EDU Tutorial: DNS Privacy

Sara Dickinson
Sinodun
sara@sinodun.com

EDU Tutorial @ IETF_97 Seoul (Nov 2017)
Overview

• Goal:
  • Give audience historical background on why DNS Privacy is an important topic
  • Chart progress during last 3 years
  • Present current status and tools
Agenda

• Internet Privacy - presented by dkg
• DNS Privacy - A brief history
• DPRIVE WG et al.
• Implementation & deployment today
• Meet Stubby - a privacy stub resolver
• Ongoing & future work
Internet Privacy

Daniel Kahn Gillmor
ACLU
DNS Privacy
- A brief history
## IETF Privacy activity

<table>
<thead>
<tr>
<th>Date</th>
<th>Event/Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2011</td>
<td><strong>I-D:</strong> Privacy Considerations for Internet Protocols (IAB)</td>
</tr>
<tr>
<td>June 2013</td>
<td>Snowdon revelations</td>
</tr>
<tr>
<td>June 2013</td>
<td>RFC6973: Privacy Considerations for Internet Protocols</td>
</tr>
<tr>
<td>July 2013</td>
<td>RFC7258: Pervasive Monitoring is an Attack</td>
</tr>
<tr>
<td>May 2014</td>
<td>RFC7624: Confidentiality in the Face of Pervasive Surveillance: A Threat model and Problem Statement</td>
</tr>
<tr>
<td>August 2015</td>
<td>Much other ongoing work.....</td>
</tr>
<tr>
<td></td>
<td>What timing!</td>
</tr>
</tbody>
</table>
RFC 7258

“The IETF community's technical assessment is that PM is an attack on the privacy of Internet users and organisations.”

“The IETF community has expressed strong agreement that PM is an attack that needs to be mitigated where possible, via the design of protocols that make PM significantly more expensive or infeasible.”
DNS Privacy in 2013?

- DNS [RFC1034/5 - 1987] - original design availability, redundancy and speed!

- DNS standards:
  - UDP (99% of traffic to root)
  - TCP only for ‘fallback’ when UDP MTU exceeded and XFR (support only mandatory from 2010)

- Perception: The DNS is public, right? It is not sensitive/personal information….it doesn’t need to be encrypted

DNS sent in clear text => NSA: ‘MORECOWBELL’
DNS monitoring
DNS Disclosure Example 1

Leak information → datatracker.ietf.org

Rec

datatracker.ietf.org

datatracker.ietf.org

datatracker.ietf.org

datatracker.ietf.org

Root

Auth for .org

Auth for ietf.org

DNS Privacy Tutorial @ IETF 97

Nov 2016, Seoul
DNS Privacy in 2013?

- RFC6891: Extension Mechanisms for DNS (EDNS0)

  Intended to enhance DNS protocol capabilities

- But…. mechanism enabled addition of end-user data into DNS queries (non-standard options)

- Client subnet (RFC7871*)

  CDN justification: Faster content (geo location)

- User MAC addresses or user name/id

  ISP justification: Parental Filtering (per device)

* Informational
DNS Disclosure Example 2

Stub

CPE

[ietf.org ? [00:00:53:00:53:00]]

Rec

[ietf.org ? [192.168.1]]

Auth

[User src address] MAC address in DNS query

Client Subnet option contains source subnet in DNS query
DNS Disclosure Example 2

Even behind a NAT, do not have anonymity!

Even behind a recursive do not have anonymity!
DNS Disclosure Example 3

Who monitors or has access here?
• When at home…
• When in a coffee shop…

Who monitors or has access here?
DNS - complications

• Basic problem is leakage of meta data
  • Allows re-identification of individuals
• But.. legal requirements on providers regarding access to user data (country specific)
• Traffic analysis is possible based just on timings and cache snooping
  • DNS Filtering is becoming more prevalent
## DNS Risk Matrix

<table>
<thead>
<tr>
<th>Risk</th>
<th>In-Flight</th>
<th>At Rest</th>
<th>At Recursive</th>
<th>At Authoritative</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stub =&gt; Rec</td>
<td>Rec =&gt; Auth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passive Monitoring</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Monitoring</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Disclosure Risks</td>
<td>...</td>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Run a local resolver?

