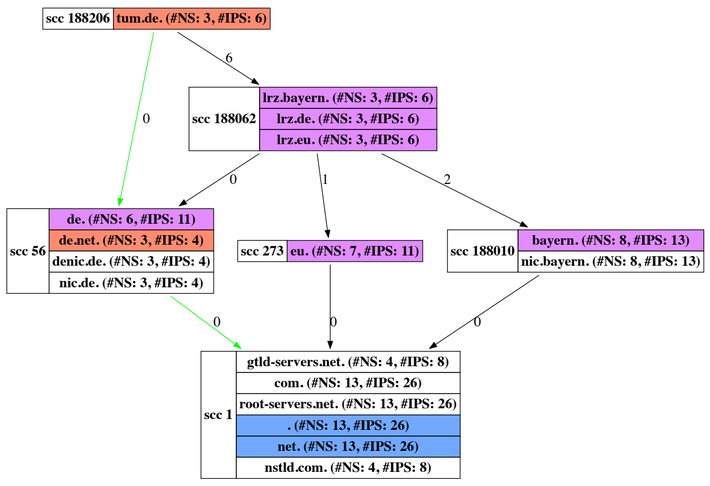
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

# Evaluating DNS Configurations through DNS Providers

*Presenter:* Patrick Sattler

## Research Topic




- Analysis of trusted computing base (TCB) properties and its structure

## Related Work

- In 2005 Ramasubramanian et al. analyzed DNS structure, TCB sizes, and the centralization of DNS [1]
  - We provide an up-to-date evaluation of these properties
- Borgolte et al. analyzed the takeover of domains hosted on dynamic cloud IP addresses [2]
  - We can check for nameserver IP addresses in dynamic cloud IP addresses ranges
- Vissers et al. evaluated the possibility to hijack domains by its nameserver [3]
  - Nameserver typosquatting (6k domains with nameserver names open for registration; 41k proactive registered)
  - In future we will check for typosqatting errors and using our structural information we can find the most impacting errors

## Our Dataset

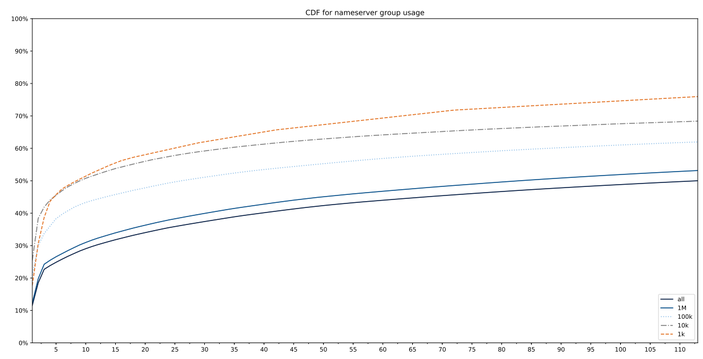
**Input sources:**

- Alexa Top 1M
- Majestic Million
- Umbrella Top 1M
- 64th part of the `.com` zone

**Data processing:**

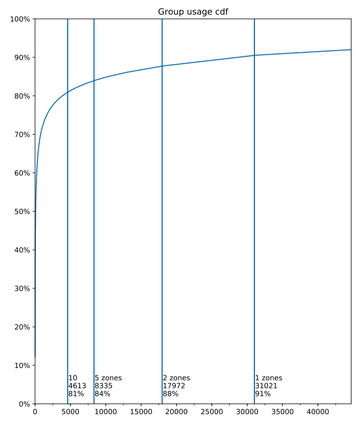
- GoDNS Scanner resolves the input domains by exploring the TCB
- More than 50 Million queries for the Alexa Top 1M list
- Import data into database (Postgresql)
- Resolving transitive relations is time intensive
- Including evaluation tables and all indices the database is 14GB large
- Focus on automation for everyday analysis

## Basic Scan Results



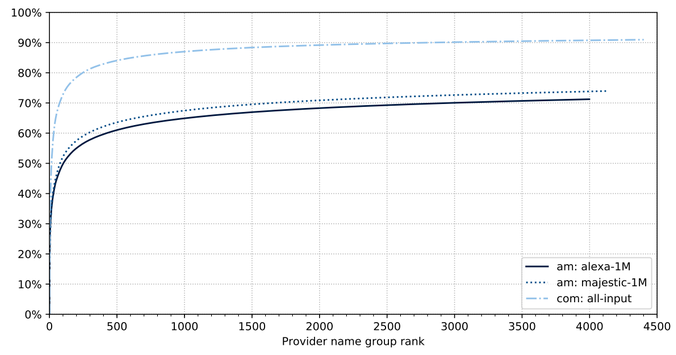

- In 2005 10% (of 593k domains) were controlled by 125 nameservers [1]
- Alexa 1M has only 126176 nameservers names (166771 nameservers were discovered by Ramasubramanian et al. [1])
- Vissers et al. [3] found Alexa Top 1M contains 23 typosquatted nameserver names
- A zone uses 2.8 nameserver names in average and its TCB average is 19 (excluding the root SCC)

## Provider classification




- The classification eliminates the need to analyze all domains by sampling the providers → more time for special cases
- Example provider `cloudflare.com`: 99,66% (of 115k domains) managed by `*.cloudflare.com`.
- Example provider `domaincontrol.com` aka GoDaddy: 98,77% (of 69k domains) managed by `*.domaincontrol.com`.

## Provider Evaluation




- The top 100 provider cover 73% of the `.com` zone and about 50% of the top lists
- Enables a simplified analysis on configuration issues (e.g. nameserver IP addresses in only one subnet)

[1] V. Ramasubramanian and E. G. Sirer, “Perils of Transitive Trust in the Domain Name System,” in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, pp. 35–35, USENIX Association, 2005.
[2] K. Borgolte, T. Fiebig, S. Hao, C. Kruegel, and G. Vigna, “Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates,” in *Proceedings of Internet Society Symposium on Network and Distributed System Security (NDSS)*, 2018.
[3] T. Vissers, T. Barron, T. Van Goethem, W. Joosen, and N. Nikiforakis, “The Wolf of Name Street: Hijacking Domains Through Their Nameservers,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 957–970, ACM, 2017.
[4] M. Allman, “Comments on DNS Robustness,” in *ACM Internet Measurement Conference*, Nov 2018.