Snowden documents reveal NSA operation to break encryption codes

Jerry White
6 September 2013

Documents recently released by National Security Agency leaker Edward Snowden uncover a decade-long operation by the NSA to break personal privacy encryption codes, enabling it to spy on the emails, Internet activity, cell phone calls and business transactions of millions of people in the US and around the world.

The 50,000 or so documents Snowden provided to the British *Guardian* newspaper, expose details of two highly classified programs, codenamed "Bullrun" by the NSA and "Edgehill" by its British counterpart, the Government Communications Headquarters (GCHQ). The information published by the *Guardian* and the *New York Times* Thursday provides further insight into the US government's violation of core Constitutional protections against unreasonable searches and seizures.

The files show how the NSA and GCHQ spy on the world's population, running roughshod over privacy rights and collaborating with Internet providers and other companies, which falsely assure customers that their communications, online banking and medical records are not decipherable to identity thieves and governments.

The *Guardian* notes: "Those methods include covert measures to ensure NSA control over setting of international encryption standards, the use of supercomputers to break encryption with 'brute force,' and—the most closely guarded secret of all—collaboration with technology companies and internet service providers themselves.

"Through these covert partnerships, the agencies have inserted secret vulnerabilities—known as backdoors or trapdoors—into commercial encryption software."

Snowden previously revealed how Microsoft and other Silicon Valley technology giants worked with the NSA—in the top-secret Prism program—to circumvent encryption programs and open web chats, emails and Skype communications to NSA and FBI spying.

Funding for the newly revealed program—$254.9 million a year and $800 million since 2011—dwarfs that of the Prism program, which costs $20 million annually. The "Bullrun" operations are detailed in the NSA's top secret 2013 budget request under the heading "Sigint [signals intelligence] enabling."

The program "actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs," the document states. None of the companies involved in such partnerships are named.

Among other things, the program is designed to "insert vulnerabilities into commercial encryption systems." These would be known to the NSA, the *Guardian* notes, but not to any one else, including ordinary customers, who are tellingly referred to in the document as "adversaries."

"These design changes make the systems in question exploitable through Sigint collection … with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact."

The document notes that the program's aims include making commercial encryption software "more tractable" to NSA surveillance by "shaping" the worldwide marketplace and continuing efforts to break into the encryption used by the next generation of 4G phones.

Two decades ago, US intelligence agencies, concerned over the spread of encryption software like Pretty Good Privacy, sought to impose a "Clipper Chip" which would have given the NSA a permanent key to break digital encryption. The effort was defeated after a backlash by political and business interests

concerned about undermining America's global technology edge, along with civil liberties groups.

The NSA immediately set out to circumvent this. The *Times* reports: "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."

With the collaboration of technology companies in the US, employing specialized computers, the *Times* continues, "the N.S.A. hacked into 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."

Paul Kocher, who helped design the widely used Secure Sockets Layer (SSL) encryption technology, told the *Times* that after the NSA failed to insert the Clipper Chip, "they went and did it anyway, without telling anyone. The intelligence community has worried about 'going dark' forever, but today they are conducting instant total invasion of privacy with limited effort. This is the golden age of spying."

The NSA shares its code-breaking capabilities internationally with its so-called Five Eyes partners, which include intelligence agencies in Britain, Australia, New Zealand and Canada. A 2010 memo describing a NSA briefing to its British counterparts, said: "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable." Another memo, noted that when British intelligence analysts were first told about the program, "those not already in briefed were gobsmacked!"

Another document—the 2013 budget request by Director of National Intelligence James R. Clapper, Jr.—notes the agency's ongoing spying efforts. "We are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit Internet traffic." The budget memo also highlights "partnerships with major telecommunications carriers to shape the global network to benefit other collection accesses."

Speaking in Stockholm earlier this week, President Obama—who is spearheading an international manhunt to silence Snowden—declared the US government was "not going around snooping at people's emails or listening to their phone calls." In fact this is precisely what the Obama administration is doing.

Facing popular opposition in the US and around the world to another neo-colonial war against Syria, and explosive social tensions within the United States itself, the American ruling class is dispensing with democratic forms and increasingly employing police-state methods.