IETF Hackathon

IETF 115

5-6 November 2022

London, UK

Hackathon Project

- PDMv2 / Extension Header Testing
  - draft-elkins-v6ops-eh-deepdive-fw
  - draft-elkins-v6ops-eh-deepdive-cs
  - draft-elkins-ippm-encrypted-pdmv2

- Participants

  Nalini Elkins, Mike Ackermann: Industry Network Technology Council, Dhruv Dhody, Praneet Kaur: India Internet Engineering , Society, Dr. Mohit Tahiliani: NITK Surathkal, Dr. Priyanka Sinha: Zenatix Solutions, Ameya Deshpande: Google, Balajinaidu V, Chinmaya Sharma, and Amogh Umesh, Sudesh Gowda, Kavya Bhat, Advaith Prasad: NITK

Hackathon Plan

Working on:

- Cloud testing
- Registration protocol for PDMv2
- eBPF and FreeRtr presentations

Can IPv6 Extension Headers Be Used on the Internet?

- Controversy for many years
- A number of studies showing that IPv6 extension headers “don’t work”
- Studies (by and large) sent “fake” IPv6 extension headers to Alexa top n sites
- If this is true, our work on our IPv6 Extension Header Destination Option Performance and Diagnostic Metrics (PDM) is really for naught

IAB Workshop: Encrypted Mgmt Techniques

- How to manage encrypted networks a big problem
- Our proposal to use PDMv2 (encrypted Dest. Options IPv6 Extension Header) accepted to IAB workshop
- As soon as we have a stable implementation, will try to collocate at various points in the Internet
- Crucial that EH works

Deep Dive: Why?

- Find out what is the ACTUAL situation -- do EHs really work?
- If not, then why?
- Is it blocked:
  - At the source?
  - At the destination?
  - In a transit network?
- Then
  - Is it intentional?

Let’s look at topologies

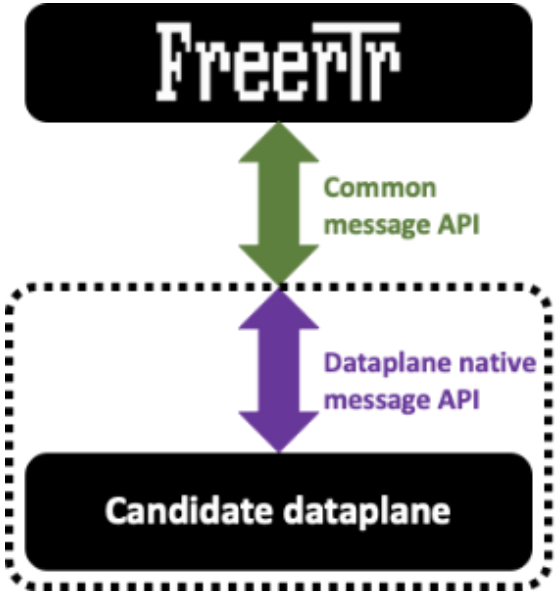
- Client – Internet – Server
- Client – Internet – CDN Cache Server – CDN network – Origin Server
  - (Internal to CDN may have multiple more complex topologies)
- Client – Internet – Edge of Cloud Provider – Origin server hosted by cloud provider

eBPF

- Run sandboxed programs within OS during runtime.
- Make use of privileges & control the kernel has over everything during runtime
- Guaranteed safety & efficiency (not much different than kernel instructions)

What is Freertr?