• Some users chose to run a local resolver on their client machine (e.g. Unbound) for increased privacy
  • bypass intermediate resolvers
  • have local DNSSEC validation
• But still sending queries in clear text, still querying authoritative servers
DNS Privacy options (2013)

- **DNSCurve**
  - Daniel J. Bernstein, initial interest but not adoption

- **DNSCrypt**
  - Many implementations, several open DNSCrypt Resolvers ([OpenDNS](#)), [Yandex browser](#)

- **Authentication** with some privacy
- Documented but not standard
DNS Privacy options (2014)

- **DNSTrigger** (NLNet Labs)
  - Client software to enable DNSSEC
  - Used TLS on port 443 as last ditch attempt to enable DNSSEC
  - So… there was a DNS-over-TLS implementation in Unbound recursive resolver

Goal was DNSSEC, not Privacy!
DPRIVE WG

- DPRIVE WG create in 2014

Charter: Primary Focus is Stub to recursive

- Why not tackle whole problem?
  - Don’t boil the ocean
  - Rec to Auth is a particularly hard problem
  - Step-by-step solution
DNS Privacy problem

Relationship: 1 to ‘a few’ some of whom are known (ISP)

Rec

Relationship: 1 to many most of whom are not known
=> Authentication is hard

Auth for .org

Root
RFC 7626 - DNS Privacy Considerations

Worth a read - many interesting issues here!

- Problem statement: Expert coverage of risks throughout DNS ecosystem

- Rebuts “alleged public nature of DNS data”
  - The data may be public, but a DNS ‘transaction’ is not/should not be.

“A typical example from outside the DNS world is: the web site of Alcoholics Anonymous is public; the fact that you visit it should not be.”
Choices, choices…

• So… we know the problem but what mechanism to use for encrypting DNS?

• STARTTLS

• TLS

• DTLS

• Confidential DNS draft

Drafts submitted on all these solutions to the working group
# Encryption Options

<table>
<thead>
<tr>
<th></th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STARTTLS</strong></td>
<td>• Port 53</td>
<td>• Downgrade attack on negotiation</td>
</tr>
<tr>
<td></td>
<td>• Known technique</td>
<td>• Port 53 - middleboxes blocking?</td>
</tr>
<tr>
<td></td>
<td>• Incrementation deployment</td>
<td>• Latency from negotiation</td>
</tr>
<tr>
<td><strong>TLS</strong></td>
<td>• New DNS port (no interference with port 53)</td>
<td>• New port assignment</td>
</tr>
<tr>
<td>(new port)</td>
<td>• Existing implementations</td>
<td>• Scalability?</td>
</tr>
<tr>
<td><strong>DTLS</strong></td>
<td>• UDP based</td>
<td>• Truncation of DNS messages (just like UDP)</td>
</tr>
<tr>
<td>(new port)</td>
<td>• Not as widely used/deployed</td>
<td>▶️ Fallback to TLS or clear text</td>
</tr>
<tr>
<td></td>
<td></td>
<td>❌ Can’t be standalone solution</td>
</tr>
</tbody>
</table>
Encrypted DNS ‘TODO’ list

• Get a new port
• DNS-over-TLS: Address issues with DNS-over-TCP in standards and implementations
• Tackle authentication of DNS Privacy servers
• What about traffic analysis of encrypted traffic (padding, etc.)
Get a new port!

- Oct 2015 - **853** is the magic number

Your request has been processed. We have assigned the following system port number as an early allocations per RFC7120, with the DPRIVE Chairs as the point of contact:

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-s</td>
<td>853</td>
<td>tcp</td>
<td>DNS query-response protocol run over TLS/DTLS</td>
</tr>
<tr>
<td>domain-s</td>
<td>853</td>
<td>udp</td>
<td>DNS query-response protocol run over TLS/DTLS</td>
</tr>
</tbody>
</table>
DNS + TCP/TLS?

- TCP/TLS is a new challenge for DNS operators
- DNS-over-TCP history:
  - typical DNS clients do ‘one-shot’ TCP
  - DNS servers have very basic TCP capabilities
  - No attention paid to TCP tuning, robustness
  - Performance tools based on one-shot TCP
Fix DNS-over-TCP/TLS

<table>
<thead>
<tr>
<th>Goal</th>
<th>How?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimise set up &amp; resumption</td>
<td>TFO Fast Open TLS session resumption [TLS 1.3]</td>
</tr>
<tr>
<td>Amortise cost of TCP/TLS setup</td>
<td><strong>RFC7766</strong> (bis of RFC5966) - March 2016: Client pipelining (not one-shot!), Server concurrent processing, Out-of-order responses</td>
</tr>
<tr>
<td></td>
<td><strong>RFC7858</strong>: Persistent connections (Keepalive)</td>
</tr>
<tr>
<td>Servers handle many connections robustly</td>
<td>Learn from HTTP world!</td>
</tr>
</tbody>
</table>
Performance (RFC7766)

**Client** - pipeline requests, keep connection open and handle out-of-order response

**Server** - concurrent processing of requests sending of out of order responses

---

**in-order**

q1, q2

q2 delayed waiting for q1 (+1 RTT)

**concurrent, OOOR**

q1, q2

0 extra RTT

reply as soon as possible
Authentication in DNS-over-(D)TLS

2 Usage Profiles:

- **Strict**
  - “Do or do not. There is no try.”

