Extrait du Spyworld Actu

http://mail.spyworld.fr/spip.php?article5459

Point, Click ... Eavesdrop : How the FBI Wiretap Net Operates (EN)

- Renseignement - International -

Date de mise en ligne : jeudi 30 août 2007

Spyworld Actu

The FBI has quietly built a sophisticated, point-and-click surveillance system that performs instant wiretaps on almost any communications device, according to nearly a thousand pages of restricted documents newly released under the Freedom of Information Act.

The surveillance system, called DCSNet, for Digital Collection System Network, connects FBI wiretapping rooms to switches controlled by traditional land-line operators, internet-telephony providers and cellular companies. It is far more intricately woven into the nation's telecom infrastructure than observers suspected.

It's a "comprehensive wiretap system that intercepts wire-line phones, cellular phones, SMS and push-to-talk systems," says Steven Bellovin, a Columbia University computer science professor and longtime surveillance expert.

DCSNet is a suite of software that collects, sifts and stores phone numbers, phone calls and text messages. The system directly connects FBI wiretapping outposts around the country to a far-reaching private communications network.

Many of the details of the system and its full capabilities were redacted from the [documents](#) acquired by the Electronic Frontier Foundation, but they show that DCSNet includes at least three collection components, each running on Windows-based computers.

The $10 million DCS-3000 client, also known as Red Hook, handles pen-registers and trap-and-traces, a type of surveillance that collects signaling information â€" primarily the numbers dialed from a telephone â€" but no communications content. (Pen registers record outgoing calls ; trap-and-traces record incoming calls.)

DCS-6000, known as Digital Storm, captures and collects the content of phone calls and text messages for full wiretap orders.

A third, classified system, called DCS-5000, is used for wiretaps targeting spies or terrorists.

What DCSNet Can Do

Together, the surveillance systems let FBI agents play back recordings even as they are being captured (like TiVo), create master wiretap files, send digital recordings to translators, track the rough location of targets in real time using cell-tower information, and even stream intercepts outward to mobile surveillance vans.

FBI wiretapping rooms in field offices and undercover locations around the country are connected through a private, encrypted backbone that is separated from the internet. Sprint runs it on the government's behalf.

The network allows an FBI agent in New York, for example, to remotely set up a wiretap on a cell phone based in Sacramento, California, and immediately learn the phone's location, then begin receiving conversations, text messages and voicemail pass codes in New York. With a few keystrokes, the agent can route the recordings to language specialists for translation.

The numbers dialed are automatically sent to FBI analysts trained to interpret phone-call patterns, and are transferred nightly, by external storage devices, to the bureau's Telephone Application Database, where they're subjected to a type of data mining called link analysis.

FBI endpoints on DCSNet have swelled over the years, from 20 "central monitoring plants" at the program's inception, to 57 in 2005, according to undated pages in the released documents. By 2002, those endpoints connected to more than 350 switches.

Today, most carriers maintain their own central hub, called a "mediation switch," that's networked to all the individual switches owned by that carrier, according to the FBI. The FBI's DCS software links to those mediation switches over the internet, likely using an encrypted VPN. Some carriers run the mediation switch themselves, while others pay companies like VeriSign to handle the whole wiretapping process for them.

The numerical scope of DCSNet surveillance is still guarded. But we do know that as telecoms have become more wiretap-friendly, the number of criminal wiretaps alone has climbed from 1,150 in 1996 to 1,839 in 2006. That's a 60 percent jump. And in 2005, 92 percent of those criminal wiretaps targeted cell phones, according to a report published last year.

These figures include both state and federal wiretaps, and do not include antiterrorism wiretaps, which dramatically expanded after 9/11. They also don't count the DCS-3000's collection of incoming and outgoing phone numbers dialed. Far more common than full-blown wiretaps, this level of surveillance requires only that investigators certify that the phone numbers are relevant to an investigation.

The Justice Department reports the number of pen registers to Congress annually, but those numbers aren't public. According to the last figures leaked to the Electronic Privacy Information Center, judges signed 4,886 pen register orders in 1998, along with 4,621 time extensions.

