Report: NSA cracked most online encryption

5 September 2013, by Jack Gillum

The National Security Agency (NSA) headquarters at Fort Meade, Maryland, as seen from the air, January 29, 2010. US and British intelligence agencies have cracked the encryption that secures a wide range of online communications including emails, banking transactions and phone conversations, according to newly leaked documents.

The National Security Agency, working with the British government, has secretly been unraveling encryption technology that billions of Internet users rely upon to keep their electronic messages and confidential data safe from prying eyes, according to published reports based on internal U.S. government documents.

The NSA has bypassed or cracked much of the digital encryption used by businesses and everyday Web users, according to reports Thursday in The New York Times, Britain's Guardian newspaper and the nonprofit news website ProPublica. The reports describe how the NSA invested billions of dollars since 2000 to make nearly everyone's secrets available for government consumption.

In doing so, the NSA built powerful supercomputers to break encryption codes and partnered with unnamed technology companies to insert "back doors" into their software, the reports said. Such a practice would give the government access to users' digital information before it was encrypted and sent over the Internet.

"For the past decade, NSA has led an aggressive, multipronged effort to break widely used Internet encryption technologies," according to a 2010 briefing document about the NSA's accomplishments meant for its UK counterpart, Government Communications Headquarters, or GCHQ. Security experts told the news organizations such a code-breaking practice would ultimately undermine Internet security and leave everyday Web users vulnerable to hackers.

The revelations stem from documents leaked by former NSA contractor Edward Snowden, who sought asylum in Russia this summer. His leaks, first published by the Guardian, revealed a massive effort by the U.S. government to collect and analyze all sorts of digital data that Americans send at home and around the world.

Those revelations prompted a renewed debate in the United States about the proper balance between civil liberties and keeping the country safe from terrorists. President Barack Obama said he welcomed the debate and called it "healthy for our democracy" but criticized the leaks; the Justice Department charged Snowden under the federal Espionage Act.

Thursday's reports described how some of the NSA's "most intensive efforts" focused on Secure Sockets Layer, a type of encryption widely used on the Web by online retailers and corporate networks to secure their Internet traffic. One document said GCHQ had been trying for years to exploit traffic from popular companies like Google, Yahoo, Microsoft and Facebook.

GCHQ, they said, developed "new access

opportunities" into Google's computers by 2012 but said the newly released documents didn't elaborate on how extensive the project was or what kind of data it could access.

Even though the latest document disclosures suggest the NSA is able to compromise many encryption programs, Snowden himself touted using encryption software when he first surfaced with his media revelations in June.

During a Web chat organized by the Guardian on June 17, Snowden told one questioner that "encryption works." Snowden said that "properly implemented strong crypto systems" were reliable, but he then alluded to the NSA's capability to crack tough encryption systems. "Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it," Snowden said.

It was unclear if Snowden drew a distinction between everyday encryption used on the Internet—the kind described in Thursday's reports—versus more-secure encryption algorithms used to store data on hard drives and often requires more processing power to break or decode. Snowden used an encrypted email account from a now-closed private email company, Lavabit, when he sent out invitations to a mid-July meeting at Moscow's Sheremetyevo International Airport.

The operator of Lavabit LLC, Ladar Levison, suspended operations of the encrypted mail service in August, citing a pending "fight in the 4th (U.S.) Circuit Court of Appeals." Levison did not explain the pressures that forced him to shut the firm down but added that "a favorable decision would allow me to resurrect Lavabit as an American company."

The government asked the news organizations not to publish their stories, saying foreign enemies would switch to new forms of communication and make it harder for the NSA to break. The organizations removed some specific details but still published the story, they said, because of the "value of a public debate regarding government actions that weaken the most powerful tools for protecting the privacy of Americans and others."

Such tensions between government officials and journalists, while not new, have become more apparent since Snowden's leaks. Last month, Guardian editor Alan Rusbridger said that British government officials came by his newspaper's London offices to destroy hard drives containing leaked information. "You've had your debate," one UK official told him. "There's no need to write any more."