Building an eBPF-based Firewall from Scratch

UG Ljubljana

About me

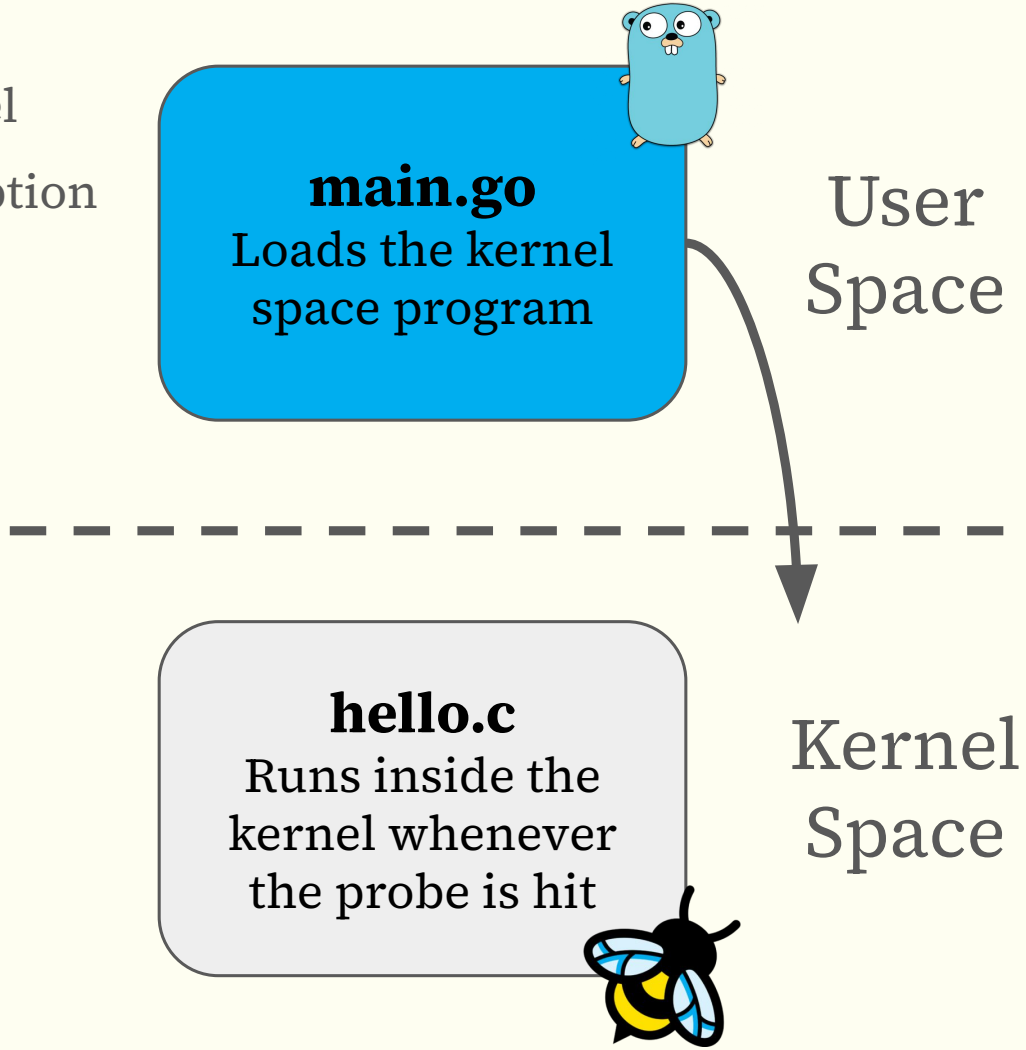
- I'm **Teodor J. Podobnik** from Slovenia 🇸🇮
- **Cloud Operations Team Lead** at Prewave GmbH, Vienna
- **Author** of eBPFChirp
- **eBPF Mentor, eBPF Hackathon Judge** and **eBPF Fellowship Recipient**

eBPFChirp

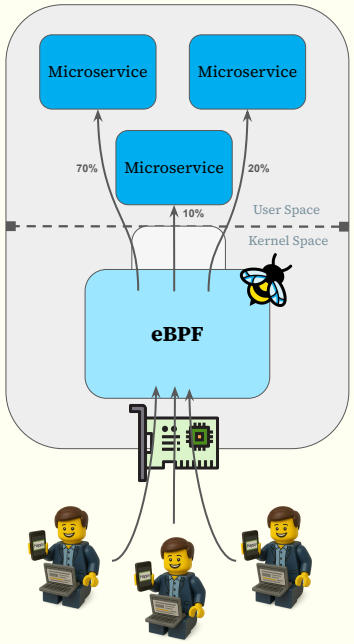
https://www.prewave.com
https://ebpfchirp.substack.com
https://www.linkedin.com/in/teodor-janez-podobnik/

eBPF in short

- Safely runs in the Kernel
- Low Resource Consumption
- Paradigm shift
- Use Cases:
  - Observability
  - Security
  - Networking

