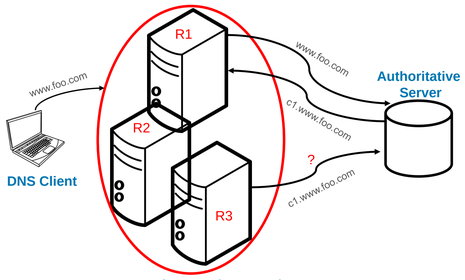
Practical Challenge-Response for DNS

Rami Al-Dalky, Michael Rabinovich and Mark Allman

Problem

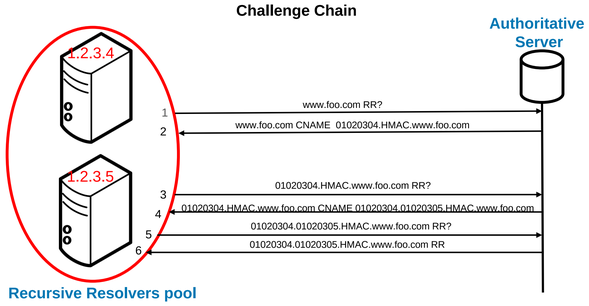
- DNS has been widely abused as a conduit of reflection/amplification attacks.
- Several challenge-response schemes have been proposed to defend against amplification attacks. Unfortunately, none of them work in the presence of DNS resolvers (RDNS)



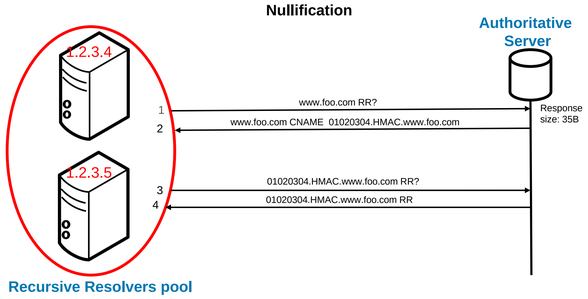
Basic Challenge-Response

Our challenge-response scheme contains two components:

Challenge Chain



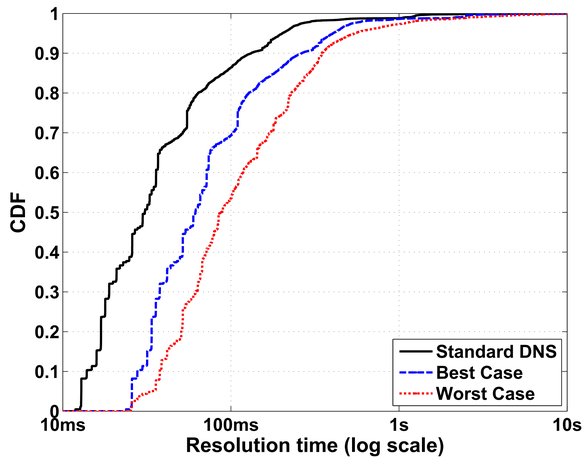
Nullification



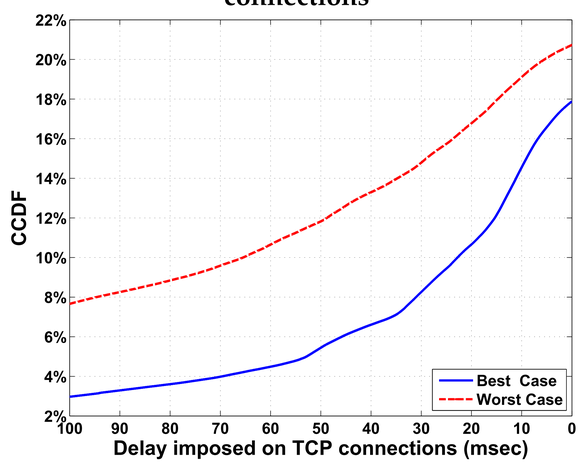
Performance Results

- 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.

