downloads page for a list of a few that won't
- Cost you anything.
- Use a text file encrypted with a strong encryption utility.
- Choose passwords that you find easier to remember.

How would a potential hacker get hold of my password anyway?

1) Steal it
2) Guess it
3) A brute force attack
4) A dictionary attack

Using Password Manager

- Password managers are one of the best ways to store, back up and manage your passwords.
- A good password is hard to remember and that's where a password manager comes in handy.
- It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

What is a password manager?

- A password manager is software that helps a user to manage passwords and important information so that it can be accessed any time and anywhere.
- It helps to store information securely without compromising safety.
- All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

Why you should use it?

- If you find it hard to remember passwords for every website and don't want to go through the 'Forgot password?' routine off and on.
- It designed to store all kinds of critical login information related to different websites.

How does it work?

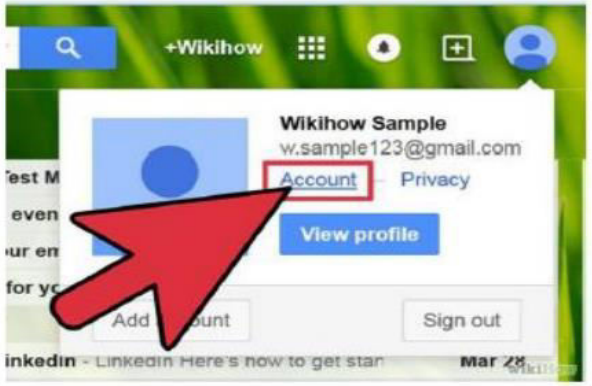
- Password managers may be stored online or locally.
- Online password managers store information in an online cloud, which can be accessed anytime from anywhere.
- Local password managers store information on the local server, which makes them less accessible.
- Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server.

Some popular Password managers

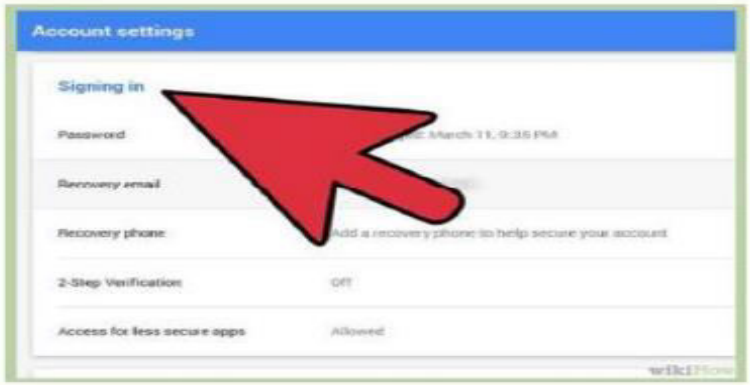
- KeePassX
- Clipperz
- PAsword Gorilla
- GPasword Manager
- Paword Safe

Enabling Two-Step Verification

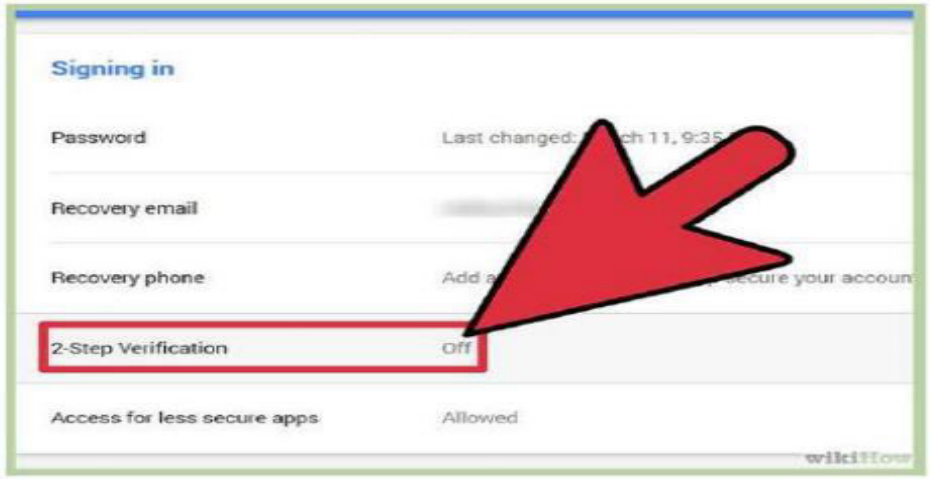
- Every day, tens of thousands of personal accounts are hacked.
- Personal information is compromised, passwords are cracked, and lives are put in jeopardy.
- If you ever use one password for multiple accounts, you are exponentially increasing your vulnerability to being hacked.
- Google has launched its 2-step verification system: anytime an unknown device is used to sign into your Google account, the user has to provide a verification code in addition to the password.
- Step 1: Sign into your Gmail account. Click on a thumbnail of your avatar on the right side of the top menu bar, and then click "Account" to update your settings.



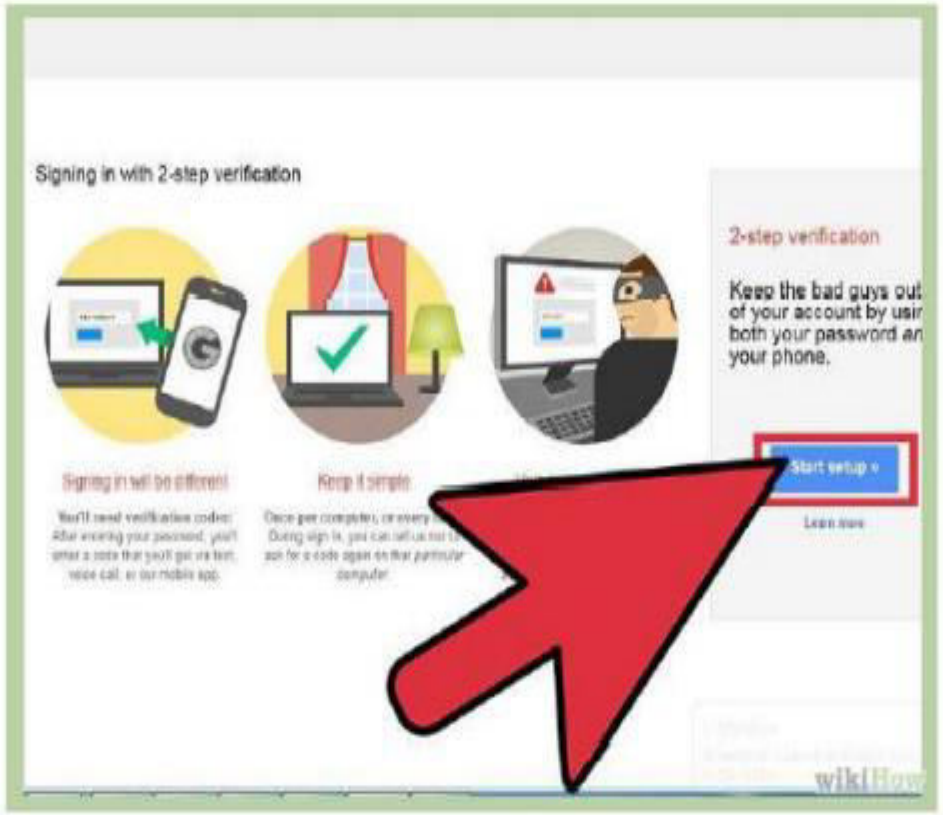
Step 2: You will land on your Account Settings page. Scroll down until you find a blue bar that says "signing



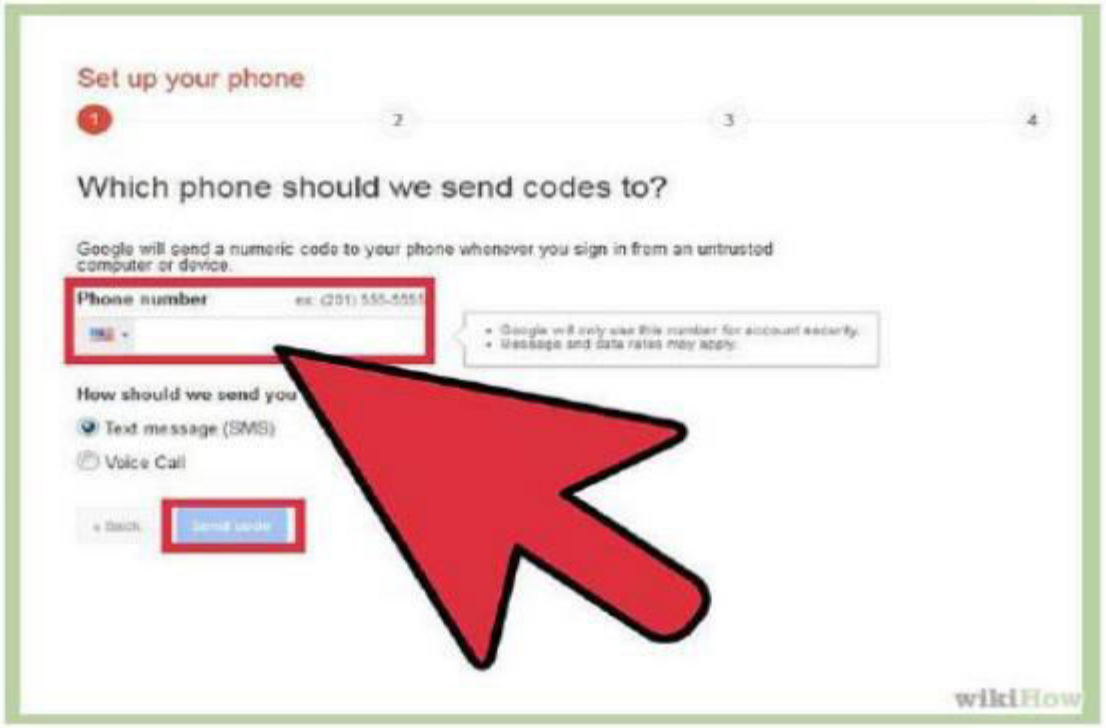
Step 3: In the 2-step verification section, you'll see if you already have 2-step verification turned on. If it says "OFF," click "Edit" to set the feature up.



Step 4: You'll see a page that briefly walks through the steps of setting up 2-step verification. Hover over the steps for more detail. Once you're ready, click "Start setup."

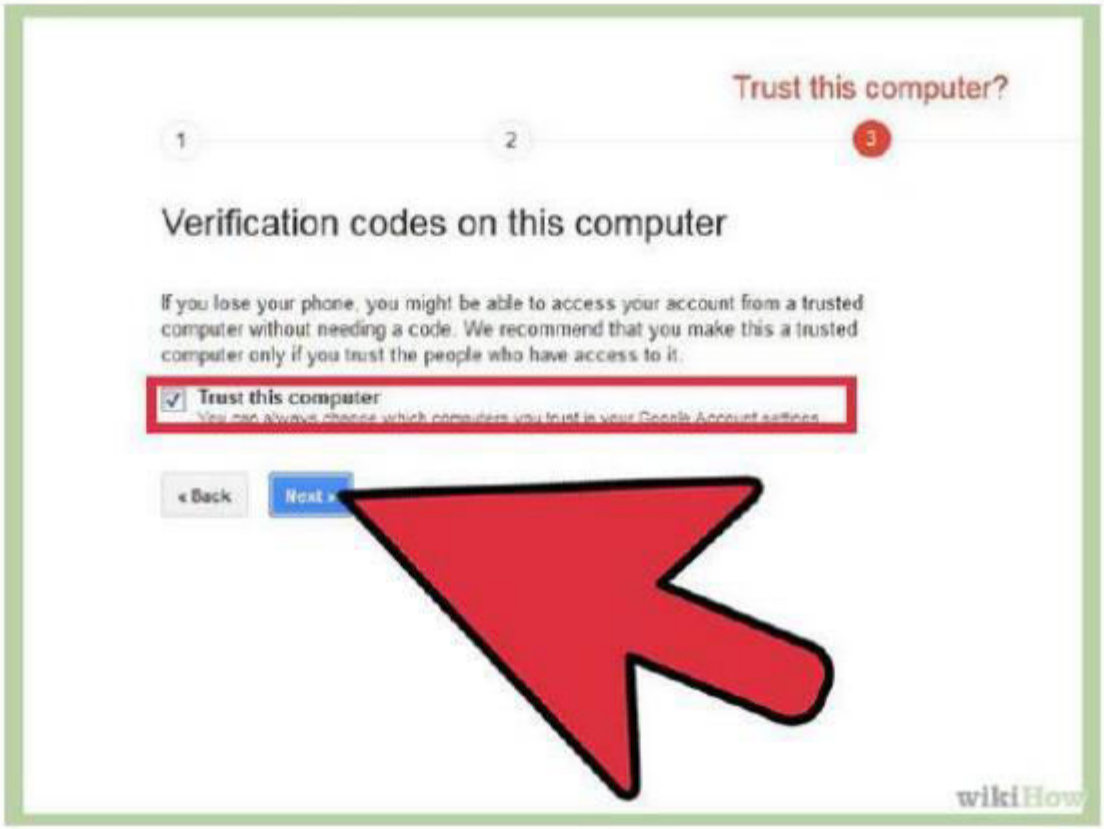


Step 5: Type in your cell phone number. This will be the phone associated with your Google account. Anytime you sign into your Google account from an unknown device (e.g., a public computer), Google will send a verification code to your phone and you will need to enter that before you can sign in.



Step 6: Select whether you'd like to receive a text message or Google Voice call with your verification code. Press submit. Then wait for the code to arrive to your phone and enter it in.

Step 7: Decide whether to trust this device. If you are turning on 2-step verification from a personal computer or trusted device, check the "trust this device" box. You will only be asked to enter a verification code when you sign into this account once per 30 days.



Step 8: Press OK, and you have just set up 2-step verification for your Google account!

Securing Computer Using Free Antivirus

1. Avast Antivirus:

- Avast is one of the best free anti-virus software available that provides a complete protection against security threats.
- This full-featured antivirus package has the following feature: Built in Anti-spyware, Anti-Rootkit, Web shield, Strong self protection, P2P and IM shield, Anti-Virus kernel, System integration, Windows 64 bit support, Integrated Virus Cleaner etc
- It can be downloaded from https://www.avast.com/index

2. AVG Antivirus

- AVG anti-virus free edition provides basic antivirus and anti-spyware protection for Windows.
- Following features included in the free edition: Anti-virus , anti-spyware and Safe surf feature.
- It can be downloaded from http://free.avg.com/

3.Avira AntiVir Personal

- Avira is a comprehensive, easy to use antivirus program, designed to reliable free of charge virus protection to home-users.
- Features included are: Protection from virus , worms and Trojans, Anti-rootkit, Anti-fishing, Anti dialers.
- It can be downloaded from http://www.free-av.com/

4. BitDefender

- Free Edition uses the same ICSA Labs certified scanning engines found in Pro version of BitDefender , allowing you to enjoy basic virus protection for no cost at all.
- Features includes: On demand Virus Scanner and Remover and Scheduled scanning.
- It can be downloaded from http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html

5. Blink Personal

- An all-in one security suite with antivirus limited for one year.
- Blink personal Security suite features - Antivirus and Anti spyware, Anti root kit, Built-in Firewall protection and Identity protection.
- It can be downloaded from http://free-antivirus.eeye.com/

6. Calmwin antivirus

- An open source, free Antivirus program for Windows 98/2000/XP/2003 and Vista.
- Features include - high detection rates for viruses and spyware; automatic downloads of regularly updated Virus Database, Standalone virus scanner. It does not include an on-access real-time scanner.
- It can be downloaded from http://www.clamwin.com/

7. Comodo Antivirus

- It has all the functionality of a paid AV without the price
- Features includesDetects and remove viruses from computers and networks.
- It can be downloaded from http://antivirus.comodo.com/

8. Moon Secure Antivirus

- It is Free Antivirus for Windows under GPL license.
- It offers multiple scan engines, Net shield, Firewall, On access, on Exec scanner and rootkits preventions plus features from Commercial Antivirus applications.
- It can be downloaded from http://sourceforge.net/projects/moonav/

9)PCTools Antivirus

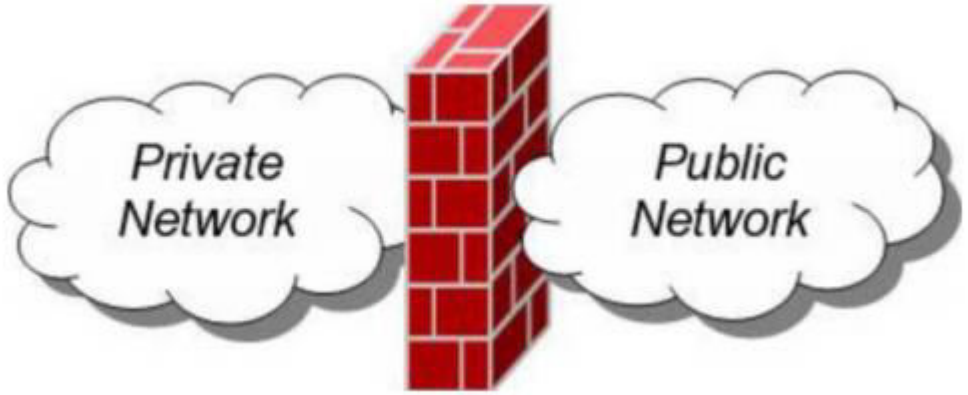
- with PC Tools Anti Virus Free Edition you are protected against the cyber-threats attempting to gain access to your PC and personal information.
- It protects you from Virus, worm, Trojan and has Smart Updates, IntelliGuard Protection, file guard and email guard.
- It can be downloaded from http://www.pctools.com/free-antivirus/

10) Rising Antivirus

- Rising Antivirus Free Edition is a solution with no cost to personal users for the life of the product while still provides the same level of detection and protection capability as RISING Antivirus .
- It protects your computers against all types of viruses, Trojans, worms, rootkits and other malicious programs. Ease of use and Smart update technology make it an "install and forget" product and entitles you to focus on your own jobs with your computer.
- It can be downloaded from http://www.freerav.com/

Configuring Firewall On Mac Computer

- Every Mac ships with a built-in firewall - a service that can be configured to disallow information from entering your Mac.
- Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information.
- A firewall can help prevent bad packets from entering your Mac.
- To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall.
- It will close your Mac's open ports and disallow random network scams.



Unit – I Completed

UNIT II

Working with window firewalls in windows – Finding the best browser According to the user requirement – Guidelines for safe browsing – Tips for buying online – Clearing cache for browsers.

Wireless Security: What is wireless LAN – Major issues with WLAN.

Email and Social Media Security: Safe browsing guideline for social networking sites – Email Security tips.

Today Topics

- Working with window firewalls in windows
- Finding the best browser According to the user requirement
- Guidelines for safe browsing

Working With Windows Firewalls in Window 7

- Two firewalls in Windows 7

1) Windows Firewall
2) Windows Firewall with Advanced Security (WFAS)

1)Windows Firewall

It directly relate to a program or a service.

2)Windows Firewall with Advanced Security (WFAS)

WFAS can be configured based on protocols, ports, addresses and authentication.

