Cyber Security – lecture 6

Contents

- What is Malware
- Viruses
- Worms
- Trojan
- Backdoors
- Steganography

What is Malware: Definition

- Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, spyware etc…. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

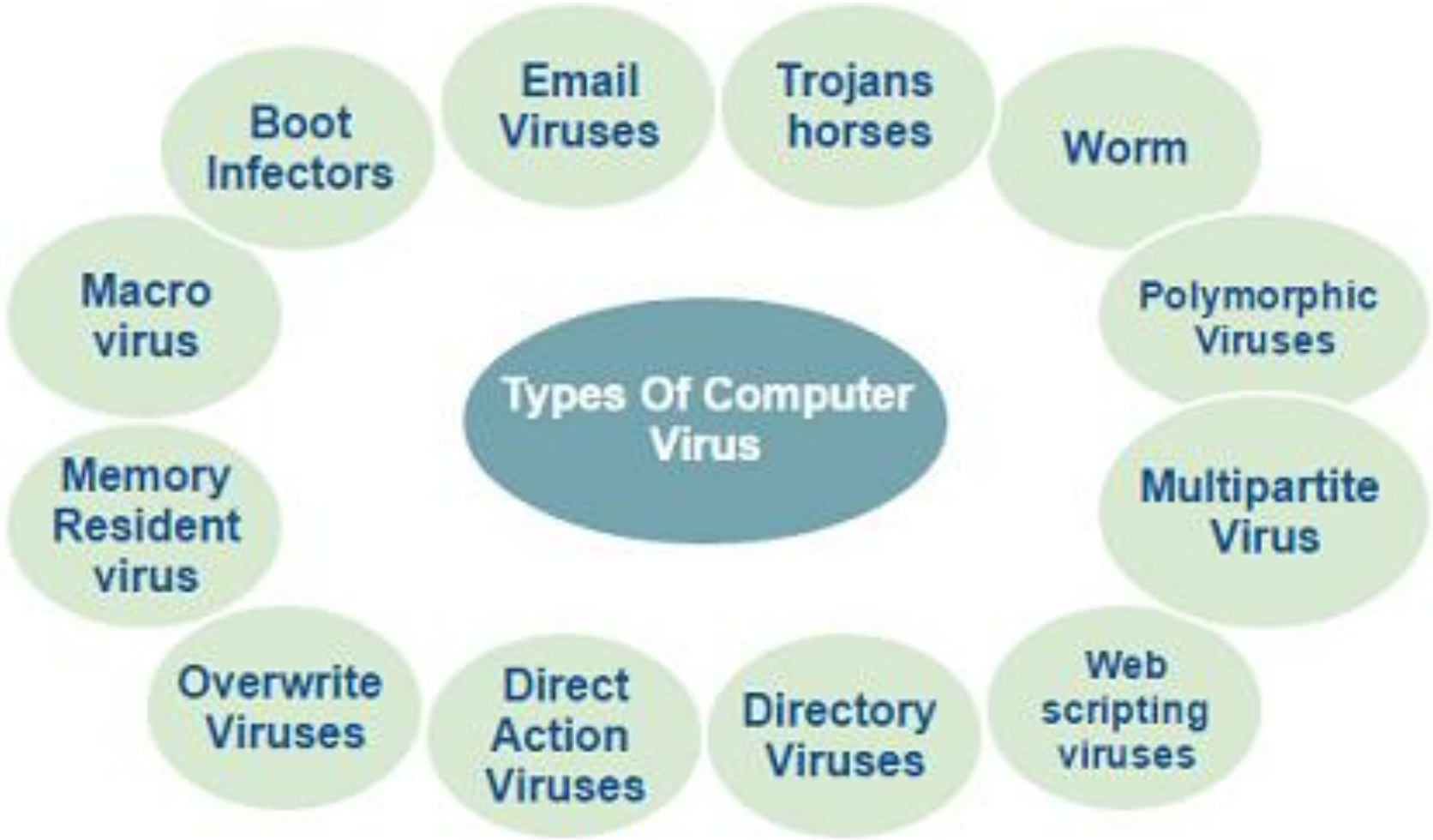
Virus

- Viruses are malicious programs that attaches itself to another executable program.
- Whenever the host program is executed, virus code is also executed and it can make a copy of itself and infect other executable files found in your memory or hard drive
- A virus cannot be spread without a human action. That means it cannot spread unless you run infected application or click on infected attachment.
- Early viruses spread on to different applications on your computer
- Present viruses spread as attachments through E-mail, and they will mail themselves to people from your address book

