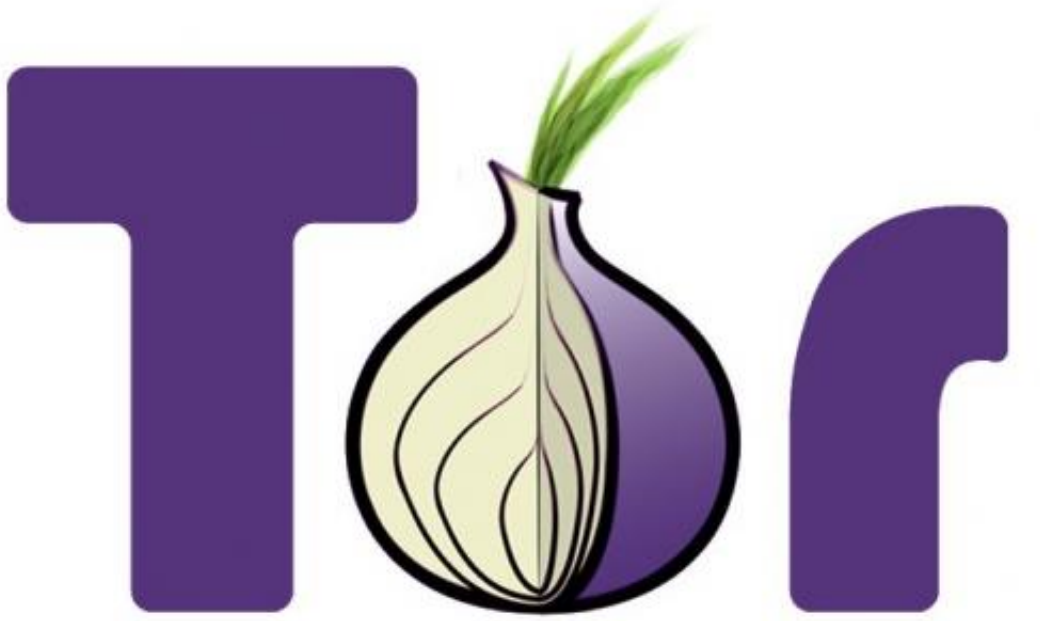
Next question: can the NSA crack Tor keys?

September 9 2013, by Nancy Owano



(Phys.org) —"After more revelations, and expert analysis, we still aren't precisely sure what crypto the NSA can break. But everyone seems to agree that if anything, the NSA can break 1024 RSA/DH [DH refers to Diffie-Hellman] keys." With that Friday blog post, Errata Security CEO Robert Graham ignited a spark of outside posts reporting on Graham's observations about Tor.

"The problem with Tor is that it still uses these 1024 bit keys for much

of its crypto," he said, "particularly because most people are still using older versions of the software. The older 2.3 versions of Tor uses keys the NSA can crack, but few have upgraded to the newer 2.4 version with better keys." Tor is short for The Onion Router, a service that offers anonymous browsing. Tor takes a user's Internet traffic and masks its location. He suggested that the Tor community do a better job getting people to upgrade to 2.4.

His speculation follows an exercise where he ran his own "hostile" exit node on Tor and surveyed encryption algorithms established by incoming connections. TOR still uses 1024 RSA/DH keys for much of its crypto.

About 76 percent of the 22,920 connections that he polled used some form of the older version keys. "Only about 24 percent of incoming connections were using the newer software," he said.

With the newer keys. the operations involved are more computationally intensive. According to the NSA site posting back in 2009, the US National Institute for Standards and Technology recommended that these 1024-bit systems be upgraded to something providing more security. The NSA discussion, titled "The Case for Elliptic Curve Cryptography." said that the US National Institute for Standards and Technology recommended that these 1024-bit systems were sufficient for use until 2010. "The question is what should these systems be changed to? One option is to simply increase the public key parameter size to a level appropriate for another decade of use. Another option is to take advantage of the past 30 years of public key research and analysis and move from first generation public key algorithms and on to elliptic curves."

"Of course, this is still just guessing about the NSA's capabilities," noted Graham.

More information: blog.erratasec.com/2013/09/tor … le.html#.UiyNAca1HA5
larstechnica.com/security/2013/ … nsa-researcher-says/
www.nsa.gov/business/programs/elliptic_curve.shtml