AdaDoQ: Adaptive DNSSEC

Yehuda Afek
Tel-Aviv University

Anat Bremler-Barr
Reichman University

Daniel Dubnikov
Tel-Aviv University

Supported By:

ICRC
Blavatnik Interdisciplinary Cyber Research Center

GÉANT
NXDomain Request

Recursive Resolver

1. fake.example.com ??
2. Ref NS for .com
3. fake.example.com ??
4. Ref NS for example.com
5. fake.example.com ??
6. NX-DOMAIN fake.example.com

Empty cache

Client

Empty cache

root

a.root-servers.net

TLDs

.com .edu .us .net

SLDs

ns.example.com
NXDomain Attack

RANDOM DNS Request Flood

Resolvers

Rxy1xhggsgVCER.sony.com
XVBY$&HGDRxy2.sony.com
FJH*^DHGAKRxy3.sony.com
RxUYQVMNLKAY4.sony.com
RzHW$RE43CBJs$7.sony.com

.com

ns.sony.com
With DNSSEC

<table>
<thead>
<tr>
<th></th>
<th>Max Queries Per Second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain DNS</td>
<td>23,524</td>
</tr>
<tr>
<td>DNSSEC: NSEC</td>
<td>9,510</td>
</tr>
<tr>
<td>DNSSEC: NSEC3</td>
<td>8,989</td>
</tr>
</tbody>
</table>

Client

fake.example.com ??

Empty cache

Recursive Resolver

a.root-servers.net

NS root-servers.net

Max Queries Per Second

Plain DNS: 23,524

DNSSEC: NSEC: 9,510

DNSSEC: NSEC3: 8,989

Client

Recursive Resolver

fake.example.com ??

Empty cache

NX-DOMAIN fake.example.com

TLDs

.com .edu .us .net

SLDs

ns.example.com

Under NXDomain attack
Motivation

- DNSSEC is important
- DNS with DNSSEC does not scale, specifically,
  ➔ Vulnerable to NXDomain flood attacks

Goal

1. To measure DNSSEC scalability relative to Plain DNS
2. Develop a method for <resolver ↔ authoritative> collaboration that is
   (a) Scalable, (b) as secure as DNSSEC, and (c) introduces no new
   vulnerabilities.

   a. Provides the same security level as DNSSEC, and
   b. Provides performances close to that of Plain-DNS, and
   c. Does not enable new vulnerabilities.
DNSSEC

- Increase packet size
- Increase response count
- Add CPU load
- DoS Amplification

W/B Lies + NSEC5

NSEC/3

- Aggressive Caching

- Zone Walking
- Scalability (for CDNs)
- Disposable Domains
Conclusions

• DNSSEC degrades DNS performance
  • Make NXDOMAIN attacks worse (DDoS amplification)

• AdaDoQ – Hybrid Solution
  • Light and fast connections
  • One time encryption overheads
  • Close to Plain DNS throughput
  • No Security Compromises
    • No Zone Walking
  • No Scalability Issues
Questions?