US and UK intelligence agencies hacked cell phone encryption keys

Nick Barrickman
21 February 2015

Beginning in 2010, a previously undisclosed unit of the British GCHQ acting with support from the NSA, the Mobile Handset Exploitation Team (MHET), penetrated the internal networks of cell phone SIM card manufacturing companies in order to steal encryption keys before the phones came to market, according to documents revealed by NSA whistleblower Edward Snowden and published this week on the *Intercept* .

The latest revelations of hacking to spy on cell phone communications underscore the criminality of the operations undertaken by the NSA and GCHQ and their companion agencies in imperialist countries around the world.

The documents show that MHET agents "cyberstalked" employers at SIM card manufacturers, monitoring their social media accounts, emails and other personal information with technology provided by the NSA in order to gain means to infiltrate their employers' networks. "These people were specifically hunted and targeted by intelligence agencies, not because they did anything wrong, but because they could be used as a means to an end," said the ACLU's Christopher Soghoian to the *Intercept* .

Subscriber identity modules, or SIM cards, store identification information for cell phone users, including encryption keys that protect vital personal information that is transferred from a phone to a wireless carrier. By obtaining the encryption keys of mobile devices, intelligence agencies are able to bypass a phone's security to monitor all communication on a given device, including voice communication, text messages and emails.

Over a three month period, "millions of keys were harvested" and shared with the NSA, which has the capability to process millions of keys per second, according to the *Intercept*. Gemalto, the world's largest producer of SIM card technology, had hundreds of thousands of encryption keys stolen as part of the GCHQ's DAPINO GAMMA program in early 2010, while MHET sought to develop similar means to infiltrate other manufacturing firms. The *Intercept* notes that the team's largest "score" of keys was in its hacking of the Chinese technology firm Huawei, a company that the US government has accused of collaborating with Chinese intelligence.

The documents expose as lies claims made by President Obama in early 2014 that "… people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten our national security and that we take their privacy concerns into account in our policies and procedures."

"Gaining access to a database of keys is pretty much game over for cellular encryption," Matthew Green, a cryptology expert at the Johns Hopkins Information Security Institute, told the *Intercep* t. Green stated that the latest revelations were "bad news for phone security. Really bad news."

The *Intercept* notes that, due to the document only revealing the activities of MHET in its incipient period, "It is impossible to know how many keys have been stolen by the NSA and GCHQ to date," adding that, "even using conservative math, the numbers are likely staggering." Considering the fact that the NSA/GCHQ obtained each user's encryption key illegally, allowing them to circumvent requirements to obtain warrants and other formalities, there is no official record of who the government is monitoring.

The documents show that, in addition to operating in collusion with private firms to monitor the population, the intelligence agencies also freely break the law in order to achieve the same ends.

The monitoring of the world's population illegally by the US and Britain goes far beyond the practices engaged in by those countries, such as China and Russia, that western imperialism seeks to target for military intervention and often accuses of cyber espionage.

The latest documents come as representatives of the US intelligence community have called for the ending of encryption software altogether, claiming that it hampers the job of law enforcement. "Encryption isn't just a technical feature; it's a marketing pitch. … And my question is, at what cost," said FBI director James Comey to an audience late last year at the liberal Brookings Institution.

"Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust," Comey said in reference to the public's reaction to the whistleblower's revealing of mass government spying.