- Both firewalls come with predefined set of rules that allow us to utilize network resources.
- This includes things like browsing the web, receiving e-mails, etc.
- Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance.

- Windows 7 configure inbound and outbound rules.
- Inbound - Traffic is allowed
- Outbound - Traffic initiated from external sources is automatically blocked.

- When we first connect to some network, we are prompted to select a network location. This feature is known as **Network Location Awareness (NLA).**
- It enables us to assign a network profile to the connection based on the location.
- In Windows 7, different network profiles can be configured on different interfaces.
- For example, our wired interface can have different profile than our wireless interface.
- There are three different network profiles available:

1)Public Home/Work

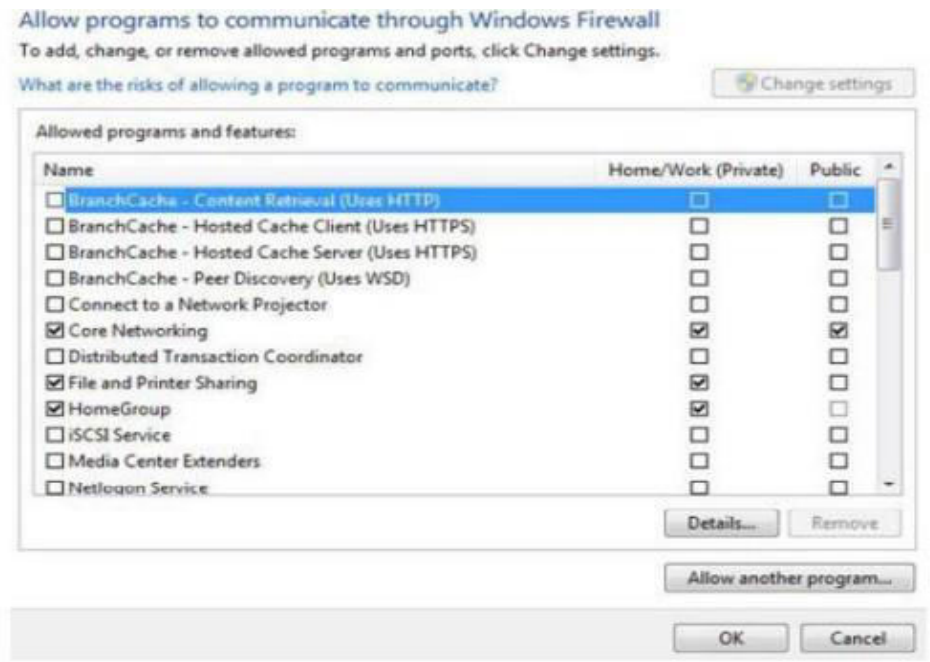
2)Private network Domain

3)Used within a domain

Configuring Windows Firewall

To open Windows Firewall we can go to Start > Control Panel > Windows Firewall.
By default, Windows Firewall is enabled for both private (home or work) and public networks.

To configure exceptions we can go to the menu on the left and select "Allow a program or feature trough Windows Firewall" option.

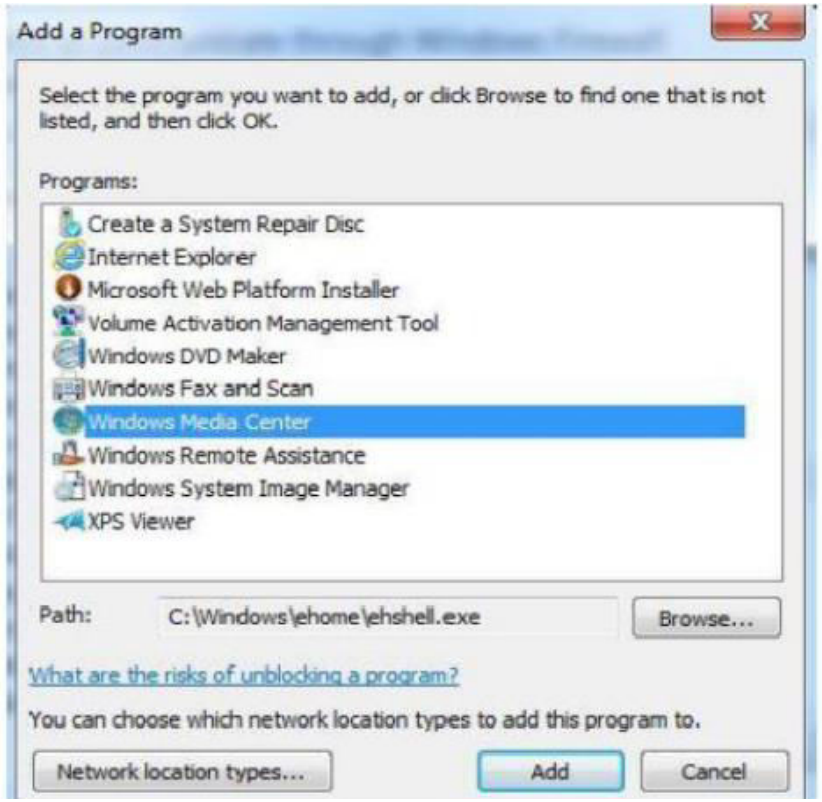


Exceptions

- To change settings in this window we have to click the "Change settings" button.
- A list of predefined programs and features that can be allowed to communicate on private or public networks.
- For example, notice that the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks.
- We can also see the details of the items in the list by selecting it and then clicking the Details button.

Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.



Add a Program

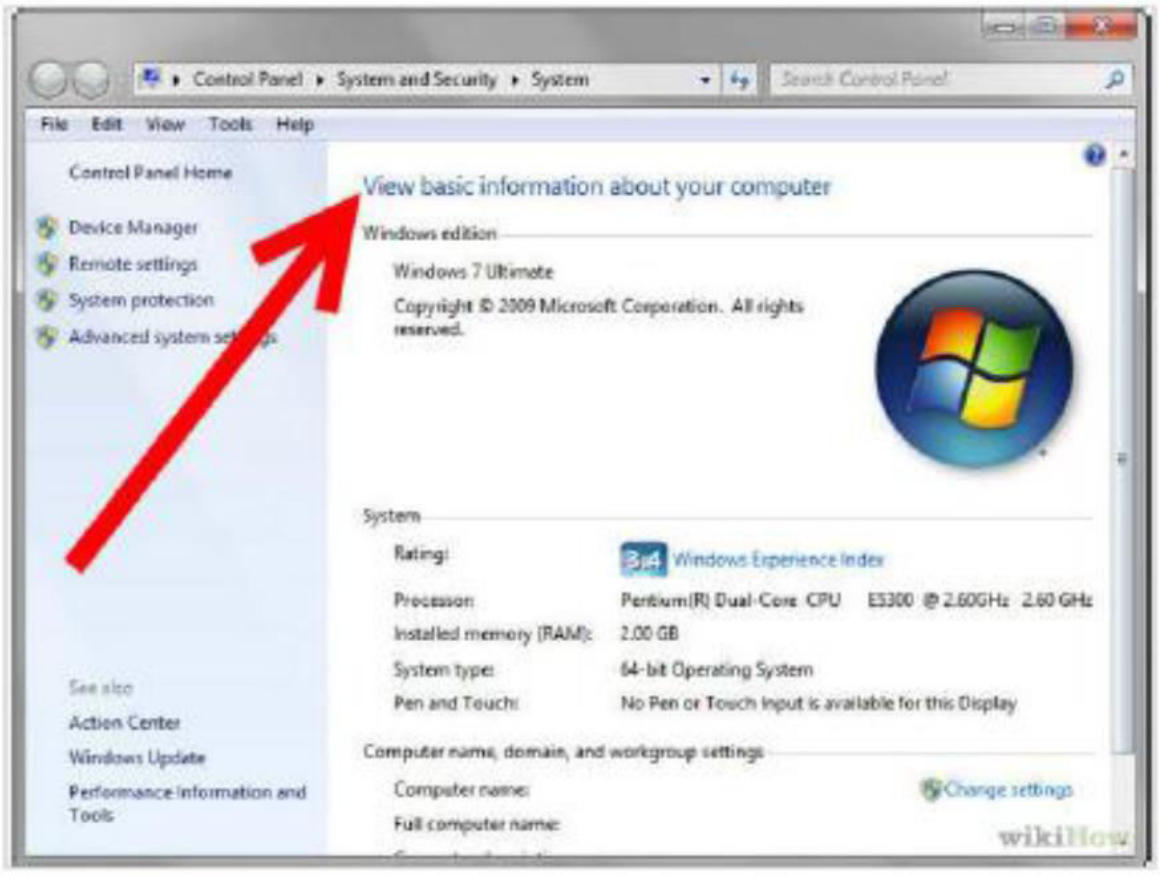
Browse the executable of our program and then click the Add button.
Choose location types on which this program will be allowed.

Network Locations

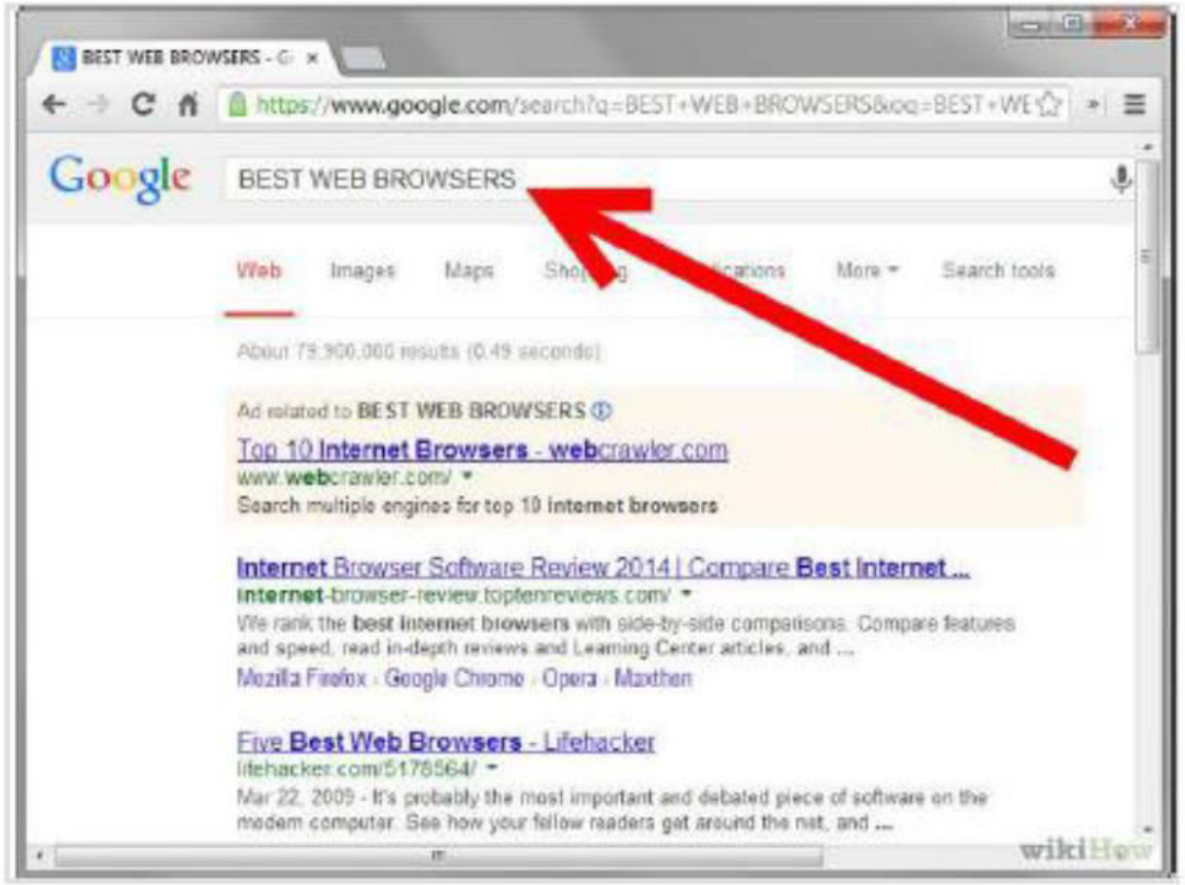
- Many applications will automatically configure proper exceptions in Windows Firewall when we run them.
- For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming.
- The same thing is if we enable Remote Desktop feature from the system properties window.
- By enabling Remote Desktop feature we actually create an exception in Windows Firewall.
- Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.

Finding the Best Browser According To the Users Requirement

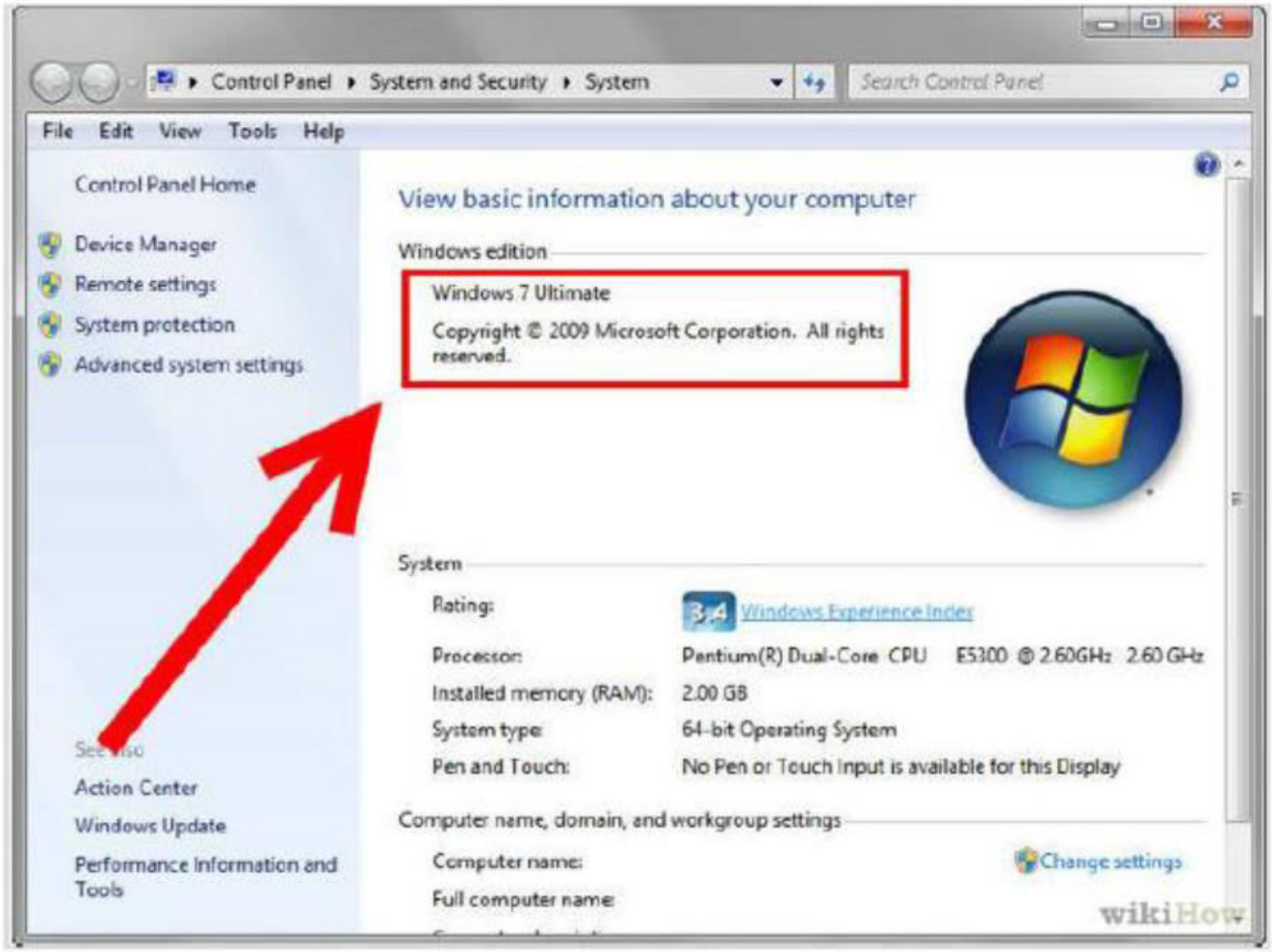
- **Step 1:** Determine the age of your computer. How old is your computer? Is it a mobile device? Know your systems specifications as this may be more suited to some browsers than others.



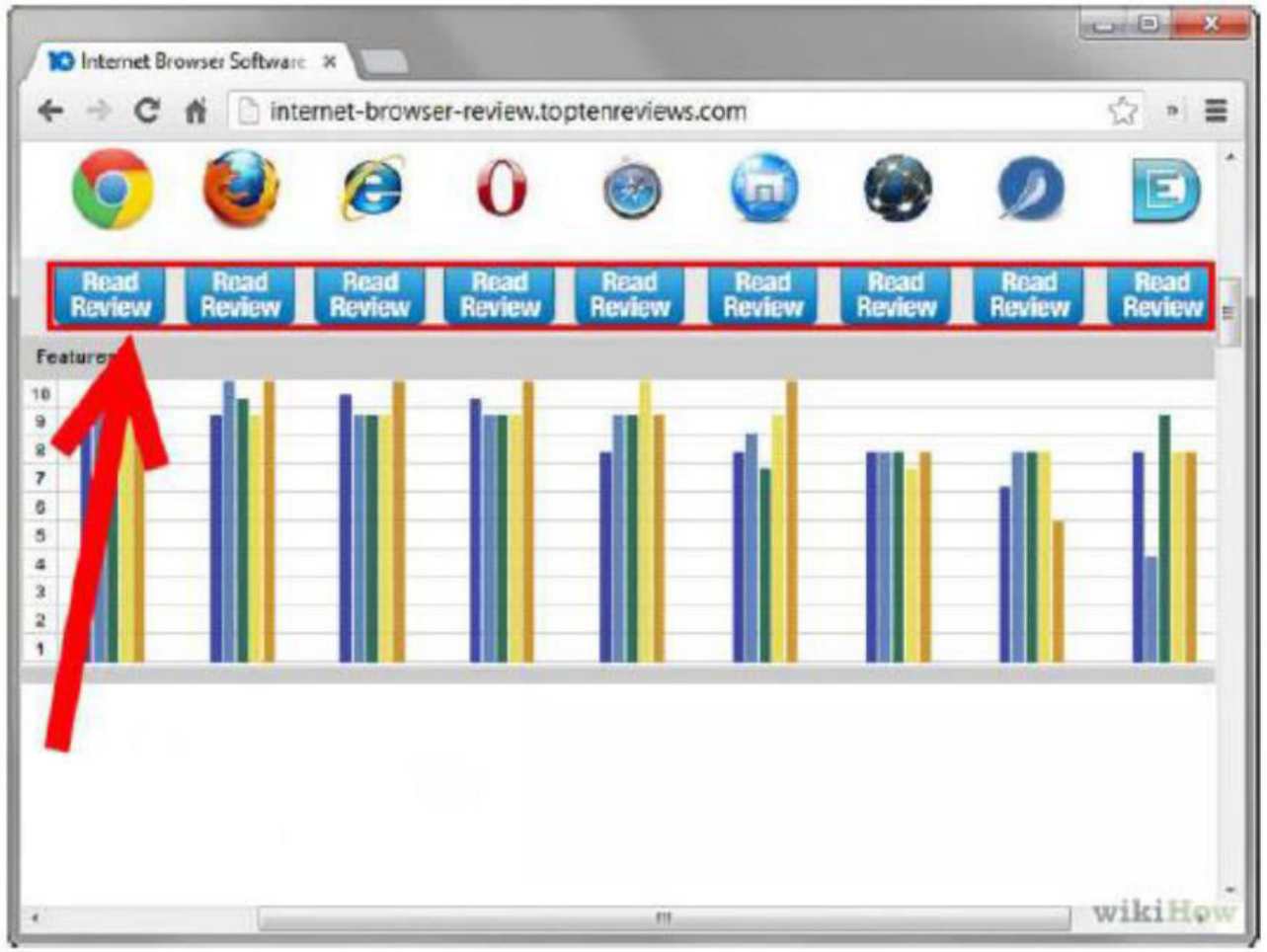
Step 2: Think about your ideal browser; what would it be able to do? You may want it to be quite simple, handling only the bare necessities. You may want some basic features like web feed reading, bookmarking (favorites), or search boxes. Some browsers have a lot more, and that's where it starts to get confusing.

