Computer Network Security

TE - IT

Lecture -8
01/08/2022

Session: 12:00 - 1:00 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

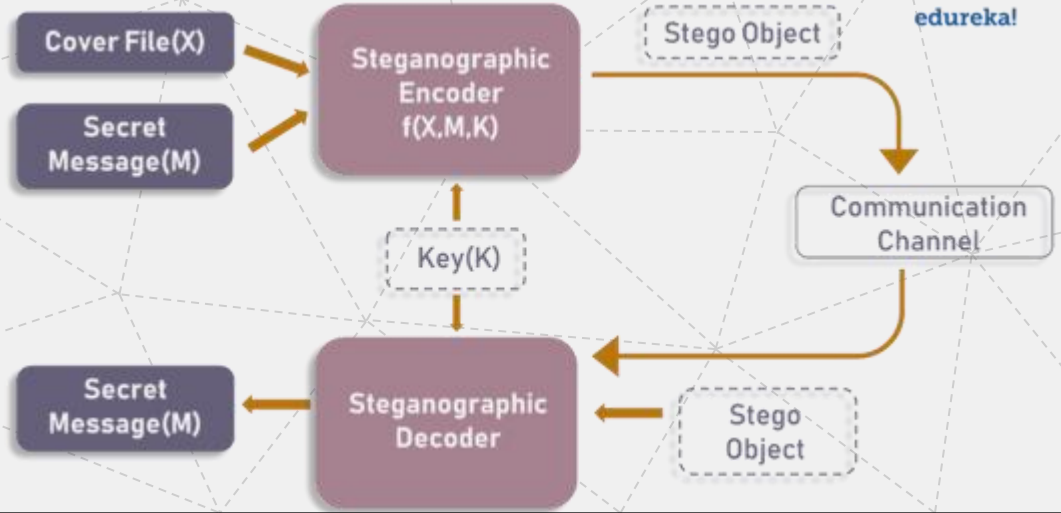
Module-1

✓ Contents

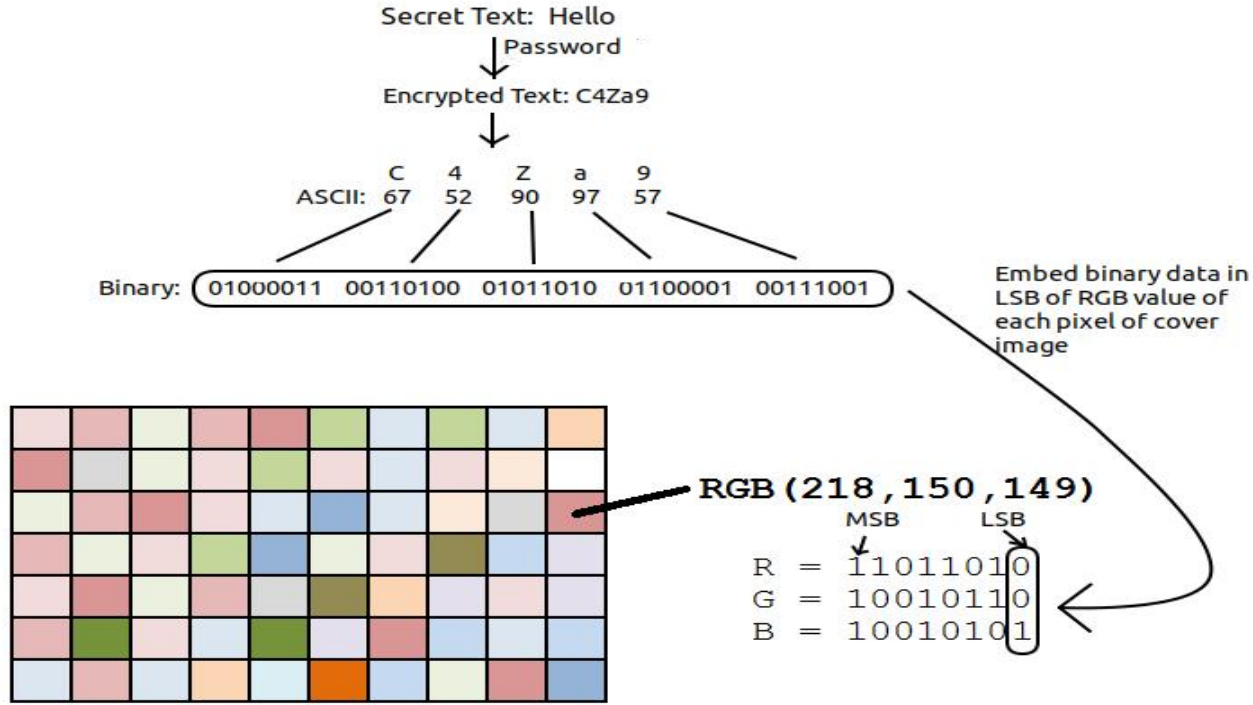
1. Steganography Model
3. Malicious Softwares

