Technische Universität München, Department of Informatics

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

Thesis B.Sc.

Thesis M.Sc.

Advancing malicious packet detection through evaluation of inbound Time to Live headers

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. Using this field for anomaly and spoofing detection features two major benefits: Firstly, it is passively available in every single packet, hence providing a continuous flow of recent data as opposed to active measurements, which can not be conducted continuously. Secondly, this approach automatically focuses on recent communication partners instead of measuring the whole internet. Evaluation against both historic data of (*network , typical TTL*) pairs as well as current data (active tracebacks, correlation with TTL, correlation with BGP) are possible.

Your Task

- Analyze inbound TTL distribution (all tasks IPv4 and IPv6) per flow, host and prefix on existing infrastructure
- Build a database of either *(host, typical TTL)* or *(prefix, typical TTL)* pairs
- Evaluate traceback / ping-back for active TTL validation through hop-count and round-trip time (RTT)
- Compare TTL and RTT to BGP and geo-location services

Contact

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

http://go.tum.de/644204