CALEA Switches Rules on Switches

The law that makes the FBI's surveillance network possible had its genesis in the Clinton administration. In the 1990s, the Justice Department began complaining to Congress that digital technology, cellular phones and features like call forwarding would make it difficult for investigators to continue to conduct wiretaps. Congress responded by passing the Communications Assistance for Law Enforcement Act, or CALEA, in 1994, mandating backdoors in U.S. telephone switches.

CALEA requires telecommunications companies to install only telephone-switching equipment that meets detailed wiretapping standards. Prior to CALEA, the FBI would get a court order for a wiretap and present it to a phone company, which would then create a physical tap of the phone system.

With new CALEA-compliant digital switches, the FBI now logs directly into the telecom's network. Once a court order has been sent to a carrier and the carrier turns on the wiretap, the communications data on a surveillance target streams into the FBI's computers in real time.

The Electronic Frontier Foundation requested documents on the system under the Freedom of Information Act, and successfully sued the Justice Department in October 2006.

In May, a federal judge ordered the FBI to provide relevant documents to the EFF every month until it has satisfied the FOIA request.

"So little has been known up until now about how DCS works," says EFF attorney Marcia Hofmann. "This is why it's so important for FOIA requesters to file lawsuits for information they really want."

Special Agent Anthony DiClemente, chief of the Data Acquisition and Intercept Section of the FBI's Operational Technology Division, said the DCS was originally intended in 1997 to be a temporary solution, but has grown into a full-featured CALEA-collection software suite.

"CALEA revolutionizes how law enforcement gets intercept information," DiClemente told Wired News. "Before CALEA, it was a rudimentary system that mimicked Ma Bell."

Privacy groups and security experts have protested CALEA design mandates from the start, but that didn't stop federal regulators from recently expanding the law's reach to force broadband internet service providers and some voice-over-internet companies, such as Vonage, to similarly retrofit their networks for government surveillance.

New Technologies

Meanwhile, the FBI's efforts to keep up with the current communications explosion is never-ending, according to DiClemente.

The released documents suggest that the FBI's wiretapping engineers are struggling with peer-to-peer telephony provider Skype, which offers no central location to wiretap, and with innovations like caller-ID spoofing and phone-number portability.

But DCSNet seems to have kept pace with at least some new technologies, such as cell-phone push-to-talk features and most VOIP internet telephony.

"It is fair to say we can do push-to-talk," DiClemente says. "All of the carriers are living up to their responsibilities under CALEA."

Matt Blaze, a security researcher at the University of Pennsylvania who helped assess the FBI's now-retired Carnivore internet-wiretapping application in 2000, was surprised to see that DCSNet seems equipped to handle such modern communications tools. The FBI has been complaining for years that it couldn't tap these services.

The redacted documentation left Blaze with many questions, however. In particular, he said it's unclear what role the carriers have in opening up a tap, and how that process is secured.

"The real question is the switch architecture on cell networks," said Blaze. "What's the carrier side look like ?"

Randy Cadenhead, the privacy counsel for Cox Communications, which offers VOIP phone service and internet access, says the FBI has no independent access to his company's switches.

"Nothing ever gets connected or disconnected until I say so, based upon a court order in our hands," Cadenhead says. "We run the interception process off of my desk, and we track them coming in. We give instructions to relevant field people who allow for interconnection and to make verbal connections with technical representatives at the FBI."

The nation's largest cell-phone providers â€" whose customers are targeted in the majority of wiretaps â€" were less forthcoming. AT&T politely declined to comment, while Sprint, T-Mobile and Verizon simply ignored requests for comment.

Agent DiClemente, however, seconded Cadenhead's description.

"The carriers have complete control. That's consistent with CALEA," DiClemente said. "The carriers have legal teams to read the order, and they have procedures in place to review the court orders, and they also verify the information and that the target is one of their subscribers."

Cost

Despite its ease of use, the new technology is proving more expensive than a traditional wiretap. Telecoms charge the government an average of $2,200 for a 30-day CALEA wiretap, while a traditional intercept costs only $250, according to the Justice Department inspector general. A federal wiretap order in 2006 cost taxpayers $67,000 on average, according to the most recent U.S. Court wiretap report.

What's more, under CALEA, the government had to pay to make pre-1995 phone switches wiretap-friendly. The FBI has spent almost $500 million on that effort, but many traditional wire-line switches still aren't compliant.

