CCgen.v2 Wrapper

Generate, inject and extract covert channels in network traffic

FIV, Nov 2021
KM, Oct 2022

Introduction

The main purpose of the CCgen-wrapper is to allow the automatic injection of multiple covert channels in the same pcap. It has three different parts:

1. Searching for matching flows and creating corresponding ccGen configurations.
2. Injecting the covert channels.
3. Extracting the covert channels to evaluate the previous injection

To run the wrapper follow the steps below:

1. Download and install go-flows

The CCgen wrapper requires installing go-flows within the [wrapper] folder. Download **go-flows** from: https://github.com/CN-TU/go-flows and make sure that the folder is named [go-flows-master].
Inside the wrapper folder, a installer script for go-flows is provided. Please run the `instal_go-flows.sh` script to install go-flows. It should do everything automatically.
To test if installation succeeded, move to go-flows-master directory, open terminal and enter `./go-flows`. This should return a message where the usage of go-flows is described.

2. Configure the CCgen-wrapper

In the CCgen.v2 *Configurator* after configuring a valid injection, press the validate button and there in the summary view you have the option to add this configuration to the wrapper. By choosing this option the configured configuration is put to wrapper. The wrapper config is built with following data:

PROF

- *Input file*: .pcap file which is used as the source file for injection covert channels
- *Output file*: .pcap file where the injected covert channels are saved.
- *Message*: The message is taken from the configurator message field.
- *Mapping*: refers to the technique, parameters and symbol-to-value correspondence to use in the injection of the covert channels. In the *~/CCgen.v2/ccgen/techniques/README.md* file you will find suitable examples of mappings, which are stored in the database.
- *Key*: stands for the flowkey to inject the channel. Options are:
    - "1tup" (for srcIP)
    - "2tup" (for -srcIP, dstIP-)
    - "3tup" (for -srcIP, dstIP, Protocol-)

    - "4tup" (for -srcIP, dstIP, srcPort, dstPort-)
    - "5tup" (for -srcIP, dstIP, Protocol, srcPort, dstPort-)

- *Constraints*: is included to specify additional constraints. This is important for techniques that can only be implemented in certain protocols. Implemented options:

    - "None" (default)
    - "tcp"
    - "udp"
    - "tcp/udp".

- *Repetition*: is the number of repetition that the same configuration must be injected in different flows (by default '1').

3. Run CCgen.v2 Wrapper

After configuring all desired techniques and messages, proceed by clicking the top right validation button. If wrapper could process the configuration without error, you should redirected to the CCgen.v2 *Dashboard* where all injecting and extracting tasks of the wrapper configuration should be listed and processed automatically one after the other.