Virus

- How Do Viruses Spread?
  - You receive infected E-mail attachment
  - You download infected code
  - Your thumb drive gets infected
- What Can Viruses Do?
  - Wipe your hard drive
  - Modify or delete files
  - Steal files
  - Spread further
  - Halt system
  - Abnormal screen behavior etc….

Virus Types


Types Of Computer Virus
Boot Infectors
Email Viruses
Trojans horses
Worm
Polymorphic Viruses
Multipartite Virus
Web scripting viruses
Directory Viruses
Direct Action Viruses
Overwrite Viruses
Memory Resident virus
Macro virus

Virus Types

- File Infector Virus
  - This virus also infects executable files or programs. When you run these programs, the file infector virus is activated as well which can slow down the program and produce other damaging effects. A large block of existing viruses belongs to this category.
- System (boot-sector) infectors:
  - Infect boot sector area on disk. It load themselves on boot and then remain memory-resident.
- Hybrid:
  - Infect both files and boot sectors
- Directory Virus
  - Directory viruses change file paths. When you run programs and software that are infected with directory viruses, the virus program also runs in the background. Further, it may be difficult for you to locate the original app or software once infected with directory viruses.

Virus Types

- Resident Virus
  - Resident viruses live in your RAM memory. It can interfere with normal system operation which can lead to the corruption of files and programs.
- Overwrite Virus
  - From the name itself, this virus overwrites the content of a file, losing the original content. It infects folders, files, and even programs. To delete this virus, you also need to get rid of your file. Therefor, it is important to back up your data.
- Web Scripting Virus
  - This virus lives in certain links, ads, image placement, videos, and layout of a website. These may carry malicious codes in which when you click, the viruses will be automatically downloaded or will direct you to malicious websites.

Virus Types

- Companions
  - Creates new file with similar name as the host program.
  - When host program is called, virus is executed instead
  - Virus calls host program in the end. This fools integrity checkers that only look at existing files
- Stealth Virus
  - Stealth viruses trick antivirus software by appearing like they are real files or programs and by intercepting its requests to the OS. Some antivirus software cannot detect them. Sometimes, it temporarily removes itself from the system without deletion.

Virus Types

- Sparse Infector
  - Sparse infectors use different techniques to minimize its detection. They are viruses that infect “occasionally”. For example, they may only want to infect a program every tenth execution. Because they are occasional infectors, antivirus software has a hard time detecting them.

Worms

- A worm is similar to view by design and is considered to be a sub-class of a virus. It is an independent program that does not modify other programs, but reproduces itself over and over again until it slows down or shuts down a computer system or network.
- Worms spread from one computer to another it has the capability to travel without any human action.
- It uses computer network to spread itself.
- It consumes too much system memory.
- It infects the environment rather than specific objects.
- Worms send a copy of itself to everyone listed on your email address book.

Worms

- Why Are Worms Dangerous?
  - They spread extremely fast
  - They are silent
  - Once they are out, they cannot be recalled
  - They usually install malicious code in the system like DDoS tool, Backdoor etc.
  - It make the network in jammed condition.

Key Difference Between Virus And Worms

Virus	Worms
Viruses spread to different systems through executable files	Worms use Computer Networks to spread itself
Slow in spreading	Spreading speed of a Worm is faster.
The virus tends to damage, destroy or alter the files of target computers	Worms does not modify any file but aims to harm the resources.
The virus needs human action to replicate	Worms don't need any user action to spread – they spread silently and on their own
Virus corrupts or modifies the data on the target computer	Worms harm the network by consuming the bandwidth, deleting files or sending emails.
Virus are executable files or attach themselves to other executable files to operate.	Worms are independent files that exist within the memory of an infected computer.

