Deep packet inspection meets 'Net neutrality, CALEA

By Nate Anderson | Last updated July 25, 2007 11:10 PM

Snooping for the feds: CALEA compliance

That's doubly true when it comes to doing user surveillance, since DPI gear makes it simple to collect and offload any user's entire datastream. ISPs are required to possess this capability under the Communications Assistance to Law Enforcement Act (CALEA), which started life as an update to traditional wiretapping laws. It has now been extended to VoIP operators and ISPs, who need a way to grab, archive, and submit to law enforcement any wiretap information requested in a warrant.

Much DPI gear is also CALEA-compliant. The boxes generally contain an "aux" port that can spit out a real-time copy of any required information: all traffic from a specific IP address, e-mail, Internet phone calls, URLs. The rules are simply programmed into the box's GUI and bam!—instant surveillance.

Full CALEA compliance can be a lot of work. It involves having someone available at all times to respond to any warrants that come in, someone who can set up and implement the correct rules, and more gear that can take the data and format it according to federal specifications, then make it available to the government. Many network operators don't want anything to do with this, so they simply install the DPI gear that makes it possible and contract out all the support and data formatting issues to another company, referred to as a "trusted third party" (TTP).

These TTPs handle all the grunt work; if given permission, they can even add the necessary surveillance rules to the DPI box remotely. Data from the user in question then flows from the ISP network to the TTP network, where it is passed along to the Feds. For this sort of logging to be most effective, DPI equipment needs to be installed near the edge of the network or as part of a gateway in order to ensure that both incoming and outgoing communications can be logged. It's extremely common for traffic between two places on the Internet to flow over different paths in each direction, so a box placed incorrectly can't observe both sides of the conversation, which is often necessary to really know what's going on.

Real-time monitoring is great, but what happens when you need to investigate a crime after it's happened? Plenty of information can also be logged to disk so that it can be accessed after the fact and used in these kinds of investigations. Storage needs to be thought out carefully, though; logging unfiltered traffic from a single gigabit Ethernet link can generate up to 10 terabytes a day, in *each* direction.

Procera touts the story of LP Broadband, a small Colorado ISP that serves rural customers. LP Broadband was using a PL7600 DPI box with an optional statistics server, which logs far more traffic details than routine monitoring software. When an LP customer found that a business server had been compromised by hackers one night, they went to the authorities and obtained a court order that directed LP to turn over relevant records from the event.

The company was able to isolate the hacker's IP address and identified the time and duration of the hacking session; if the customer wanted, the Procera gear could simply block all further access from that particular IP address.

Coming soon to an ISP near you

DPI gear can be expensive, especially the kind that can simultaneously monitor hundreds of thousands of connections. But bandwidth isn't cheap, either, and disgruntled customers equal lost revenue. Blocking viruses, DDoS attacks, and hacking traffic on a network can also save bandwidth, user frustration, and tech support time. Both Ellacoya and Procera claim that their products pay for themselves within nine months (Ellacoya) or three to twelve months (Procera).

The rise of "lawful intercept" (CALEA) requirements and the growth of online video (both P2P and over HTTP) are making monitoring and shaping increasingly important to ISPs. Because of the firestorm surrounding network neutrality in the US, ISPs here tend to take a cautious approach to using this equipment, but it's far more common overseas.

BT, for instance, recent became Ellacoya's single largest customer, using its gear to support more than 3 million broadband subscribers. According to BT, deep packet inspection enables them to better monitor their network, but it also allows them to apply QoS to two important services. VoIP, to be useful, needs to move quickly, so BT gives it priority on the network. BT also runs its own IPTV system, with the data apparently flowing over the same network as user data. To prevent distortion in the TV signal whenever half the country decides to download an episode of *Little Britain* using P2P, BT uses QoS to make sure a fixed amount of bandwidth is always available to IPTV.

As services like voice and TV continue their migration onto IP networks, DPI gear will only grow in importance. Is that a bad thing? It certainly doesn't have to be, but the time to debate the proper limits of shaping, blocking, and spying is now, before they become ubiquitous features of the ISP landscape.