- **Opportunistic**
  - “Success is stumbling from failure to failure with no loss of enthusiasm”

Encrypt & Authenticate or Nothing

Try (in order):

- Authentication & Encryption then
- Encryption then
- Clear text
Authentication in DNS-over-(D)TLS

• Authentication based on either:
  • Authentication domain name
  • SPKI pinset

• Shouldn’t DNS use DANE…? Well - even better:
  • draft-shore-tls-dnssec-chain-extension
DNS Auth using DANE

1: Obtain a Auth Domain name & IP address

(1a)
- Configure Auth domain name
- Do Opportunistic SRV lookup

2a:
- Opportunistic lookup of DANE records for server
- Validate locally with DNSSEC

DNS Privacy client [DNSSEC]

DNS Privacy server

TLS
TLS DNSSEC Chain Extension

1: Obtain a Auth Domain name & IP address

(1a) • Configure Auth domain name • Do Opportunistic SRV lookup

Server Hello: Server DANE records

Client Hello: TLS DNSSEC Chain Ext

DNS Privacy client

DNS Privacy server

0 (or 2): Obtains DANE records for itself!

• Reduces Latency
• Eliminates need for validating recursive
## DPRIVE Solution Documents (stub to recursive)

<table>
<thead>
<tr>
<th>Document</th>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC7858</td>
<td>May 2016</td>
<td>DNS-over-TLS</td>
</tr>
<tr>
<td>RFC7830</td>
<td>May 2016</td>
<td>Padding</td>
</tr>
<tr>
<td>draft-ietf-dprime-dnsodtls*</td>
<td>Completed WGLC</td>
<td>DNS-over-DTLS</td>
</tr>
<tr>
<td>draft-ietf-dprime-dtls-and-tls-profiles</td>
<td>In WGLC</td>
<td>Authentication for DNS-over-(D)TLS</td>
</tr>
</tbody>
</table>

*Intended status: Experimental*
What about Recursive to Authoritative?

- DPRIVE - Next step is to tackle this issue with encryption
  - draft-bortzmeyer-dprive-step-2
    - Presents 6 authentication options/models
  - Authoritative DNS servers using TLS…
  - Re-charter? WG discussion on this here in Seoul (Fri)!
- DNSOP - RFC7816: QNAME Minimisation (mitigates)
DNS Disclosure Example 1

Leaks information

datatracker.ietf.org

Root

Rec

datatracker.ietf.org

dataetracker.ietf.org

dataetracker.ietf.org

dataetracker.ietf.org

Auth for .org

Auth for ietf.org
QNAME Minimisation

datatracker.ietf.org

Rec

org

Auth for .org

Root

Auth for ietf.org

ietf.org

datatracker.ietf.org
DNS-over-HTTP(S)

• DNS-over-HTTP(S) has been around a while…
  • draft-shane-review-dns-over-http

• Privacy (HTTPS authentication)

• Bypass port 53 interference (middlebox, captive portals)

• Higher level API
DNS-over-HTTP(S)

- Google: DNS-over-HTTPS
- draft-ietf-dnsop-dns-wireformat-http
  - “Servers and clients SHOULD use TLS for communication.”
- draft-hoffman-dns-over-http - DNS Queries over HTTPS
- Non-WG Mailing list and Bar BOF here (Tuesday)
Data handling policies

• Do you read the small print of your ISPs contract?

• More work/research needed in this area

  • Transparency from providers

  • Methods for de-identification of user data (e.g. DITL)

• Use of ‘PassiveDNS’ data for research/security analysis
## Risk Mitigation Matrix

<table>
<thead>
<tr>
<th>Risk</th>
<th>In-Flight</th>
<th>At Rest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stub =&gt; Rec</td>
<td>Rec =&gt; Auth</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>Encryption (e.g. TLS, HTTPS)</td>
<td>QNAME Minimization</td>
</tr>
<tr>
<td>Passive monitoring</td>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Active monitoring</td>
<td>Authentication &amp; Encryption</td>
<td></td>
</tr>
<tr>
<td>Other Disclosure Risks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e.g. Data breaches</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implementation Status
# Recursive implementations

