Ceng519 Term Project Phase 2 Report

Çoban, Alim Bican
2237196

April 13, 2025

Related Work

I've used this paper as reference for my work: Covert File Transfer Protocol Based on the IP Record Route Option

The protocol from the paper uses some flags and sequence numbers to implement some more sophisticated use cases, such as user authentication. The Paper also discusses detection and mitigation of the channel, and briefly mentions encrypting the data we put on the channel.

Covert channel description

My selection: Option Fields: Using optional header fields in IPv4 for data encoding. Use Record Route Option.

I've used netfilter queue in combination with scapy to implement a covert sender/receiver pair. Unfortunately I was not able to complete my implementation or benchmark it within the given deadline.My idea was to add our secret message (and any relevant padding) to the Record route option field to all outgoing messages, and strip them from the incoming messages.

I'm planning to use the following parameters:
1. % of packets to inject our secret data to: We do not want to have every packet coming from a host to have record route option, that would look suspicious.
2. How long should our record route option field be (out of maximum total of 40 bytes of IP Options space): We might want to change this as to make our record route options look unrelated and natural
3. How much of the record route option should carry our data (as opposed to the rest being open for legitimate IP addresses): We might want to let some devices along the way to note down their IPs alongside our message so as to make detectors' life harder

Additionally, we would ideally change the parameters in response to changes on the host machine. For example, during times of high traffic, we might want to turn down "% of packets to inject our secret data to" to not slow down the traffic and stay hidden. Or, we might want to increase it to increase our bytes carried per hour if we need the throughput.

Comments

Thank you for your efforts.

Unfortunately I was not able to complete this phase in time, but I plan to complete it as soon as I can to be able to work on phase 3 & 4.