Worms – Example - Morris Worm

- Robert Tappan Morris is an American computer scientist and entrepreneur. He is best known for creating the Morris Worm in 1988, considered the first computer worm on the Internet.
- The Morris worm was not written to cause damage, but to measure the size of the Internet.
- At that time Internet was small consist of 60,000 computers
- Morris Worm infected around 6,000 computers, one tenth of Internet, in a day

Trojan

- A Trojan horse, also known as Trojan, is a program that appears to be something safe, but it is performing tasks such as giving access to your computer or sending personal information to other computers.
- Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or do not propagate themselves.

Trojan

- Purposes and uses of TROJAN
  - Crashing the computer or device.
  - Modification or deletion of files.
  - Data corruption.
  - Formatting disks, destroying all contents.
  - Spread malware across the network.
  - Spy on user activities and access sensitive information
  - It can intercept communications from the target computer.
  - They can disable the task manager
  - The can disable the control panel
  - They can slowdown, restart or shut down the system.
  - They can upload or download files without knowledge

Trojan

- How systems get infected by TROJAN?
  - Pirated Software.
    - A site offers a free download to a program or game that normally costs money. Downloading the pirated version of a program or game allows you to illegally use or play, however, during the install it also installs a Trojan horse onto the computer.
  - Email Attachments.
    - You receive an e-mail that appears to be from a friend asking you to view this fantastic new program or look at a file. Opening the file infects your computer with a Trojan horse virus.
  - Visiting untrusted websites.
    - A popular screen saver website has become infected or uploaded infected screen savers. Downloading the screen saver to your computer also installs a Trojan horse onto the computer.

Backdoors

- A backdoor in a computer system is a method of bypassing normal authentication and securing unauthorized remote access to a computer.
- In *Programmer point of view* he may sometimes install a backdoor so that program can be accessed for troubleshooting purposes.
- In *hackers point of view* he often use backdoors as part of an exploit.

Backdoors - HOW THEY WORK???

- Backdoors are usually based on a client-server network communication, where the server is the attacked machine, and the client is the attacker.
- A typical backdoor consists of 2 components –
  - ***the server program***, which can be installed on multiple computers (that means computers which is to be compromised by the hacker)
  - ***the client program*** which is installed on hacker's computer that can be used to control all the compromised computers.
- The backdoor generally installs a server component on the compromised machine. That server component then opens a certain port or service allowing the attacker to connect to it using the client component of the backdoor software.

Backdoors

- Attackers can distribute copies of the server program to potential victims in numerous ways –
  - As part of the payload for a worm or Trojan, as a reliable email attachment etc….
  - Through social engineering or exploiting a vulnerability attacker can install the backdoor on a computer.
- Once the server program is installed on a system, it will open a network port and communicate with the client program. An attacker can then use the client to issue commands to the machine.
- Some backdoor programs will even alert the attacker when a compromised computer is available online.

Backdoors

- What can a Backdoor Virus do to Your System?
  - Permits the intruder to create, delete, rename, edit or copy any file.
  - Permits the intruder to execute different commands, change any system settings, adjust the Windows registry, run, control and terminate applications, and install other software and parasites.
  - Records keystrokes and captures screenshots.
  - Allows the attacker to control computer hardware devices, alter related settings, restart or shutdown a computer without asking for permission.
  - Steals sensitive personal data, passwords, login names, identity details, and valuable documents.
  - Record user activity and tracks web browsing habits.