Processing all the phone calls sucked in by DCSNet is also costly. At the backend of the data collection, the conversations and phone numbers are transferred to the FBI's Electronic Surveillance Data Management System, an Oracle SQL database that's seen a 62 percent growth in wiretap volume over the last three years â€" and more than 3,000 percent growth in digital files like e-mail. Through 2007, the FBI has spent $39 million on the system, which indexes and analyzes data for agents, translators and intelligence analysts.

Security Flaws

To security experts, though, the biggest concern over DCSNet isn't the cost : It's the possibility that push-button wiretapping opens new security holes in the telecommunications network.

More than 100 government officials in Greece learned in 2005 that their cell phones had been bugged, after an unknown hacker exploited CALEA-like functionality in wireless-carrier Vodafone's network. The infiltrator used the switches' wiretap-management software to send copies of officials' phone calls and text messages to other phones, while simultaneously hiding the taps from auditing software.

The FBI's DiClemente says DCSNet has never suffered a similar breach, so far as he knows.

"I know of no issue of compromise, internal or external," DiClemente says. He says the system's security is more than adequate, in part because the wiretaps still "require the assistance of a provider." The FBI also uses physical-security measures to control access to DCSNet end points, and has erected firewalls and other measures to render them "sufficiently isolated," according to DiClemente.

But the documents show that an internal 2003 audit uncovered numerous security vulnerabilities in DCSNet â€" many of which mirror problems unearthed in the bureau's Carnivore application years earlier.

In particular, the DCS-3000 machines lacked adequate logging, had insufficient password management, were missing antivirus software, allowed unlimited numbers of incorrect passwords without locking the machine, and used shared logins rather than individual accounts.

The system also required that DCS-3000's user accounts have administrative privileges in Windows, which would allow a hacker who got into the machine to gain complete control.

Columbia's Bellovin says the flaws are appalling and show that the FBI fails to appreciate the risk from insiders.

"The underlying problem isn't so much the weaknesses here, as the FBI attitude towards security," he says. The FBI assumes "the threat is from the outside, not the inside," he adds, and it believes that "to the extent that inside threats exist, they can be controlled by process rather than technology."

Bellovin says any wiretap system faces a slew of risks, such as surveillance targets discovering a tap, or an outsider or corrupt insider setting up unauthorized taps. Moreover, the architectural changes to accommodate easy surveillance on phone switches and the internet can introduce new security and privacy holes.

"Any time something is tappable there is a risk," Bellovin says. "I'm not saying, 'Don't do wiretaps,' but when you start designing a system to be wiretappable, you start to create a new vulnerability. A wiretap is, by definition, a vulnerability from the point of the third party. The question is, can you control it ?"
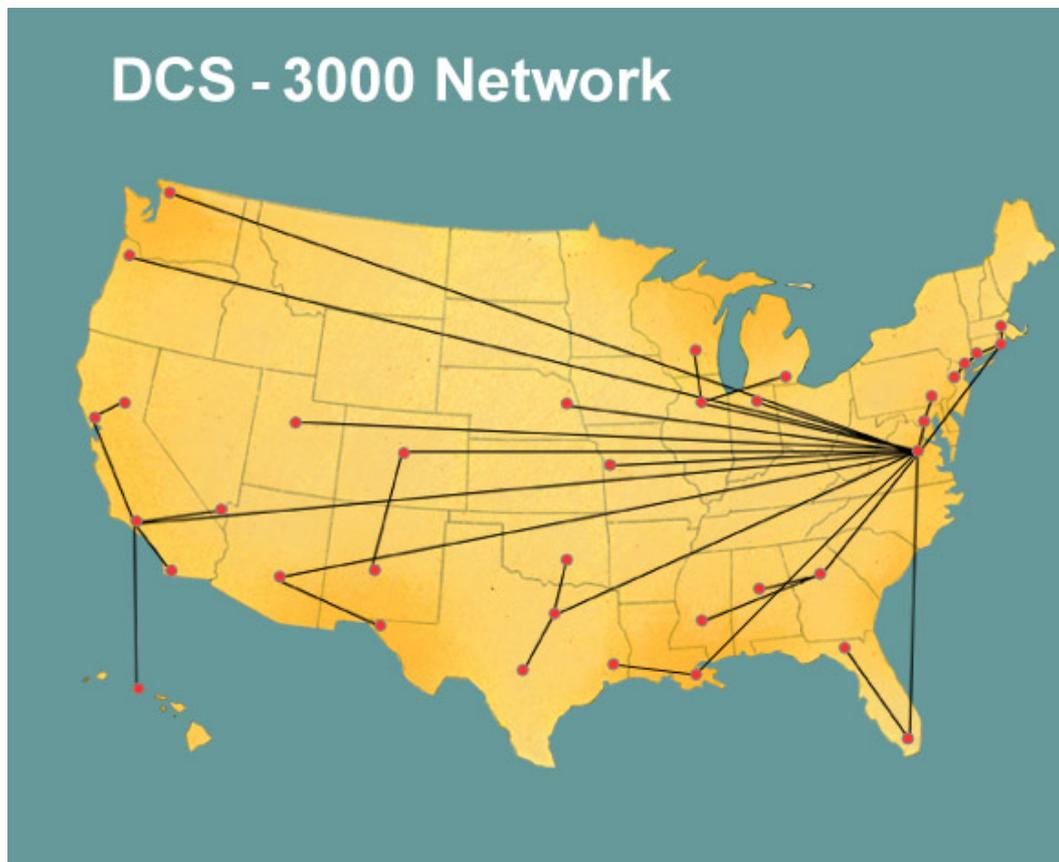
DCS 3000 Network Map

