What the CIA WikiLeaks dump tells us: Encryption works

March 10 2017, by Anick Jesdanun And Michael Liedtke

In this Thursday, Oct. 16, 2014, file photo, FBI Director James Comey speaks about the impact of technology on law enforcement, at Brookings Institution in Washington. If the tech industry is drawing one lesson from the latest WikiLeaks disclosures, it's that data-scrambling encryption works, and the industry should use more of it. On Wednesday, March 8, 2017, Comey acknowledged the challenges posed by encryption. He said there should be a balance between privacy and the FBI's ability to lawfully access information. Comey also said the FBI needs to recruit talented computer personnel who might otherwise go to work for Apple or Google. (AP Photo/Jose Luis Magana, File)

If the tech industry is drawing one lesson from the latest WikiLeaks disclosures, it's that data-scrambling encryption works, and the industry should use more of it.

Documents purportedly outlining a massive CIA surveillance program suggest that CIA agents must go to great lengths to circumvent encryption they can't break. In many cases, physical presence is required to carry off these targeted attacks.

"We are in a world where if the U.S. government wants to get your data, they can't hope to break the encryption," said Nicholas Weaver, who teaches networking and security at the University of California, Berkeley. "They have to resort to targeted attacks, and that is costly, risky and the kind of thing you do only on targets you care about. Seeing the CIA have to do stuff like this should reassure civil libertarians that the situation is better now than it was four years ago."

MORE ENCRYPTION

Four years ago is when former NSA contractor Edward Snowden revealed details of huge and secret U.S. eavesdropping programs. To help thwart spies and snoops, the tech industry began to protectively encrypt email and messaging apps, a process that turns their contents into indecipherable gibberish without the coded "keys" that can unscramble them.

The NSA revelations shattered earlier assumptions that internet data was nearly impossible to intercept for meaningful surveillance, said Joseph Lorenzo Hall, chief technologist at the Washington-based civil-liberties group Center for Democracy & Technology. That was because any given internet message gets split into a multitude of tiny "packets," each of which traces its own unpredictable route across the network to its destination.

The realization that spy agencies had figured out that problem spurred efforts to better shield data as it transits the internet. A few services such as Facebook's WhatsApp followed the earlier example of Apple's iMessage and took the extra step of encrypting data in ways even the companies couldn't unscramble, a method called end-to-end encryption.

CHALLENGES FOR AUTHORITIES

In the past, spy agencies like the CIA could have hacked servers at WhatsApp or similar services to see what people were saying. End-to-end encryption, though, makes that prohibitively difficult. So the CIA has to resort to tapping individual phones and intercepting data before it is encrypted or after it's decoded.

It's much like the old days when "they would have broken into a house to plant a microphone," said Steven Bellovin, a Columbia University professor who has long studied cybersecurity issues.

Cindy Cohn, executive director for Electronic Frontier Foundation, a group focused on online privacy, likened the CIA's approach to "fishing with a line and pole rather than fishing with a driftnet."

Encryption has grown so strong that even the FBI had to seek Apple's help last year in cracking the locked iPhone used by one of the San Bernardino attackers. Apple resisted what it considered an intrusive request, and the FBI ultimately broke into the phone by turning to an unidentified party for a hacking tool—presumably one similar to those the CIA allegedly had at its disposal.

On Wednesday, FBI Director James Comey acknowledged the challenges posed by encryption. He said there should be a balance between privacy and the FBI's ability to lawfully access information. He also said the FBI needs to recruit talented computer personnel who might otherwise go to work for Apple or Google.

Government officials have long wanted to force tech companies to build "back doors" into encrypted devices, so that the companies can help law enforcement descramble messages with a warrant. But security experts warn that doing so would undermine security and privacy for everyone. As Apple CEO Tim Cook pointed out last year , a back door for good guys can also be a back door for bad guys. So far, efforts to pass such a mandate have stalled.

STILL A PATCHWORK

At the moment, though, end-to-end encrypted services such as iMessage and WhatsApp are still the exception. While encryption is far more widely used than it was in 2013, many messaging companies encode user data in ways that let them read or scan it. Authorities can force these companies to divulge message contents with warrants or other legal orders. With end-to-end encryption, the companies wouldn't even have the keys to do so.

Further expanding the use of end-to-end encryption presents some challenges. That's partly because encryption will make it more difficult to perform popular tasks such as searching years of emails for mentions of a specific keyword. Google announced in mid-2014 that it was working on end-to-end encryption for email, but the tools have yet to materialize beyond research environments.

Instead, Google's Gmail encrypts messages in transit. But even that isn't possible unless it's adopted by the recipient's mail system as well.

And encryption isn't a panacea, as the WikiLeaks disclosures suggest.

According to the purported CIA documents, spies have found ways to exploit holes in phone and computer software to grab messages when they haven't been encrypted yet. Although Apple, Google and Microsoft say they have fixed many of the vulnerabilities alluded to in the CIA documents, it's not known how many holes remain open.

"There are different levels where attacks take place, said Daniel Castro, vice president with the Information Technology and Innovation Foundation. "We may have secured one level (with encryption), but there are other weaknesses out there we should be focused on as well."

Cohn said people should still use encryption, even with these bypass techniques.

"It's better than nothing," she said. "The answer to the fact that your front door might be cracked open isn't to open all your windows and walk around naked, too."

Citation: What the CIA WikiLeaks dump tells us: Encryption works (2017, March 10) retrieved 2 May 2024 from https://phys.org/news/2017-03-cia-wikileaks-dump-encryption.html