Backdoors

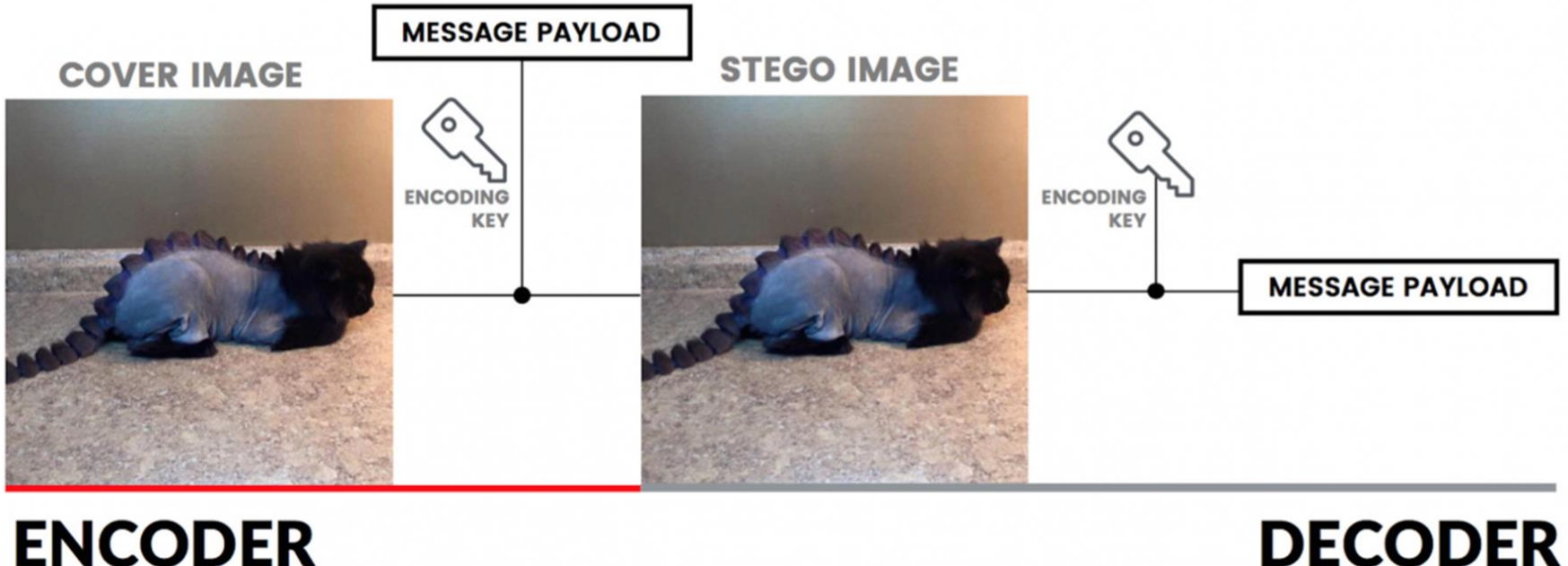
- What can a Backdoor Virus do to Your System?
  - Infects files, damages the entire system, and corrupts installed applications.
  - Prevents its removal by providing no uninstall feature
  - Reduces Internet connection speed and overall system performance.
  - Distributes infected files to remote computers with specific security vulnerabilities and executes attacks against hacker defined remote hosts.
  - Installs hidden FTP server that can be employed by malicious individuals for different illegal purposes.

Backdoors

- How to protect yourself?
  - Get a good anti-virus
  - Know what malicious programs look like
  - Be aware of e-mail attachment
  - Avoid the Third Party Downloads
  - Have a Hardware-based firewall and deploy DNS
  - Don’t Forget to Avoid Autorun
  - Regular Backup Your Data
  - Check SSL before dealing with E-commerce
    - It is safe to deal with an online website that has implemented SSL security.