The FBI's private, encrypted backbone, DCSNet, connects 37 FBI field offices, according to some documents. Other documents suggest the network now extends to 52 field offices, including locations in Alaska and Puerto Rico. This enhanced image is based on black-and-white FBI documents.
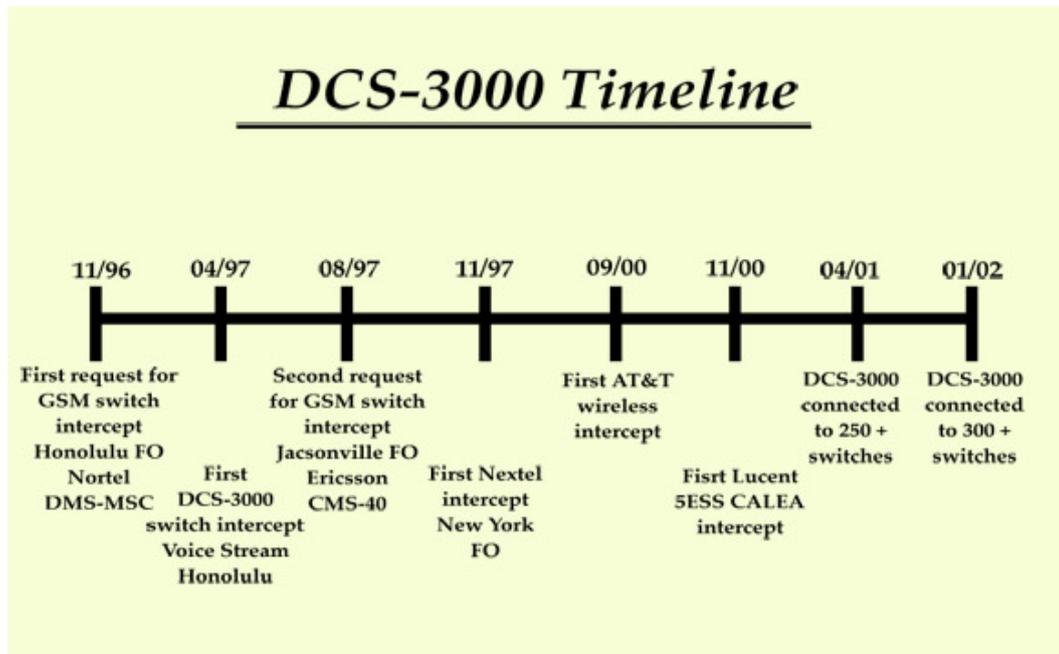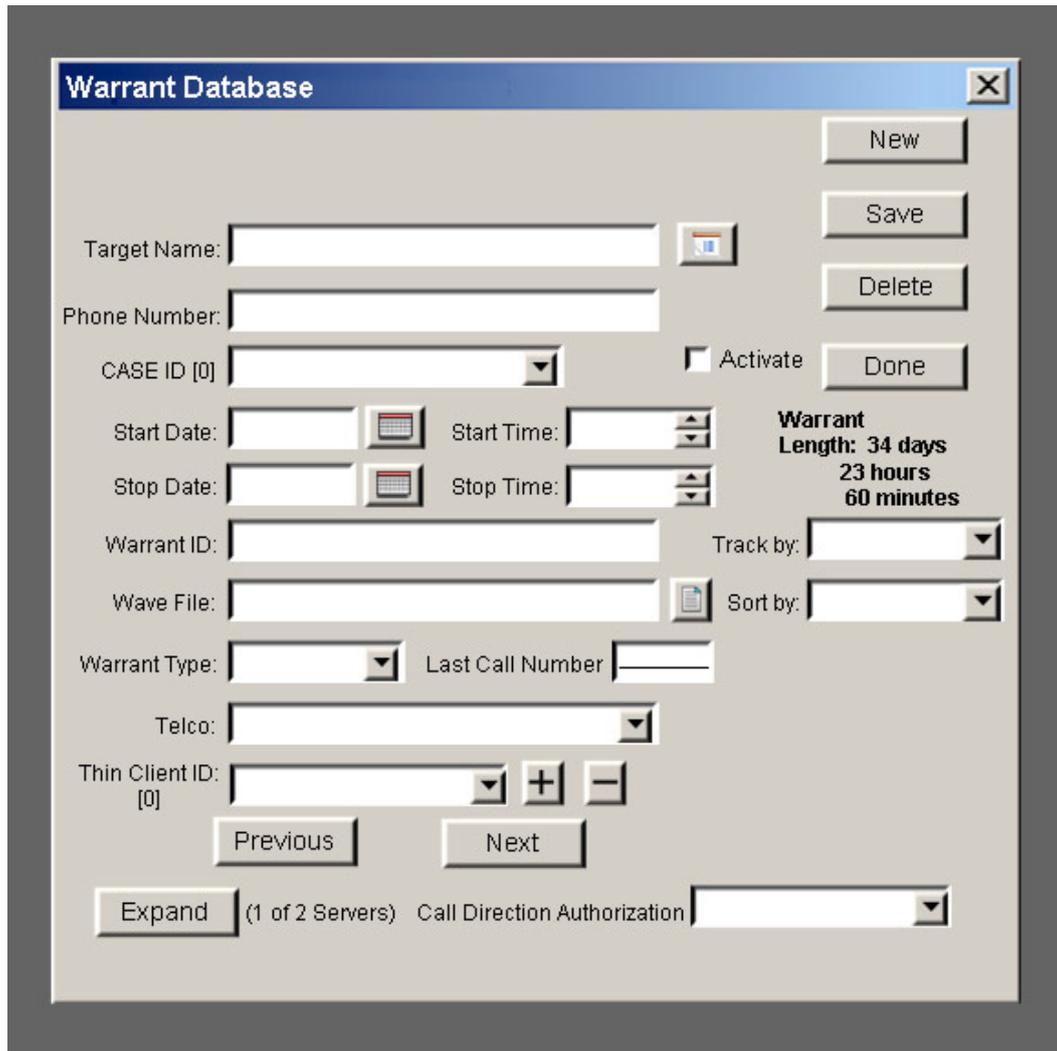
DCS-3000 Timeline

The growth of DCS-3000 from a temporary solution for getting call information from wireless networks is shown becoming a full-featured player in the FBI's growing surveillance architecture. This enhanced image is based on black-and-white FBI documents.

DCS Logo

An owl, an animal known for its exceptional vision dominates the logo of the Telecommunications Intercept and Collection Technology Unit, or TICTU, which developed the DCS-3000. This enhanced image is based on black-and-white FBI documents.

DCS Warrant Database

FBI employees with Top Secret clearances begin and end collection of call information from targets using a typical Windows program UI. Here, employees enter the court-order information, along with the case number and the start and stop times for the warrant. This enhanced image is based on black-and-white FBI documents.

Post-scriptum :

http://www.wired.com/politics/secur...