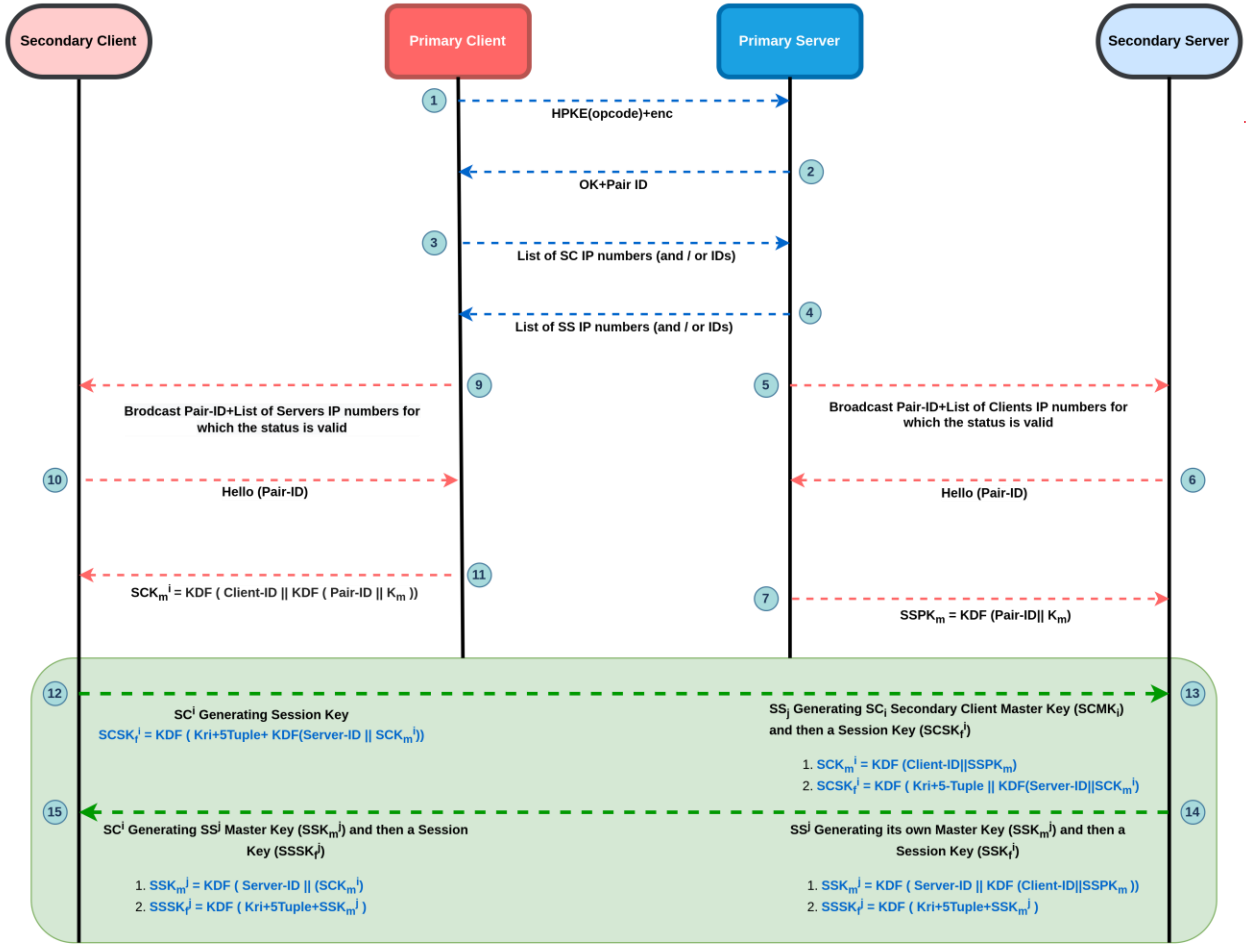
- A free, open source, router control plane software.
- Has immense protocol portfolio.
- “One image for all the protocols you'll ever need in routing”
- Currently has been used and developed at RARE (Router for Academia, Research & Education RARE project).
- System independent as it handles packets at the socket level.
- Natively relies on UDP sockets.



Source : Modular Design of Freertr

Registration Design

- **Same master key for all SSs.**
  - $SSPK_m$
- **Different master keys for all SCs.**
  - SCK_m^i
- **Any SS unable to decrypt the packet destined to other SS.**
  - 5-Tuple (Src and Dest ports are unknown)
- **SC always don't need a different key to talk with different SS.**
  - ~~Hello(pair-ID, Server-ID)~~



Work Continues …

- More breaking news at it happens!