Response time distribution for cache misses



Distribution of delay imposed on TCP connections



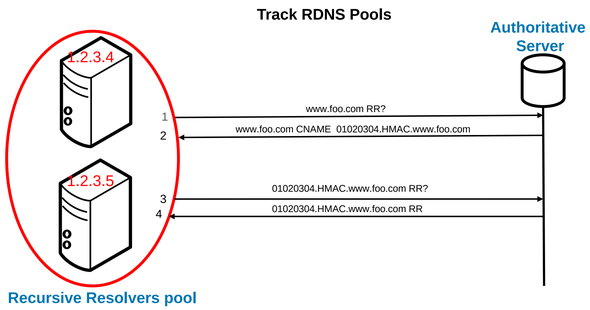
Track RNDS pools

Explicitly track RNDS pools

- This extension uses the challenge chains to develop an understanding of RDNS pools.

Implicitly track RNDS pools

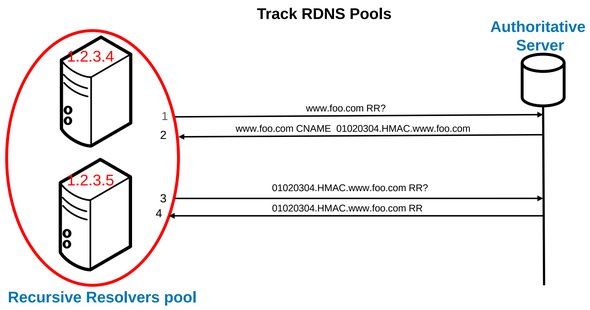
- The Auth server can assume that IP addresses in a given network block (e.g. /24) are working together.



Distribution of challenge chain lengths

Chain length	Basic scheme (%)	Explicit RDNS pool tracking (%)	Implicit RDNS pool tracking (%)
1	76.2	99.7	92.7
2	81.0	99.9	98.9
3	84.1	99.9	∼100
4	86.4	∼100	
5	88.2		
6	90.4		
7	91.5		
8+	100		

Random chain Termination



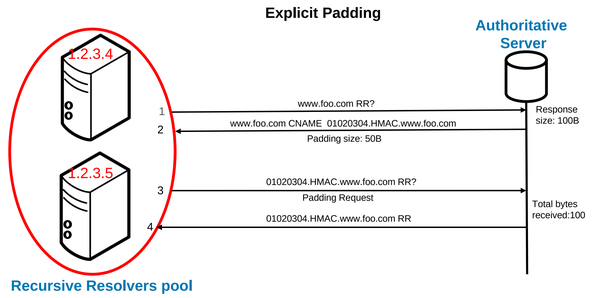
Distribution of challenge chain with Prob.

n	Nullification (%)	Probabilistic Responses (%)
1	44.5	72.3
2	72.8	92.2
3	92.0	97.8
4	96.6	98.9
5	97.8	99.2
6	98.5	99.4
7	∼100	∼100

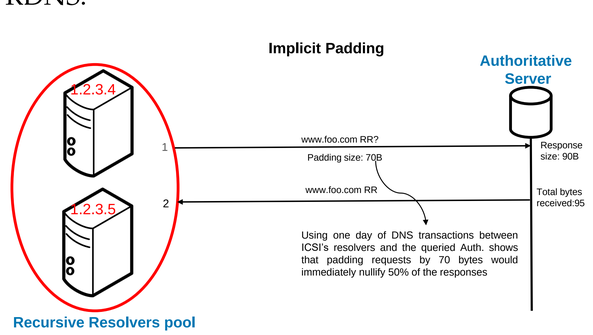
Request Padding

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.



References

For more details, please refer to our paper:
Rami Al-Dalky, Michael Rabinovich, Mark Allman. Practical Challenge-Response for DNS. ACM Computer Communication Review, 48(3), July 2018. (to appear)