NSA datamining pushes tech envelope

May 25 2006

Amid the political firestorm surrounding the National Security Agency's use of wiretapping for domestic phone calls, inquiries as to technology as well as legality have become prevalent.

Key to most of this is the question as to whether the National Security Agency has overstepped its bounds. Founded in 1952 as a component of the Department of Defense and primarily responsible for the collection and analysis of foreign communications as well as the security of government communications, the NSA has typically drawn a lower profile than the CIA despite its influential role.

While its duties have grown, the NSA's charter has remained that the organization collect information that constitutes "foreign intelligence or counterintelligence" and forbids domestic work -- "acquiring information concerning the domestic activities of United States persons."

When domestic work needed to be performed, the NSA would traditionally hand it off to agencies such as the Federal Bureau of Investigation, which were specifically chartered and tasked towards a domestic agenda.

As needs for surveillance grew, so did technologies. Home to the largest contingent of mathematicians and supercomputers in any government agency, with a historically larger budget than the CIA, the NSA has developed its own suite of surveillance technologies.

ThinThread, a technology developed in the late '90s for wiretapping and providing sophisticated analysis of large amounts of resulting data was one of these projects. Designed to both collect data as well as encrypt sensitive or private information for later analysis, the program operated within legal and privacy-based boundaries via that encryption.

After the Sept. 11, 2001, attacks, policy changed and the ThinThread project evolved into a system known as Trailblazer. Designed to gather similar data but without the encryption feature built into the ThinThread technology to provide privacy aspects, the Trailblazer technology and the resulting phone-tap efforts that have grown from this have been deployed as a critical terrorist-locating tool and defended as "critical to our national security" via the Bush administration.

In a report recently published by Wired News, former AT&T technician Mark Klein revealed that in 2003 AT&T had constructed "secret rooms" hidden deep within its corporate offices in various major cities filled with surveillance equipment designed to monitor Internet traffic and analyze data as it passed through the network. The project, rooted into the Department of Defense's Total Information Awareness program, which has been criticized as allowing the department access to widespread Internet data without the need for a search warrant. The Total Information Awareness effort has been defended by representatives of the Defense Advanced Research Projects Agency as assertions have been made that they were only conducting research using "artificial synthetic data" and no privacy violations had occurred.

Funding for the Total Information Awareness project was scaled back after the controversy was made public and a congressional investigation took place.

To date, AT&T, BellSouth and Verizon have become involved in a class-action lawsuit that alleges the companies illegally participated in the

NSA's domestic surveillance program. The complaint, which has been filed through the Manhattan District Court, demands the companies pay $200 billion in fines to their 200 million customers or a minimum of $1,000 per client in damages.

Verizon and BellSouth have denied these charges, going as far as to deny that the NSA ever contacted them for access to call data at any point. AT&T has neither confirmed nor denied the charges.

As a counterpoint, Qwest Communications has issued a statement claiming the NSA approached it for access to call data, but the firm refused to participate in the program given that it appeared to violate privacy laws.

The National Security Agency has stood its ground in recent days, claiming it doesn't listen to the content of domestic calls but simply use data such as numbers, times and locations to help find patterns that may suggest terrorist activities. President Bush has furthered this by stating that the government doesn't listen to domestic calls without a court order.

Under the Foreign Intelligence Security Act, the government must obtain a court order from a secret FISA court to be able to enact a domestic phone tap.

"Given the nature of the work we do, it would be irresponsible to comment on actual or alleged operational issues; therefore, we have no information to provide," said NSA Spokesperson Don Weber. "However, it is important to note that NSA takes its legal responsibilities seriously and operates within the law."

"We haven't heard of this happening before," said Rebecca Jeschke, media coordinator for the Electronic Frontier Foundation, a technology-

centered advocacy group. "You've got this massive violation of the law as well as consumers' privacy and it needs to stop."

The Electronic Frontier Foundation has currently begun a lawsuit against AT&T for its role in the alleged domestic wiretapping effort. The next step of the case will take place June 23, when movements to dismiss the case will be heard.

"The phone companies were turning over call records, not exactly the contents of the calls. ... That information isn't illegal, but it is illegal for the phone companies to hand it over," said Clay Shields, associate professor of computer science at Georgetown University. Shields then went on to comment that without the ThinThread protocol's encryption scheme, the NSA is searching through a much larger data pool, which can lead to additional false positives.

"There are thousands of people whose patterns may look like a terrorist but aren't, because it's time consuming, cumbersome and expensive to track down false positives. The computer's casting too wide a net with how they're using the data they have," said Shields. "Now it's people who are just one or two steps away from terror suspects are being considered suspects. Just because you go to the same mosque as a terror suspect doesn't mean you're deserving of scrutiny."

Shields commented that the NSA's approach seemed reminiscent of applying technology to a human problem. He also added that the government can also obtain a retroactive FISA warrant up to 72 hours after the fact, which serves to invalidate the argument for expediency made by the Bush administration to defend the wiretapping efforts.

"When you spin up machinery this powerful, there's an irresistible temptation to apply it to other things," said Philip Zimmermann, creator of the PGP encryption protocol. "Political conditions change. By having

it be so broad, it can mask who their true targets are."

"If the question is if it's effective, I believe the answer is yes. If the question is if it's appropriate for our democracy, I believe the answer is no," said Zimmermann. "The machinery can be repurposed for any expedient political persecutions you wish to purpose."

Zimmermann then went on to mention that use of encrypted Voice over Internet Protocol clients, many of them available for free download over the Internet, could help the average phone and Internet user retain their privacy should this be a concern.

Copyright 2006 by United Press International

Citation: NSA datamining pushes tech envelope (2006, May 25) retrieved 3 May 2024 from https://phys.org/news/2006-05-nsa-datamining-tech-envelope.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.