Issued 8/20/18

DNS Requests Routinely Spied On

Most people's DNS queries – by which browsers and other software resolve domain names into IP addresses – remain unprotected while flowing over the internet. And that's because, you may not be surprised to know, the proposed standards to safeguard DNS traffic – such as DNSSEC and DNS-over-HTTPS – have yet to be fully baked and aren't yet widely adopted. DNSSEC, for one, aims to prevent miscreants tampering with intercepted domain-name lookups by digital signing the answers – making any forgeries obvious to software. DNS-over-TLS and DNS-over-HTTPS aim to do this, too, and encrypt the queries so eavesdroppers on the network can't snoop on what sites you're visiting. Without these safeguards in wide (or any) use, DNS traffic remains unencrypted and unauthenticated, meaning they can be potentially spied on and meddled with to redirect people to malicious websites masquerading as legit sites. Researchers from universities in China and the US recently decided to check whether or not this is actually happening, and found that traffic interception a reality for a small but significant portion of DNS queries – 0.66 per cent of DNS requests over TCP – across a global sample of residential and cellular IP addresses. The paper, "Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path," describes how the researchers set up a system to measure DNS interception across 148,478 residential and cellular IP addresses around the world.