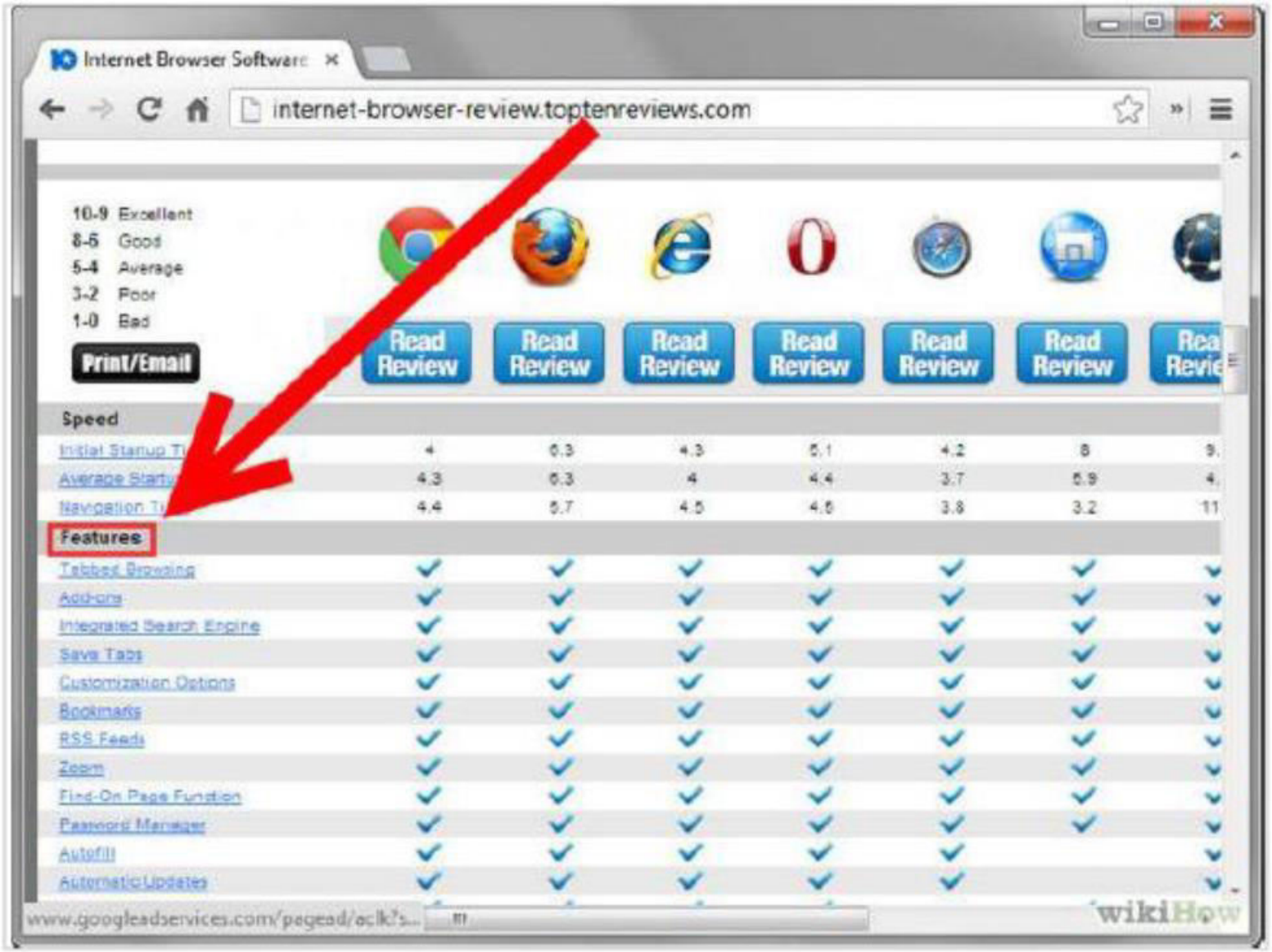


Step 3: Make sure you know what platform you are on. Some browsers are only available to a certain operating system, or not available to one operating system



Step 4: Research browsers. Tabbed browsers include Safari (runs on OS X, iPhone and is new to Windows), Firefox (general purpose with the most plug-ins), Opera(supports torrents, handles e-mail and runs on mobile devices), Konqueror (dual purpose file manager), Seamonkey (includes HTML editor and e-mail client), Off By One (tiny) and Flock (social networking).




Internet Browser Software
internet-browser-review.toptenreviews.com
10-9 Excellent
8-5 Good
5-4 Average
3-2 Poor
1-0 Bad
Print/Email
Read Review
Speed
Features
Tabbed Browsing
Add-ons
Integrated Search Engine
Save Tabs
Customization Options
Bookmarks
RSS Feeds
Zoom
Find-On Page Function
Password Manager
Autofill
Automatic Updates
wikiHow

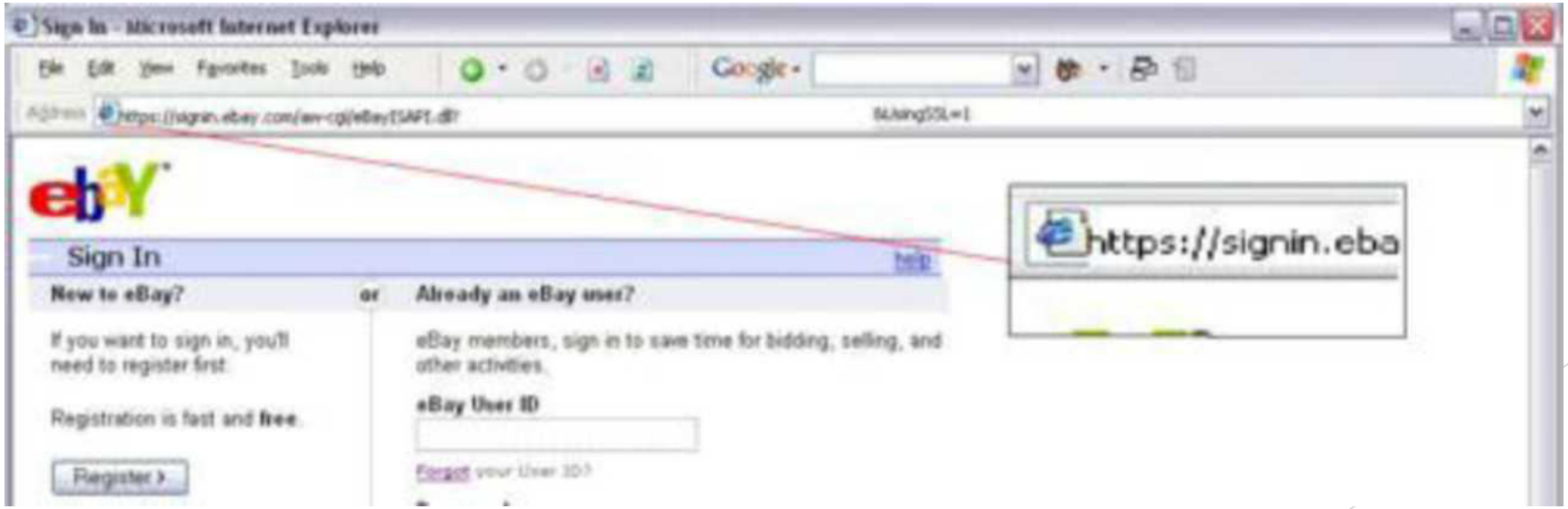
Guidelines for Safe Internet Browsing

Safe Browsing

- **The user must know if a website is secure** or not while surfing the internet.
- A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities.
- When the browser opens a secured connection, "https" can be seen in the URL instead of just http.
- To **know if a website is secure** or not, look for the locked yellow colour padlock symbol on the lower right corner of the browser window.

How do I know if a website is secure?

- To know if your browser is viewing a secure web site, you can look in the lower right part of the window.
- There is a small box in the frame of the window to the left of the area that describes which zone you are in (usually the Internet zone, with a globe icon).
- If you see a yellow padlock icon, the web site you are viewing is a "secure web site.“
- If the box is empty, the web site does not have a secure connection with your browser.



UNIT II

Working with window firewalls in windows – Finding the best browser According to the user requirement – Guidelines for safe browsing – Tips for buying online – Clearing cache for browsers.

Wireless Security: What is wireless LAN – Major issues with WLAN.

Email and Social Media Security: Safe browsing guideline for social networking sites – Email Security tips.

Previous Topics

- Working with window firewalls in windows
- Finding the best browser According to the user requirement
- Guidelines for safe browsing

Today topics

- Tips for buying online
- Clearing cache for browsers

- Wireless Security:

  What is wireless LAN

Tips for buying online

- Shopping online can be cheaper and more convenient for you and for businesses.
- However, make sure you understand your rights and the risks before you shop online or bid in an online auction.

I. **Pay securely:** Don't make any payment unless:

- You are on a secure website,
- You can make a secure payment.
- This will protect you against fraud and unauthorised credit card transactions.
- A secure website address will always:
- begin with 'https://', not 'http://'
- display the image of a closed padlock (usually in the bottom right corner of your browser window).

II. Know the business:

- Only buy from websites you know and trust.
- Check that the company has a physical street address and landline phone number.
- If the company operates from overseas, you might have trouble getting a refund or repair.

III. Know the product: Make sure you check whether:

- the product is legal
- the product will work in Australia
- any warranties or guarantees offered are valid in Australia
- the product has an authorised repairer nearby.

IV. **Check the contract:** Make sure you read and understand:

- the terms and conditions of sale
- the refund policy
- the delivery details
- returns and repairs policies, including any associated costs.

V. **Check the full cost:** Be aware of the full cost of your purchase.

Additional costs may include:

- currency conversion
- taxes
- postage and delivery fees
- packaging.
- It might end up being cheaper to buy the product at a local shop.

VI. **Protect your privacy:**

- Only buy online if you are comfortable with a business'privacy policy.
- Do not give out information unless they require it to complete the sale.
- Remember, if a deal sounds too good to be true.

VII. **Keep records:**

Always write down any reference numbers and print out copies of:

- the order form (both before and after you confirm the order)
- receipts (can come by email or in a pop-up window).

Always make sure all charges are correct by checking the receipt against your:

- credit card statement
- merchant account statement (such as PayPal)
- bank statement.
- The charges may be converted from another currency.

VIII. **Online auction sites:** Most online auction sites (like eBay) offer a dispute resolution process for buyers and sellers.

This should be your first step to resolve a dispute if:

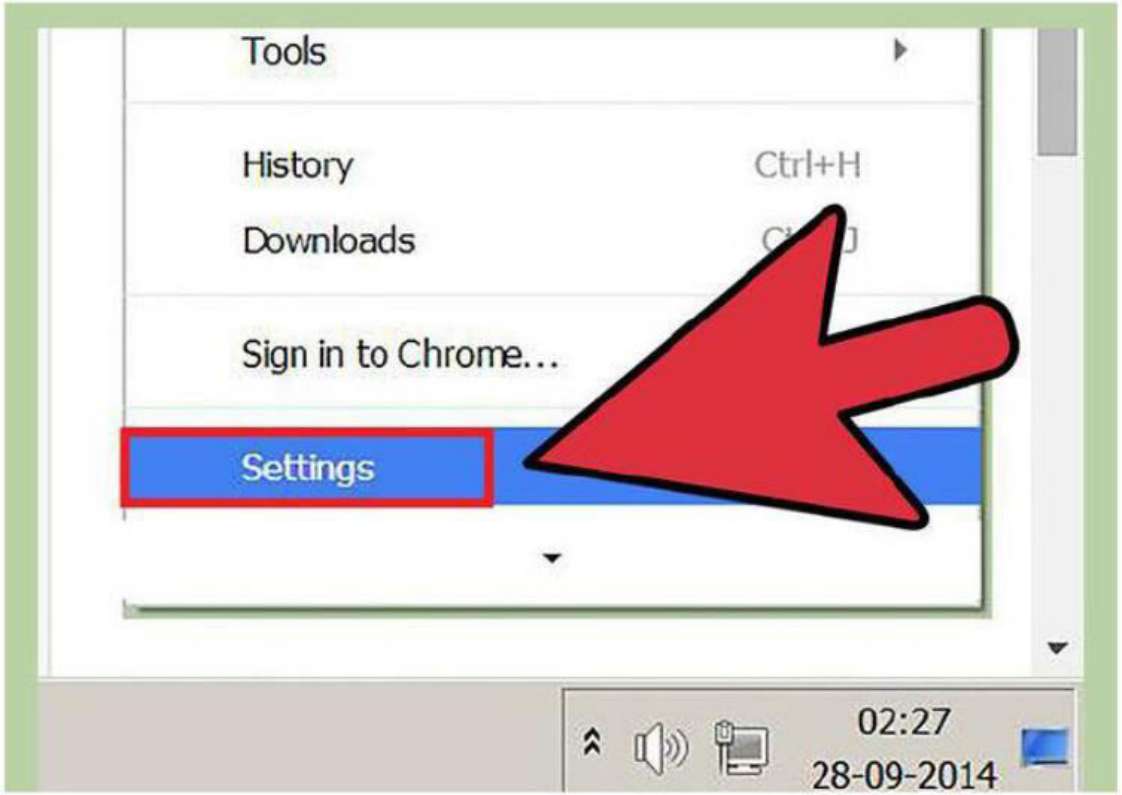
- you did not receive the items you bought
- you did not receive payment for items you sold
- you received items that were significantly different from their description.
- The eBay website has an example of this facility.

Clearing Cache for Browsers

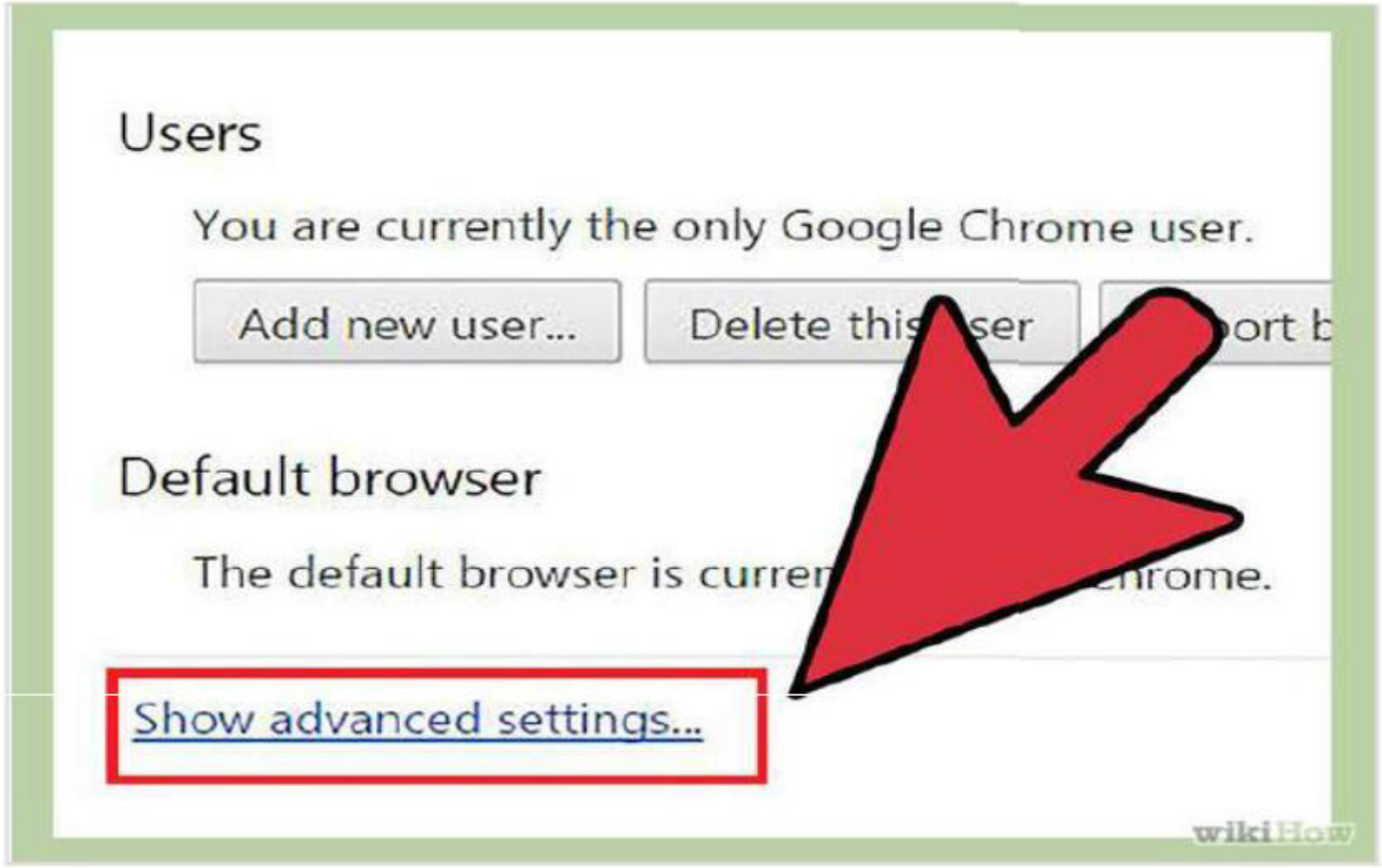
- Internet browser's cache stores certain information (snapshots) of webpages.
- Visit on your computer or mobile device so that they'll load more quickly upon future visits and while navigating through websites that use the same images on multiple pages so that you do not download the same image multiple times .
- Cache can prevent you from seeing updated content, or cause functional problems when stored content conflicts with live content.
- You can fix many browser problems simply by clearing your cache.
- The instructions given with screenshots on how to clear the cache for all major browsers.