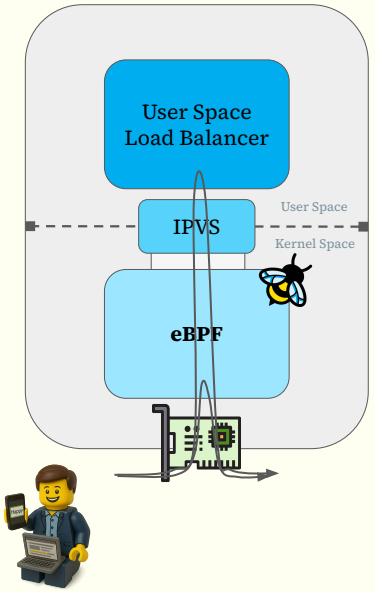


Cloudflare: Network Bandwidth Control



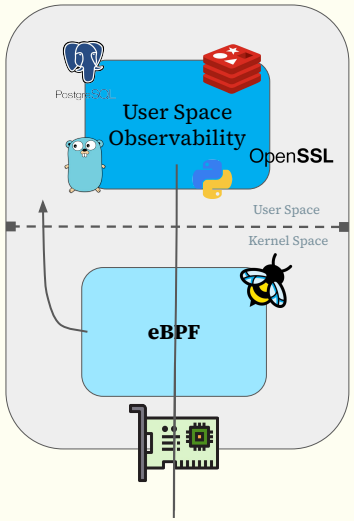
⬆️throughput
⬇️latency

Meta: Load Balancing (Katran)



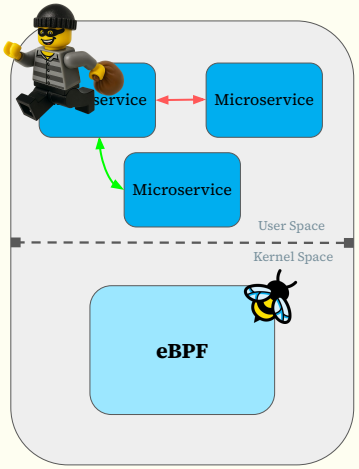
⬆️throughput
⬇️latency
⬇️CPU
⬇️memory
⬇️cost

Netflix: L7 Traffic Observability



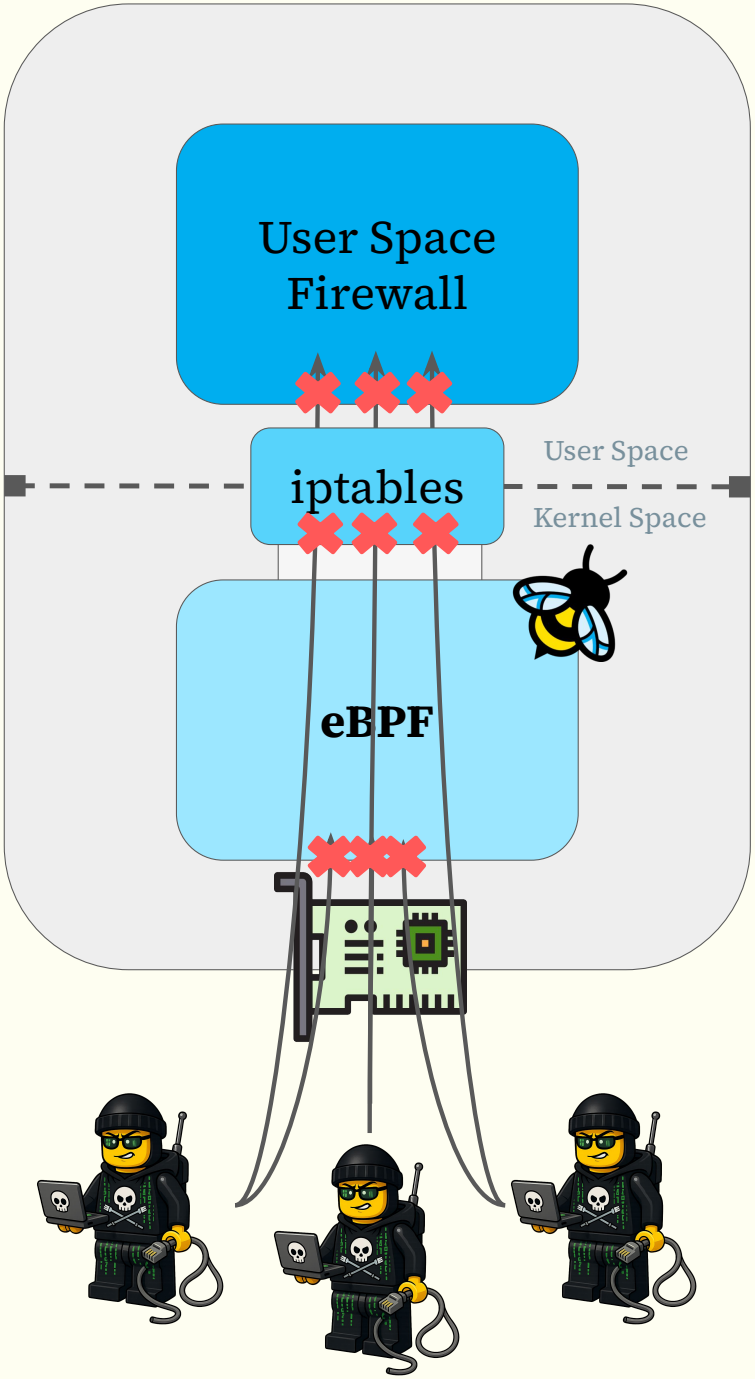
⬆️throughput
⬇️latency
⬇️CPU
⬇️memory
⬇️cost

