N.S.A. Able to Foil Basic Safeguards of Privacy on Web

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE

Published: September 5, 2013 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=2&hp& - commentsContainer#commentsContainer

http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=1&_r=2&hp&

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor.

Beginning in 2000, as encryption tools were gradually blanketing the Web, the N.S.A. invested billions of dollars in a clandestine campaign to preserve its ability to eavesdrop. Having lost a public battle in the 1990s to insert its own “back door” in all encryption, it set out to accomplish the same goal by stealth.

The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated.

The N.S.A. hacked into target computers to snare messages before they were encrypted. In some cases, companies say they were coerced by the government into handing over their master encryption keys or building in a back door. And the agency used its influence as the world’s most experienced code maker to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world.

“For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies,” said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart, Government Communications Headquarters, or GCHQ. “Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable.”

When the British analysts, who often work side by side with N.S.A. officers, were first told about the program, another memo said, “those not already briefed were gobsmacked!”

An intelligence budget document makes clear that the effort is still going strong. “We are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit Internet traffic,” the director of national intelligence, James R. Clapper Jr., wrote in his budget request for the current year.

In recent months, the documents disclosed by Mr. Snowden have described the N.S.A.’s reach in scooping up vast amounts of communications around the world. The encryption documents now show, in striking detail, how the agency works to ensure that it is actually able to read the information it collects.

The agency’s success in defeating many of the privacy protections offered by encryption does not change the rules that prohibit the deliberate targeting of Americans’ e-mails or phone calls without a warrant. But it shows that the agency, which was sharply rebuked by a federal judge in 2011 for violating the rules and misleading the Foreign Intelligence Surveillance Court, cannot necessarily be restrained by privacy technology. N.S.A. rules permit the agency to store any encrypted communication, domestic or foreign, for as long as the agency is trying to decrypt it or analyze its technical features.

The N.S.A., which has specialized in code-breaking since its creation in 1952, sees that task as essential to its mission. If it cannot decipher the messages of terrorists, foreign spies and other adversaries, the United States will be at serious risk, agency officials say.

Just in recent weeks, the Obama administration has called on the intelligence agencies for details of communications by leaders of Al Qaeda about a terrorist plot and of Syrian officials’ messages about the chemical weapons attack outside Damascus. If such communications can be hidden by unbreakable encryption, N.S.A. officials say, the agency cannot do its work.