theguardian

The NSA's Heartbleed problem is the problem with the NSA

What the agency's denial isn't telling you: it didn't even need know about the bug to vacuum your privacy and store it indefinitely

Julian Sanchez

Saturday, April 12th, 2014

The American intelligence community is forcefully denying reports that the National Security Agency has long known about the Heartbleed bug, a catastrophic vulnerability inside one of the most widely-used encryption protocols upon which we rely every day to secure our web communications. But the denial itself serves as a reminder that NSA's two fundamental missions – one defensive, one offensive – are fundamentally incompatible, and that they can't both be handled credibly by the same government agency.

In case you've spent the past week under a rock, Heartbleed is the name security researchers have given to a subtle but serious bug in OpenSSL, a popular version of the Transport Layer Security (TLS) protocol – successor to the earlier Secure Sockets Layer (SSL) – that safeguards Internet traffic from prying eyes. When you log in to your online banking account or webmail service, the little lock icon that appears in your browser means SSL/TLS is scrambling the data to keep aspiring eavesdroppers away from your personal information. But an update to OpenSSL rolled out over two years ago contained a bug that would allow a hacker to trick sites into leaking information – including not only user passwords, but the master encryption keys used to secure all the site's traffic and verify that you're actually connected to MyBank.com rather than an impostor.

It's exactly the kind of bug you'd expect NSA to be on the lookout for, since documents leaked by Edward Snowden confirm that the agency has long been engaged in an "aggressive, multi-pronged effort to break widely used Internet encryption technologies". In fact, that effort appears to have yielded a major breakthrough against SSL/TLS way back in 2010, two years *before* the Heartbleed bug was introduced – a revelation that sparked a flurry of speculation among encryption experts, who wondered what hidden flaw the agency had found in the protocol so essential to the Internet's security.

On Friday, Bloomberg News reported that Heartbleed had indeed been added to NSA's arsenal almost immediately after the bug appeared, citing two anonymous sources "familiar with the matter". Within hours, the intelligence community's issued an unusually straightforward denial,

free from the weasely language intelligence officials sometimes employ to almost-but-not-quite deny allegations. As the statement pointed out, the federal government itself "relies on OpenSSL to protect the privacy of users of government websites and other online services." If NSA had found such a serious security hole, the agency would have disclosed it, officials asserted. Moreover, the White House has recently "reinvigorated" the "Vulnerabilities Equities Process" designed to ensure that newly-discovered exploits aren't kept secret any longer than is absolutely necessary for vital intelligence purposes.

As Indiana University cybersecurity expert Fred Cate points out, however, the intelligence community's track record of misleading statements about its capabilities means even such a seemingly unambiguous denial has been greeted with some skepticism. And even if we take that denial at face value when it comes to Heartbleed, reports of NSA's 2010 "breakthrough" suggest they may be sitting on other, still-undisclosed vulnerabilities.

Here, however, is the really crucial point to recognize: NSA doesn't need to have known about Heartbleed all along to take advantage of it.

The agency's recently-disclosed minimization procedures permit "retention of all communications that are enciphered." In other words, when NSA encounters encryption it can't crack, it's allowed to – and apparently does – vacuum up all that scrambled traffic and store it indefinitely, in hopes of finding a way to break into it months or years in the future. As security experts recently confirmed, Heartbleed can be used to steal a site's master encryption keys – keys that would suddenly enable anyone with a huge database of encrypted traffic to unlock it, at least for the vast majority of sites that don't practice what's known as "forward security", regularly generating new keys as a safeguard against retroactive exposure.

If NSA moved quickly enough – as dedicated spies are supposed to – the agency could have exploited the bug to steal those keys *before* most sites got around to fixing the bug, gaining access to a vast treasure trove of stored traffic.

That creates a huge dilemma for private sector security experts. Normally, when they discover a vulnerability of this magnitude, they want to give their colleagues a discreet heads-up before going public, ensuring that the techies at major sites have a few days to patch the hole before the whole world learns about it.

The geeks at NSA's massive Information Assurance Directorate – the part of the agency tasked with protecting secrets and improving security – very much want to be in that loop. But they're part of an organization that's also dedicated to *stealing* secrets and *breaking* security. And security companies have been burned by cooperation with NSA before: the influential firm RSA trusted the agency to help them improve one of their popular security tools, only to discover via another set of Snowden documents that the spies had schemed to *weaken* the software instead.

Giving NSA advance warning of Heartbleed could help the agency protect all those government systems that were relying on OpenSSL to protect user data – but it also would aid them in exploiting the bug to compromise privacy and security on a massive scale in the window before the fix was widely deployed.

Little wonder, then, that the President's Review Group on Intelligence and Communications Technologies – informally known as the Surveillance Review Group – dedicated a large section of its recent report, Liberty and Security in a Changing World, to this basic tension. "NSA now has multiple missions and mandates, some of which are blurred, inherently conflicting, or both," the Review Group wrote. "Fundamentally NSA is and should be a foreign intelligence organization" rather than "an information assurance organization."

Because Internet security depends on trust and cooperation between researchers, the mission of a security-breaking agency is fundamentally incompatible with that of a security-protecting agency. It's time to spin off NSA's "defense" division from the "offense" team. It's time to create an organization that's fully devoted to safeguarding the security of Internet users – even if that might make life harder for government hackers.

Julian Sanchez is a research fellow at the Cato Institute. He is the former Washington editor for the technology news site Ars Technica and a founding editor of the blog Just Security. You can follow him on Twitter at @normative.