Clearing cache for Chrome Browsers above version 10

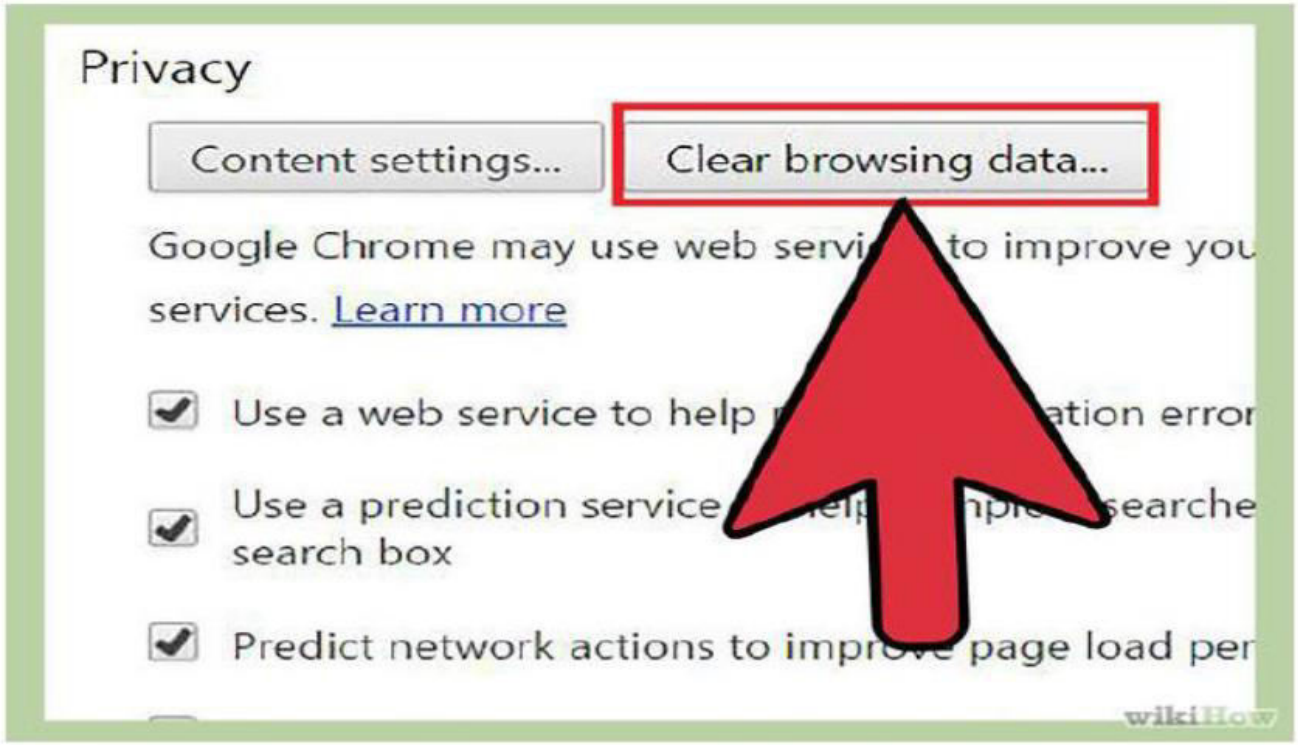
- **Step 1:** Open the settings on Chrome. Click the menu icon in the upper right corner of the browser to the right. Click settings on the bottom of the menu.



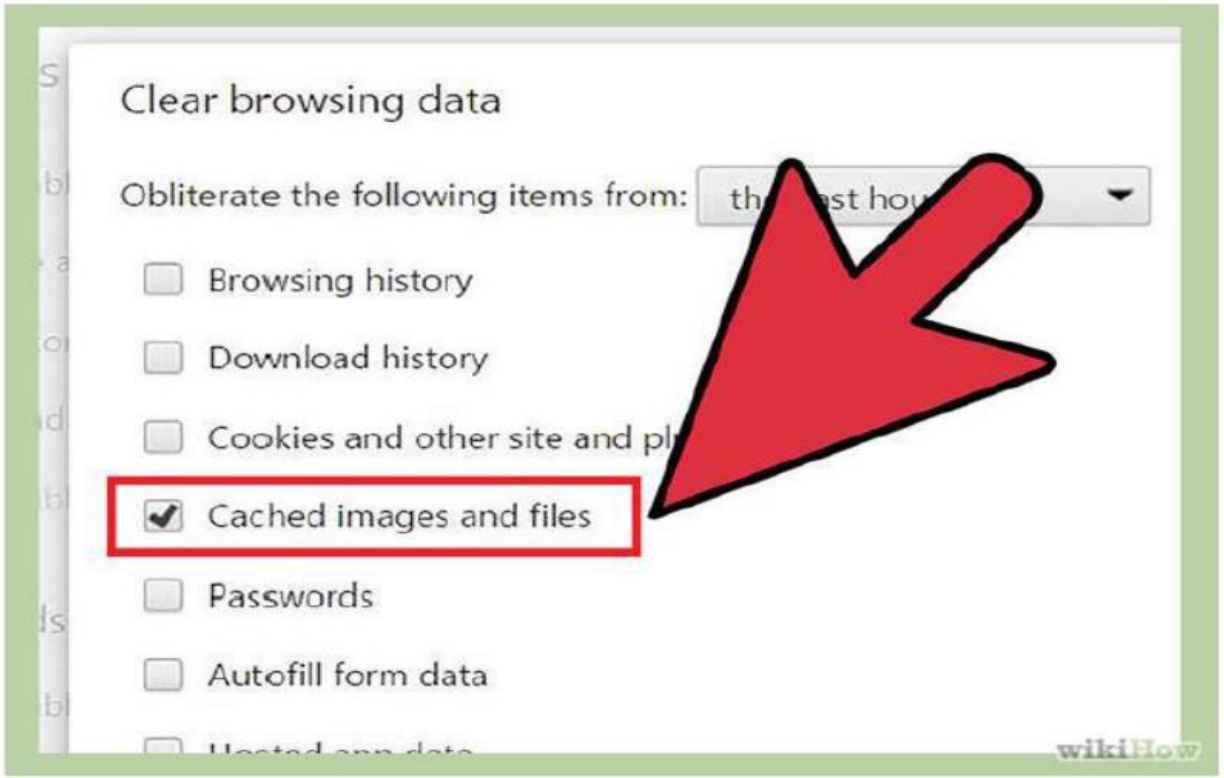
Step 2: From settings, click "Show advanced settings. It's located at the very bottom of the settings section.



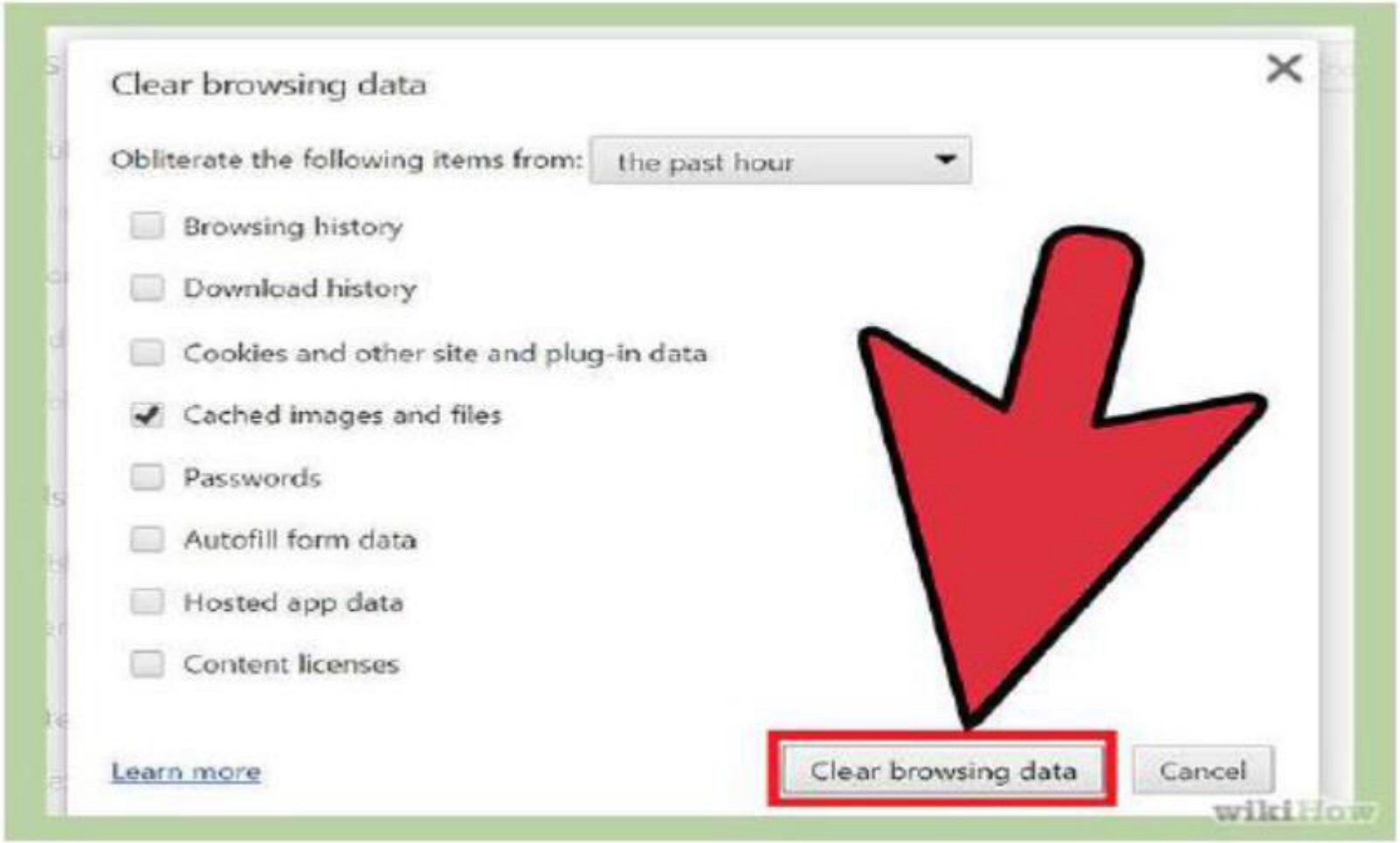
Step 3: Scroll to the privacy section and click "Clear browsing data.



Step 4: Select "Cached images and files". Uncheck all other options to avoid deleting browser history, cookies and other things you may wish to retain. Change "Obliterate the following items from" to "the beginning of time".



Step 5: Press "Clear browsing data". You are done!



Wireless Security
What is wireless LAN?

- The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days.
- In offices and homes, WLAN has become an alternative way of communication compared to wired LAN.
- The convenience to connect different devices is both cost effective and easily maintainable.
- The Wikipedia says: "Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free."

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.

2. WLANs are cost effective. Cabling all the way in the offices, hotels etc are not needed. So it's cheap and provides same quality of service.

3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.

4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.

More secure as most of APs support best encryption methods which protect them from sniffing

Web security is secure as most of APs support best encryption methods which protect them from sniffing and Other attacks.

UNIT II

Working with window firewalls in windows – Finding the best browser According to the user requirement – Guidelines for safe browsing – Tips for buying online – Clearing cache for browsers.

Wireless Security: What is wireless LAN – Major issues with WLAN.

Email and Social Media Security: Safe browsing guideline for social networking sites – Email Security tips.

Previous topics

- Tips for buying online
- Clearing cache for browsers

- Wireless Security:

  What is wireless LAN

Today topics

- Major issues with WLAN
- Email and Social Media Security:

  Safe browsing guideline for social networking sites

  Email Security tips

Major issues with WLAN

- WLAN are also as prone to various attacks as their counterpart wired LANs . Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation.
- No need to be in contact of physical wires to hack can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly.
- Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), De authentication attacks, War driving etc.
- Concentrate on best practices- how to install and use WLAN securely which can that a number of above mentioned attacks.

Secure WLAN

- Wireless Security mainly depends on these 3 factors:
  - How much is your wireless network secured in terms of encryption being used.
  - Monitoring for suspicious and unusual activities.
  - User awareness and education.
- These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

Wi-Fi at home

- ✓ Protecting a home wireless network is altogether a different side of the coin as compared to wired networks.
- ✓ Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to fend for her.
- ✓ So make sure, your network is secured from being maliciously used.

Steps for secure your network

1. **Use most secure possible encryption**:

- Industry standard encryptions.
- WEP-Wired Equivalent Privacy, has been known to be broken.
- Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel.
- Instead use secure protocols such as WPA 2 - Wi-Fi Protected Access- 2, which uses strong 128 bits AES ciphers.

Attacks mitigated: WEP Key cracking, Sniffing, Capturing/Eavesdropping

2. Use Firewall:

- All the wireless routers come with built-in firewalls.
- Enable them with all the security features.
- You should block any anonymous ping requests and place restrictions on website browsing.

Attacks mitigated: Fingerprinting, System compromise

3. Have a monitoring system in place:

- If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures.
- Deploy WIPS/WIDS for monitoring suspicious activities.

Attacks mitigated: Scanning, DoS

4. Don't use default credentials:

- Every wireless router comes with a set of default username/password.
- Username and passwords are used by computers or other devices to connect to wireless router.
- Some default username combinations are: admin/admin, admin/password or admin/ " ".

Attacks mitigated: Unauthorized access, War driving

5. Disable Auto-connect feature:

- Some users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack.
- Attackers keep their APs alive and kicking for such kind of unsuspecting users.
- They also use luring names as 'HotSpot', 'SecureConnect', 'GovtNetworks' etc. The user will never suspect them and keep surfing the wireless network

Email and Social Media Security

- Email used to communicate and to share information about particular subjects.
- Social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are.
- These functions are not new or unique - any of these actions can also be performed via the internet without joining a social networking site.

General Tips on using Social Networking platforms safely

- Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.
- Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.
- Consider using **separate accounts/identities,** or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine.
- **Access social networking sites using https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.

Posting Personal Details

- Social networking sites ask your data about yourself to make it easier for other users to find and connect to you.
- The more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities.
- The online activities of Diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- education and employment history

Status Updates

- On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening?
- The most important thing to understand about the status update is who can actually see it.
- The default setting for the status update on most social networking applications is that anyone on the internet can see it.
- If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

Sharing Videos and Photos

- Photos and videos can reveal people's identities very easily.
- It's important that you have the consent of the subject/s of any photo or video that you post.
- If you are posting an image of someone else, be aware of how you may be compromising their privacy.
- Never post a video or photo of anyone without getting their consent first.

Email Security Tips

1. Don't open email attachments that you are not expecting, or which have come from someone you do not know.

2. You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is ***Tor,***
3. You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly.
4. You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading.

- Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information,

- Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account.

3.

Unit –II Completed

UNIT III

Cyber Security Fundamentals: Network and Security Concepts – Information assurance and fundamentals – Basic cryptography – Symmetric Encryption – Public key encryption – Domain name system – Firewalls - Microsoft Windows security principles – Windows Tokens – Windows messaging.

Topics discuss to…..

- Cyber Security Fundamentals:
  - Network and Security Concepts
  - Information assurance and fundamentals
  - Basic cryptography
  - Symmetric Encryption

Cyber Security Fundamentals
Network and Security Concepts:

- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- It involves the authorization of access to data in a network, which is controlled by the network administrator.
- Network security covers a variety of computer networks, both public and private.
- Network security is involved in organizations, enterprises, and other types of institutions.
- Network security is any activity designed to protect the usability and integrity of the network and data.

Information Assurance Fundamentals

- Three key concepts,

  Confidentiality, Integrity, and Availability it known as the CIA triad.

- ✓ Authentication is any secure system, as it is the key to verifying the source of a message or that an individual is whom he or she claims.
- ✓ When an authentication system requires more than one of these factors, the security community classifies it as a system requiring multifactor authentication.
- ✓ Two instances of the same factor, such as a password combined with a user's mother's name and combining a fingerprint scan and a personal identification number (PIN).
- ✓ Authorization as "access privileges granted to a user, program, or process."

Nonrepudiation

"Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."

Confidentiality

"Assurance that information is not disclosed to unauthorized individuals, processes, or devices."

Integrity

Quality of an IS (Information System) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

Availability

"Timely, reliable access to data and information services for authorized users."

The best-known attack on availability is a denial of service (DoS) attack

Basic Cryptography

- Cryptography derives "hidden writing."
- The most famous classical cipher is the substitution cipher.
- Substitution ciphers work by substituting each letter in the alphabet with another one when writing a message.

Ex:

abcdefghijklmnopqrstuvwxyz

nopqrstuvwxyzabcdefghijklm

Using this cipher, the message "**the act starts at midnight**" would be written as "**gur npg fgnegf ng zvqavtug**."

This is a very simple substitution cipher known as the Caesar cipher.

- By replacing all instances of the letters g, u, and r with t, h, and e, the ciphertext changes to

  the npt ftnetf nt zvqavtht

- Next, the analyst might notice that the fourth word is only two letters long and ends with t.
- There are two likely possibilities for this word: at and it.
- He chooses at and replaces all occurrences of n in the sentence with an a.

  the apt ftaetf at zvqavtht

- With at in place, the pattern is clearer, and the analyst guesses that if the letter g translates to t, the adjacent letter f may translate to s.

  the apt staets at zvqavtht

- The word sta_ts now looks very close to starts, and the analyst makes another substitution, indicating that rst is equivalent to efg, which reveals the full pattern of the cipher and the message.
- While the message is now clear, the meaning of "the act starts at midnight" is not.

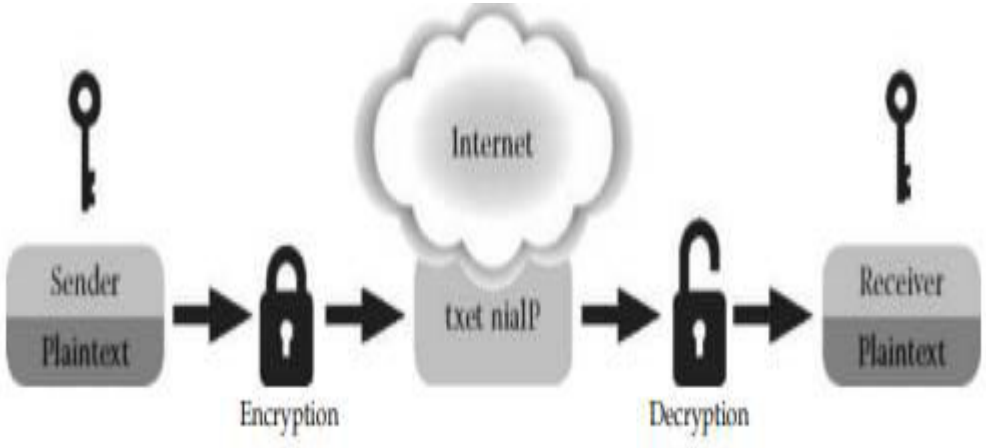
Code words are an excellent way of hiding a message but, unlike cryptography, cannot hide the meaning of arbitrary information without agreement on the meaning of the code words in advance

LETTER	FREQUENCY	LETTER	FREQUENCY
e	12.70%	m	2.41%
t	9.06%	w	2.36%
a	8.17%	f	2.23%
o	7.51%	g	2.02%
i	6.97%	y	1.97%
n	6.75%	p	1.93%
s	6.33%	b	1.49%
h	6.09%	v	0.98%
r	5.99%	k	0.77%
d	4.25%	J	0.15%
l	4.03%	x	0.15%
c	2.78%	q	0.10%
u	2.76%	z	0.07%

- Sender send a plaintext during the encryption the plain text convert in cipher text.
- Receiver decrypt the cipher text in plain text.

