DNS privacy, where are we?

Stéphane Bortzmeyer
bortzmeyer@nic.fr
DNS privacy

- DNS in clear most of the time,
- Too much information sent (FQDN to the root...),
- Some requests are too revealing,
- Requests are sent outside of the “normal path”.
DNS privacy

- DNS in clear most of the time,
DNS privacy

- DNS in clear most of the time,
- Too much information sent (FQDN to the root...),
DNS privacy

- DNS in clear most of the time,
- Too much information sent (FQDN to the root...),
- Some requests are too revealing
  (“_bittorrent-tracker._tcp.domain.example”),
DNS privacy

- DNS in clear most of the time,
- Too much information sent (FQDN to the root...),
- Some requests are too revealing,
- Requests are sent outside of the “normal path” (more ASes can see them, no “Schengen routing” for DNS).
The past

- June 2013, CENTR meeting in Amsterdam, first talk about DNS privacy,
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations (including MoreCowBell, surveillance using the DNS),
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver, the “DNS privacy” projects informally starts,
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, The **excellent** DNS library for C programmers getdns has DNS-over-TLS,
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, getdns has DNS-over-TLS,
- August 2015, RFC 7626 “DNS Privacy Considerations” (description of the problem),
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, getdns has DNS-over-TLS,
- August 2015, RFC 7626 “DNS Privacy Considerations”,
- October 2015, the resolver Unbound gets DNS-over-TLS (non-standard version was there a long time ago),
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, getdns has DNS-over-TLS,
- August 2015, RFC 7626 “DNS Privacy Considerations”,
- October 2015, the resolver Unbound gets DNS-over-TLS,
- March 2016, RFC 7816 “DNS Query Name Minimisation to Improve Privacy” (stop sending the FQDN to the auth. server),
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, getdns has DNS-over-TLS,
- August 2015, RFC 7626 “DNS Privacy Considerations”,
- October 2015, the resolver Unbound gets DNS-over-TLS,
- March 2016, RFC 7816 “DNS Query Name Minimisation”,
- May 2016, RFC 7858 “Specification for DNS over Transport Layer Security (TLS)” (encrypt DNS traffic, port 853, remember privacy needs encryption and minimisation), this is stub-to-resolver only,
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, getdns has DNS-over-TLS,
- August 2015, RFC 7626 “DNS Privacy Considerations”,
- October 2015, the resolver Unbound gets DNS-over-TLS,
- March 2016, RFC 7816 “DNS Query Name Minimisation”,
- May 2016, RFC 7858 “Specification for DNS over TLS”,
- May 2016, RFC 7830 “The EDNS(0) Padding Option” (to hamper packet size analysis),
The past

- June 2013, CENTR meeting in Amsterdam,
- June 2013, Snowden revelations,
- November 2013, IETF meeting in Vancouver,
- March 2015, getdns has DNS-over-TLS,
- August 2015, RFC 7626 “DNS Privacy Considerations”,
- October 2015, the resolver Unbound gets DNS-over-TLS,
- March 2016, RFC 7816 “DNS Query Name Minimisation”,
- May 2016, RFC 7858 “Specification for DNS over TLS”,
- May 2016, RFC 7830 “The EDNS(0) Padding Option”,
- July 2017, Stubby, a daemon to use on the end-user machine to forward requests with DNS-over-TLS to other resolvers.
The present

We have an almost complete set of technical standards, we have some running code, servers and libraries, we have a big public resolver deploying DNS-over-TLS and a few small ones as well, QNAME minimisation in the resolvers Unbound and Knot. We have an excellent information portal https://dnsprivacy.org/ We are far from wide deployment.
The present

- We have an almost complete set of technical standards,
The present

- We have an almost complete set of technical standards,
- We have some running code (although sometimes a bit rough), servers and libraries (the excellent Go-DNS),
The present

- We have an almost complete set of technical standards,
- We have some running code, servers and libraries,
- We have a big public resolver deploying DNS-over-TLS (Quad9) and a few small ones as well,
The present

