1: Design and implementation of a covert channel

Motivation

A covert channel enables participants to transmit information through a legitimate channel while the covert transmission remains undetected. There are different settings in which such a covert channel can be used. Attackers can use it to send hidden control commands to the nodes of a botnet while avoiding the detection through a monitoring system. Users that are affected by Internet censorship can hide sensitive information in legitimate communication messages to exchange data that otherwise gets blocked. From a technical perspective, we can summarize many different approaches under this term, ranging from bit-encoded secrets in image files to acoustic signals hidden in a live conversation.

Instructions

You design and implement a covert channel. This is a creative project and you are completely free to chose a hiding technique and a transmission medium! Please follow the steps documented below to structure your project.

1. Literature research: What types of covert channels exist? What are the use cases behind the different implementations? What are their advantages and disadvantages?
2. Transmission medium: Decide *where* you want to hide information. This can be images (compressed or uncompressed), videos, audio signals, documents (PDF, txt, word), binary files, ... What are the pros and cons?
3. Hiding technique: Gather different technical solutions for hiding information. You can refer to existing approaches or design your own new technique. Think about possible challenges and limitations. Think about the context in which your covert channel would be used.
4. Implementation: Bring it to live and implement a script or program that hides information. What kind of information do you want to hide? What is the use case and how would this happen? How would the file/medium be transmitted?
5. Security analysis: Think about all the things that can go wrong. How could an attacker get to know the hidden information? Would it be possible to detect that something was hidden? What are the security requirements of your system and what happens when they break?

Goals

You should focus on the following goals:

- Design and implement a covert channel.
- Demonstrate how it hides information from an attacker.
- Group presentation (~10 minutes) at the end of the project where you elaborate on the findings of your research.