<table>
<thead>
<tr>
<th>Features</th>
<th>Recursive resolver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Unbound</td>
</tr>
<tr>
<td>TCP/TLS  Features</td>
<td></td>
</tr>
<tr>
<td>TCP fast open</td>
<td>🟢</td>
</tr>
<tr>
<td>Process pipelined queries</td>
<td>✅</td>
</tr>
<tr>
<td>Provide OOOR</td>
<td>🟢</td>
</tr>
<tr>
<td>EDNS0 Keepalive</td>
<td>🟢</td>
</tr>
<tr>
<td>TLS Features</td>
<td></td>
</tr>
<tr>
<td>TLS on port 853</td>
<td>🟢</td>
</tr>
<tr>
<td>Provide server certificate</td>
<td>✅</td>
</tr>
<tr>
<td>EDNS0 Padding</td>
<td>✅</td>
</tr>
<tr>
<td>Rec =&gt; Auth</td>
<td>QNAME Minimisation</td>
</tr>
</tbody>
</table>

- **Dark Green**: Latest stable release supports this
- **Light Green**: Patch available
- **Yellow**: Patch/work in progress, or requires building a patched dependency
- **Purple**: Workaround available
- **Grey**: Not applicable or not yet planned

---

DNS Privacy Tutorial @ IETF 97

Nov 2016, Seoul
Alternative server side solutions

• *dnsdist* from PowerDNS would be great…
  • But no support yet

• Pure TLS load balancer
  • *NGINX, HAProxy*
  • *BIND article* on using stunnel

Disadvantages
• server must still have decent TCP capabilities
• DNS specific access control is missing
• pass through of edns0-tcp-keepalive option
# Stub implementations

<table>
<thead>
<tr>
<th>TCP/TLS Features</th>
<th>TCP fast open</th>
<th>Connection reuse</th>
<th>Pipelining of queries</th>
<th>Process OOOR</th>
<th>EDNS0 Keepalive</th>
<th>TLS on port 853</th>
<th>Authentication of server</th>
<th>EDNS0 Padding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idns</td>
<td>Dark Green</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>digit</td>
<td>Light Green</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>getdns</td>
<td>Yellow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIND (dig)</td>
<td>Grey</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*getdns uses libunbound in recursive mode*
Implementation Status

• Increasing uptake of better DNS-over-TCP
• Several implementations of DNS-over-TLS
• None yet of DNS-over-DTLS
• Key is enabling end users and application developers to easily adopt DNS Privacy
Deployment Status
## DNS-over-TLS Servers

<table>
<thead>
<tr>
<th>Hosted by</th>
<th>Software</th>
<th>Supports Strict?</th>
</tr>
</thead>
<tbody>
<tr>
<td>NLnet Labs</td>
<td>Unbound</td>
<td>Y</td>
</tr>
<tr>
<td>OARC</td>
<td>Unbound</td>
<td></td>
</tr>
<tr>
<td>Surfnet (Sinodun)</td>
<td>Bind + HAProxy</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Bind + nginx</td>
<td></td>
</tr>
<tr>
<td>IETF?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+test+servers](https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+test+servers)
RIPE NCC

• RIPE DNS WG: Discussion support of experimental DNS Privacy Services

• RIPE NCC have expressed interest in a community effort:
  • Research various solutions and issues
  • ‘DNS-over-TLS operational guidance’
• Modern **async DNSSEC** enabled API
  
  • [https://getdnsapi.net](https://getdnsapi.net)

• Written in C, several bindings

• DNS-over-TLS, validating DNSSEC stub

• ‘Stubby’ now available for testing
Meet Stubby - A Privacy Enabling Stub Resolver
Stubby - getdns_query by another name

- 1.1.0a3 - getdns_query tool extended to
  - Run as daemon handling requests
    - Configure OS DNS resolution to point at 127.0.0.1
    - Reads default from /etc/stubby.conf (TLS)
    - Supports domain name and SPKI pinset authentication, Strict and Opportunistic
Stubby Demo

• How to build and use Stubby
Ongoing and Future work

- Hacking this weekend at the IETF 97 Hackathon
- Lots of work on Stubby!
- More complete recursive implementations
- Increased deployment
- More DPRIVE work: Recursive to Auth....
Summary

• DNS Privacy is important issue
• Active work on the large solution space
• Can test DNS Privacy today using Stubby & current test recursive servers
• More DNS Privacy services on the way…
Thank you!

Any Questions?

sara@sinodun.com