Technische Universität München, Department of Informatics

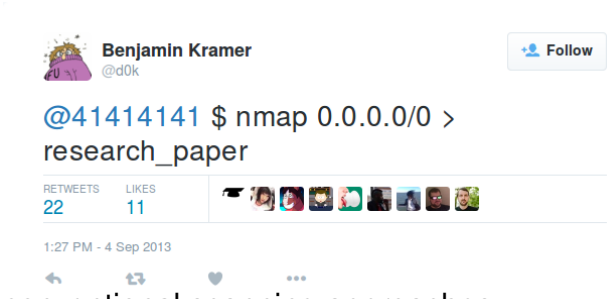
Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

Thesis B.Sc. Thesis M.Sc. IDP

Large Scale DNS Scanner in Go

Motivation

The DNS is a fundamental building block of the Internet. In order to understand this infrastructure, we employ large scale scans. However, sound and reliable DNS scans revealing the inner dependencies are not yet as practical as other scanners[1].
For the purpose of DNS scanning we developed a full DNS resolver[2], which in hindsight made some questionable choices regarding the used tools[3] and libraries[4].
In order to reliably produce sound DNS scans, we want to reimplement the scanner using more sensible choices, while fixing known weaknesses (efficient large scale reverse DNS lookup).
For the testing of the scanner, we recently developed a flexible blackbox testing framework for DNS resolvers.



conventional scanning approaches
Source: https://twitter.com/d0k/status/375354379660169216

[1] even when using the `nmap -sL` mode
[2] only ≈5k lines python while using an existing DNS packet parser
[3] We were forced to disable GC in python, since GC regularly took more than 5s
[4] SWIG wrapper, mostly memory leaks

Your Task

- Understand DNS in depth, in order to understand architecture of the existing scanner
- Investigate which (DNS) libraries can be used, and if they need to be improved
- Implement a DNS Scanner suitable for large scale scans using Go
- Depending on type of Work: IPv6, extending the scanner, measurements

Prerequisites

- Preferably master level, depending on skills and knowledge a bachelor's thesis is also possible
- Go, understanding of Python
- Interest in DNS and network measurements
- You live the GIYF motto

Contact

Johannes Naab naab@net.in.tum.de
Oliver Gasser gasser@net.in.tum.de

https://net.in.tum.de/~naab