Living on the Edge: (Re)focus DNS Efforts on the End-Points

Benno Overeinder
NLnet Labs
RIPE 75, Dubai, UAE

http://www.nlnetlabs.nl/
Complexity at Core-Middle-Edge

- Simple
  - Application
    - Stub
  - OS
- Complex
  - Recursive Resolver
    - Ripe75.ripe.net
    - 193.0.19.34
- Moderate
  - Authoritative Net
  - Authoritative Ripe
- E2E-ness Complex
- E2E-ness Moderate
- E2E-ness Simple
From the ground-up security

... and now for something completely different
Customer–Web Portal Interaction

Diagram:
- Customer
- Browser
- Host
- Full recursive resolver
- Web portal
- HTTP/HTTPS
- IP address
- Auth name servers
- Domain names: portal.acme.com, com, acme, portal
DNS Spoofing

• DNS Spoofing by cache poisoning
  • attacker flood a DNS resolver with phony information with bogus DNS results
  • by the law of large numbers, these attacks get a match and plant a bogus result into the cache

• Man-in-the-middle attacks
  • redirect to wrong Internet sites
  • email to non-authorized email server
The “Too Many CAs” Problem

• TLS clients have abundance of TAs
  • modern web browsers have 1300+ TAs
  • any of them can issue certificate for example.com

 TLS client accepts both!!  

example.com

example.com

http://www.nlnetlabs.nl/ 

credits wes.hardaker@parsons.com
Customer–Web Portal Interaction

http://www.nlnetlabs.nl/
DNSSEC-Based Secure Customer–Web Portal Interaction
Resolver Hijack?!

ARP, DHCP or routing tricks

host

browser

6.6.6.1

portal.acme.com

DNSSEC

auth name servers

com. acme. portal.

http/https

http

web portal

http server

IP address

DANE
Countering Resolver Hijack

- DNSSEC on the stub

- DNS-over-TLS
Countering Resolver Hijack (cont’d)

- DNS-over-TLS

- DNS-over-TLS

- DNSSEC protects against cache poisoning
- But not against resolver hijacking
- Another possibility: DNS over TLS

Validation Recursive resolver

Authoritative

dns-oarc.net

WebSrv

Browser (application)

OS

TLS hijack of DNS-over-TLS

Authenticate DNS-over-TLS with DANE?

Bootstrap the TLSA lookup with regular DNS?

Chicken and egg problem.
DNSSEC Data Blob-over-TLS

• TLSA record + the complete DNSSEC authentication chain embedded in a TLS extension
• TLS DNSSEC authentication to prevent “Too many CA’s” problem
DNS Privacy and Standards

• DNS privacy requirements

<table>
<thead>
<tr>
<th>Capability</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS-over-TLS</td>
<td>RFC7858</td>
</tr>
<tr>
<td>Reuse/pipelining/OOOP</td>
<td>RFC7766</td>
</tr>
<tr>
<td>TCP fast open</td>
<td>RFC7413</td>
</tr>
<tr>
<td>ENDS0 keep alive</td>
<td>RFC7828</td>
</tr>
<tr>
<td>ENDS0 padding</td>
<td>RFC7830</td>
</tr>
<tr>
<td>PKIX support for authentication</td>
<td>(various)</td>
</tr>
<tr>
<td>DNSSEC support (for address lookup and authentication)</td>
<td>(various)</td>
</tr>
</tbody>
</table>
DNSSEC Roadblocks

Consequences of living on the edge
DNSSEC Roadblocks

- Resolving DNSSEC (to cross the first mile) needs DNSSEC aware recursive resolver

http://www.nlnetlabs.nl/
DNSSEC Roadblock Avoidance

- DNSSEC roadblock avoidance + full recursion capability
DNSSEC Roadblock Avoidance

• DNSSEC roadblock avoidance + full recursion capability
  • https://tools.ietf.org/html/rfc8027
DNSSEC with DNS64 & NAT64

- Jen Linkova’s “Let’s talk about IPv6 DNS64 & DNSSEC”
  - [https://blog.apnic.net/2016/06/09/lets-talk-ipv6-dns64-dnssec/](https://blog.apnic.net/2016/06/09/lets-talk-ipv6-dns64-dnssec/)
- With IPv6 prefix discovery, stub can do DNSSEC validation of A RR itself

http://www.nlnetlabs.nl/
DNSSEC with DNS64 & NAT64

- IPv6 address synthesis prefix discovery + DNS64 capability
KSK Root Rollover

More roadblocks ahead
RFC5011 for DNSSEC Validating Stubs

- DNSSEC validating stub **must** do RFC5011

**In-band RFC5011 tracking with DNSSEC auth chain TLS extension**

- Browser (application)
- stub
- OS
- Validation Recursive resolver
- Authoritative .
- Authoritative net
dns-oarc.net
- Authoritative dns-oarc.net
- Authoritative getdnsapi.net
- WebSrV
- 853._tcp.getdnsapi.net
- TLSA
- getdnsapi.net
- DNSSKEY DS
- getdnsapi.net
- DNSSKEY DS
- getdnsapi.net
- DNSSKEY

---

http://www.nlnetlabs.nl/
KSK Root Rollover for Stub Library

• A stub library for DANE
  • runs with user’s privileges
  • no system config
  • bootstrap DNSSEC capabilities
    • https://tools.ietf.org/html/rfc7958
    • unbound-anchor functionality
DNSSEC Roadblocks and Standards

- DNSSEC stubs capability requirements

<table>
<thead>
<tr>
<th>Capability</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSSEC validation</td>
<td>(various)</td>
</tr>
<tr>
<td>DNSSEC roadblock avoidance</td>
<td>RFC8027</td>
</tr>
<tr>
<td>IPv6 prefix discovery</td>
<td>RFC7050</td>
</tr>
<tr>
<td>IPv6 address synthesis</td>
<td>RFC6147</td>
</tr>
<tr>
<td>Automated trust anchor updates</td>
<td>RFC5011</td>
</tr>
<tr>
<td>Automated initial trust anchor retrieval</td>
<td>RFC7958</td>
</tr>
</tbody>
</table>
Living on the Edge

“Final Thoughts”
Wrapping Up

• Stub resolver/library experience complex e2e-ness
  • at the edge of the network many kinds of roadblocks/brokenness

• DNS-based security from the ground up
  • bootstraps with the stub

• Closing the gap in the last mile with ongoing work
  • overview of RFCs and drafts
  • most of discussed work is implemented in getdns and its stub resolver **Stubby**

• DNSSEC Authentication Chain Extension