Technische Universität München, Department of Informatics

Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis B.Sc.

Thesis M.Sc.

Payload Extraction for Flows with Anomalous Time-to-Live Behaviour

Motivation

Malicious packets in the Internet are frequently sent with a faked source address (”spoofed”) or from hijacked source networks. Current defense mechanisms mainly rely on correlation of insights through external vendors, e.g. various ”blacklist” providers.
One approach to build a spoofing detection system locally is through leveraging the ”Time to Live” field which is present in all IP headers. It counts the number of routers traversed by a packet from its source to its destination, which should be relatively stable for a (*source, destination*) pair. This work builds on previous work at our chair and aims to expand FlowScope with possibilities to detect and dump flows with TTL anomalies in real time.

https://github.com/emmericp/FlowScope/

Your Task

- Expand FlowScope to support multiple “dumper” processes
- Program a FlowScope filter to detect anomalous flows
- Evaluate payload of anomalous flows

Contact

Quirin Scheitle scheitle@net.in.tum.de
Paul Emmerich emmericp@net.in.tum.de
Oliver Gasser gasser@net.in.tum.de

http://go.tum.de/644204