The Intercept_

# THE GREAT SIM HEIST

## How Spies Stole the Keys to the Encryption Castle

406


Jeremy Scahill, Josh Begley
Feb. 19 2015, 2:25 p.m.

**AMERICAN AND BRITISH** spies hacked into the internal computer network of the largest manufacturer of SIM cards in the world, stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to *The Intercept* by National Security Agency whistleblower Edward Snowden.

The hack was perpetrated by a joint unit consisting of operatives from the NSA and its British counterpart Government Communications Headquarters, or GCHQ. The breach, detailed in a secret 2010 GCHQ document, gave the surveillance agencies the potential to secretly monitor a large portion of the world's cellular communications, including both voice and data.

The company targeted by the intelligence agencies, Gemalto, is a multinational firm incorporated in the Netherlands that makes the chips used in mobile phones and next-generation credit cards. Among its clients are AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network providers around the world. The company operates in 85 countries

and has more than 40 manufacturing facilities. One of its three global headquarters is in Austin, Texas and it has a large factory in Pennsylvania.

In all, Gemalto produces some 2 billion SIM cards a year. Its motto is "Security to be Free."

With these stolen encryption keys, intelligence agencies can monitor mobile communications without seeking or receiving approval from telecom companies and foreign governments. Possessing the keys also sidesteps the need to get a warrant or a wiretap, while leaving no trace on the wireless provider's network that the communications were intercepted. Bulk key theft additionally enables the intelligence agencies to unlock any previously encrypted communications they had already intercepted, but did not yet have the ability to decrypt.

As part of the covert operations against Gemalto, spies from GCHQ — with support from the NSA — mined the private communications of unwitting engineers and other company employees in multiple countries.

Gemalto was totally oblivious to the penetration of its systems — and the spying on its employees. "I'm disturbed, quite concerned that this has happened," Paul Beverly, a Gemalto executive vice president, told *The Intercept*. "The most important thing for me is to understand exactly how this was done, so we can take every measure to ensure that it doesn't happen again, and also to make sure that there's no impact on the telecom operators that we have served in a very trusted manner for many years. What I want to understand is what sort of ramifications it has, or could have, on any of our customers." He

added that "the most important thing for us now is to understand the degree" of the breach.

Leading privacy advocates and security experts say that the theft of encryption keys from major wireless network providers is tantamount to a thief obtaining the master ring of a building superintendent who holds the keys to every apartment. "Once you have the keys, decrypting traffic is trivial," says Christopher Soghoian, the principal technologist for the American Civil Liberties Union. "The news of this key theft will send a shock wave through the security community."

## [redacted] The massive key theft is "bad news for phone security. Really bad news."

Beverly said that after being contacted by *The Intercept*, Gemalto's internal security team began on Wednesday to investigate how their system was penetrated and could find no trace of the hacks. When asked if the NSA or GCHQ had ever requested access to Gemalto-manufactured encryption keys, Beverly said, "I am totally unaware. To the best of my knowledge, no."

According to one secret GCHQ slide, the British intelligence agency penetrated Gemalto's

internal networks, planting malware on several computers, giving GCHQ secret access. We "believe we have their entire network," the slide's author boasted about the operation against Gemalto.

Additionally, the spy agency targeted unnamed cellular companies' core networks, giving it access to "sales staff machines for customer information and network engineers machines for network maps." GCHQ also claimed the ability to manipulate the billing servers of cell companies to "suppress" charges in an effort to conceal the spy agency's secret actions against an individual's phone. Most significantly, GCHQ also penetrated "authentication servers," allowing it to decrypt data and voice communications between a targeted individual's phone and his or her telecom provider's network. A note accompanying the slide asserted that the spy agency was "very happy with the data so far and [was] working through the vast quantity of product."

The Mobile Handset Exploitation Team (MHET), whose existence has never before been disclosed, was formed in April 2010 to target vulnerabilities in cellphones. One of its main missions was to covertly penetrate computer networks of corporations that manufacture SIM cards, as well as those of wireless network providers. The team included operatives from both GCHQ and the NSA.

While the FBI and other U.S. agencies can obtain court orders compelling U.S.-based telecom companies to allow them to wiretap or intercept the communications of their customers, on the international front this type of data collection is much more challenging. Unless a foreign telecom or foreign government grants access to their citizens' data to a

U.S. intelligence agency, the NSA or CIA would have to hack into the network or specifically target the user's device for a more risky "active" form of surveillance that could be detected by sophisticated targets. Moreover, foreign intelligence agencies would not allow U.S. or U.K. spy agencies access to the mobile communications of their heads of state or other government officials.