  2 keys used in encryption

- Public key
- Private key



Symmetric Encryption

- Symmetric encryption is a form of computerized cryptography using a singular encryption key to guise an electronic message.
- Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message.
- Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.
- Symmetric encryption is also known as **private-key encryption** and **secure-key encryption.**
- Both communication endpoints to know the same key in order to send and receive encrypted messages.
- Symmetric encryption depends upon the secrecy of a key.
- Key exchanges or pre-shared keys present a challenge to keeping the encrypted text's confidentiality and are usually performed out of band using different protocols.

- Algorithms in this category are usually fast because their operations use cryptographic primitives.
- Permutation, or altering the order, is another cryptographic primitive that many symmetric algorithms also use in practice.
- All of the most popular symmetric algorithms use block ciphers with a combination of substitution and permutation.
- These include the following:

  - 1977 DES
  - 1991 IDEA
  - 1993 Blowfish
  - 1994 RC5
  - 1998 Triple DES
  - 1998 AES

UNIT III

Cyber Security Fundamentals: Network and Security Concepts – Information assurance and fundamentals – Basic cryptography – Symmetric Encryption – Public key encryption – Domain name system – Firewalls - Microsoft Windows security principles – Windows Tokens – Windows messaging.

Previous topics

- Cyber Security Fundamentals:
  - Network and Security Concepts
  - Information assurance and fundamentals
  - Basic cryptography
  - Symmetric Encryption

Topics discuss to…..

- Public key encryption
- Domain name system
- Firewalls
- Microsoft Windows security principles
- Windows Tokens
- Windows messaging

Public key encryption

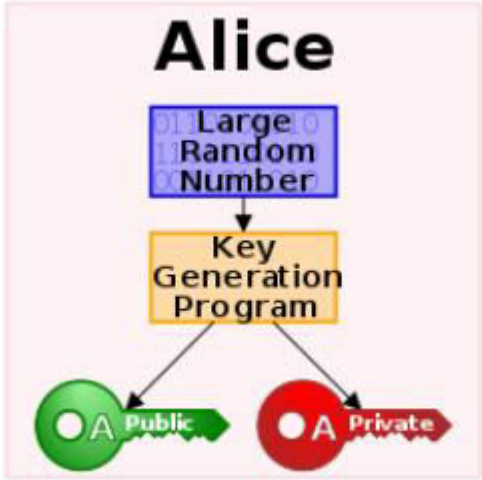
- A branch of cryptography for which the distinguishing attribute of the system is the use of two linked keys for encryption and decryption, rather than a single key.
- Each system shares one common attribute: each public key system uses one key, known as the public key, to encrypt data, and a second key, known as the private key, to decrypt the encrypted data.

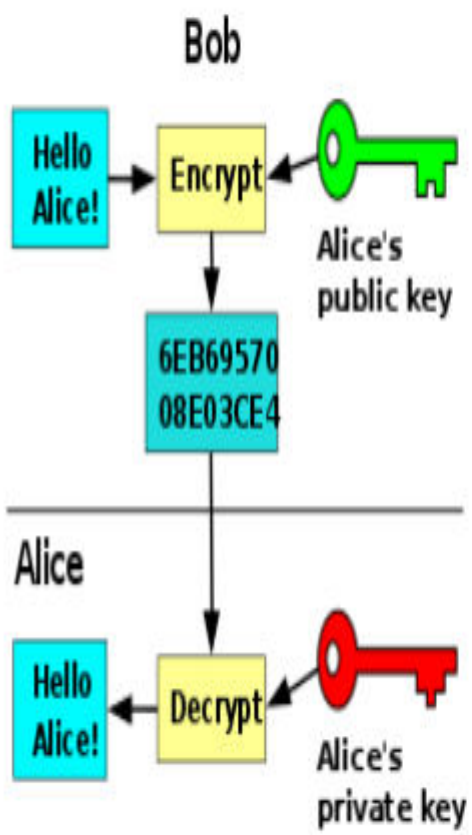
Public key

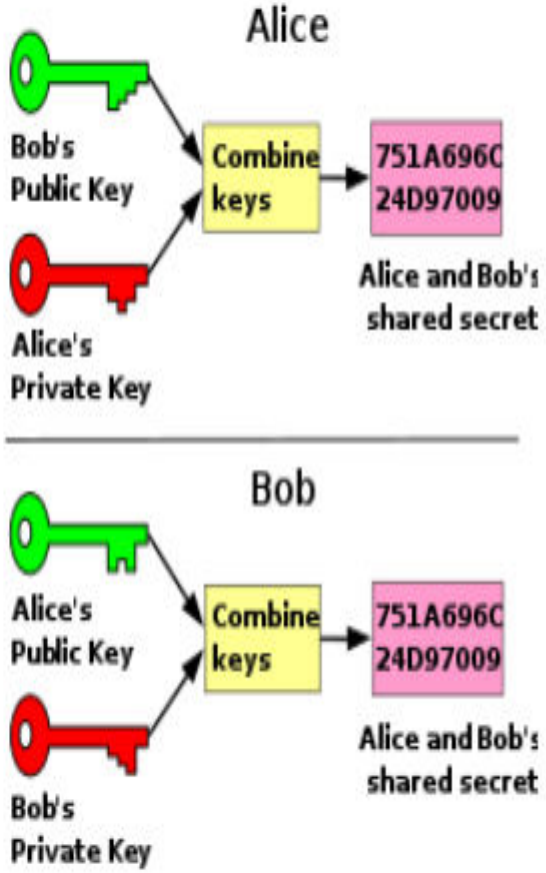
- ✓ In public key systems, the intended recipient of a secure communication publishes his or her public key.
- ✓ to send a secure datagram to the recipient uses the recipient's public key to encrypt the communication;
- ✓ the public key cannot use the key to decrypt the communication.
- ✓ The use of a public key is a one-way cryptographic operation.
- ✓ This allows recipients to give out their public keys without the risk of someone using the same public keys to reveal the original content of the messages sent.

Private key

- The private key has a mathematical relationship to the public key.
- The recipient uses the private key to decrypt messages encoded with the public key, it is permanent that the owner of the private key keeps it secure at all times.
- The process of encrypting and decrypting a message using the public key method is similar to the process of using symmetric encryption.

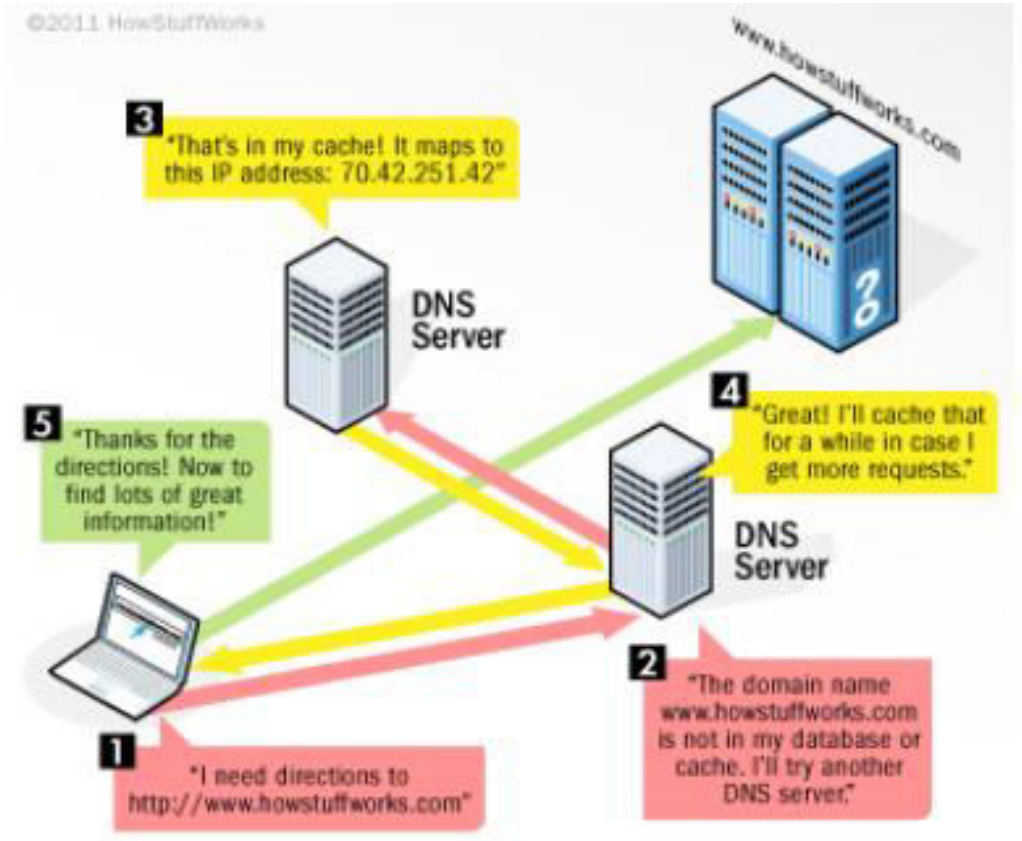



Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

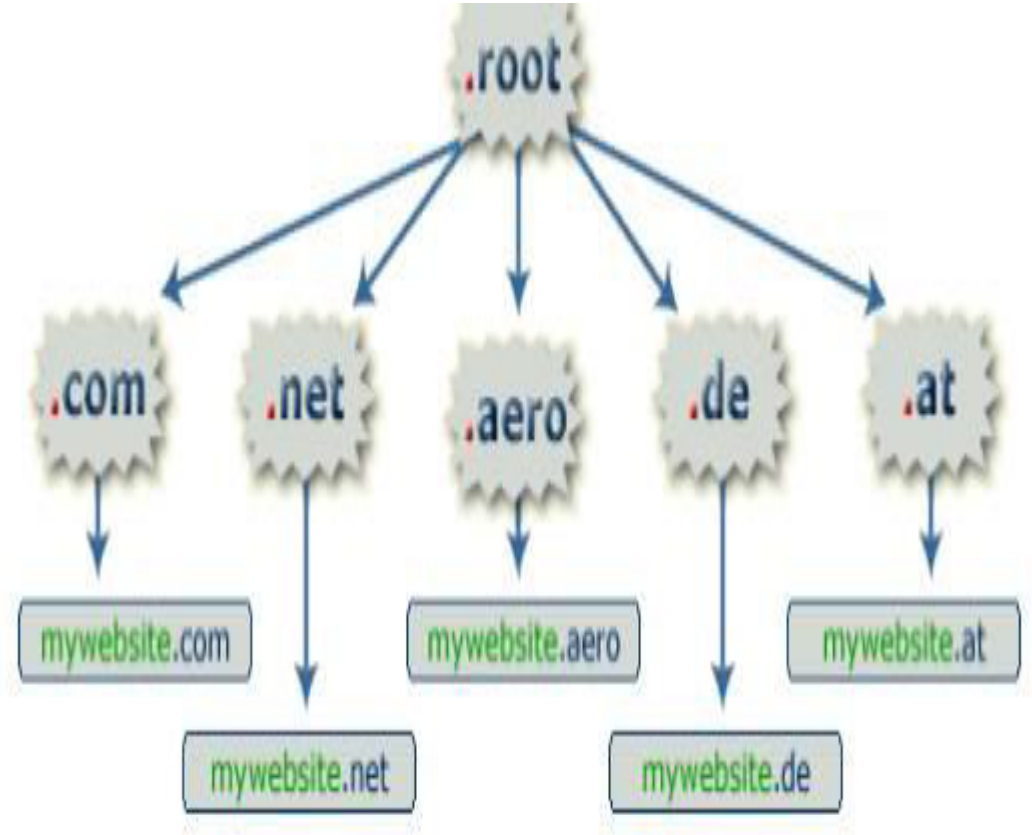

Alice
Bob's Public Key
Alice's Private Key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret
Bob
Alice's Public Key
Bob's Private Key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret

Domain Name System (DNS)

- DNS is a fundamental piece of the Internet architecture.
- Knowledge of how the DNS works is necessary to understand how attacks on the system can affect the Internet as a whole and how criminal infrastructure.
- Each computer with Internet access has an assigned IP address so that other systems can send traffic to it.
- Each IP address consists of four numbers between 0 and 255 separated by periods, such as 74.125.45.100.
- These numbers are perfect for computers that always deal with bits and bytes but are not easy for humans to remember.
- To solve this problem, the DNS was invented in 1983 to create easy-to-remember names that map to IP address.


©2011 HowStuffWorks
www.howstuffworks.com
3
"That's in my cache! It maps to this IP address: 70.42.251.42"
DNS Server
4
"Great! I'll cache that for a while in case I get more requests."
5
"Thanks for the directions! Now to find lots of great information!"
DNS Server
2
"The domain name www.howstuffworks.com is not in my database or cache. I'll try another DNS server."
1
"I need directions to http://www.howstuffworks.com"

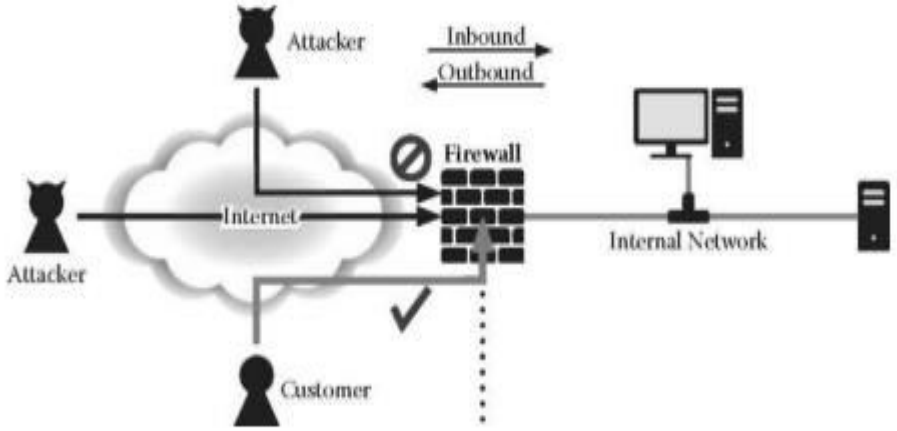
- Each user to download a multi thousand-line file named hosts.txt from a single server.
- To create a truly scalable system, the designers chose to create a hierarchy of "domains."
- At the top of the hierarchy is the "root" domain under which all other domains reside.
- The root domain are top level domains (TLD) that break up the major categories of domains such as .com, .gov, and the country code TLDs.
- Below the TLDs are second-level domains that organizations and individuals can register with the registry that manages that TLD.
- The DNS uses computers known as name servers to map domain names to the corresponding IP addresses using a database of records.
- Name servers are granted authority over a domain by the domain above them, in this case .com.
- When a name server has this authority, it aptly receives the title of authoritative name server for that domain.


.root
.com
.net
.aero
.de
.at
mywebsite.com
mywebsite.net
mywebsite.aero
mywebsite.de
mywebsite.at

Firewall

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.
- Firewalls are often categorized as either network firewalls or host-based firewalls.
- Network firewalls filter traffic between two or more networks and run on network hardware.
- Host-based firewalls run on host computers and control network traffic in and out of those machines.
- There are three basic types of firewall:
  - ✓ packet-filtering firewalls,
  - ✓ stateful firewalls,
  - ✓ application gateway firewalls.

- Different firewall types performs the same basic operation of filtering undesirable traffic, they go about the task in different manners and at different levels of the network stack.
- Host-based firewalls have found their way into most operating systems. Windows XP and later versions have a built-in firewall called the Windows Firewall.



First Generation Packet Filters

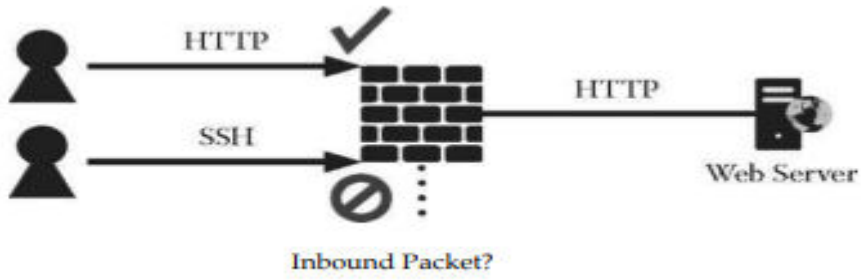
- The first reported type of network firewall is called a packet filter.
- Packet filters look at network addresses and ports of packets to determine if they must be allowed, dropped, or rejected.
- Packet filters act by inspecting packets transferred between computers.
- When a packet does not match the packet filter's set of filtering rules, the packet filter either drops (silently discards) the packet, or rejects the packet.
- Packets may be filtered by source and destination addresses, protocol, source and destination ports.
- The bulk of Internet communication in 20th and early 21st century used either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) in conjunction with well-known ports.

Second generation: stateful filters

- From 1989–1990 three colleagues from AT&T Bell Laboratories, Dave Presotto, Janardan Sharma, and Kshitij Nigam, developed the second generation of firewalls, calling them circuit-level gateways.
- Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model.
- This is achieved by retaining packets until enough information is available to make a judgment about its state.
- A risk to be aware are denial-of-service attacks that bombard the firewall with thousands (or more) of fake connections in an attempt to overwhelm the firewall by filling its connection state memory.

Third generation: application layer

- Application Gateway Firewalls Application gateway firewalls, also known as proxies.
- A classic example of an application gate- way firewall is a Web proxy or e-mail-filtering proxy.
- A Web proxy, for instance, understands the proper HTTP protocol and will prevent an improperly un structed request from passing.



Microsoft Windows Security

- Windows Communication Foundation (WCF) is a SOAP message-based distributed programming platform, and securing messages between clients and services is essential to protecting data.
- WCF provides a versatile and interoperable platform for exchanging secure messages based upon both the existing security infrastructure and the recognized security standards for SOAP messages.

Windows Tokens

- ✓ Windows users access tokens to determine if a program can perform an operation or interact with an object.
- ✓ Tokens provide the security context for processes and threads when accessing objects on a s system.
- ✓ These objects, also known as securable objects, include all named objects ranging from files and directories to registry keys.

