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

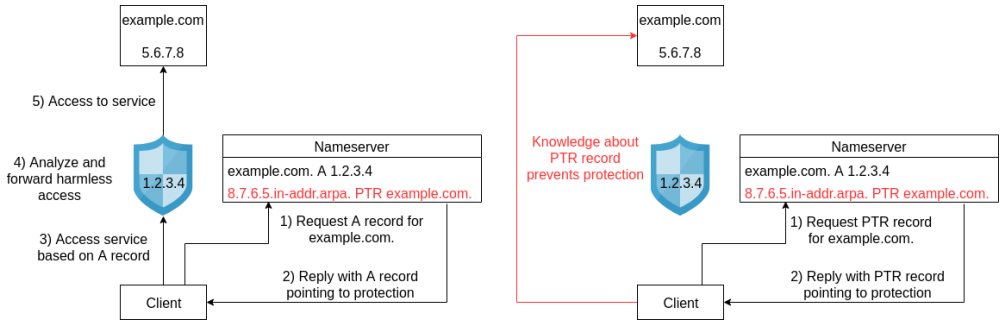
Thesis B.Sc. Thesis M.Sc. IDP

rDNS Leaks
Disclosing the Real Infrastructure of Shadowed Services

Motivation

Several protection mechanisms, e.g. against DDoS attacks, are set up as an intermediary service between clients and the protected service. Traffic has to pass this intermediary service, and is only forwarded to the actual target if it is labeled harmless. A simple mechanism to relay traffic to the intermediary is to change DNS records for a service. These new records resolve to the protection intermediary instead of the actual service. The real address of the service should not be revealed to a client to mitigate attacks.

This approach requires consistency between all DNS records of a service. If for example PTR records are not set up properly, they could leak information about the real address of a service.



Your Task

- Find differences between Forward and Reverse records in existing datasets
- Measure possible leaks and effects (Outdated information, inconsistencies, ...)
- Quantify the severity of information leaks
- Possible implementation: Add Forward DNS or IPv4 to an IPv6 rDNS scanner

Requirements

- Basic knowledge about DNS
- Familiarity with GIYF-Based work approaches

Contact

Johannes Zirngibl zirngibl@net.in.tum.de
Patrick Sattler sattler@net.in.tum.de

https://net.in.tum.de/members/zirngibl/