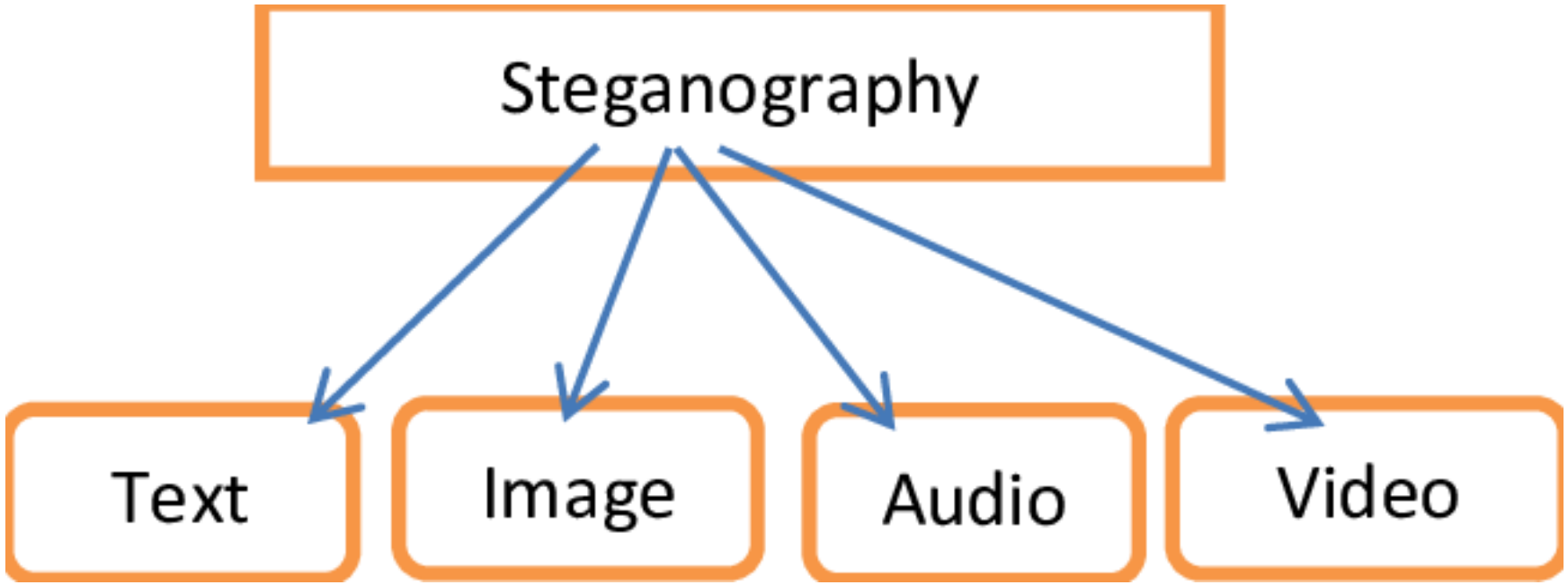
Steganography

- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection. The secret data is then extracted at its destination.
- Steganography is practiced by those who wishing to convey a secret message or code.
- While there are many legitimate uses for steganography, malware developers have also been found to use steganography to hide the transmission of malicious code.



