GlobalResearch
Center for Research on Globalization

Inside the Secret Room at the NSA: The Ultimate Net Monitoring Tool

By Robert Poe
Global Research, May 18, 2006
Wired News 18 May 2006
Region: USA

The equipment that technician Mark Klein learned was installed in the National Security Agency's "secret room" inside AT&T's San Francisco switching office isn't some sinister Big Brother box designed solely to help governments eavesdrop on citizens' internet communications.

Rather, it's a powerful commercial network-analysis product with all sorts of valuable uses for network operators. It just happens to be capable of doing things that make it one of the best internet spy tools around.

"Anything that comes through (an internet protocol network), we can record," says Steve Bannerman, marketing vice president of Narus, a Mountain View, California, company. "We can reconstruct all of their e-mails along with attachments, see what web pages they clicked on, we can reconstruct their (voice over internet protocol) calls."

Inside the Secret Room

Courtroom Clash! A federal judge refuses to give AT&T back its internal documents, but orders the EFF not to give them out.

Whistle-blower's Precognition Years before the NSA's warrantless surveillance program made national headlines, then-AT&T technician Mark Klein suspected his company was colluding with the government to spy on Americans.

Exhibit A? Former AT&T technician Mark Klein offers a firsthand account of his alleged discovery of a secret room routing American internet traffic straight to the NSA — and provides documents he says proves his case.

The Ultimate Net Monitoring Tool A little-known company called Narus makes the packet-inspection technology said to be the basis of the NSA's internet surveillance. Here's how it works.

Plus: Daily updates from 27B Stroke 6, the Wired News security and privacy blog Narus' product, the Semantic Traffic Analyzer, is a software application that runs on standard IBM or Dell servers using the Linux operating system. It's renowned within certain circles for its ability to inspect traffic in real time on high-bandwidth pipes, identifying packets of interest as they race by at up to 10 Gbps.

Internet companies can install the analyzers at every entrance and exit point of their

networks, at their “cores” or centers, or both. The analyzers communicate with centralized “logic servers” running specialized applications. The combination can keep track of, analyze and record nearly every form of internet communication, whether e-mail, instant message, video streams or VOIP phone calls that cross the network.

Brasil Telecom and several other Brazilian phone companies are using Narus products to charge each other for VOIP calls they send over one another’s IP networks. Internet companies in China and the Middle East use them to block VOIP calls altogether.

But even before the product’s alleged role in the NSA’s operations emerged, its potential as a surveillance tool was not lost on corporate America.

In December, VeriSign, also of Mountain View, chose Narus’ product as the backbone of its lawful-intercept-outsourcing service, which helps network operators comply with court-authorized surveillance orders from law enforcement agencies. A special Narus lawful-intercept application does this spying with ease, sorting through torrents of IP traffic to pick out specific messages based on a targeted e-mail address, IP address or, in the case of VOIP, phone number.

“We needed their fast packet-detection and inspection capability,” says VeriSign Vice President Raj Puri. “They do it with specialized software that can isolate packets for a specific target.”

Narus has little control over how its products are used after they’re sold. For example, although its lawful-intercept application has a sophisticated system for making sure the surveillance complies with the terms of a warrant, it’s up to the operator whether to type those terms into the system, says Bannerman.

That legal eavesdropping application was launched in February 2005, well after whistle-blower Klein allegedly learned that AT&T was installing Narus boxes in secure, NSA-controlled rooms in switching centers around the country. But that doesn’t mean the government couldn’t write its own code to do the dirty work. Narus even offers software-development kits to customers.

“Our product is designed to comply (with) all of the laws in all of the countries we ship to,” says Bannerman. “Many of our customers have built their own applications. We have no idea what they do.”

Articles by: Robert Poe