DNS over Secure Transports

Emerging Identifiers Technology

Paul Hoffman

ICANN 64, Kōbe
12 March 2019

Emerging transports, not emerging identifiers

- This session describes two methods of getting DNS information that have been standardized in recent years are are starting to see more deployment

- This is still the DNS: the data is the same

- What’s new is that the data is secured with TLS

- This causes some important policy implications

DNS-over-TLS and DNS-over-HTTPS: an overview

- Normal DNS queries and responses are sent in the clear on port 53
  - Susceptible to monitoring
  - Susceptible to falsification
- Usually over UDP, sometimes over TCP
- DNS traffic is sent primarily between end-user systems and recursive resolvers

DNS-over-TLS (DoT)

- IETF started work in April 2015 to protect DNS traffic between stub resolvers and recursive resolvers with TLS
- Standardized in May 2016
- DNS protocol is unchanged: it just runs under TLS on port 853
- Note that TLS is *always* TCP
- Easy to implement in both operating systems and in recursive resolvers, but implementation in OSs is scarce
- Was recently added to Android in promiscuous mode

DNS-over-HTTPS (DoH)

- IETF started work in December 2017 to protect DNS traffic between browsers and recursive resolvers with TLS
- Standardized in October 2018
- DNS protocol is turned into HTTP messages that are transferred under HTTPS
- Note that TLS is always TCP
- Easy to implement in both browsers and in recursive resolvers, and lots of implementations appeared before the spec was even complete

Comparison of DoT and DoH

- DoT was designed for operating systems (stub resolvers), DoH was designed for browsers and web applications (Javascript)
- DoT runs on its own port (853), DoH runs under HTTPS on normal port 443
- Neither DoT nor DoH specify how the user should be able to set up the protocol, or whether they can even tell that the protocol is running
- DoT seemed uncontroversial because people assumed computers would be configured to use the same recursive resolver that was already trusted by the user
- DoH quickly became controversial because Firefox performed tests using a cloud provider that was not necessarily trusted by the user

This is not DNSSEC

- DNSSEC is authentication-only: it does not add encryption
- DNSSEC assures that the answer is what the zone owner intended, but only if it is used
- Most large commercial domains do not sign their DNS records with DNSSEC
- Most recursive resolvers do not validate DNSSEC responses
- Current data suggests that only about 15% of Internet users use a resolver that validates DNSSEC responses

Policy implications: service blocking

- Privacy is good
- However, the reduced visibility can block the service providers you trust
- Some providers, particularly enterprises, rely on cleartext DNS on port 53 in order to provide services such as malware and exfiltration detection

Policy implications: centralization

- DoT is generally only configured for resolvers that the user would have likely used anyway, but DoH is controlled by browsers and web applications
- The DNS queries can go anywhere that the browser or application wants
- Typically, this will be to large, well-known resolvers
- Those resolvers will then have much more information about users than they might have before, and will be targets for people who want that information

Policy implications: split views

- It is common in enterprises to have domain names that resolve differently if you are “inside” the enterprise network than if you are “outside”
- DoH (and DoT to unknown resolvers) breaks that model, so names will be resolved externally much more often
- In addition to accessibility problems, this can cause security problems because users may end up on sites they don’t expect

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: paul.hoffman@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann