DNS over X

Dmitry Kohmanyuk :: Hostmaster.UA
EEDNS Forum :: Yerevan 2019.10.11
Why that name?

Let's use a common name for DoT and DoH: DoE (DNS-over-encryption.)

I didn't invent this: the credit goes to Prof. Shuang Hao, UoT (that's University of Texas)

For contrast, we can call conventional DNS, Do53

DoT is described in RFC 7858 and updated in 8310

Note that 8310 adds encrypted datagram support.

Similarly, DoH is in RFC 8484.
Facts
Facts

1. DNS is important protocol for the rest of Internet
2. DNS queries should be encrypted for exact same reason as mail and web traffic should
3. We never seriously considered updating DNS
4. IETF is slow machine with unpredictable results
Beliefs
Beliefs

1. DNS as today is just fine
2. DNS does not change or needs change
3. Evil people would use encrypted DNS to do harm; good people don’t use encryption
4. Ability to control (monitor, alter, block) DNS traffic by your ISP/parent/corporation is good
5. Google is Evil. Mozilla is puppet of Google. Resistance is futile
More Facts
More Facts

1. DoE is modernising DNS transport without touching its response logic
2. If you view DNS as a mathematical function, it stays the same
3. One should separate rise of “DaaS” (DNS as a service providers) from DoE itself
4. We had OpenDNS for years, suddenly the Google/IBM+PCH/Cloudflare is evil?
5. It is a choice your browser lets you make. Its you who makes it
Takeaways
Takeaways

1. Your ISP MAY block, intercept, record, or alter DNS and OTHER traffic for no good reason
2. DoE MAY make those activities little harder
3. There is no substitute for good network security policy
4. Expect DoE to stay. Expect governments to hate it.
5. If you know how to run your own DNS server, consider augmenting it with encrypted query support
Questions?

Dmitry Kohmanyuk
dk@hostmaster.ua

(Doing DNS before DNS was cool)