"It's unbelievable. Unbelievable," said Gerard Schouw, a member of the Dutch Parliament, when told of the spy agencies' actions. Schouw, the intelligence spokesperson for D66, the largest opposition party in the Netherlands, told *The Intercept*, "We don't want to have the secret services from other countries doing things like this." Schouw added that he and other lawmakers will ask the Dutch government to provide an official explanation and to clarify whether the country's intelligence services were aware of the targeting of Gemalto, whose official headquarters is in Amsterdam.

Last November, the Dutch government proposed an amendment to its constitution to include explicit protection for the privacy of digital communications, including those made on mobile devices. "We have, in the Netherlands, a law on the [activities] of secret services. And hacking is not allowed," Schouw said. Under Dutch law, the interior minister would have to sign off on such operations by foreign governments' intelligence agencies. "I don't believe that he has given his permission for these kind of actions."

The U.S. and British intelligence agencies pulled off the encryption key heist in great stealth, giving them the ability to intercept and decrypt communications without alerting the wireless network provider, the foreign government or the individual user that they

have been targeted. “Gaining access to a database of keys is pretty much game over for cellular encryption,” says Matthew Green, a cryptography specialist at the Johns Hopkins Information Security Institute. The massive key theft is “bad news for phone security. Really bad news.”

**S CONSUMERS BEGAN** to adopt cellular phones en masse in the mid-1990s, there were no effective privacy protections in place. Anyone could buy a cheap device from RadioShack capable of intercepting calls placed on mobile phones. The shift from analog to digital networks introduced basic encryption technology, though it was still crackable by tech savvy computer science graduate students, as well as the FBI and other law enforcement agencies, using readily available equipment.

Today, second-generation (2G) phone technology, which relies on a deeply flawed encryption system, remains the dominant platform globally, though U.S. and European cellphone companies now use 3G, 4G and LTE technology in urban areas. These include more secure, though not invincible, methods of encryption, and wireless carriers throughout the world are upgrading their networks to use these newer technologies.

It is in the context of such growing technical challenges to data collection that intelligence agencies, such as the NSA, have become interested in acquiring cellular encryption keys. “With old-fashioned [2G], there are other ways to work around cellphone security without those keys,” says Green, the Johns Hopkins cryptographer. “With newer 3G, 4G and LTE protocols, however, the algorithms aren’t as vulnerable, so getting those keys would be essential.”

The privacy of all mobile communications — voice calls, text messages and Internet access — depends on an encrypted connection between the cellphone and the wireless carrier's network, using keys stored on the SIM, a tiny chip smaller than a postage stamp, which is inserted into the phone. All mobile communications on the phone depend on the SIM, which stores and guards the encryption keys created by companies like Gemalto. SIM cards can be used to store contacts, text messages, and other important data, like one's phone number. In some countries, SIM cards are used to transfer money. As *The Intercept* reported last year, having the wrong SIM card can make you the target of a drone strike.

SIM cards were not invented to protect individual communications — they were designed to do something much simpler: ensure proper billing and prevent fraud, which was pervasive in the early days of cellphones. Soghoian compares the use of encryption keys on SIM cards to the way Social Security numbers are used today. "Social security numbers were designed in the 1930s to track your contributions to your government pension," he says. "Today they are used as a quasi national identity number, which was never their intended purpose."

Because the SIM card wasn't created with call confidentiality in mind, the manufacturers and wireless carriers don't make a great effort to secure their supply chain. As a result, the SIM card is an extremely vulnerable component of a mobile phone. "I doubt anyone is treating those things very carefully," says Green. "Cell companies probably don't treat them as essential security tokens. They probably just care that nobody is defrauding their networks." The ACLU's Soghoian adds, "These keys are so valuable that it makes sense for

intel agencies to go after them."

As a general rule, phone companies do not manufacture SIM cards, nor program them with secret encryption keys. It is cheaper and more efficient for them to outsource this sensitive step in the SIM card production process. They purchase them in bulk with the keys pre-loaded by other corporations. Gemalto is the largest of these SIM "personalization" companies.

After a SIM card is manufactured, the encryption key, known as a "Ki," is burned directly onto the chip. A copy of the key is also given to the cellular provider, allowing its network to recognize an individual's phone. In order for the phone to be able to connect to the wireless carrier's network, the phone — with the help of the SIM — authenticates itself using the Ki that has been programmed onto the SIM. The phone conducts a secret "handshake" that validates that the Ki on the SIM matches the Ki held by the mobile company. Once that happens, the communications between the phone and the network are encrypted. Even if GCHQ or the NSA were to intercept the phone signals as they are transmitted through the air, the intercepted data would be a garbled mess. Decrypting it can be challenging and time-consuming. Stealing the keys, on the other hand, is beautifully simple, from the intelligence agencies' point of view, as the pipeline for producing and distributing SIM cards was never designed to thwart mass surveillance efforts.