- Tokens have four parts that include an identity, privileges, type, and access controls.
- The token belongs, much like a driver's license includes the owner's name.
- The identity consists of two parts: a user and a group, just as the name on a driver's license consists of both a first and last name.
- If a person were to use a credit card, the merchant might ask to see the person's license to check if the name on the credit card is the same as the name listed on the driver's license.
- If the names matched, the merchant would allow the person to use the credit card.
- In Windows, if a user has access to a directory, Windows would check to see if the token had the same user listed.
- If it is the one listed, Windows would grant access to the directory

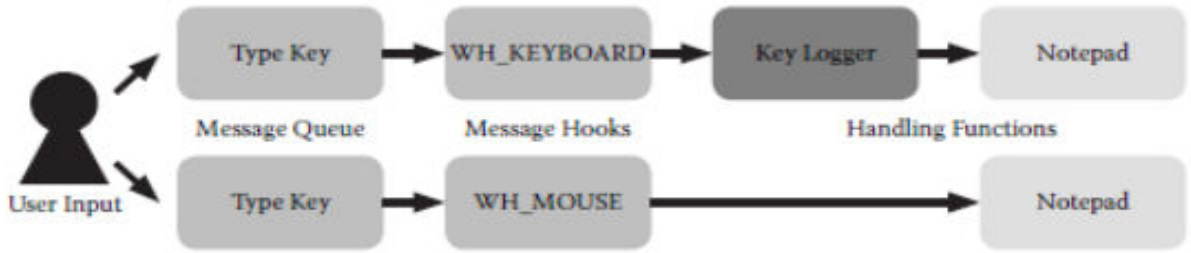
Windows Messaging

- The window-messaging queue, which handles events such as mouse clicks and keyboard input, allows program windows on Microsoft operating systems to interact.
- Monitoring window message hooks can reveal malicious behavior such as key logging or graphical user input.
- Programs that run on Microsoft operating systems with visible windows can accept and handle new events using window messaging (and the window-messaging queue).
- Malicious and nonmalicious programs install message hooks to process message events.
- For instance, notepad.exe installs a message hook for keyboard (WH_KEYBOARD) and mouse (WH_MOUSE) messages to accept user input.

- The system delivers messages using a first in, first out (FIFO) message queue or by sending messages directly to a handling function.
- Each thread that has a graphical user interface (GUI) has its own message queue, and there is a special message queue for system messages.
- Whenever a window does not accept these messages within a timeout period of a few seconds, the window may show “Not Responding” until the program handles the message.
- When a user logs on, he or she will also call the Create Desktop function, which associates the desktop with the current window station.
- With fast user switching, for instance, multiple users can log on at the same time and each has a unique desktop.
- A desktop restricts window messages from other desktops, preventing a user from sending window messages to another active desktop.

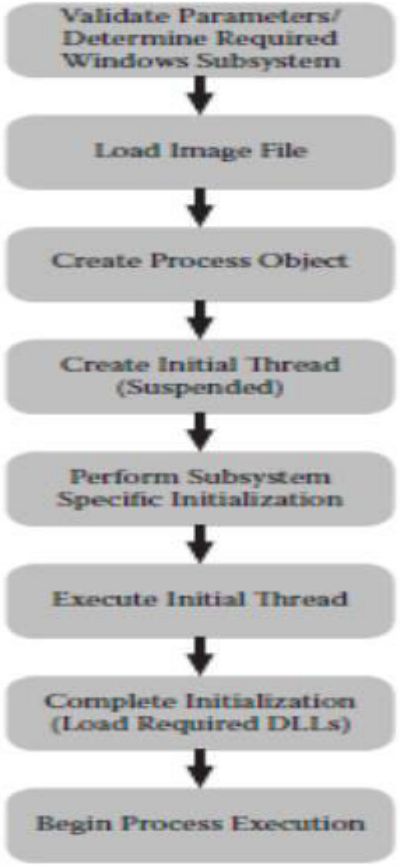
Malicious Uses of Window Messages

- Malicious code authors can use window messages and hooks for malicious purposes, including monitoring, covert communication, and exploiting vulnerabilities.
- One malicious use of window messages is for monitoring. An attacker can use the SetWindowsHookEx function with WH_KEYBOARD to install a key logger.
- Window messages can also serve as a covert communication channel that is often invisible to users and administrators.
- Rootkits or other malicious programs can communicate using custom window messages



Validation of Parameters

- The call to NtCreateProcessEx con-tains a variety of parameters that the function must verify before it can attempt to load an executable image.
- The scheduling priority parameter consists of a set of independent bytes, each of which specifies a particular priority class such as Idle, Below Normal, Normal, Above Normal, High, and Real-Time.



Unit –III completed

UNIT IV

Attacker Techniques and motivations: How hackers cover their tracks – Tunneling techniques – Fraud Techniques - Phishing, Smishing, Vishing and Mobile Malicious Code - Rogue Antivirus - Click Fraud – Threat infrastructure.

Topics discuss to…..

- Attacker Techniques and motivations:
  - How hackers cover their tracks
  - Tunneling techniques

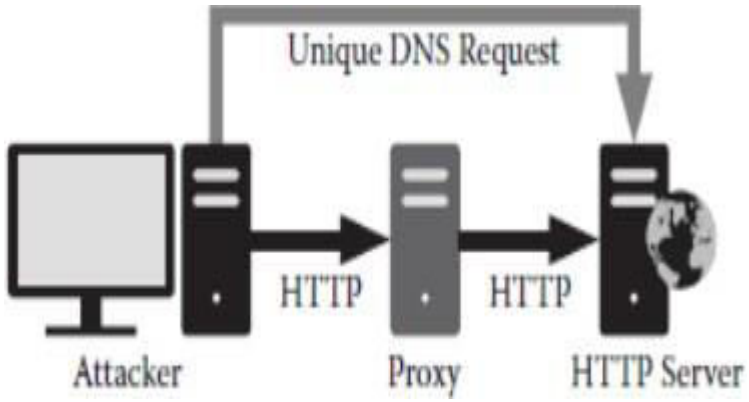
Attacker Techniques and Motivations How Hackers Cover Their Tracks

- Masking one's IP address is a standard practice when conducting illicit activities.
- A proxy allows actors to send network traffic through another computer, which satisfies requests and returns the result.
- Students or employees can use proxies to communicate with blocked services such as Internet Relay Chat (IRC) and instant messaging, or to browse websites that administrators block.
- Attackers also use proxies because Internet Protocol (IP) addresses are traceable, and they do not want to reveal their true locations.
- Proxies are also a common source of spam e-mail messages, which use open relays (a simple mail transfer protocol [SMTP] proxy).
- Proxies provide attackers with a way to lower their risks of investigator identification of their true IP address

Types of Proxies

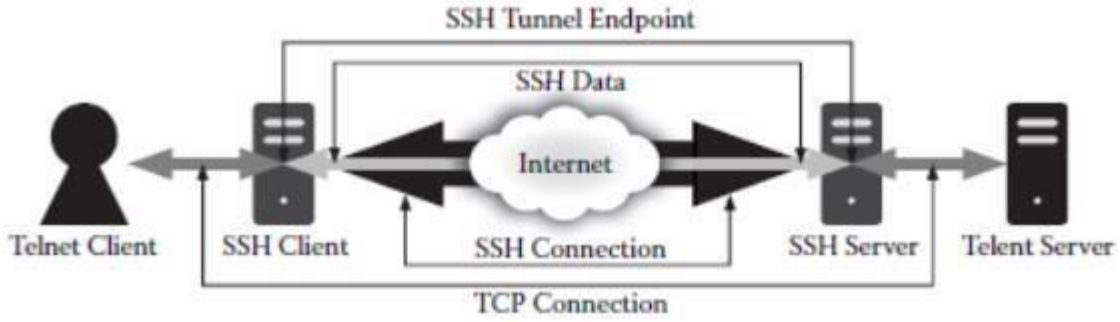
- Proxies are so common that many attackers scan the Internet for common listening proxy ports.
- The most com-mon proxies listen on TCP port 80 (HTTP proxies), 8000, 8081, 443, 1080 (SOCKS Proxy), and 3128 (Squid Proxy), and some also handle User Datagram Protocol (UDP).
- A virtual private network (VPN) acts as a more versatile proxy and supports more security features.
- Instead of configuring the application to use a proxy, users can tunnel all traffic through the VPN.
- VPN services usually support strong authentication and are less likely to leak information that could identify the user of a proxy.
- The application links the DNS request to the user's IP address and verifies that the HTTP request originates from the same IP address

- The following application plug-ins to determine the true IP address of a proxy user:
  - Word
  - Java
  - Flash
  - QuickTime
  - iTunes



Tunneling Techniques

- Tunneling data through other protocols often bypasses these controls and may allow sensitive data to exit the network and unwanted data to enter.
- It is even possible to extend all networks through these means without ever triggering an alert or log entry.
- Most researchers cannot help but think of secure shell (SSH) when hearing the word tunneling.
- A common, simple form of traffic tunneling in SSH is the tunneling of a Transmission Control Protocol (TCP) port.



Telnet Tunneled over a Secure Shell (SSH) Connection

HTTP

- HTTP has become the de facto high-level protocol on the Internet.
- As the protocol used for accessing content on the World Wide Web, developers adapted it to carry much more than just the static text and images of Web pages.
- HTTPS, which is HTTP secured over a secure socket layer (SSL) against eavesdropping and tampering, is no different from HTTP except that it makes detection harder.
- If a malicious actor cannot eavesdrop, he or she does not have a chance to detect known signatures of tunnels.
- Proxies that support HTTPS through a CONNECT method may actually make matters far worse, as the CONNECT method simply establishes an arbitrary TCP connection that can send or receive any data.

DNS

- The DNS is the core directory service of the Internet.
- Translations between names, such as www.verisign.com and IP addresses, could not happen, and it would be difficult, if not impossible, to manage the daily operations of the Internet.
- DNS is a service that an administrator cannot block and must always make available, it is also a good choice for data exfiltration and tunneling.
- The basic construct of DNS is different from HTTP and other content delivery protocols.
- The most common delivery mechanism for DNS is the UDP, not TCP, so the specifications do not guarantee communication reliability.

ICMP

- ICMP is a signaling protocol for IP. It is used mostly to deliver status and error messages when IP-based communication errors occur or to troubleshoot and test connectivity status.
- Although most enterprise policies already block outbound ICMP packets, some Internet service provider (ISP) solutions may not, and its use as a tunnel is mostly to bypass ISP authentication requirements or as a simple covert channel.
- Most ICMP messages offer little in the way of embedding payload, and implementation details may make it difficult to get the messages delivered;
- ICMP echo messages, which users and administrators alike use to test the accessibility of a host, are well suited for tunneling.
- Ping, as the most common software that implements this ICMP mechanism, sends data to a host and expects a reply

Intermediaries, Steganography, and Other Concepts

- packet inspection requires that a given protocol at least match the appropriate syntax (headers must match, no arbitrary data, etc.), toolwriters can coerce even FTP, SMTP, and the like into becoming covert channels.
- All such tunnels have one thing in common, however: it is apparent where their destinations.
- Steganography is the practice of hiding messages and data in content that is not readily apparent and is a form of security through obscurity.
- For example, steganographic software and tools can encode messages and data into images so that only users who know where the data exists can retrieve it.
- Tunnels that use intermediaries for data exchange can deposit payloads that are steganographically encoded to make it harder to detect the covert communication.

Detection and Prevention

- The potential of covertly extending a network to the outside world is a clearly unacceptable risk.
- While the firewalls and IDS that are in place today have their roles to play, they may not be able to identify or prevent tunneling.
- Tunnels abuse proto-cols in a way that matches the syntax or the rules of the specifications but not the intent, so despite the efforts of vendors using static signatures for detection
- for example, iodine signatures available for Snort—it is trivial to —hack‖ tunnels to foil the current crop of defenses.
- Attackers can easily modify open-source tools to appear slightly different from the original, thus defeating a static rule.
- Any protocol can quickly become a tunnel harbor. Packet inspection firewall rules and IDSscan go only so far in identifying and blocking the threats. Tunnels do have a weakness.

UNIT IV

Attacker Techniques and motivations: How hackers cover their tracks – Tunneling techniques – Fraud Techniques - Phishing, Smishing, Vishing and Mobile Malicious Code - Rogue Antivirus - Click Fraud – Threat infrastructure.

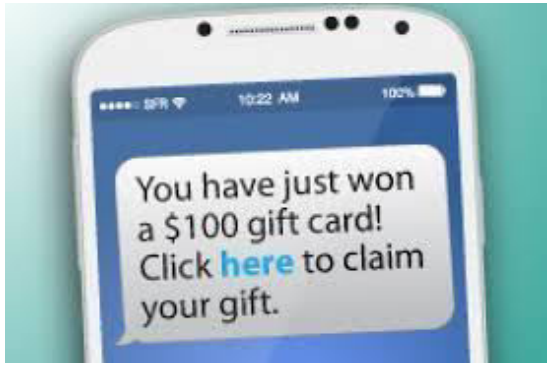
Previous topics

- Attacker Techniques and motivations:
  - How hackers cover their tracks
  - Tunneling techniques

Topics discuss to…..

- Fraud Techniques:
  - Phishing, Smishing, Vishing and Mobile Malicious Code
  - Rogue Antivirus
  - Click Fraud
- Threat infrastructure.

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.



The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

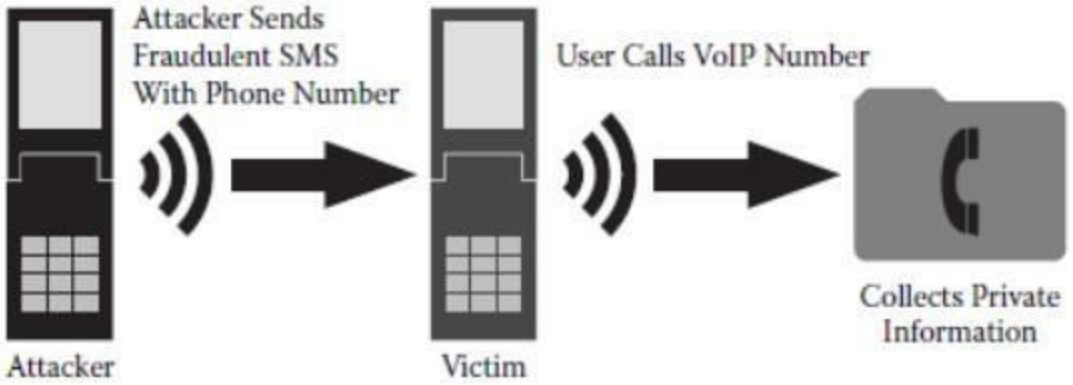
The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

Phishing, Smishing, Vishing, and Mobile Malicious Code

- Phishing attacks against mobile devices use short message service (SMS, or smishing) and voice-over Internet protocol (VoIP, or vishing) to distribute lures and collect personal information.
- Attackers often send fraudulent SMS messages containing a URL or phone number using traditional phishing themes.
- Responders either enter their personal information into a fraudulent website, as with traditional e-mail phishing, or, if calling phone numbers, may even provide their information directly to other people.
- To limit exposure to these growing threats, organizations should not send contact information to users via SMS but instead should be sure phone numbers are readily available on their websites.
- Financial institutions should carefully consider using mobile devices as two-factor authentication devices, given that customers may use the same mobile device to access the online banking system

Phishing against Mobile Devices

- Most instances of SMS phishing (smishing) target banks or financial institutions by sending a phone number that the victim calls after receiving the message, resulting in a vishing attack.
- Attackers used vishing against random targets and were successful at evading defensive filters.
- For instance, actors have used SMS gateways that allow users to send e-mails instead of spending money per SMS message
- SMS gateway providers have responded to abuse by rejecting excessive numbers of messages or fraudulent messages.
- This is dependent upon the cooperation of the Internet service providers (ISPs)



Rogue Antivirus

- Rogue security software is a form of malicious software and internet fraud that misleads users into believing there is a virus on their computer and aims to convince them to pay for a fake malware removal tool that actually installs malware on their computer.
- Attackers aggressively target users with Trojan applications that claim to be antivirus programs. These rogue antivirus applications, once installed, falsely report security issues to mislead victims into purchasing a purported —full version

Click Fraud

- Click fraud is a type of fraud that occurs on the Internet in pay-per-click online advertising.
- In this type of advertising, the owners of websites that post the ads are paid an amount of money determined by how many visitors to the sites click on the ads.
- Direct relationship between the number of clicks and the amount of money earned by the publisher has resulted in a form of fraud.

Pay-per-Click

- Any advertising transaction has three primary parties:

  1)Advertiser 2)Publisher 3)viewer

The advertiser is a company that produces content it would like to display to potential customers.

This content is an advertisement for a specific product or service that is likely to generate revenue for the advertiser.

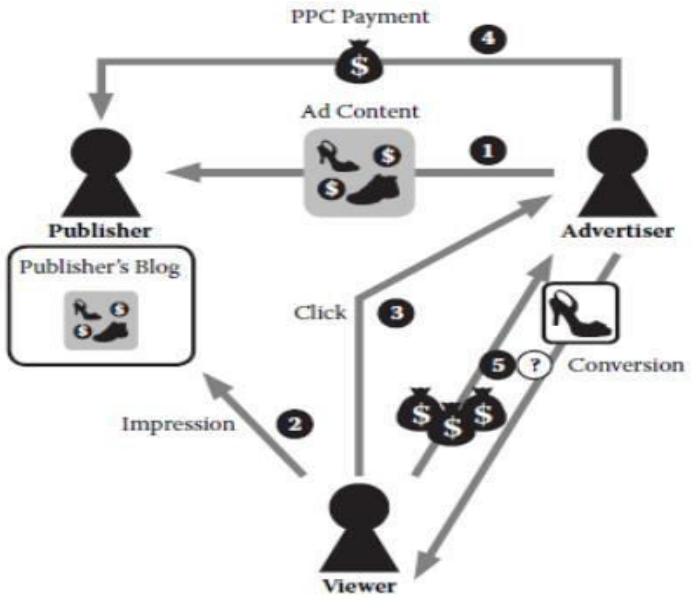
The publisher is a creative outlet that produces content that will draw visitors to its medium.

These visitors view the ad and, ideally, purchase the advertised product or service.

The advertiser pays a fee for a specific number of **impressions** which is the estimated number of times a viewer will see the ad.

This model is essentially the same across all forms of media, including print, radio, and television.

- The ultimate goal for the advertiser is to convert ad clicks to actions that generate more revenue than the advertising campaign costs.
- When the viewer takes the desired action, be it signing up for a newsletter or purchasing a new car, a conversion has occurred. This conversion completes the PPC business model.



Pay Per Click Business Model

Click Fraud Motivations

- Click fraud occurs when an ad network charges an advertiser for a click when there was no opportunity for a legitimate conversion.
- There are many possible motivations for a person to click an advertisement without any intention to purchase a product or service.
- Publishers perform the most obvious and common form of click fraud.
- Clicking an ad on one's own website directly generates revenue for the publisher. Clicking the ad fifty times generates even more revenue.
- Competing publishers might also be motivated to commit click fraud.
- Most advertising networks work very hard to detect it and will ban affiliates suspected of committing click fraud.
- Nonfinancial motivations might also cause a person to commit click fraud.
- In the case of clicks from a competitor, the intent is to harm the advertisers, but the outcome also benefits the publisher.

