DNS over TLS defines how DNS packets would be encrypted using TLS and transmitted over the widely used Transmission Control Protocol (TCP). By default, DNS travels over Port 53 via TCP or the User Datagram Protocol (an alternative to TCP). With DNS over TLS, all encrypted packets are sent over Port 853.

Most public servers, including Cloudflare, Quad9, and Google, already support DNS over TLS, and many applications and devices already work with this option. Still, Paul Vixie, the inventor of DNS and CEO of Farsight Security, acknowledges the solution isn't "Web friendly" in the sense that there isn't a simple interface to enable it.

DNS over HTTPS is designed for the Web, as it throws all the data packets into the HTTPS stream with all other encrypted Web traffic. Since all packets look the same, anyone monitoring the standard HTTPS port won't be able to distinguish DNS queries from other Web traffic.

For the privacy minded, DNS over TLS isn't good enough, because anyone monitoring the network will know that any activity on Port 853 must be DNS related. Another downside is that it requires software developers and device makers to make changes so that their applications and hardware support the protocol.

DNS over HTTPS is more democratic, as anyone using a supported Web browser automatically gets encrypted DNS. And DNS over HTTPS stops all third parties from seeing which sites people are browsing.

That's exactly what privacy advocates want, but it's the opposite of what network administrators and security teams need. DNS over HTTPS treats privacy as absolute—but parental control applications, antivirus and security software, corporate firewalls, and other networking tools don't share that ethos.

Privacy vs. Security

Mozilla has said that DNS over HTTPS will be the default for Firefox users in the United States. To support it, Firefox automatically relays all DNS traffic to Cloudflare—bypassing all network-based filtering rules.

Google also turned on DNS over HTTPS for Chrome users, but in that case the browser defaults to DNS over HTTPS only if the user has a compatible service. Microsoft is trying to have it both ways, and plans to support DNS over HTTPS in Windows, but will allow Windows administrators to maintain some control.

DNS is a "reasonable place to restrict access" to bad entities, says Tim April, a principal architect at networking company Akamai. Network operators block host names used by malware or redirect users who try to access banned sites. Operators of public Wi-Fi networks modify DNS queries to load a network sign-on page for new users. DNS over HTTPS interferes with all of these use cases.

That's partly why Mozilla is not turning on DNS over HTTPS for Firefox users in the United Kingdom, as U.K. law requires Internet service providers to block access to illegal websites. Losing visibility over the network is dangerous, April adds.

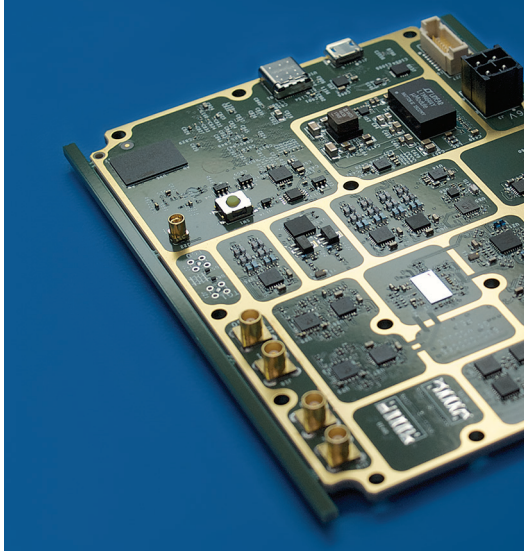
Privacy advocates believe that users should be in charge of their Web browsing, not ISPs. However, Mozilla's decision forces Firefox users to rely on Cloudflare.

Most users won't notice a difference when encrypted DNS becomes the default—a change that has already happened for Chrome and Firefox. But in this case, the price for increased privacy appears to be reduced security.

—FAHMIDA Y. RASHID

An extended version of this article appears in our Tech Talk blog.

