Cryptography could add privacy protections to NSA phone surveillance

MIT Technology Review

Since several large-scale U.S. surveillance programs were revealed in documents leaked by Edward Snowden last summer, many companies and individuals have made an effort to make wider use of encryption. Now one Microsoft researcher says cryptography tools could also be used inside intelligence agencies to rein in surveillance, by making data stores and data searches more respectful of privacy and resistant to misuse.

Cryptography researcher Seny Kamara [1], who works at Microsoft's research lab in Redmond, Washington, has sketched out a design for such a system, called MetaCrypt. It would let intelligence analysts search phone records while protecting those records against leaks or unnecessary trawling. Kamara was inspired to develop MetaCrypt after reading about the NSA's phone records database, which stores details of all calls made in the last five years through major U.S. communications companies such as Verizon (see "NSA Phone-Record Tracking Troubles Privacy Scholars [2]").

MetaCrypt is a set of cryptographic protocols that could keep the information in such a database encrypted at all times. They would enforce various controls on how the information inside was used. For example, analysts would be limited to performing only certain types of search query, and the results of those queries would be the only data from a collection that they could decrypt.

With others at Microsoft, Kamara has been working for around a decade on ways to search encrypted data without having to ever decrypt it (see "Searching an Encrypted Cloud [3]"). MetaCrypt is an individual research project, not part of any wider Microsoft project, and the company declined to comment on Kamara's work. But he presented his design at the Financial Cryptography conference in Barbados last month (see slides [4]), and a technical paper is forthcoming.

Under the MetaCrypt design, phone records would be stored in a strongly encrypted form. Just as with the existing phone records database, agencies could search through records by providing a phone number of interest. They would get back records showing the calls made from that number and from the numbers called from that phone—a so-called "two hop" query. However, under Kamara's design the query numbers would be supplied to the data store in an encrypted form, preventing anyone else from discovering what was being looked for. The records that come back would themselves be encrypted, and would be meaningless to anyone who intercepted them on their way back to the analyst who made the query.

The MetaCrypt design also includes a way to ensure that only approved searches

are performed in the first place. Generating an encrypted search query that the data store will process requires that two analysts and at least one supervisor contribute their personal cryptographic keys. Another check is performed when it comes to decrypting the result that comes back.

Kamara's work only shows that it's possible to use existing encryption methods this way. Implementing MetaCrypt on a system handling large volumes of data would require significant extra work, and the end result might fall short of the performance considered practical by systems designers at a large company or government agency.

Still, Kamara's proposal comes at a time when the NSA's phone surveillance program is in flux. President Obama said in January that the agency should no longer hold a domestic phone records database and suggested a third party could do so instead (see "Obama Promises Reform of Bulk Phone Surveillance Program [5]"). Then, in March, the president said that the NSA would query records held by individual phone companies. However, that proposal must be approved by Congress, and for now the current database—and its five years of call records—remains in place.

Whatever form the new phone surveillance system ends up taking, ideas such as Kamara's are unlikely to ever gain much traction in the U.S. intelligence community, says William Binney, a former NSA analyst and cryptographer who has been a vocal critic of the agency since retiring in 2001.

Binney led design of a system called Thin Thread while working for the agency. It combined surveillance information from phone records and other sources, but also kept data on U.S. citizens encrypted unless a warrant had been secured. Binney says that second feature contributed to the program being canceled soon after a successful pilot. "It was seen as an impediment to them being able to do searches of any kind that they wanted," says Binney, despite the fact that the feature didn't interfere with the analysis the system was intended to be used for. "It was politically unacceptable."

Binney believes government access to large stores of domestic surveillance data, even if held by third parties, is unconstitutional. And he doesn't think that proposals like Kamara's would get a welcome reception today inside U.S. intelligence agencies, despite recent public attention to their activities. "It's a good idea," he says, "but it would still be unacceptable."

Links:
[1] http://research.microsoft.com/en-us/um/people/senyk/
[2] http://www.technologyreview.com/news/515861/nsa-surveillance-reflects-a-

broader-interpretation-of-the-patriot-act/
[3] http://www.technologyreview.com/news/416254/searching-an-encrypted-cloud/
[4] http://research.microsoft.com/en-us/um/people/senyk/slides/metacrypt.pdf
[5] http://www.technologyreview.com/news/523766/obama-promises-reform-of-bulk-phone-record-surveillance-program/