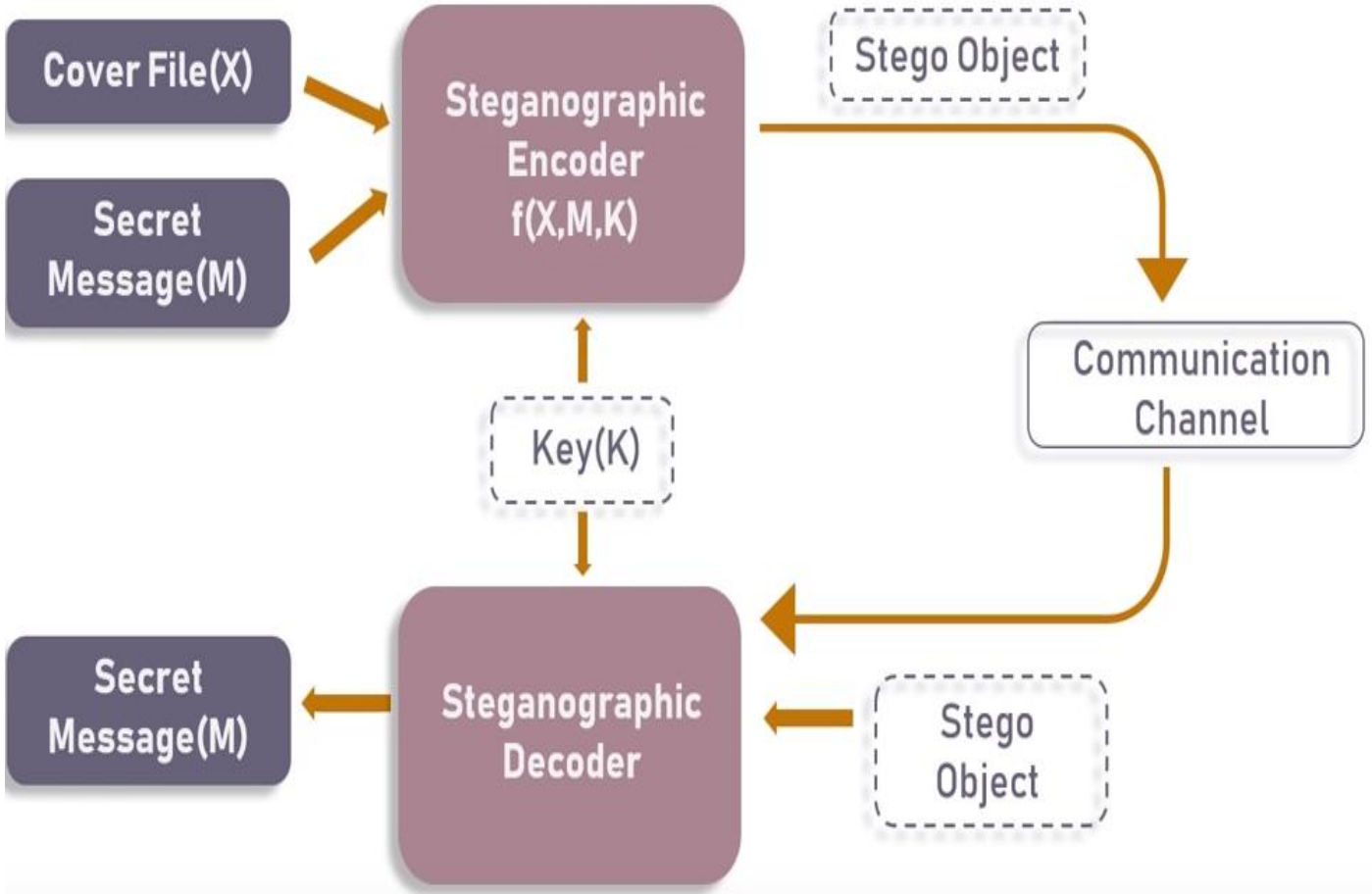
Steganography

- Steganography can be used to hide almost any type of digital content, including text, image, video or audio content.



Steganography: Basic model

- The data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography is called hidden text or secret message.
- The content by which the secret message is covered is known as cover file or cover text.



Steganography

- ADVANTAGES :
  - Difficult to detect and only receiver can detect
  - It can be done faster with large no. of softwares
  - Provides better security for sharing data in LAN, MAN & WAN
  - Potential capability to hide the existence of confidential data
  - Strengthening of the secrecy of the encrypted data
  - Protection of data alteration

Steganography

- DISADVANTAGES:
  - The confidentiality of information is maintained by the algorithms, and if the algorithms are known then this technique is of no use
  - Password leakage may occur and it leads to the unauthorized access of data.
  - If this technique is gone in the wrong hands like hackers can be very much dangerous for all

Steganography V/s Cryptography

Cryptography	Steganography
Cryptography is about protecting the content of messages (their meaning). Here a third party can detect the existence of a message.	Steganography is about concealing the existence of messages. Here a third party canot detect the existence of a message.
Here encryption is used which prevents an unauthorized party from discovering the contents of a communication	Steganography prevents discovery of the existence of communication
Cryptography alter the structure of the secret message	Steganography does not alter the structure of the secret message
Most of algorithm known by all	Technology still being develop for certain formats
Strong current algorithm are resistant to attacks ,larger expensive computing power is required for cracking	Once detected message is known
Common technology	Little known technology