GlobalResearch
Center for Research on Globalization

How the NSA Hacks Cellphone Networks Worldwide

By Ryan Gallagher
Global Research, December 04, 2014
The Intercept

Region: USA
Theme: Intelligence, Police State & Civil Rights

In March 2011, two weeks before the Western intervention in Libya, a secret message was delivered to the National Security Agency. An intelligence unit within the U.S. military's Africa Command needed help to hack into Libya's cellphone networks and monitor text messages.

For the NSA, the task was easy. The agency had already obtained technical information about the cellphone carriers' internal systems by spying on documents sent among company employees, and these details would provide the perfect blueprint to help the military break into the networks.

The NSA's assistance in the Libya operation, however, was not an isolated case. It was part of a much larger surveillance program—global in its scope and ramifications—targeted not just at hostile countries.

According to documents contained in the archive of material provided to*The Intercept* by whistleblower Edward Snowden, the NSA has spied on hundreds of companies and organizations internationally, including in countries closely allied to the United States, in an effort to find security weaknesses in cellphone technology that it can exploit for surveillance.

The documents also reveal how the NSA plans to secretly introduce new flaws into communication systems so that they can be tapped into—a controversial tactic that security experts say could be exposing the general population to criminal hackers.

Codenamed AURORAGOLD, the covert operation has monitored the content of messages sent and received by more than 1,200 email accounts associated with major cellphone network operators, intercepting confidential company planning papers that help the NSA hack into phone networks.

One high-profile surveillance target is the GSM Association, an influential U.K.-headquartered trade group that works closely with large U.S.-based firms including Microsoft, Facebook, AT&T, and Cisco, and is currently being funded by the U.S. government to develop privacy-enhancing technologies.

Karsten Nohl, a leading cellphone security expert and cryptographer who was consulted by *The Intercept* about details contained in the AURORAGOLD documents, said that the broad scope of information swept up in the operation appears aimed at ensuring virtually every cellphone network in the world is NSA accessible.

THE OPERATION APPEARS AIMED AT ENSURING VIRTUALLY EVERY CELLPHONE

NETWORK IN THE WORLD IS NSA ACCESSIBLE.

“Collecting an inventory [like this] on world networks has big ramifications,” Nohl said, because it allows the NSA to track and circumvent upgrades in encryption technology used by cellphone companies to shield calls and texts from eavesdropping. Evidence that the agency has deliberately plotted to weaken the security of communication infrastructure, he added, was particularly alarming.

“Even if you love the NSA and you say you have nothing to hide, you should be against a policy that introduces security vulnerabilities,” Nohl said, “because once NSA introduces a weakness, a vulnerability, it’s not only the NSA that can exploit it.”

NSA spokeswoman Vanee’ Vines told *The Intercept* in a statement that the agency “works to identify and report on the communications of valid foreign targets” to anticipate threats to the United States and its allies.

Vines said: “NSA collects only those communications that it is authorized by law to collect in response to valid foreign intelligence and counterintelligence requirements—regardless of the technical means used by foreign targets, or the means by which those targets attempt to hide their communications.”

Network coverage

The AURORAGOLD operation is carried out by specialist NSA surveillance units whose existence has not been publicly disclosed: the Wireless Portfolio Management Office, which defines and carries out the NSA’s strategy for exploiting wireless communications, and the Target Technology Trends Center, which monitors the development of new communication technology to ensure that the NSA isn’t blindsided by innovations that could evade its surveillance reach. The center’s logo is a picture of the Earth overshadowed by a large telescope; its motto is “Predict – Plan – Prevent.”

The NSA documents reveal that, as of May 2012, the agency had collected technical information on about 70 percent of cellphone networks worldwide—701 of an estimated 985—and was maintaining a list of 1,201 email “selectors” used to intercept internal company details from employees. (“Selector” is an agency term for a unique identifier like an email address or phone number.) From November 2011 to April 2012, between 363 and 1,354 selectors were “tasked” by the NSA for surveillance each month as part of AURORAGOLD, according to the documents. The secret operation appears to have been active since at least 2010.The information collected from the companies is passed onto NSA “signals development” teams that focus on infiltrating communication networks. It is also shared with other U.S. Intelligence Community agencies and with the NSA’s counterparts in countries that are part of the so-called “Five Eyes” surveillance alliance—the United Kingdom, Canada, Australia, and New Zealand.

Aside from mentions of a handful of operators in Libya, China, and Iran, names of the targeted companies are not disclosed in the NSA’s documents. However, a top-secret world map featured in a June 2012 presentation on AURORAGOLD suggests that the NSA has some degree of “network coverage” in almost all countries on every continent, including in the United States and in closely allied countries such as the United Kingdom, Australia, New

Zealand, Germany, and France.

One of the prime targets monitored under the AURORAGOLD program is the London-headquartered trade group, the GSM Association, or the GSMA, which represents the interests of more than 800 major cellphone, software, and internet companies from 220 countries.

The GSMA's members include U.S.-based companies such as Verizon, AT&T, Sprint, Microsoft, Facebook, Intel, Cisco, and Oracle, as well as large international firms including Sony, Nokia, Samsung, Ericsson, and Vodafone.

The trade organization brings together its members for regular meetings at which new technologies and policies are discussed among various "working groups." The Snowden files reveal that the NSA specifically targeted the GSMA's working groups for surveillance.

Claire Cranton, a spokeswoman for the GSMA, said that the group would not respond to details uncovered by *The Intercept* until its lawyers had studied the documents related to the spying.

"If there is something there that is illegal then they will take it up with the police," Cranton said.