Click Fraud Tactics and Detection

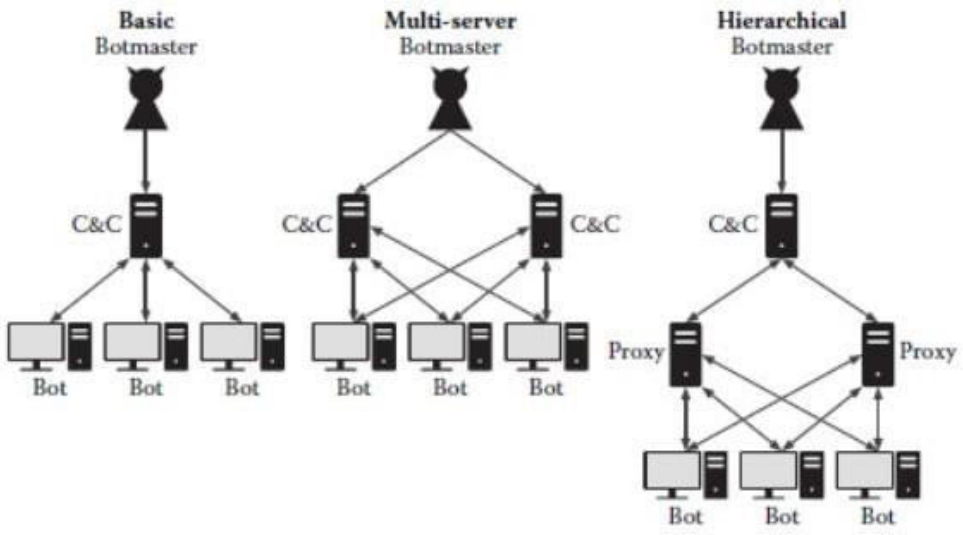
- The simplest form of click fraud involves manually clicking advertisements through the browser.
- First, the fraudster must create a website that displays advertisements. A popular way to do this is to create a search engine that only displays advertisements relevant to a queried word.
- A click fraud botnet can generate clicks in multiple ways.
- The botnet may simply download a list of key words and visit a random ad returned by the query for each word.
- Another technique is to redirect actual searches made by the infected system.
- When an infected user makes a query to a search engine, the malicious software will alter the results returned so that clicking them results in an ad click controlled by the fraudster.
- This technique may be more effective at evading detection because real users may actually click additional links on the page and potentially even purchase products.

Threat Infrastructure

- Systems connected to the Internet are at risk of infection from exposure to socialengineering attacks or vulnerability exploitation.
- the infection vector, compromised machines can wait for commands from the attacker, which turns the system into a bot.
- A bot is a single node added to a network of other infected systems called a botnet.
- A botnet is a network of infected systems controlled by an administrator known as a botmaster.
- A botmaster controls many bots by issuing commands throughout the botnet infrastructure.

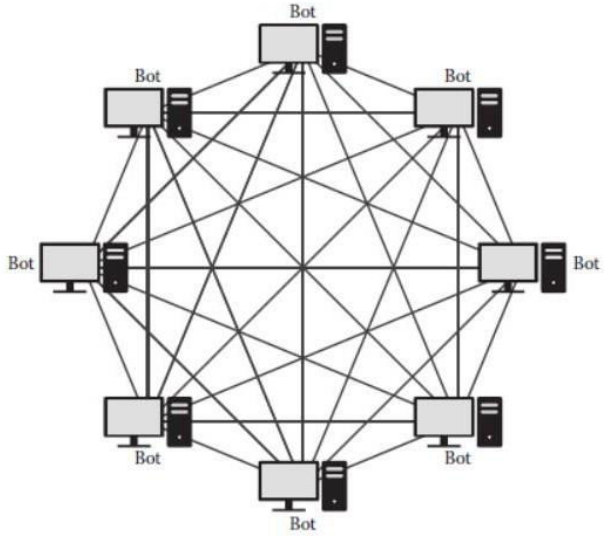
- A multiserver builds on the basic centralized botnet topology by using more than one server for C&C.
- Multiple C&C servers make botnets more reliable and less vulnerable to takedown attempts.
- This type of topology allows bots to receive commands even if one server is unreachable.
- If a server goes offline, the botmaster can still communicate with bots through other C&C servers.
- Most botnets rely on the domain name system (DNS) and domain name lookups for bots to locate the C&C server.
- To use the DNS, a bot queries its name server for the IP addresses that resolve the domain name of the C&C server.
- The DNS allows the botmaster to introduce reliability and resiliency for a server takedown by using multiple IP addresses or fast-flux to resolve domain names

- Communication within a botnet is crucial, and many botnets use Internet Relay Chat (IRC) as a rally point to manage infected machines.
- Typically, IRC botnets allow a botmaster to issue commands to bots connected to an IRC channel.
- For example, the IRC botnet known as SDBot used NOTICE, TOPIC, or private message (PRIVMSG) commands to control infected machines in an IRC channel.



Centralized Botnet Architecture

- Administrators attempting to detect infected bots within their networks need to monitor traffic for botnet communication.
- Repeated anomalous traffic over IRC or nonstandard ports from a system can indicate an infected machine participating in a botnet.
- Detecting botnet activity over common ports is more difficult and requires filtering out legitimate traffic.
- To filter out legitimate traffic, the administrator needs specific knowledge of the botnet's communication and how it appears while traversing the network.



Decentralized Botnet Architecture

Unit-IV Completed

UNIT V

Exploitation: Techniques to gain a foothold – Shellcode – Integer overflow vulnerabilities – stack based buffer overflow. Malicious Code: Self Replicating Malicious code - Evading Detection and Elevating Privileges – Root kit – Spyware – Attacks against privileged user accounts - Stealing Information and Exploitation – Form grabbing – Man in the middle attacks.

Topics discuss to…..

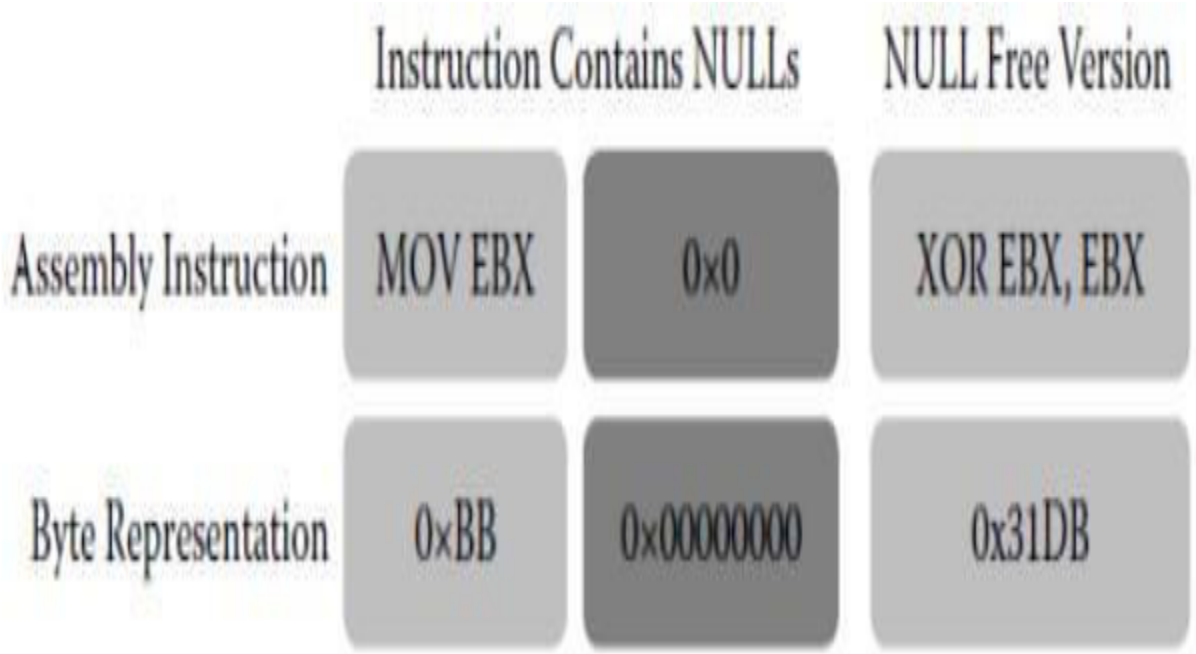
- Exploitation:
  - Techniques to gain a foothold Shellcode
  - Integer overflow vulnerabilities
  - stack based buffer overflow.
  - Malicious Code:
    - Self Replicating Malicious code

Exploitation Techniques to Gain a Foothold Shellcode

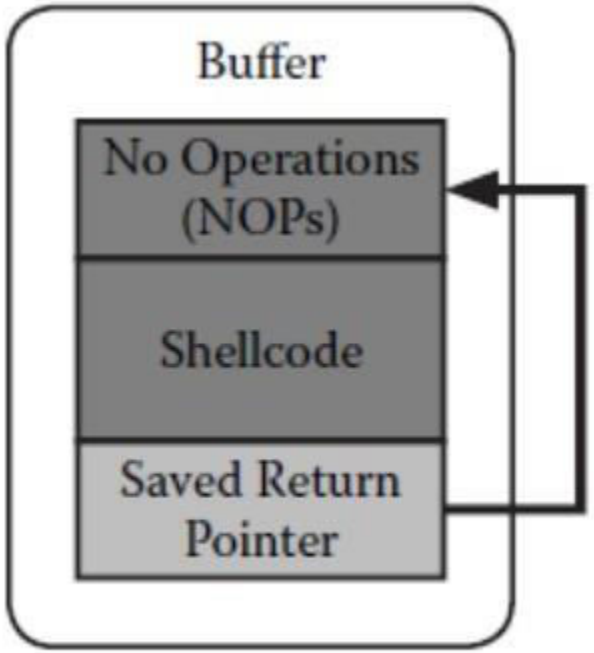
- shellcode, injectable binary code used to perform custom tasks within another process, makes it simple for even novice attackers to create highly reliable payloads for use after exploitation.
- Initially, shellcode simply spawned a shell from another process; however, it is now used to perform a variety of custom tasks.
- Shellcode is binary code used as the payload in exploitation of software vulnerabilities.
- The name shellcode originates from its initial intentions to spawn a shell within another process but has since evolved to define code that performs any custom tasks within another process.
- Written in the assembly language, shellcode passed through an assembler creates the binary machine code that the central processing unit (CPU) can execute.
- The shellcode payload is executed seamlessly, acting as if it were part of the original program..

- Shellcodes typically do not port well between Linux, UNIX, and Windows platforms due to the differences between system calls and the way these calls use the CPU.
- Linux and UNIX use the same interrupt, but Linux puts the system call number and arguments into CPU registers before issuing the interrupt, while UNIX platforms push the system call number and arguments to the stack memory.
- Windows uses a different set of syscall numbers, which renders Windows shellcode incompatible with Linux and UNIX kernels.
- Windows operating systems include system calls, but the limited set of functions and the variance of syscall numbers between versions reduce the effectiveness and reliability of the shellcode.
- Windows provides an application programming interface (API) through the use of dynamically linked libraries (DLLs) for applications to interact with the kernel.
- The functionality of the shellcode and loaded DLLs shares the same permissions of the victim process.
- Attackers use several different techniques to locate kernel32.dll for use within shellcode.

- The functionality of the shellcode and loaded DLLs shares the same permissions of the victim process.
- Attackers use several different techniques to locate kernel32.dll for use within shellcode.



- Attackers use shellcode as the payload of an attack on a vulnerability. A successful attack on a vulnerability injects the payload into the targeted process, resulting in code execution.
- Buffer overflows are a common exploit technique using shellcode as a payload to execute code within the targeted process.



Shellcode Execution in a Stack Buffer Overflow

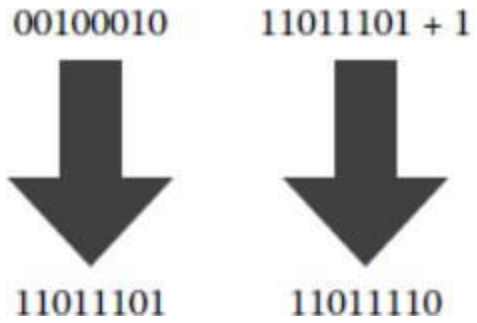
Integer Overflow Vulnerabilities

- Resulting from insufficient input validation, integer overflows can cause high-severity vulnerabilities.
- A computer's central processing unit (CPU) and memory represent integers. Software companies often supply these as input to their programs in binary formats.
- Integers might represent the size of a packet or length of a string, and applications frequently rely on them when making key decisions about how a program should proceed.
- CPU registers cannot store integers with infinite values. Their maximum value depends on the width of the register in bits.
- Additionally, there are two types of integer representations:

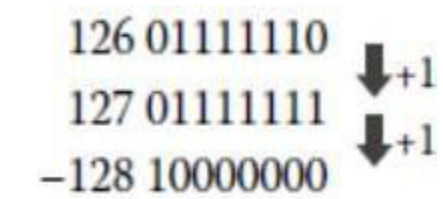
  unsigned and signed.

- Unsigned integers represent only positive numbers, and signed integers can represent positive and negative numbers.

- The decimal number 34 in binary is converted to its one's complement by inverting each of the bits.
- 1 is added to the one's complement representation, resulting in the two's complement representation of −34. First, the binary representation of the number is negated by inverting each of the bits.
- This format is known as one's complement. The second step is to simply add one to the one's complement, and the resulting value is the two's complement form.
- Two's complement representation is thus the result of adding one to a one's complement representation of a negative integer.



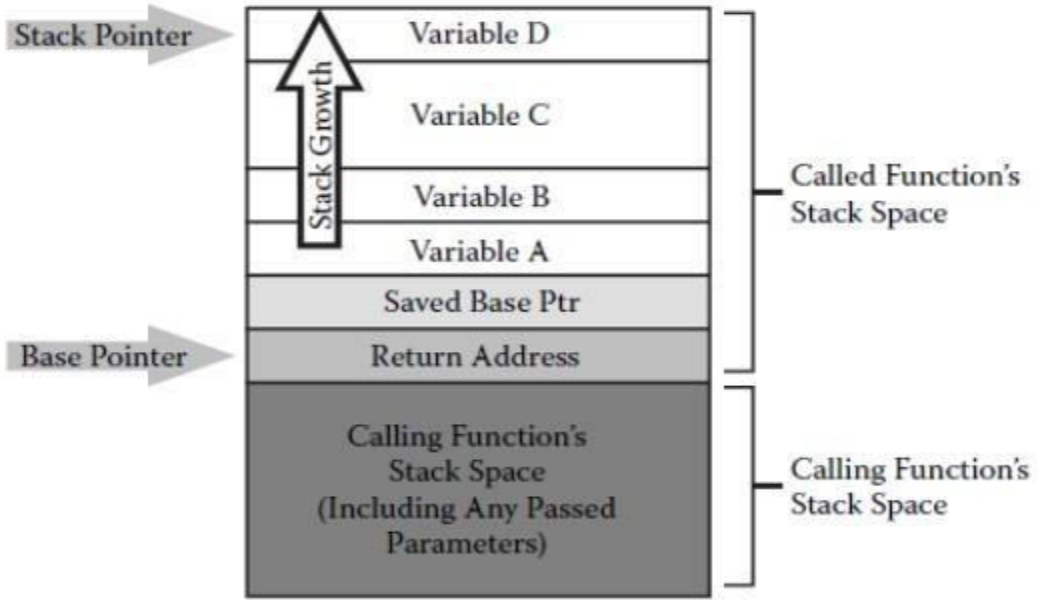
- An integer overflow occurs when an arithmetic operation produces a result larger than the maximum expected value.
- An integer that increases beyond its maximum value could result in a potential error condition that attackers may exploit.
- Integer overflow occurs in signed and unsigned integers. A signed overflow is the result of a value carried over to the sign bit.
- An unsigned overflow is the result of a value no longer representing a certain integer representation because it would require a larger register width.



An 8 Bit Signed Integer Overflow

Stack-Based Buffer Overflows

- Overflows are the result of a finite-sized buffer receiving data that are larger than the allocated space.
- Stack based buffer overflows are by far the most common type of overflow, as they are generally the easiest to exploit.
- Stacks upon Stacks At a high level, the standard computer stack consists of an array of memory bytes that a programmer can access randomly or through a series of pop-and push commands.



Protecting against Stack-Based Buffer Overflow

- Buffers allocated on a stack are of finite, predetermined sizes, and as such, it is up to the programmer to ensure that the function copying data into them is within this size constraint.
- A program should validate any data taken from an external source (external from the perspective of the application) for both size and content; user-supplied data should never be trusted outright.

Format String Vulnerabilities

- Vulnerabilities in the printf print formatting and similar functions. These vulnerabilities put the stack, a rogrammer to specify how the function should attempt to interpret the string.
- For example, the programmer may want to print the character A, the value of A as the number 65, or the hex representation of A, which is 0x41.

Malicious Code

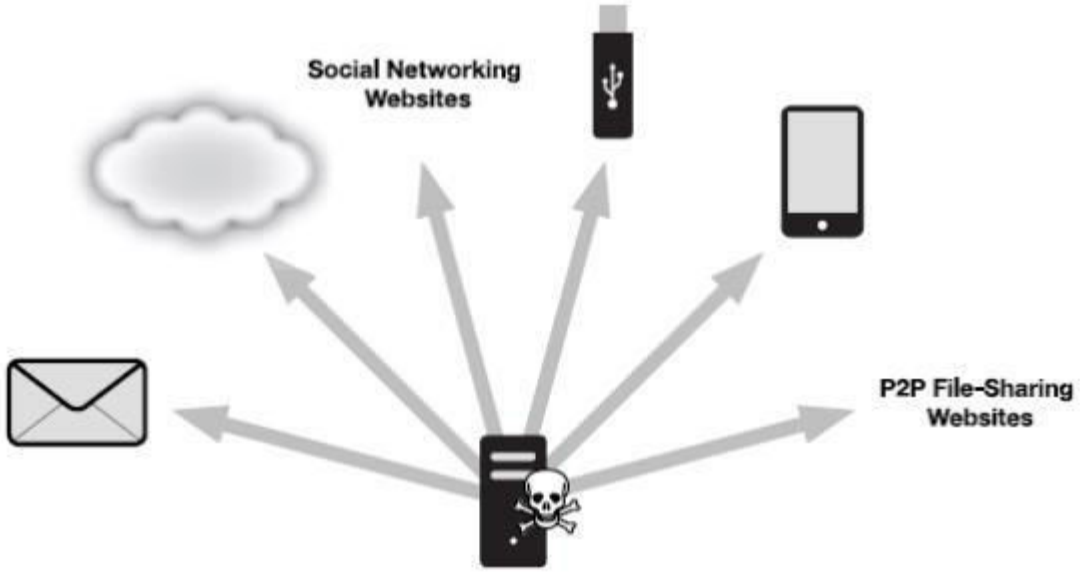
- Computer worms constitute a large class of malicious code that spreads between computers by distributing copies of themselves in a variety of ways.
- The worm is one of the earliest forms of malicious code and may be either benign or destructive.
- Malicious code is only a worm if it spreads to other systems by duplicating itself without attaching to other files.

