CRS INSIGHT

DNS over HTTPS—What Is It and Why Do People Care?

October 16, 2019 (IN11182)

|

Related Authors

- Chris Jaikaran
- Patricia Moloney Figliola

|

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)
Patricia Moloney Figliola, Specialist in Internet and Telecommunications Policy (pfigliola@crs.loc.gov, 7-2508)

Internet pioneer David Clark said: "It's not that we didn't think about security. We knew that there were untrustworthy people out there, and we thought we could exclude them." Those who created the internet were focused on enabling the utility of the network, and a repercussion of their design decisions is that internet security is not inherent but must be retrofitted. Efforts to change one of the internet's hardwired insecurities—the Domain Name System (DNS)—are ongoing but will be disruptive.

How We Get to Websites Today

When someone wants to visit a website, they type the web address into their browser, and the website loads. DNS is one of the many protocols needed to make that work. Many call DNS the "phonebook of the internet": it takes the user-readable web address and sends that information to a *DNS resolver*. The resolver retrieves the internet protocol (IP) address of the website (i.e., the network address of the server that hosts the website) and returns that information to users' computers. Knowing where to go, the browser then retrieves the website. Most users receive DNS resolver services from their internet service provider (ISP), but some choose to use another service. For instance, some businesses choose to use a resolver that provides additional security or filtering services.

Today, DNS queries are generally sent unencrypted. This allows any party between the browser and the resolver to discover which website users want to visit. Such parties can already monitor the IP address with which the browser is communicating, but monitoring DNS queries can identify which specific website users seek. As more services move to cloud computing infrastructure, this distinction becomes increasingly important, because multiple websites may be consolidated under a few IP addresses, rather than each having a unique IP address.

Uses of DNS Query Data

Information extracted from unencrypted DNS queries can be used for a variety of purposes. Network providers can determine the geographically closest instance of a website users are seeking so the content can be delivered faster. Using filters, employers can block workplace access to gambling websites, and parents can block their children from accessing adult websites at home. ISPs use DNS queries to comply with law enforcement requests for records of users' internet

activity. DNS query information can also be used to profile users' online behavior for purposes such as providing targeted advertising.

Weaknesses of DNS Queries

Unencrypted DNS queries may be intercepted or manipulated without users' knowledge. An eavesdropper—e.g., the owner of a Wi-Fi router or party in the ISP infrastructure—can see where users seek to browse, even if the content delivered from the website is encrypted. DNS queries can also be hijacked to divert a user to a malicious website instead of the intended website. In 2019, the U.S. Department of Homeland Security (DHS) issued its first emergency directive to federal agencies in response to a DNS hijacking campaign.

Encrypting DNS Queries

DNS over HTTPS (DOH) changes how DNS queries are sent. DOH encrypts DNS queries as web traffic, instead of sending them as clear text. If DOH is in use, the content of a DNS query is visible only to the users' browsers and the DNS resolver, not to third parties between them on the network. Google and Mozilla recently announced they will move to DOH for their Chrome and Firefox desktop web browsers. Statcounter estimates that Chrome has 65% of the U.S. desktop browser market and Firefox has 8%.

Google's Chrome Approach

Starting with Chrome version 78 (scheduled for release on October 22, 2019), Google will enable DOH for users who have opted to use an approved resolver. Google will not change users' choice of resolver, so the user experience should be unaffected. For example, content filtering by employers or parents should continue to work. If DOH fails, Chrome will revert to the original DNS resolver. Chrome users can choose to opt out of DOH in the browser.

Mozilla's Firefox Approach

Firefox has supported DOH since 2018, but beginning in September 2019, Mozilla began switching U.S. users to DOH by default. To do this, Firefox uses Cloudflare as its DNS resolver, although users can change this. Mozilla is deploying DOH in "fallback mode"—if the browser detects that business filtering or parental controls are present, it will automatically disable DOH and use the original DNS resolver. Firefox detects the presence of filtering via "canary domains" that seek to load test websites. If the test website doesn't load, Firefox does not activate DOH and falls back to users' original choice of DNS resolver. Firefox users can choose to opt out of DOH in the browser.

Changing the Status Quo

Controversy soon followed the companies' announcements to move to DOH, according to media reports.

One concern is that DOH inhibits content filtering controls. Indeed, Mozilla opted not to deploy DOH in the United Kingdom because of this concern. Measures such as user selection and canary domains may help to address this.

Another concern is that DOH will complicate content delivery to users. Today, content delivery networks (CDNs) host multiple instances of web content on geographically dispersed servers. This creates resiliency for web services and helps to deliver content to users more quickly. If ISPs lose the ability to view users' DNS queries, they will still be able to route users to a CDN, but not necessarily the closest or most efficient CDN. Technical measures that may alleviate this concern include sharing some user data (like general geolocation data) and CDN load management tactics.

Complying with law enforcement requests for DNS query information will change if ISPs no longer have visibility into that data. Law enforcement agencies could request the information from DNS resolvers instead, but will need to know which resolver customers use in order to present their request, and the resolvers may not retain the necessary records.

Other potential implications of DOH implementation involve issues such as international data flow and advertising competition.