Topic: Steganography

1. Introduction
   1. Steganography is the process of hiding messages; for example, hiding a message within the digital encoding of a picture or graphic so that it is almost impossible to detect that the hidden message even exists.
   2. Steganography is a very wide and vast topic which is why it needs to be narrowed down to give people a better understanding of the matter. Steganography can be broken down in this matter which is an overview of what steganography is, some specific types of steganography, history of steganography, examples of steganography, how hackers use steganography, countermeasures for steganography, steganalysis, state of the art, future of steganography, interesting facts about steganography.
2. Body
   1. Overview of steganography/basics
      1. Supporting evidence
      2. Supporting evidence
   2. History of steganography
      1. Steganography can be dated back centuries and we can figure out it was being used back in the ancient Greece era. But “...the first recorded use of the term was in 1499 by Johannes Trithemius” where he made a book disguised about magic and he did not want to print it because he did not want other people to know. Although it was not printed his text kept on living and a draft was published in 1606.
      2. If we look back we can see that hidden writing or text steganography was used by mary queen scot which would be in the mid-1500s. They would do it by hiding information in letters that would be stored in a beer barrel which was passed freely in and out of prisons. Also, image steganography was used in Peru because of the geoglyphs (a geoglyph is a work of art that is created by arranging objects within a landscape). Also, people would write messages on the body to hide them, for example, they would shave the head of a person and then write the message but before letting the person go off with a message they would make them wait until their hair would grow back. Through the many years, we have used forms of steganography without even knowing what it was and it allowed people to hide many things right before their eyes.
   3. Historical Examples of Steganography
      1. Various Examples
   4. Hackers using steganography
      1. Supporting evidence
      2. Supporting evidence
   5. Countermeasures for steganography
      1. Supporting evidence
      2. Supporting evidence
   6. Steganalysis
      1. Supporting evidence
      2. Supporting evidence
   7. State of the art
      1. Supporting evidence
      2. Supporting evidence
   8. Future of steganography
      1. Supporting evidence
      2. Supporting evidence
   9. Interesting things about steganography
      1. Supporting evidence
      2. Supporting evidence
3. Conclusion
   1. Review everything talked about and give key points from each

Notes from meeting:

Form of steg from WW1 coded into music - communicate with music

-Cryptographic forms of sten

-Derivative stuff is work thats not entirely yours

4-5 pages is too short

-Look at recent changes with stenography

-Conjecture interesting programs

-we need to pick a type of steganography or cover all of them

1. Image Steganography

We need to clarify what everyone is going to do and we will need 4 to 5 topics from everyone

Isaiah Green -  history, future, hackers

Noah Guzik - Steganalysis, state of the art, comparison between cryptography

Daniel Amar - Countermeasure, Historical Examples

Pratik Parida - Interesting things,overview

Works Cited

Whitman, M. E., & Mattord, H. J. (2019). Principles of information security. Boston, MA: Cengage.

Interesting Links -

<https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/july2004/research/2004_03_research01.htm>

State of the art <https://www.researchgate.net/publication/287630076_A_Survey_of_State_of_the_Art_techniques_of_Steganography>

Steganalysis

[A review of image steganalysis techniques for digital forensics - ScienceDirect](https://www.sciencedirect.com/science/article/pii/S2214212617300777)

[Steganalysis: An Overview (giac.org)](https://www.giac.org/paper/gsec/707/steganalysis-overview/101589)

<https://www.wired.com/story/steganography-hacker-lexicon/>

<https://usa.kaspersky.com/blog/digital-steganography/17980/>

<https://resources.infosecinstitute.com/topic/steganography-and-tools-to-perform-steganography/>

<https://www.sentinelone.com/blog/hiding-code-inside-images-malware-steganography/>

History

1. <https://www.telsy.com/steganography-from-its-origins-to-the-present/>
2. <https://www.sans.org/reading-room/whitepapers/stenganography/steganography-past-present-future-552>

Hackers using steganography

1. <https://www.computer.org/publications/tech-news/research/how-steganography-works>
2. [https://adamlevin.com/2018/02/22/steganographic-hacking-works/https://adamlevin.com/2018/02/22/steganographic-hacking-works/](https://adamlevin.com/2018/02/22/steganographic-hacking-works/https:/adamlevin.com/2018/02/22/steganographic-hacking-works/)

Example of steganography used in images

<https://stylesuxx.github.io/steganography/>

Countermeasures

<https://en.wikipedia.org/wiki/Steganography#Countermeasures_and_detection>

Overview

<https://www.garykessler.net/library/fsc_stego.html>

As it was shown previously, steganography is closely related to cryptography. The same can be said about cryptanalysis and steganalysis. The former is the process of deciphering encrypted information created by cryptography whereas the latter is the process of detecting and defeating hidden messages created by steganography. Steganalysis, like many other areas of information security, blurs the lines between art and science; there is never just one way to defeat steganography methods. An in-depth knowledge of the techniques of steganalysis is required if one hopes to discover the hidden message. There are, however, several basic attacks that can be used that have analogous attacks from cryptanalysis. These include the stego-only attack, known cover attack, known message attack, chosen message attack, and known stego attack. All of these methods require that the steganalyst has some information about the original process of creating the stego-medium. This may include just the stego-object, as with the stego-only attack, the cover object and stego-object for the known cover attack, the actual hidden message, as with the known message attack, a separately generated stego object for the chosen message attack, and the steganography algorithm or tool for the known stego attack. Each of these types of attacks has its various strengths and weaknesses for various situations.