By covertly monitoring GSMA working groups in a bid to identify and exploit security vulnerabilities, the NSA has placed itself into direct conflict with the mission of the National Institute for Standards and Technology, or NIST, the U.S. government agency responsible for recommending cybersecurity standards in the United States. NIST recently handed out a grant of more than $800,000 to GSMA so that the organization could research ways to address "security and privacy challenges" faced by users of mobile devices.

The revelation that the trade group has been targeted for surveillance may reignite deep-seated tensions between NIST and NSA that came to the fore following earlier Snowden disclosures. Last year, NIST was forced to urge people not to use an encryption standard it had previously approved after it emerged NSA had apparently covertly worked to deliberately weaken it.

Jennifer Huergo, a NIST spokewoman, told *The Intercept* that the agency was "not aware of any activities by NSA related to the GSMA." Huergo said that NIST would continue to work towards "bringing industry together with privacy and consumer advocates to jointly create a robust marketplace of more secure, easy-to-use, privacy-enhancing solutions."

GSMA headquarters in London (above)

Encryption attack

The NSA focuses on intercepting obscure but important technical documents circulated among the GSMA's members known as "IR.21s."

Most cellphone network operators share IR.21 documents among each other as part of

agreements that allow their customers to connect to foreign networks when they are "roaming" overseas on a vacation or a business trip. An IR.21, according to the NSA documents, contains information "necessary for targeting and exploitation."

The details in the IR.21s serve as a "warning mechanism" that flag new technology used by network operators, the NSA's documents state. This allows the agency to identify security vulnerabilities in the latest communication systems that can be exploited, and helps efforts to introduce new vulnerabilities "where they do not yet exist."

The IR.21s also contain details about the encryption used by cellphone companies to protect the privacy of their customers' communications as they are transmitted across networks. These details are highly sought after by the NSA, as they can aid its efforts to crack the encryption and eavesdrop on conversations.

Last year, the *Washington Post* reported that the NSA had already managed to break the most commonly used cellphone encryption algorithm in the world, known as A5/1. But the information collected under AURORAGOLD allows the agency to focus on circumventing newer and stronger versions of A5 cellphone encryption, such as A5/3.

The documents note that the agency intercepts information from cellphone operators about "the type of A5 cipher algorithm version" they use, and monitors the development of new algorithms in order to find ways to bypass the encryption.

In 2009, the British surveillance agency Government Communications Headquarters conducted a similar effort to subvert phone encryption under a project called OPULANT PUP, using powerful computers to perform a "crypt attack" to penetrate the A5/3 algorithm, secret memos reveal. By 2011, GCHQ was collaborating with the NSA on another operation, calledWOLFRAMITE, to attack A5/3 encryption. (GCHQ declined to comment for this story, other than to say that it operates within legal parameters.)

The extensive attempts to attack cellphone encryption have been replicated across the Five Eyes surveillance alliance. Australia's top spy agency, for instance, infiltrated an Indonesian cellphone company and stole nearly 1.8 million encryption keys used to protect communications, the *New York Times* reported in February.

The NSA's documents show that it focuses on collecting details about virtually all technical standards used by cellphone operators, and the agency's efforts to stay ahead of the technology curve occasionally yield significant results. In early 2010, for instance, its operatives had alreadyfound ways to penetrate a variant of the newest "fourth generation" smartphone-era technology for surveillance, years before it became widely adopted by millions of people in dozens of countries.

The NSA says that its efforts are targeted at terrorists, weapons proliferators, and other foreign targets, not "ordinary people." But the methods used by the agency and its partners to gain access to cellphone communications risk significant blowback.

According to Mikko Hypponen, a security expert at Finland-based F-Secure, criminal hackers and foreign government adversaries could be among the inadvertent beneficiaries of any security vulnerabilities or encryption weaknesses inserted by the NSA into communication systems using data collected by the AURORAGOLD project.

“If there are vulnerabilities on those systems known to the NSA that are not being patched on purpose, it’s quite likely they are being misused by completely other kinds of attackers,” said Hypponen. “When they start to introduce new vulnerabilities, it affects everybody who uses that technology; it makes all of us less secure.”

> “IT AFFECTS EVERYBODY WHO USES THAT TECHNOLOGY; IT MAKES ALL OF US LESS SECURE.”

In December, a surveillance review panel convened by President Obama concluded that the NSA should not “in any way subvert, undermine, weaken, or make vulnerable generally available commercial software.” The panel also recommended that the NSA should notify companies if it discovers previously unknown security vulnerabilities in their software or systems—known as “zero days” because developers have been given zero days to fix them—except in rare cases involving “high priority intelligence collection.”

In April, White House officials confirmed that Obama had ordered NSA to disclose vulnerabilities it finds, though qualified that with a loophole allowing the flaws to be secretly exploited so long as there is deemed to be “a clear national security or law enforcement” use.

Vines, the NSA spokeswoman, told *The Intercept* that the agency was committed to ensuring an “open, interoperable, and secure global internet.”

“NSA deeply values these principles and takes great care to honor them in the performance of its lawful foreign-intelligence mission,” Vines said.

She declined to discuss the tactics used as part of AURORAGOLD, or comment on whether the operation remains active.

———

Documents published with this article:

- AURORAGOLD – Project Overview
- AURORAGOLD Working Group
- IR.21 – A Technology Warning Mechanism
- AURORAGOLD – Target Technology Trends Center support to WPMO
- NSA First-Ever Collect of High-Interest 4G Cellular Signal
- AURORAGOLD Working Aid
- WOLFRAMITE Encryption Attack
- OPULANT PUP Encryption Attack
- NSA/GCHQ/CSEC Network Tradecraft Advancement Team

———

Photo: Cell tower: Justin Sullivan/Getty Images; GSMA headquarters: Google Maps

Email the author: ryan.gallagher@theintercept.com

Articles by: **Ryan Gallagher**