Self-Replicating Malicious Code

- Worms typically have two roles.

  1) spread to additional computers 2) payload.

- A worm's payload is what the attacker programs the worm to accomplish after it spreads.
- Distributed denial of service (DDoS) attacks, spam distribution, cyber crime, or anything else the attacker chooses.

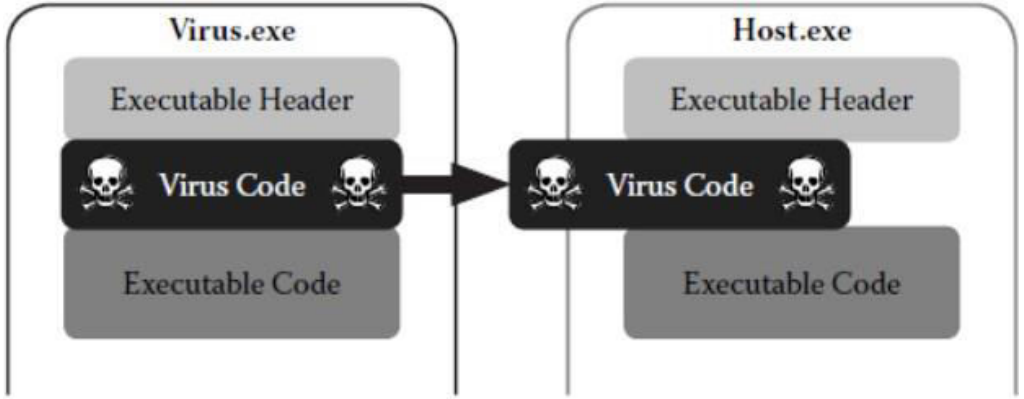


- E-mail worms spread by sending a message designed to entice the recipient into clicking a link or downloading an attachment that contains a copy of the worm.
- Network worms, which often spread without any user interaction, can infect many computers in a very short amount of time.
- To mitigate the threat from computer worms, administrators must protect systems from all propagation techniques

- The worm infection in a network:
  - Use antivirus products to scan incoming e-mails for malicious links.
  - Disable auto run functionality for USB devices.
  - Apply patches for vulnerabilities in network services in a timely manner.
  - Disable access to P2P networks.
  - Educate users on the dangers of worms that use social-engineering techniques

Viruses

- A *computer virus* is a type of malicious code or program written to alter the way a *computer* operates and is designed to spread from one *computer* to another.
- A *virus* operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.
- Viral code within infected host files often has three distinct parts: the discovery module, the replication module, and the payload.
- The discovery module enables the virus to locate host files, and the replication module carries out the infection by copying the entire viral code into the host file..



A Virus Infecting a Host files

UNIT V

Exploitation: Techniques to gain a foothold – Shellcode – Integer overflow vulnerabilities – stack based buffer overflow. Malicious Code: Self Replicating Malicious code - Evading Detection and Elevating Privileges – Root kit – Spyware – Attacks against privileged user accounts - Stealing Information and Exploitation – Form grabbing – Man in the middle attacks.

Previous topics

- Exploitation:
  - Techniques to gain a foothold Shellcode
  - Integer overflow vulnerabilities
  - stack based buffer overflow.
  - Malicious Code:
    - Self Replicating Malicious code

Topics discuss to…..

- Evading Detection and Elevating Privileges
- Root kit
- Spyware
- Attacks against privileged user accounts
- Stealing Information and Exploitation
- Form grabbing
- Man in the middle attacks.

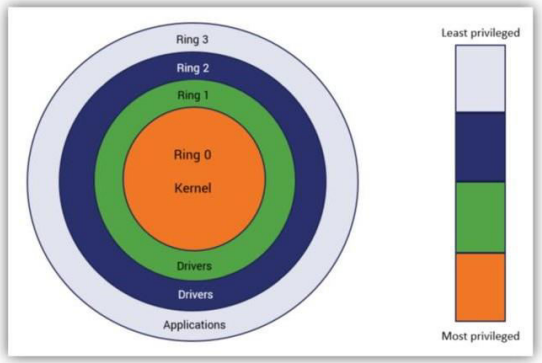
Evading Detection and Elevating Privileges

- The level of difficulty in analyzing data and code depends on the effort put forth by the developer to obscure related information and deter analysts.
- Developers use a technique known as obfuscation to transform data or source code into obscure or unclear representations while retaining the original functionality.
- Developers, both benign and malicious, use obfuscation techniques to hide the data or the behavior of an application.
- Source code obfuscation seen in malicious code and commercial applications reduces the chances of successful decompilation and increases the difficulty of reverse engineering.
- Many programming languages require source code to pass through a compiler to create an executable or byte code file.
- Inversely, decompiles take executables and byte code files and attempt to convert them into the original source code.
- Exposed source code leaks sensitive information by revealing the inner workings of the application.
- Legitimate developers use obfuscation in an attempt to hide possible vulnerabilities, trade secrets, and intellectual property.

- Many obfuscation techniques exist in the wild to change code or data into an unclear representation of itself.
- The variety of obfuscation techniques available depends on the intended result and the environment in which the code or data exist.
- Regardless of the result or environment, obfuscation transformations obscure yet retain the original functionality.
- Typical modifications include encoding, concatenating, obscuring variable and function names, and adding or removing white space and new lines.
- Concatenation is an obfuscation technique that connects several pieces of code or data to form one continuous block.
- Concatenating the individual parts together retains the original functionality but confuses the analysis by potentially displaying the block in out-of-sequence chunks.
- Intentionally splitting data and code into multiple individual parts can make it difficult to understand and obscures the original context.

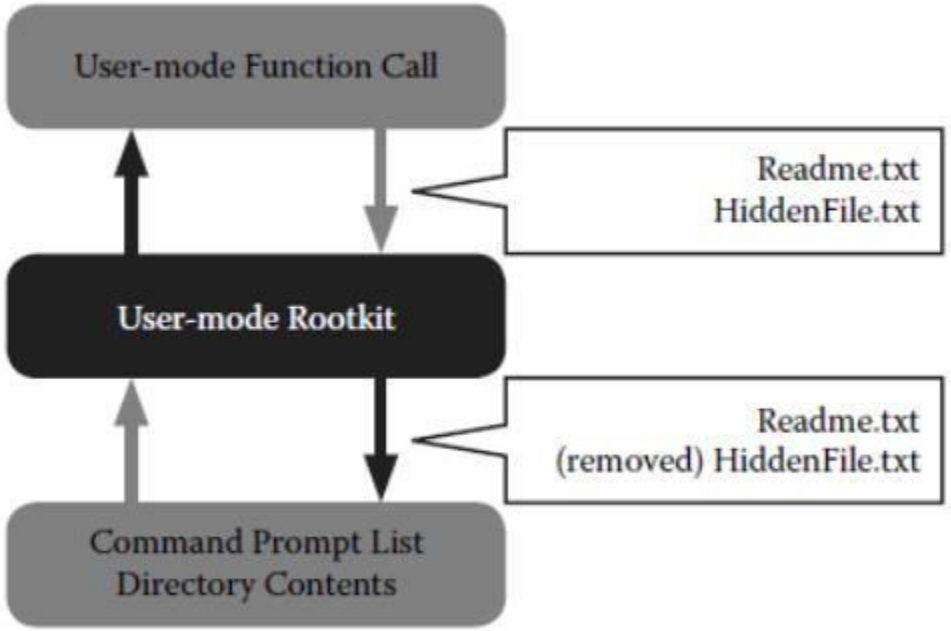
Rootkit

- A rootkit is a tool that allows actors to retain their administrative (or root) privileges and to hide their activity.
- A rootkit achieves stealth by modifying the way a user program receives information from the operating system.
- Rootkits often modify processes or modify the system to falsify and hide information.
- The simplest and earliest rootkits replaced system utilities (like ls) to change their functionalities and hide certain files.
- More complex rootkits have similar goals, providing a way for attackers to hide files or processes with certain attributes.
- Rootkits fall into either the user mode or kernel mode categories, depending on the type of hooks they use and how they influence processes or the system



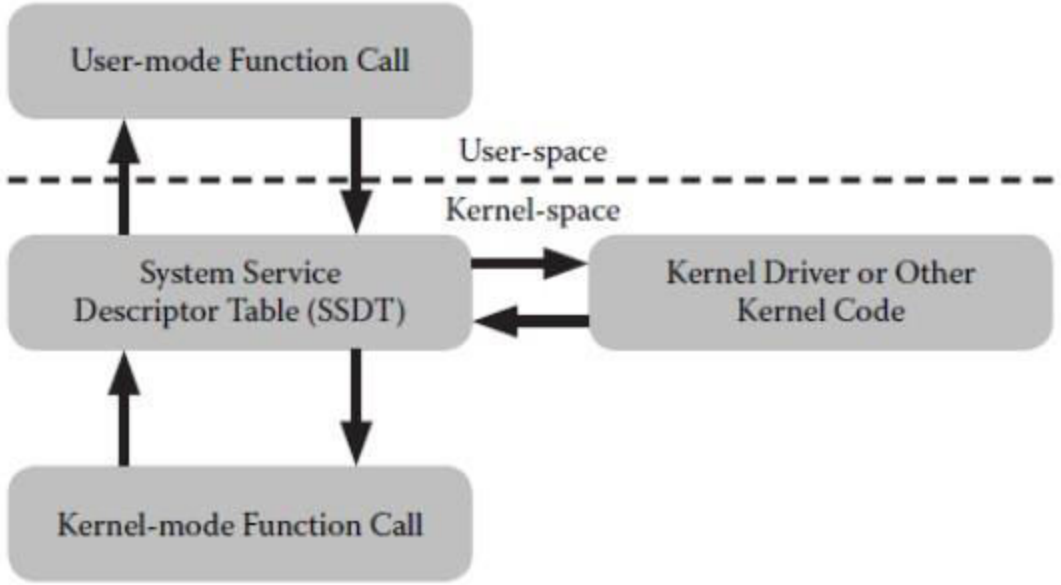
User Mode Rootkits

- User mode rootkits are able to hide information by targeting a user's running processes.
- The rootkit can hook critical functions of a process by altering the process's import address table (IAT) or by injecting a dynamic link library (DLL) or other code into the memory of a running process.



Kernel Mode Rootkits

- A kernel mode rootkit may make changes to critical kernel memory structures to hook and alter certain kernel mode function calls on the system.
- Rootkits may also target the CPU interrupt descriptor table (IDT). This involves altering the function addresses whenever the CPU executes INT (short for interrupt) or SYSENTER assembly instructions.



Spyware

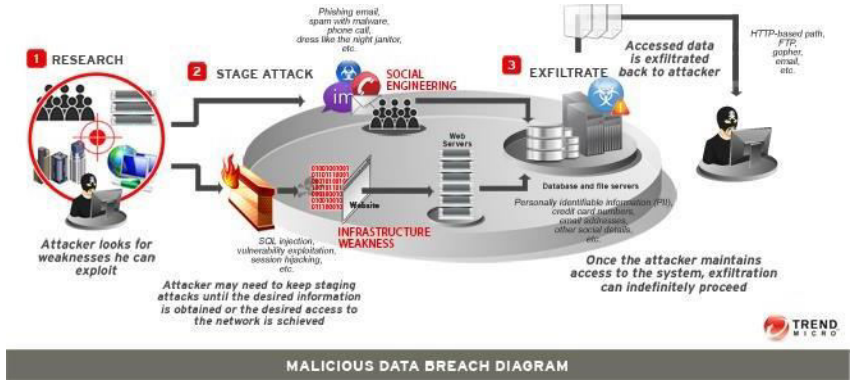
- Malicious software takes on many different forms, but one form, known as spyware, can cause a victim great hardship.
- The term spyware describes a class of malware based on the functionality of its payload.
- This class differs from other malware classifications, such as worms and viruses, which classify the malware based on the propagation method.
- Spyware is a type of malware that received its name based on its main intention of monitoring (spying on) a user's activity without the user's consent.
- The lack of consent often causes confusion when classifying programs as spyware. To qualify as spyware, programs must lack an End User License Agreement (EULA) or a privacy policy.
- Attackers' motives to use spyware to steal sensitive information and credentials generally involve identity theft or account access.
- An attacker can use sensitive information in identity theft schemes, such as opening a credit card with the victim's name

Attacks against Privileged User Accounts

- User access control is a powerful tool to limit what users can do, including files they can access, network resources, and important configuration settings.
- In the corporate network environment, many organizations use limited user accounts to prevent damage from malicious code.
- In this way, administrators prevent attackers from modifying critical system files, writing to directories (such as \WINDOWS\ or \Program Files\), and modifying registry values.
- Vulnerabilities that increase the privileges of the current user, known as privilege escalation, are a serious problem for desktops and servers, and these vulnerabilities affect all operating systems.
- Such attacks indicate the importance of limiting exposure within other parts of the system and using multiple levels of defense, which could prevent damage when attackers use privilege escalation attacks.

Stealing Information and Exploitation

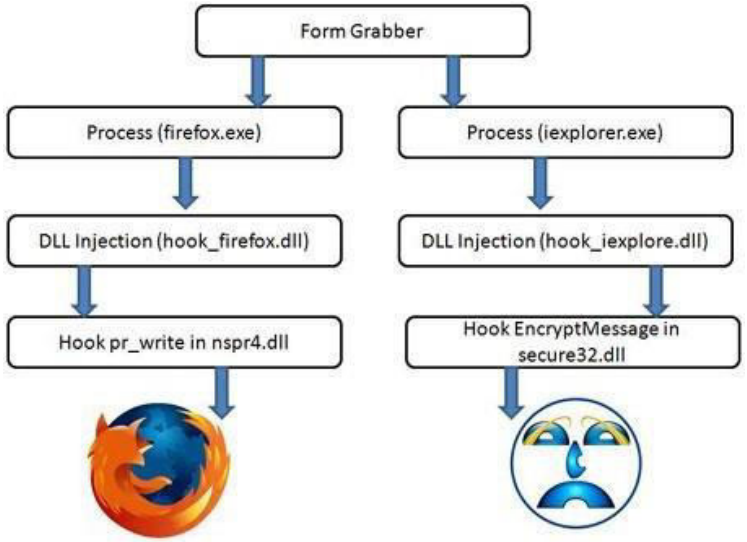
- Key logging, once the favored method of capturing user input, has largely given way to form-grabbing Trojans, which provide much cleaner, better structured data.
- Whereas key loggers target keystrokes and therefore miss sensitive data that a user may paste into a form or select via an options dropdown, form grabbers target Web applications by capturing the form's data elements before the user submits it.
- In this way, a form grabber yields the same key and value pairs received by the Web application, thereby assuring accurate and complete information.
- Trojan via antivirus signatures and limiting user privileges to prevent the installation of browser helper objects (BHOs)



MALICIOUS DATA BREACH DIAGRAM

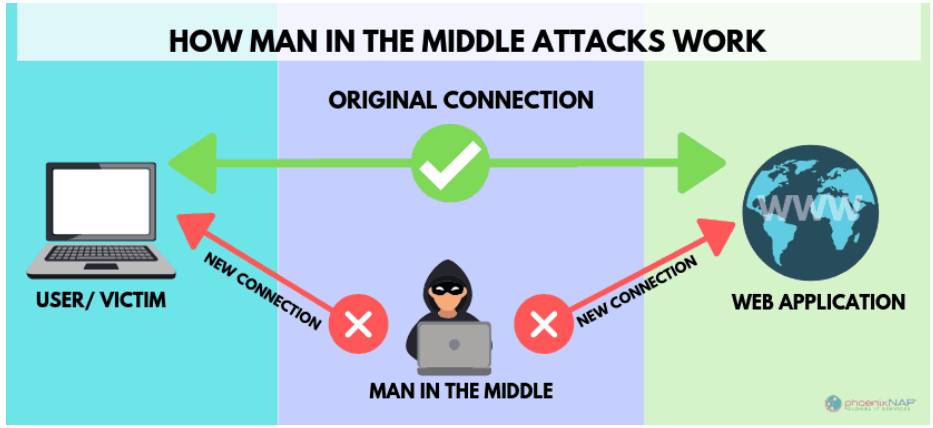
Form Grabbing

- Form grabbing is a data theft technique implemented by many information-stealing malicious code families.
- To mitigate the threat from form grabbers, administrators should deploy countermeasures to prevent the installation of these Trojans.
- Antivirus engines commonly detect information-stealing Trojans.
- Intrusion detection system (IDS) signatures that detect the outbound POST requests generated by a specific form grabber might also be available.

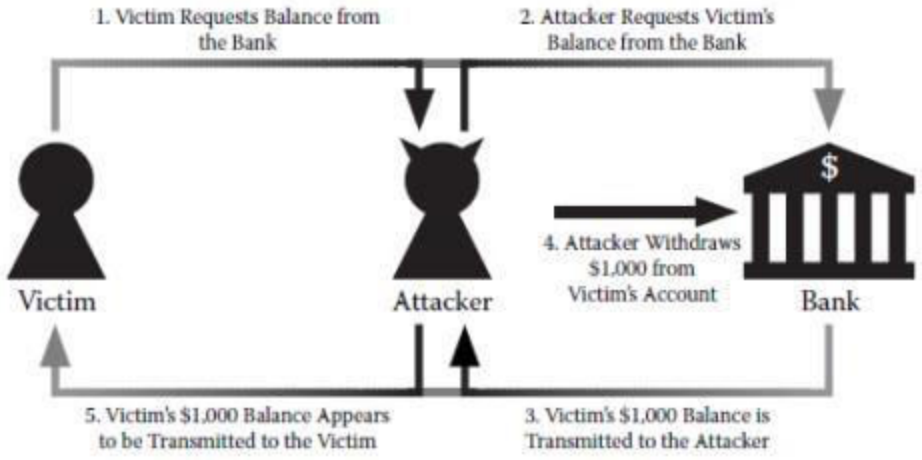


Man in the Middle Attack

- MITM attacks allow an actor to intercept, view, and alter sensitive data. MITM is a generic type of attack whereby an attacker inserts him or herself between the victim and the intended party during communication.
- Attackers may launch MITM attacks to enhance exploitation, steal information, defeat authentication systems, and masquerade or take actions as victims.
- Malicious code authors integrated network-based MITM attacks with both address resolution protocol (ARP) and domain name system (DNS) spoofing.
- The ARP allows local computers to determine the location of other computers according to their hardware (MAC) address.



- MITM attacks allow an actor to intercept, view, and alter sensitive data.
- MITM is a generic type of attack whereby an attacker inserts him or herself between the victim and the intended party during communication.
- Attackers may launch MITM attacks to enhance exploitation, steal information, defeat authentication systems, and masquerade or take actions as victims



- Attackers also use MITM attacks while phishing when the phishing tool used acts as a proxy to the real server.
- Phishing websites often do not use HTTPS; therefore, users do not have a strong way to verify the server's identity using the server's certificate.
- If users provide their information to a phishing website despite the lack of server identity information, attackers will have access to the user's current session.
- Financial institutions can detect a large number of successful logon attempts from the same IP address to identify a potential phishing website acting as a proxy for MITM attacks.