U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

Steganography

October 2023

cyberforcecompetition@anl.gov

Steganography 101

Steganography

Steganography is the act of hiding one message (covert communication) inside of a different, more obvious, message (overt communication). This process dates back to the ancient Greeks. They would carve a message onto a wood tablet and cover it with wax. Then, they would carve a different message into the wax. When the intended recipient received the tablet, they would melt the wax and read the message on the wood.

In modern times, steganography is used digitally. The most common ways people use it to disguise messages is through texts, images, videos, audio recordings and network traffic.

Steganography Type	Explanation
Text	Messages can be hidden within texts such as reports, letters, carvings and more. For example, if someone wants to send a secret message in a letter, they can use word choice so the first letter in each sentence spells the message.
Image	It is possible to take a reference image and change small parts (like singular bits) so it contains a secret message when properly decoded.
Video	Video steganography is almost the same as images, except it can be stretched out over the entire (or part) of the video.
Audio	Audio steganography is the practice of hiding a message inside an audio recording, either in the actual audio or the signals/bits.
Network	People can use network protocols to hide messages in packet headers, gaps between packets, addresses and more.

Least Significant Bit

Least Significant Bit is one of the most common methods of image steganography. This is done by changing the last 1 or 2 bits in a byte (the 2 lowest values) for each pixel in the image. When the changed bits are all put together, they create a series of bytes which can be translated into plaintext for a person to read. If done correctly, this should not have a visible effect on the image.

Steghide

Steghide is a free opensource Linux based software that uses steganography to hide messages in image and audio files. It uses a Least Significant Bit program to encode and decode the message. Steghide is also resistant to known methods of identifying LSB steganography.

Sources

- https://www.kali.org/tools/steghide/
- https://www.sciencedirect.com/topics/computer-science/steganographic-technique
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-steganography-guide-meaning-types-tools/
- https://www.youtube.com/watch?v=TWEXCYQKyDc