- We have an almost complete set of technical standards,
- We have some running code, servers and libraries,
- We have a big public resolver deploying DNS-over-TLS and a few small ones as well,
- QNAME minimisation in the resolvers Unbound and Knot. In Europe, 2% of RIPE Atlas probes have a resolver with QNAME min.
The present

- We have an almost complete set of technical standards,
- We have some running code, servers and libraries,
- We have a big public resolver deploying DNS-over-TLS and a few small ones as well,
- QNAME minimisation in the resolvers Unbound and Knot.
- We have an excellent information portal https://dnsprivacy.org/
The present

- We have an almost complete set of technical standards,
- We have some running code, servers and libraries,
- We have a big public resolver deploying DNS-over-TLS and a few small ones as well,
- QNAME minimisation in the resolvers Unbound and Knot.
- We have an excellent information portal
  https://dnsprivacy.org/
- We are far from wide deployment.
The future

Very soon now, RFC on authentication of DNS-over-TLS resolvers, May 2018, GDPR is enforceable, Work at the IETF on encrypting resolver-to-auth link?

Android released with DNS-over-TLS client, DNS-over-HTTPS, currently under standardisation at IETF,
The future

- Very soon now, RFC on authentication of DNS-over-TLS resolvers, and the RFC on padding profiles,
The future

- Very soon now, RFC on authentication of DNS-over-TLS resolvers,
- May 2018, GDPR is enforceable,
The future

- Very soon now, RFC on authentication of DNS-over-TLS resolvers,
- May 2018, GDPR is enforceable,
- Work at the IETF on encrypting resolver-to-auth link?
The future

- Very soon now, RFC on authentication of DNS-over-TLS resolvers,
- May 2018, GDPR is enforceable,
- Work at the IETF on encrypting resolver-to-auth link?
- Android released with DNS-over-TLS client (today already committed but not yet released),
The future

- Very soon now, RFC on authentication of DNS-over-TLS resolvers,
- May 2018, GDPR is enforceable,
- Work at the IETF on encrypting resolver-to-auth link?
- Android released with DNS-over-TLS client,
- DNS-over-HTTP/2 (DNS wire format over HTTP/2), currently under standardisation at IETF (please participate! Cool hackathon in London, march 2018),
Putting bricks together

We have a set of bricks,
How to put them together?
Use your ISP's resolver?
Stub to a public resolver like Quad9?
Everything done locally?
A mix?
DNS-over-TLS or everything-over-port-443?
Putting bricks together

- We have a set of bricks,
Putting bricks together

- We have a set of bricks,
- How to put them together?
Putting bricks together

- We have a set of bricks,
- How to put them together?
- Use your ISP’s resolver?
Putting bricks together

- We have a set of bricks,
- How to put them together?
- Use your ISP’s resolver?
- Stub to a public resolver like Quad9? Requires full confidence in the resolver.
Putting bricks together

- We have a set of bricks,
- How to put them together?
- Use your ISP’s resolver?
- Stub to a public resolver like Quad9?
- Everything done locally? In systemd? A box like the Turris Omnia? Better user control but no cache sharing and personal IP address outside.
Putting bricks together

- We have a set of bricks,
- How to put them together?
- Use your ISP’s resolver?
- Stub to a public resolver like Quad9?
- Everything done locally?
- A mix? stubby dispatching to several public resolvers chosen randomly? Best of both worlds?
Putting bricks together

- We have a set of bricks,
- How to put them together?
- Use your ISP’s resolver?
- Stub to a public resolver like Quad9?
- Everything done locally?
- A mix?
- DNS-over-TLS or everything-over-port-443?
We need you
We need you

- Standards are done (except resolver-to-auth and DNS-over-HTTPS) but,
We need you

- Standards are done but,
- Much more code needed,
We need you

- Standards are done but,
- Much more code needed,
- Much more deployment needed,
We need you

- Standards are done but,
- Much more code needed,
- Much more deployment needed,
- Outreach necessary.
Merci !