One of the creators of the encryption protocol that is widely used today for securing emails, Adi Shamir, famously asserted: "Cryptography is typically bypassed, not penetrated." In other words, it is much easier (and sneakier) to open a locked door when you have the key

than it is to break down the door using brute force. While the NSA and GCHQ have substantial resources dedicated to breaking encryption, it is not the only way — and certainly not always the most efficient — to get at the data they want. "NSA has more mathematicians on its payroll than any other entity in the U.S.," says the ACLU's Soghoian. "But the NSA's hackers are way busier than its mathematicians."

GCHQ and the NSA could have taken any number of routes to steal SIM encryption keys and other data. They could have physically broken into a manufacturing plant. They could have broken into a wireless carrier's office. They could have bribed, blackmailed or coerced an employee of the manufacturer or cellphone provider. But all of that comes with substantial risk of exposure. In the case of Gemalto, hackers working for GCHQ remotely penetrated the company's computer network in order to steal the keys in bulk as they were en route to the wireless network providers.

SIM card "personalization" companies like Gemalto ship hundreds of thousands of SIM cards at a time to mobile phone operators across the world. International shipping records obtained by *The Intercept* show that in 2011, Gemalto shipped 450,000 smart cards from its plant in Mexico to Germany's Deutsche Telekom in just one shipment.

In order for the cards to work and for the phones' communications to be secure, Gemalto also needs to provide the mobile company with a file containing the encryption keys for each of the new SIM cards. These master key files could be shipped via FedEx, DHL, UPS or another snail mail provider. More commonly, they could be sent via email or through File Transfer Protocol, FTP, a method of sending files over the Internet.

The moment the master key set is generated by Gemalto or another personalization company, but before it is sent to the wireless carrier, is the most vulnerable moment for interception. “The value of getting them at the point of manufacture is you can presumably get a lot of keys in one go, since SIM chips get made in big batches,” says Green, the cryptographer. “SIM cards get made for lots of different carriers in one facility.” In Gemalto’s case, GCHQ hit the jackpot, as the company manufactures SIMs for hundreds of wireless network providers, including all of the leading U.S. — and many of the largest European — companies.

But obtaining the encryption keys while Gemalto still held them required finding a way into the company’s internal systems.