Steganography Model

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. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

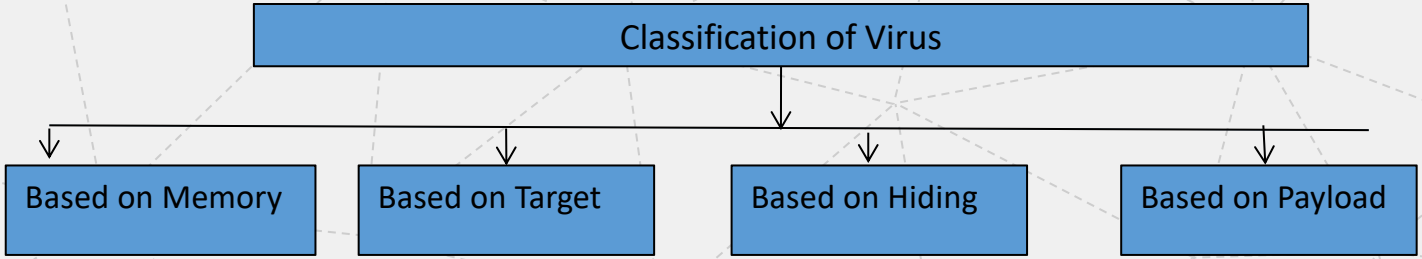


Steganography



Chapter 3 - Malware

Viruses



1. Resident Virus
2. Temporary Resident Virus
3. Non - Resident Virus
4. Swapping mode
5. User Process
6. Kernel Process

1. Compiled Virus
a. File Infectors Virus
b. Boot Sectors Virus
2. Interpreted Virus
a. Macro Virus
b. Script Virus
3. Multiparite Virus

1. No hiding
2. Encryption
3. Oligomorphic
4. Metamorphic
5. Polymorphic
6. Stealth
7. Armoring
8. Tunneling
9. Retro

1. No Payload
2. Non Destructive Payload
3. Destructive
4. Droppers

Viruses - Based on Memory

Virus: It is a category of Malicious Code that cannot self replicate itself to deliver the payload.

1. Resident Virus - Stays in Memory and affect the file which is opened
2. Temporary Resident Virus - stays for sometime and vacate the memory
3. Non - Resident Virus - do not stay in memory. It copies its payload to the files directly
4. Swapping mode - It uses swap space for residing. When It affects it goes from swap sapce to memory, performs attack and return back to swap space from memory.
5. User Process - It runs on user level access and priviliges. Infects only user files
6. Kernel Process- It is installed on the system level applications. It runs with administrative access and infect any file in the system

Viruses - Based on Memory

Based on Target:

1. Compiled Virus - It run as machine Executable, directly run by OS. Its source code run as EXE files

a. File Infectors Virus - Corrupts specific type of file, Corrupts the header to run directly the malicious code

b. Boot Sectors Virus - Infects boot sectors on the hard disk

2. Interpreted Virus - It runs at the execution timeline by line

a. Macro Virus - It presents within the document. The code blocks are usually automates the calculation steps within the document

b. Script Virus - It affects windows batch scripts, linux shell scripts and affects the power shell

3. Multiparite Virus - It spreads infection throughout the system.

Viruses - Based on hiding

1. No hiding - no special measure to hide
2. Encryption - virus uses encryption to hide
3. Oligomorphic - it is a semi polymorphic which uses several decryption routines
4. Metamorphic - it has mutation engines that changes the apperance of the viruses
5. Polymorphic - it changes the virus body insted of appearance
6. Stealth - Inorder to hide, it restores the older properties of the file
7. Armoring - It uses various technique for removal and detection
8. Tunneling - It attach themselves in the system interrupts
9. Retro - It bypass the security tools such as firewalls, IDS and security programs

Viruses - Based on Payload

1. No Payload - It just slow down the system
2. Non Destructive Payload -It affects the device drivers such as keyboard, mouse, CD Rom and generate multiple pop ups
3. Destructive - causes severe damage, affects boot sector, file programs, applications
4. Droppers - It sits on the system and let the attacker use the systems resources to launch other attacks

THANK YOU