**Problem**
- DNS has been widely abused as a conduit of reflection/amplification attacks.
- Several challenge-response schemes have been proposed to defend against amplification attacks. Unfortunately, none of them work in the presence of DNS resolvers (RDNS)

**Performance Results**
- We assess our scheme via trace-driven simulation using passive traffic from Case Connection Zone (CCZ).
- We simulate the RDNS behavior based on the workload observed from CCZ clients.
- We bound our results with best case – single resolver– and worst case –reaching nullification– scenarios.

**Basic Challenge-Response**
Our challenge-response scheme contains two components:

**Request Padding**
Padding requests by a resolver can reduce the time required to nullify a response (e.g. using the EDNS(0) Padding Option). There are two options:
- Explicit padding padding size is signaled by Auth server.
- Implicit padding padding size is decided by the RDNS.

**Track RDNS Pools**
Explicitly track RDNS pools
- This extension sizes the challenge chains to develop an understanding of RDNS pools.

Implicitly track RDNS pools
- The Auth server can assume that IP addresses in a given network block (e.g. /24) are working together.

**Random Chain Termination**
Distribution of challenge chain lengths

**References**