The Washington Post

Back to previous page

By cracking cellphone code, NSA has capacity for decoding private conversations

By Craig Timberg and Ashkan Soltani, Published: December 13

The cellphone encryption technology used most widely across the world can be easily defeated by the National Security Agency, an internal document shows, giving the agency the means to decode most of the billions of calls and texts that travel over public airwaves every day.

While the military and law enforcement agencies long have been able to hack into individual cellphones, the NSA's capability appears to be far more sweeping because of the agency's global signals collection operation. The agency's ability to crack encryption used by the majority of cellphones in the world offers it wide-ranging powers to listen in on private conversations.

U.S. law prohibits the NSA from collecting the content of conversations between Americans without a court order. But experts say that if the NSA has developed the capacity to easily decode encrypted cellphone conversations, then other nations likely can do the same through their own intelligence services, potentially to Americans' calls, as well.

Encryption experts have complained for years that the most commonly used technology, known as A5/1, is vulnerable and have urged providers to upgrade to newer systems that are much harder to crack. Most companies worldwide have not done so, even as controversy has intensified in recent months over NSA collection of cellphone traffic, including of such world leaders as German Chancellor Angela Merkel.

The extent of the NSA's collection of cellphone signals and its use of tools to decode encryption are not clear from a top-secret document provided by former contractor Edward Snowden. But it states that the agency "can process encrypted A5/1" even when the agency has not acquired an encryption key, which unscrambles communications so that they are readable.

Experts say the agency may also be able to decode newer forms of encryption, but only with a much heavier investment in time and computing power, making mass surveillance of cellphone conversations less practical.

"At that point, you can still listen to any [individual person's] phone call, but not everybody's," said Karsten Nohl, chief scientist at Security Research Labs in Berlin.

The vulnerability outlined in the NSA document concerns encryption developed in the 1980s but still used widely by cellphones that rely on technology called second-generation (2G) GSM. It is dominant in most of the world but less so in the wealthiest nations, including the United States, where newer networks such as 3G and 4G increasingly provide faster speeds and better encryption, industry officials say.

But even where such updated networks are available, they are not always used, because many phones often still rely on 2G networks to make or receive calls. More than 80 percent of cellphones worldwide use weak or no encryption for at least some of their calls, Nohl said. Hackers also can trick phones into using these

less-secure networks, even when better ones are available. When a phone indicates a 3G or 4G network, a voice call might actually be carried over an older frequency and susceptible to decoding by the NSA.

The document does not make clear if the encryption in another major cellphone technology — called CDMA and used by Verizon, Sprint and a small number of foreign companies — has been broken by the NSA as well. The document also does not specify whether the NSA can decode data flows from cellular devices, which typically are encrypted using different technology.

The NSA has repeatedly stressed that its data collection efforts are aimed at overseas targets, whose legal protections are much lower than U.S. citizens'. When questioned for this story, the agency issued a statement, saying: "Throughout history nations have used encryption to protect their secrets, and today terrorists, cyber criminals, human traffickers and others also use technology to hide their activities. The Intelligence Community tries to counter that in order to understand the intent of foreign adversaries and prevent them from bringing harm to Americans and allies."

German news magazine Der Spiegel reported in October that a listening station atop the U.S. Embassy in Berlin allowed the NSA to spy on Merkel's cellphone calls. It also reported that the NSA's Special Collection Service runs similar operations from 80 U.S. embassies and other government facilities worldwide. These revelations — and especially reports about eavesdropping on the calls of friendly foreign leaders — have caused serious diplomatic fallouts for the Obama administration.

Cellphone conversations long have been much easier to intercept than ones conducted on traditional telephones because the signals are broadcast through the air, making for easy collection. Police scanners and even some older televisions once were able to routinely pick up people talking on their cellphones, as a Florida couple did in 1996 when they recorded an overheard conversation involving then-House Speaker Newt Gingrich.

Digital transmission and encryption have become almost universally available in the United States, and they are now standard throughout much of the world. Governments typically dictate what kind of encryption technology, if any, can be deployed by cellphone service providers. As a result, cellular communications in some nations, including China, feature weak encryption or none at all.

A5/1 has been repeatedly cracked by researchers in demonstration projects for more than a decade.

The encryption technology "was designed 30 years ago, and you wouldn't expect a 30-year-old car to have the latest safety mechanisms," said David Wagner, a computer scientist at the University of California at Berkeley.

Collecting cellphone signals has become such a common tactic for intelligence, military and law enforcement work worldwide that several companies market devices specifically for that purpose.

Some are capable of mimicking cell towers to trick individual phones into directing all communications to the interception devices in a way that automatically defeats encryption. USA Today reported Monday that at least 25 police departments in the United States own such devices, the most popular of which go by the brand name Harris StingRay. Experts say they are in widespread use by governments overseas, as well.

Even more common, however, are what experts call "passive" collection devices, in which cell signals are secretly gathered by antennas that do not mimic cellphone towers or connect directly with individual phones. These systems collect signals that are then decoded in order for the content of the calls or texts to be understood by analysts.

Matthew Blaze, a University of Pennsylvania cryptology expert, said the weakness of A5/1 encryption is "a pretty sweeping, large vulnerability" that helps the NSA listen to cellphone calls overseas and likely also

allows foreign governments to listen to the calls of Americans.

"If the NSA knows how to do this, presumably other intelligence agencies, which may be more hostile to the United States, have discovered how to do this, too," he said.

Journalists Marc Ambinder and D.B. Grady reported in their 2013 book "Deep State: Inside the Government Secrecy Industry" that the FBI "has quietly removed from several Washington, D.C.- area cell phone towers, transmitters that fed all data to wire rooms at foreign embassies."

The FBI declined to comment on that report.

Upgrading an entire network to better encryption provides substantially more privacy for users. Nohl, the German cryptographer, said that breaking a newer form of encryption, called A5/3, requires 100,000 times more computing power than breaking A5/1. But upgrading entire networks is an expensive, time-consuming undertaking that likely would cause interruptions in service for some customers as individual phones would be forced to switch to the new technology.

Amid the uproar over NSA's eavesdropping on Merkel's phone, two of the leading German cellphone service providers have announced that they are adopting the newer, stronger A5/3 encryption for their 2G networks.

They "are now doing it after not doing so for 10 years," said Nohl, who long had urged such a move. "So, thank you, NSA."

One of those companies, Deutsche Telekom, is the majority shareholder of T-Mobile. T-Mobile said in a statement this week that it was "continuously implementing advanced security technologies in accordance with worldwide recognized and trusted standards" but declined to say whether it uses A5/3 technology or plans to do so for its 2G networks in the United States.

AT&T, the largest provider of GSM cellphone services in the country, said it was deploying A5/3 encryption for parts of its network. "AT&T always protects its customers with the best encryption possible in line with what their device will support," it said in a statement.

The company already deploys stronger encryption on its 3G and 4G networks, but customers may still wind up using 2G networks in congested areas or places where fewer cell towers are available.

Even with strong encryption, the protection exists only from a phone to the cell tower, after which point the communications are decrypted for transmission on a company's internal data network. Interception is possible on those internal links, as The Washington Post reported last week. Leading technology companies, including Google and Microsoft, have announced plans in recent months to encrypt the links between their data centers to better protect their users from government surveillance and criminal hackers.

Soltani is an independent security researcher and consultant.

Follow The Post's new tech blog, The Switch, where technology and policy connect.