NSA's Decade-Long Plan to Undermine Encryption Includes Backdoors, Stolen Keys, Manipulating Standards | Threat Level | Wired.com

wired.com

It was only a matter of time before we learned that the NSA has managed to thwart much of the encryption that protects telephone and online communication, but new revelations show the extent to which the agency, and Britain's GCHQ, have gone to systematically undermine encryption.

Without the ability to actually crack the strongest algorithms that protect data, the intelligence agencies have systematically worked to thwart or bypass encryption using a variety of underhanded methods, according to revelations published by the *New York Times* and *Guardian* newspapers and the journalism non-profit ProPublica, based on documents leaked by NSA whistleblower Edward Snowden.

These methods, part of a highly secret program codenamed Bullrun, have included pressuring vendors to install backdoors in their products to allow intelligence agencies to access data, and obtaining encryption keys by pressuring vendors to hand them over or hacking into systems and stealing them.

Most surprising, however, is the revelation that the agency has worked to covertly undermine the encryption standards developers rely upon to build secure products. Undermining standards and installing backdoors don't just allow the government to spy on data but create fundamental insecurities in systems that would allow others to spy on the data as well.

"The encryption technologies that the NSA has exploited to enable its secret dragnet surveillance are the same technologies that protect our most sensitive information, including medical records, financial transactions, and commercial secrets," Christopher Soghoian, principal technologist of the ACLU's Speech, Privacy and Technology Project, said in a statement about the revelations. "Even as the NSA demands more powers to invade our privacy in the name of cybersecurity, it is making the internet less secure and exposing us to criminal hacking, foreign espionage, and unlawful surveillance. The NSA's efforts to secretly defeat encryption are recklessly shortsighted and will further erode not only the United States' reputation as a global champion of civil liberties and privacy but the economic competitiveness of its largest companies."

The revelations are the latest in a trove of documents obtained by Snowden earlier this year that detail extensive spying operations on the part of the NSA and foreign partners like the Government Communications Headquarters in the UK. Past revelations have disclosed the extensive amount of data — encrypted and unencrypted — that the agencies siphon from land

and undersea cables. Previous documents have discussed how the NSA retains encrypted traffic with an eye toward researching methods to crack it.

According to today's media reports, the NSA maintains an internal database, called a Key Provisioning Service, of encryption keys for specific commercial products to automatically decode communications. If the necessary key is missing from the collection, a request goes out to the so-called Key Recovery Service to obtain it.

"How keys are acquired is shrouded in secrecy, but independent cryptographers say many are probably collected by hacking into companies' computer servers, where they are stored," the *Times* writes. "To keep such methods secret, the N.S.A. shares decrypted messages with other agencies only if the keys could have been acquired through legal means."

"Approval to release to non-Sigint agencies," a GCHQ document says, "will depend on there being a proven non-Sigint method of acquiring keys."

It should be noted that these methods don't involve cracking the algorithms and the math underlying the encryption, but rather rely upon circumventing and otherwise undermining encryption.

"Properly implemented strong crypto systems are one of the few things that you can rely on," Snowden said in an interview with the *Guardian* earlier this year. He warned, however, that the NSA often bypassed encryption altogether by targeting the endpoint computers in order to grab communications before and after they were encrypted.

The most shocking revelation involves the NSA's efforts to deliberately weaken international encryption standards developers use to make their encryption secure, thereby undermining systems that human rights organizers, Third World activists and others depend upon to protect their communications from corrupt and oppressive regimes and U.S. companies rely upon to keep their trade secrets secret. One of the agency's stated goals in its 2013 budget was to "influence policies, standards and specifications for commercial public key technologies."

According to a classified NSA memo obtained by the *Times*, a fatal weakness in a 2006 standard, discovered by two Microsoft cryptographers in 2007, appeared to have been engineered by the NSA. The agency wrote the standard and aggressively pushed it on the international group, the paper writes, privately calling the effort "a challenge in finesse." The NSA managed to became "the sole editor" on the standard, ensuring that its underhanded efforts paid off.

The ten-year Bullrun program began after the U.S. government failed in its pla to place a backdoor, the so-called Clipper chip, into encryption that would have allowed it to eavesdrop on communications at will. Without the Clipper chip, the government launched a systematic plan using trickery and other methods to circumvent encryption and achieved an unspecified breakthrough in 2010. In the wake of this, according to one document, "vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."

Some of the methods involved the deployment of custom-built, supercomputers to break codes

in addition to collaborating with technology companies at home and abroad to include backdoors in their products. The Snowden documents don't identify the companies that participated.

The program, according to the documents, "actively engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs" to make them "exploitable." By this year, the *Times* reports, the program had found ways "inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors or by surreptitiously exploiting existing security flaws.

"The agency also expected to gain full unencrypted access to an unnamed major Internet phone call and text service; to a Middle Eastern Internet service; and to the communications of three foreign governments," the paper notes.

In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a backdoor into the product before it was shipped, a source told the *Times*

"Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on," cryptographer Bruce Schneier notes in a story by the *Guardian*. "If the backdoor is discovered, it's explained away as a mistake. And as we now know, the NSA has enjoyed enormous success from this program."

Some of the agency's most intensive efforts to gain access to encrypted internet traffic have focused on Secure Sockets Layer, or SSL, virtual private networks and the protections in 4G smartphones.

For at least three years, according to one document, Britain's GCHQ has been looking for ways to read the encrypted communications of Google, Yahoo, Facebook and Hotmail users. By 2012, GCHQ had developed "new access opportunities" into Google's systems, according to one document.

Schneier offered a handy list of five things you can do to better protect your communication, including using Tor and other hidden services to anonymize yourself. They're not foolproof, but the point is to make it a little harder and little less attractive for the NSA and other intelligence agencies to get and read your data.

Kim Zetter is a senior reporter at Wired covering cybercrime, privacy, security and civil liberties.

Read more by Kim Zetter

Follow @KimZetter and @ThreatLevel on Twitter.