Chair of Network Architectures and Services
Faculty of Informatics
Technical University of Munich

Internet Architecture and its Security Implications

Quirin Scheitle scheitle@net.in.tum.de

Advancing Research on Internet Architecture to better understand its Security Implications

Influenced by papers such as [1-3], mapped out four research goals to advance state-of-the-art

1. Implement a light-weight, yet accurate geo-location method
2. Find an algorithm to construct a state-of-the-art hitlist for IPv6
3. Leverage inbound IP TTL values for Internet Architecture research
4. Application: Mobile Messaging Services and their impact on Traffic Locality

[1] M. Roughan et al.,"10 lessons from 10 years of measuring and modeling the Internet's Autonomous Systems" *IEEE Journal on Selected Areas in Communications, 2011*
[2] Zhang et al., "How DNS Misnaming Distorts Internet Topology Mapping" *IEEE/ACM Transactions on Networking, 2010*
[3] Poese et al., "IP Geolocation Databases: Unreliable?" *SIGCOMM CCR, 2011*

Fundamentals: Geolocation

Based on a similar idea as [4], work on a new geolocation approach that is (a) light-weight and (b) highly accurate:

- Geolocation databases are very light-weight to use, but might be drastically wrong [3]
- Many latency- and structure-based measurement approaches exist, but these are typically very high-effort

Our goal is a flexible approach that can balance effort and accuracy based on user preference

[4] Huffaker et al., "DRoP: DNS-based Router Positioning" *SIGCOMM CCR, 2014*

Application: Mobile Messaging Locality

PAM'16

- Mobile Messaging Services such as WhatsApp quickly gain market share from SMS or E-Mail
- Services are neither standardized nor thoroughly researched (impeded by change frequency) [5]
- Our Hypothesis: Central server architecture heavily directs traffic out of region
- Complex testbed with control framework "MATADoR" to run 4 Apps (WhatsApp, Threema, WeChat, TextSecure/Signal) from 28 countries
- Results confirm hypothesis and call for discussion

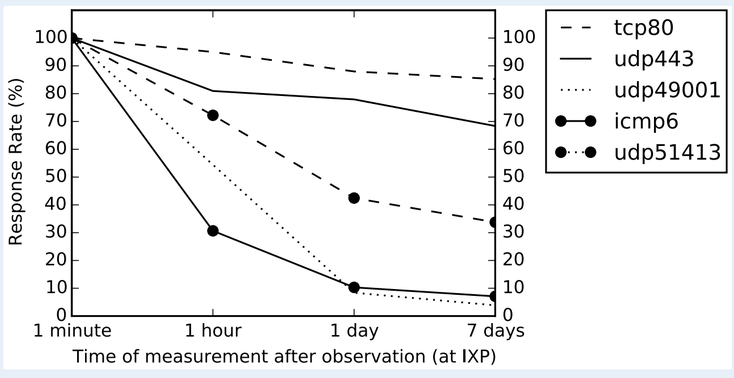
[5] Fiadino et al., "Vivisecting WhatsApp in Cellular Networks: Servers, Flows, and Quality of Experience" TMA'15

Fundamentals: IPv6 Hitlist

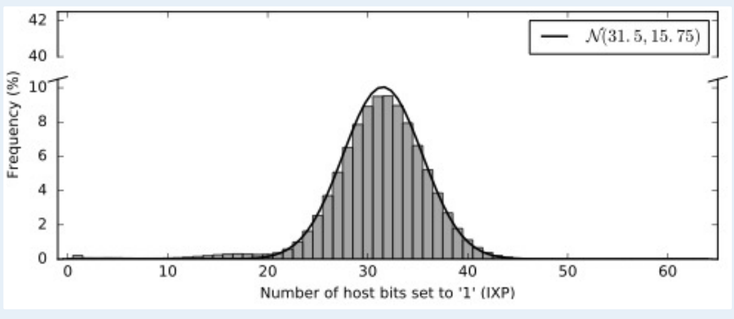
TMA'16

Joint work, personal focus on Passive Sources

- IPv4 scanning converged towards "0/0" approach
- IPv6 needs smart address selection
- Systematic investigation of various sources, assessing their attribution towards a joint hitlist, and evaluating IP quality
- My focus: IXP and MWN sources
  - Disect flows into individual IP addresses
  - Scrutinize IP validity (bogons, IANA special)
  - Do repeated connectivity evaluation
    - ICMP echo reply + "In-protocol"
    - Exponential back-off repetitions



- Passive sources largely short-lived IPs:



Traffic Measurement and Analysis Workshop (TMA), Belgium, April 2016