The case supporting the NSA's PRISM decrypting

CYBERTRUTH (/BLOG/CYBERTRUTH/) Byron Acohido, USA TODAY *1:35 p.m. EDT September 6, 2013*

(Photo: Patrick Semansky AP)

SEATTLE – More reaction from the global technology community is surfacing this morning about how the *New York Times* has spun (http://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/) the spying details contained in 50,000 pages of PRISM documents outed by Edward Snowden.

A consensus is gelling that the NSA -- in using brute-force password hacking techniques, cracking into Virtual Private Networks and Secure Sockets Layer services and taking steps to weaken certain inherently weak encryption protocols – is simply doing what the NSA has always done, and was, in fact, created to do: keep the U.S. competitive in the spy-vs-spy world.

Based on the information outed by Snowden, the global tech community, and the cyberunderground, now has more details about the narrow technical parameters the NSA has used for doing this.

Dave Jevans, chief technology officer of mobile security firm Marble Security, says it's possible that with the NSA's multi-billion dollar budget and tens of thousands of employees, the agency may have discovered mathematical techniques to weaken certain cryptographic systems.

"However, such fundamental mathematical research doesn't constitute back doors or other covert agendas," Jevans says. "Perhaps the NSA has discovered ways to crack these systems that have not been discovered by the smartest researchers in academia and industry. But there's no law against clever mathematicians creating new encryption schemes."

Jevans says he disagrees with the characterization that the NSA, through the use of billions of dollars of research, has exposed the U.S. to cyberattacks.

"It's just ludicrous," Jevans says. "It's not like the NSA posted open source tools to crack encryption."

Dave Jevans is CTO of Marble Security*(Photo: Marble Security)*

Dave Frymier, vice president and chief information security officer of IT company Unisys, opines "the NSA is doing what intelligence agencies are supposed to do – gather intelligence."

The methods and techniques outlined in the *Times'* report "have little to do with the underlying encryption technology and everything to do with compromising one side of a two-way conversation or compromising encryption keys," Frymier says. "There are many implementations of encryption algorithms, any of which are subject implementation bugs, same as any software."

Jakob Ehrensvard, chief technology officer at Yubico, an authentication security company, which also manufacturers hardware security modules, points out that Secure Sockets Layer and Transport Layer Security are the standard security technologies for establishing an encrypted link between a web server and a browser.

"There are some by-design weaknesses with the concept of SSL/TLS, which could be exploited by not only governments but also fraudulent users," Ehrensvard observes. "They basically allow anyone to connect to anyone and establish confidentiality."

Dave Anderson, a senior director with Voltage Security, emphasizes that encryption, in general, is robust technology.

"It seems likely that any possible way that the NSA might have bypassed encryption was almost certainly due to a flaw in the key management processes that support the use of encryption, rather than through the cryptography itself," says Anderson. "So, is it possible that the NSA can decrypt financial and shopping accounts? Perhaps, but only if the cryptography that was used to protect the sensitive transactions was improperly implemented."

USA NOW

Gotcha! Kimmel's tire twerk and other hoaxes | USA NOW video

Sep 10, 2013

((media/cinematic/video/2792761/gotcha-kimmels-tire-twerk-and-other-hoaxes-usa-now-video/)