

The Christian Science Monitor - CSMonitor.com

What is XKeyscore, and can it 'eavesdrop on everyone, everywhere'? (+video)

XKeyscore is apparently a tool the NSA uses to sift through massive amounts of data. Critics say it allows the NSA to dip into people's 'most private thoughts' – a claim key lawmakers reject.



This photo shows an aerial view of the NSA's Utah Data Center in Bluffdale, Utah. The long, squat buildings span 1.5 million square feet, and are filled with super-powered computers designed to store massive amounts of information gathered secretly from phone calls and e-mails.

(Rick Bowmer/AP/File)

By Mark Clayton, Staff writer / August 1, 2013 at 9:38 pm EDT

Top-secret documents leaked to The Guardian newspaper have set off a new round of debate over National Security Agency surveillance of electronic communications, with some cyber experts saying the trove reveals new and more dangerous means of digital snooping, while some members of Congress suggested that interpretation was incorrect.

The NSA's collection of "metadata" – basic call logs of phone numbers, time of the call, and duration of calls – is now well-known, with the Senate holding a hearing on the subject this week. But the tools discussed in the new Guardian documents apparently go beyond mere collection, allowing the agency to sift through the

haystack of digital global communications to find the needle of terrorist activity.

The concern is that the capabilities could be misused or misdirected at innocents. In revealing the NSA metadata program, leaker Edward Snowden told the Guardian in June: "I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal e-mail."

Rep. Mike Rogers (R) of Michigan, chairman of the House intelligence committee, rejected that claim. "It's impossible for him to do what he was saying he could do."

But the new Guardian leak appears to indicate something at least close to such capability. The program, called XKeyscore, is the "widest-reaching" Internet surveillance system, according to one of several analyst "training" documents, which included a 32-slide presentation leaked to The Guardian. An analyst has to enter only an individual e-mail address – along with a "justification" inserted into another field on the screen – to get a trove of personal e-mail sorted by time period, say analysts who reviewed the slides for the Monitor.

The program can also apparently determine which computers visited a website and when, as well as searching chats, usernames, buddy lists, and cookies. One slide in an XKeyscore document features corporate logos of a number of familiar online social media companies, saying the program lets analysts see "nearly everything a typical user does on the Internet."

Another slide illustrates how an analyst can use the program to search "within bodies of e-mail, WebPages and documents." Analysts using XKeyscore can also use a NSA tool called DNI Presenter "to read the content of Facebook chats or private messages," according to the Guardian article.

"What stands out about XKeyscore is the ease with which an NSA analyst can dip into people's lives, their most private thoughts," says James Bamford, an NSA critic who has written several books detailing the agency's inner workings.

In addition, the amount of information that XKeyscore searches and stores is massive. During a 30-day period in 2012, it collected and stored about 41 billion total records, one slide document asserts. That is a testament to the NSA's growing capability to collect data, leading to the need for a huge new data storage facility in Bluffdale, Utah, which should begin operations this fall.

"I don't think they have the capacity to figure out everything they want to keep, so they're storing it all, so they can go back and get it," says William Binney, a former NSA mathematician turned whistle-blower who worked for the agency for four decades.

The implications of having all that data to search with a powerful tool like XKeyscore are large, Mr. Bamford says.

“You just fill in an e-mail address or whatever, then how much data you want – a week, a month – then up pops all my e-mail,” he says. “It’s basically what [author George] Orwell warned about. This agency now has the capability, basically, to eavesdrop on everyone, everywhere. And that’s basically what’s happening.”

Such comments are drawing exasperated responses from government officials and lawmakers with oversight responsibilities.

“As we’ve explained, and the intelligence community has explained, allegations of widespread, unchecked analyst access to NSA collection data are false,” White House spokesman Jay Carney said Thursday.

Testifying before Congress, NSA officials have said they have “minimization procedures” to properly handle material on Americans that is caught up in the electronic search.

“Look, it’s just not possible for analysts to just go tromping around through people’s e-mails,” says James Lewis, a cybersecurity expert at the Center for Strategic and International Studies in Washington. “The idea that you have people just sitting there and reading e-mails is just silly. There are minimization procedures and audits and other mechanisms that prevent this. Yes, they collect a lot of data, but there has to be some reason and authorization to read it.”

NSA officials and lawmakers were quick to throw cold water on the leaked document and the Guardian report.

“Allegations of widespread, unchecked analyst access to NSA collection data are simply not true,” the NSA said in statement Thursday. “Access to XKeyscore, as well as all of NSA’s analytic tools, is limited to only those personnel who require access for their assigned tasks.”

Representative Rogers and Rep. Dutch Ruppersberger of Maryland, the top Democrat on the House intelligence committee, joined a group of lawmakers meeting with President Obama Thursday on the issue.

“The latest in the parade of classified leaks published today is without context and provides a completely inaccurate picture of the program,” the two congressmen said in a joint statement.

Officials have also noted the program’s success at finding terrorists. One of the new leaked documents, the 32-slide presentation, asserts that by 2008, 300 terrorists had been captured using intelligence from Xkeyscore.

Still, the NSA and its backers in Washington remain under fire, with polls showing public concern over the surveillance programs growing. But to other experts who have been watching surveillance trends, the idea of global surveillance by the US and others is nothing new – even if it has now reached worrying levels, with the

leaked documents showing Xkeyscore sitting alongside other programs with operational code names like Marina, Pinwale, Trafficthief, about which little is known.

“Nothing I’ve seen so far that Edward Snowden has released is a surprise for people that work in the industry, even though I am concerned about it,” says Jonathan Logan, a network security consultant who co-authored a 2009 study on global digital espionage. “The good thing about this [Snowden] release is that we finally can point to an outside source confirming what we’ve been saying for the last 15 years.”

© The Christian Science Monitor. All Rights Reserved. Terms under which this service is provided to you. Privacy Policy.