Has the NSA broken SSL? TLS? AES?

Summary: *Indications suggest that SSL and other fundamental Internet security technologies have indeed been compromised by the NSA.*

By Steven J. Vaughan-Nichols for Networking | September 6, 2013 -- 01:17 GMT (18:17 PDT)

Just how broken are fundamental Internet security technologies such as Secure-Socket Layer (SSL), Advanced Encryption Standard (AES), and Transport Layer Security (TLS)? We still don't know for certain. But, it's clear that the National Security Agency (NSA) has broken many kinds of Internet encryption technologies (http://www.zdnet.com/uk-us-able-to-crack-most-encryption-used-online-7000020309/) ... including the ones we use every day.

The NSA's headquarters at Fort Meade, Maryland.

In a joint report (http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption) , based on documents obtained by The Guardian, three publications, the New York Times (NYT), The Guardian, and ProPublica, are reporting the following "news:"

- The NSA has secretly and successfully worked to break many types of encryption, the widely used technology that is supposed to make it impossible to read intercepted communications.
- Referring to the NSA's efforts, a 2010 British document stated: "Vast amounts of encrypted Internet data are now exploitable." Another related British memo said: "Those not already briefed were gobsmacked!"
- The NSA has worked with American and foreign tech companies to introduce weaknesses into commercial encryption products, allowing backdoor access to data that users believe is secure.
- The NSA has deliberately weakened the international encryption standards adopted by developers around the globe.

Before I dive into the details, let me point out that much of this “news” isn't really news. Since it was founded in 1952, the NSA's job has been to intercept communications and break encryption. It's the organization's job. Only the most naïve would be surprised that the NSA has successfully broken "many kinds of encryption" and that this government agency has used any

means it could to do so.

Six ways to protect yourself from the NSA and other eavesdroppers (http://www.zdnet.com/six-ways-to-protect-yourself-from-the-nsa-and-other-eavesdroppers-7000016860/)

In fact, as I reported earlier this year, commercially available SSL interception proxy programs and devices from vendors such as Blue Coat Systems (http://www.bluecoat.com/) and Packet Forensics (http://www.packetforensics.com) enable businesses and government agencies to intercept and read SSL communications (http://www.zdnet.com/how-the-nsa-and-your-boss-can-intercept-and-break-ssl-7000016573/) .

As for the technical specifics, the reports are don't give us enough detail to spell out what security standards and products were actually broken. One major breakthrough seems to have occurred in 2010 when the United Kingdom's Government Communications Headquarters, (GCHQ) reported that the NSA "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."

Does that mean SSL, which is used by almost every "secure" Web site on the planet, itself has been broken? Maybe. Maybe not.

The groups report that the NSA has been working hard on breaking the encryption in universal use in the US, including SSL, virtual private networks (VPNs), and 4G smartphones. What these have in common is their use of 256-bit AES for encryption.

It's been estimated that a brute-force attack on a message encrypted with 256-bit AES would take even a supercomputer longer to break than the universe has been in existence (http://www.eetimes.com/document.asp?doc_id=1279619) . Of course, if AES's Rijndael encryption algorithm (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf%20) (PDF link) already had a built-in weakness it would be much easier to break.

What's Hot on ZDNet

PC industry pushes 2-in-1 hybrid devices: You buying?

The smartwatch worth waiting for

Darknets, wargames and Raspberry Pi at first-ever Balkan hacker conference

Apple testing six-inch iPhone: report

Such government emplaced weaknesses have been found before. In 2007, security expert Bruce Schneier described how Dan Shumow and Niels Ferguson had found a random number algorithm that could be used in TLS contained "a weakness that can only be described as a back-door. (http://www.schneier.com/blog/archives/2007/11/the_strange_sto.html) "

Could there be such back doors in SSL?

Paul Kocher, a cryptographer who helped design SSL, thinks so. He told the NYT that although the NSA wasn't allowed to put Clipper, an encryption system with a built-in security backdoor for the federal government on all PCs in the 1990s (http://www.zdnet.com/news/your-isp-as-net-watchdog/143302) , "they went and did it anyway, without telling anyone. (http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=2&hp) "

The other "news" is that the NSA and GCHQ have been looking for ways to access the protected traffic of the most popular Internet companies: Google, Yahoo, Facebook, and Microsoft's Hotmail. By 2012, GCHQ had developed "new access opportunities" into Google's systems. What these may be is still unknown.

And it's not just Google. The story also re-reported that Microsoft had "handed the NSA access to encrypted messages." (http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data) Microsoft, according to the report, provided more than simply access to encrypted messages. The company is said to have also given the NSA access to "Outlook e-mail, Skype Internet phone calls and chats, and to SkyDrive, the company's cloud storage service."

Microsoft has denied this (http://www.zdnet.com/microsoft-we-do-not-give-the-nsa-keys-to-bypass-email-encryption-7000018146/) . The company has since revealed that it and rival Google have joined forces in a law suit to reveal how they're handling Foreign

Intelligence Surveillance Act (FISA) requests. (http://www.zdnet.com/microsoft-and-google-to-sue-government-over-transparency-7000020076)

Eventually--and it may take years--we'll find out what's really going on with our Internet security standards, privacy, and government surveillance. For now, we keep getting more hints that the NSA does indeed have high level access to both security technologies and to the companies that sell and operate them.

Related Stories:

- UK, US able to crack most encryption used online (http://www.zdnet.com/uk-us-able-to-crack-most-encryption-used-online-7000020309/)
- The lunacy of trying to avoid NSA spying by moving e-mail and cloud out of the US (http://www.zdnet.com/the-lunacy-of-trying-to-avoid-nsa-spying-by-moving-e-mail-and-cloud-out-of-the-us-7000019908/)
- How Snowden got the NSA documents (http://www.zdnet.com/how-snowden-got-the-nsa-documents-7000019860/)
- NSA: fear of a black van (http://www.zdnet.com/nsa-fear-of-a-black-van-7000019846/)
- NSA's data reach greater than first thought, says report (http://www.zdnet.com/nsas-data-reach-greater-than-first-thought-says-report-7000019685/)
- Secret court 'troubled' by NSA surveillance, ruled illegal (http://www.zdnet.com/nsa-surveillance-ruled-illegal-and-unconstitutional-7000019699/)

Topics: Security, Government US, Government UK, Networking, Privacy

About Steven J. Vaughan-Nichols

Steven J. Vaughan-Nichols, aka sjvn, has been writing about technology and the business of technology since CP/M-80 was the cutting edge PC operating system. SJVN covers networking, Linux, open source, and operating systems.