Phase 1 Report: Delay Insertion Middlebox for a Covert Channel

Introduction

In this phase, a basic covert channel mechanism was implemented by intentionally adding random delays to network traffic. The goal is to observe how these delays influence the average round-trip time (RTT) of ping requests. This setup forms the basis for encoding information through packet timing in future stages.

System Overview

Middlebox (main.py):

The middlebox listens on two NATS topics: inpktsec and inpktinsec. When it receives a packet, it applies an exponential random delay with an average around 5 microseconds. These delays are stored in milliseconds. After applying the delay, the packet is forwarded to the corresponding output topic. Once the ping process is complete, the script calculates the mean of all delays and writes the result to a file named mean_delay.txt.

Ping Process (ping_script.py):

This script lets the user pick one of the containers (sec or insec) and sends 25 ping requests to the other. It collects the RTT values from the ping output and calculates the average RTT. This value is saved in avg_rtt.txt. To let the middlebox know the ping phase is done, it creates a file called ping_done.txt.

Plotting Tool (plot.py):

The plotting script reads the mean delay and average RTT from the two text files. It then creates a scatter plot with the x-axis showing the mean delay in milliseconds, and the y-axis showing the average RTT. A red dashed vertical and horizontal line cross at the measured data point to make the values clearer.

Results and Discussion

Although the random delay added to each packet is small, it still affects the total RTT, mainly due to the overhead in containers and networking. In our experiment, the mean inserted delay was approximately 0.00481 ms, and the average RTT recorded from the ping results was around 5.46 ms. The plot clearly shows how even low-level delays can influence overall communication time. This supports the idea that timing differences can be used to carry information covertly.

Conclusion

This experiment shows that even very small, random delays introduced into network traffic can have a measurable impact on RTT. This is a key idea for covert communication channels. The setup works as expected and sets the stage for future phases where actual data could be encoded using timing differences between packets.

GitHub Repository: https://github.com/alperenkrpnr/middlebox