POST YOUR COMMENTS AT
spectrum.ieee.org/dns-jan2020



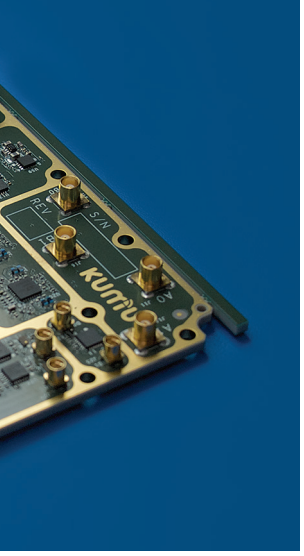
HELPING RADIOS HEAR THEMSELVES

Kumu Networks launches an analog module that cancels its own interference

IT'S A PROBLEM as old as radio: Radios cannot send and receive signals at the same time on the same frequency. Or to be more accurate, whenever they do, any signals they receive are drowned out by the strength of their transmissions.

Being able to send and receive signals simultaneously—a technique called full duplex—would make for far more efficient use of our wireless spectrum, and make radio interference less of a headache. As it stands, wireless communications generally rely on frequency- and time-division duplexing techniques, which separate the send and receive signals based on either the frequency used or when they occur, respectively, to avoid interference.

Kumu Networks, based in Sunnyvale, Calif., is now selling an analog self-interference canceller that the com-



LOUDMOUTH: Kumu Networks' new module addresses a classic problem—the signals a radio transmits are far more powerful than those it receives.

KUMU NETWORKS

pany says can be easily installed in most any wireless system. The device is a plug-and-play component that cancels out the noise of a transmitter so that a radio can hear much quieter incoming signals. It's not true full duplex, but it tackles one of radio's biggest problems: Transmitted signals are much more powerful than received signals.

"A transmitter signal is almost a trillion times more powerful than a receiver signal," says Harish Krishnaswamy, an associate professor of electrical engineering at Columbia University, in New York City. That makes it extra hard to filter out the noise, he adds.

Krishnaswamy says that in order to cancel signals with precision, you have to do it in steps. One step might involve performing some cancellation within the antenna itself. More cancellation techniques can be developed in chips and in digital layers.

While it may be theoretically possible, Krishnaswamy notes that reliably reaching that mark has proven difficult, even for engineers in the lab. Out in the world, a radio's environment is constantly changing. How a radio hears reflections and echoes of its own transmissions changes as well, and so cancellers must adapt to precisely filter out extraneous signals.

Kumu's K6 Canceller Co-Site Interference Mitigation Module (the new canceller's official name) is strictly an analog approach. Joel Brand, the vice president of product management at Kumu, says the module can achieve 50 decibels of cancellation. Put in terms of a power ratio, that means it cancels the transmitted signal by a factor of 100,000. That's still a far cry from what would be required to fully cancel the transmitted signal, but it's enough to help a radio hear signals more easily while transmitting.

Kumu's module cancels a radio's own transmissions by using analog components tuned to emit signals that are the inverse of the transmitted signals. The signal inversion allows the module to cancel out the transmitted signal and ensure that other signals the radio is listening for make it through.

Despite its limitations, Brand says there's plenty of interest in a canceller of this caliber. One example he gives is an application in defense. Radio jammers are common tools, but with self-interference cancellation, they can ignore their own jamming signal to continue listening for other radios that are trying to broadcast. Another area where Brand says Kumu's technology has received some interest is in aerospace, with one customer launching modules into space on satellites.

Kumu also develops digital cancellation techniques that can work in tandem with analog gear like its K6 canceller. However, according to Brand, digital cancellations tend to be highly bespoke. Performing them often means "cleaning" the signal after the radio has received it, which requires a deep knowledge of the radio systems involved.

Analog cancellation simply requires tuning the components to filter out the transmitted signal. And because of that simplicity, Kumu's module may well find its place in noisy wireless environments such as the home—where digital assistants like Alexa and smart home devices have already moved in.

—MICHAEL KOZIOL

POST YOUR COMMENTS AT
spectrum.ieee.org/interference-jan2020