Cisco: Kubernetes Runtime Security (Tetragon)

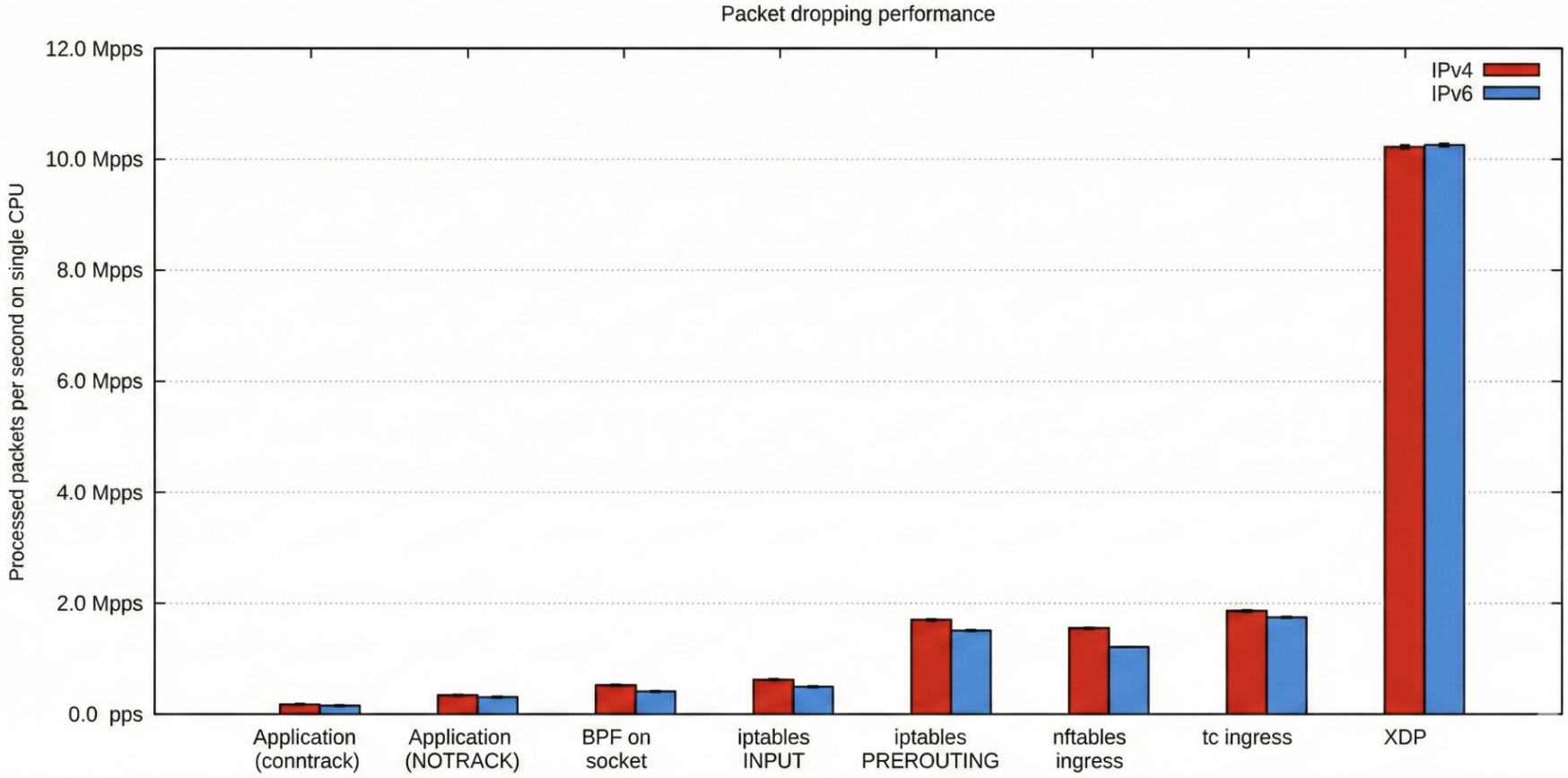


⬆️throughput
⬇️latency
⬇️CPU
⬇️memory
⬇️cost

Same Hardware / Better Performance?



⬆️pkt. drops/s
⬇️CPU
⬇️memory
⬇️cost


Packet dropping performance
Processed packets per second on single CPU
12.0 Mpps
10.0 Mpps
8.0 Mpps
6.0 Mpps
4.0 Mpps
2.0 Mpps
0.0 pps
IPv4
IPv6
Application (conntrack)
Application (NOTRACK)
BPF on socket
iptables INPUT
iptables PREROUTING
nftables ingress
tc ingress
XDP

Weekly insight to help you master eBPF!

Questions?