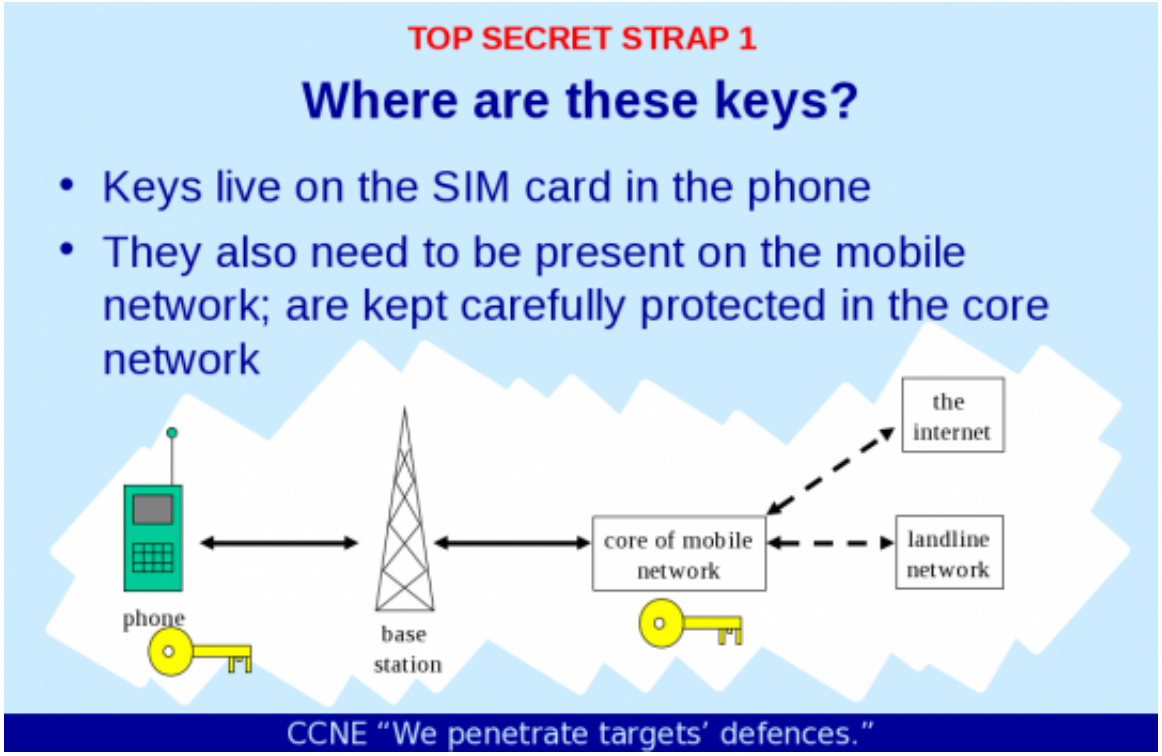



Diagram from a top-secret GCHQ slide.

[redacted]T

**OP-SECRET GCHQ** documents reveal that the intelligence agencies accessed the email and Facebook accounts of engineers and other employees of major telecom corporations and SIM card manufacturers in an effort to secretly obtain information that could give them access to millions of encryption keys. They did this by utilizing the NSA's X-KEYSCORE program, which allowed them access to private emails hosted by the

SIM card and mobile companies' servers, as well as those of major tech corporations, including Yahoo and Google.

In effect, GCHQ clandestinely cyberstalked Gemalto employees, scouring their emails in an effort to find people who may have had access to the company's core networks and Ki-generating systems. The intelligence agency's goal was to find information that would aid in breaching Gemalto's systems, making it possible to steal large quantities of encryption keys. The agency hoped to intercept the files containing the keys as they were transmitted between Gemalto and its wireless network provider customers.

GCHQ operatives identified key individuals and their positions within Gemalto and then dug into their emails. In one instance, GCHQ zeroed in on a Gemalto employee in Thailand who they observed sending PGP-encrypted files, noting that if GCHQ wanted to expand its Gemalto operations, "he would certainly be a good place to start." They did not claim to have decrypted the employee's communications, but noted that the use of PGP could mean the contents were potentially valuable.

The cyberstalking was not limited to Gemalto. GCHQ operatives wrote a script that allowed the agency to mine the private communications of employees of major telecommunications and SIM "personalization" companies for technical terms used in the assigning of secret keys to mobile phone customers. Employees for the SIM card manufacturers and wireless network providers were labeled as "known individuals and operators targeted" in a top-secret GCHQ document.

According to that April 2010 document, "PCS Harvesting at Scale," hackers working for GCHQ focused on "harvesting" massive amounts of individual encryption keys "in transit between mobile network operators and SIM card personalisation centres" like Gemalto. The spies "developed a methodology for intercepting these keys as they are transferred between various network operators and SIM card providers." By that time, GCHQ had developed "an automated technique with the aim of increasing the volume of keys that can be harvested."

The PCS Harvesting document acknowledged that, in searching for information on encryption keys, GCHQ operatives would undoubtedly vacuum up "a large number of unrelated items" from the private communications of targeted employees. "[H]owever an analyst with good knowledge of the operators involved can perform this trawl regularly and spot the transfer of large batches of [keys]."

The document noted that many SIM card manufacturers transferred the encryption keys to wireless network providers "by email or FTP with simple encryption methods that can be broken … or occasionally with no encryption at all." To get bulk access to encryption keys, all the NSA or GCHQ needed to do was intercept emails or file transfers as they were sent over the Internet — something both agencies already do millions of times per day. A footnote in the 2010 document observed that the use of "strong encryption products … is becoming increasingly common" in transferring the keys.

In its key harvesting "trial" operations in the first quarter of 2010, GCHQ successfully intercepted keys used by wireless network providers in Iran, Afghanistan, Yemen, India, Serbia, Iceland and Tajikistan. But, the agency noted, its automated key harvesting system

failed to produce results against Pakistani networks, denoted as "priority targets" in the document, despite the fact that GCHQ had a store of Kis from two providers in the country, Mobilink and Telenor. "[I]t is possible that these networks now use more secure methods to transfer Kis," the document concluded.

From December 2009 through March 2010, a month before the Mobile Handset Exploitation Team was formed, GCHQ conducted a number of trials aimed at extracting encryption keys and other personalized data for individual phones. In one two-week period, they accessed the emails of 130 people associated with wireless network providers or SIM card manufacturing and personalization. This operation produced nearly 8,000 keys matched to specific phones in 10 countries. In another two-week period, by mining just six email addresses, they produced 85,000 keys. At one point in March 2010, GCHQ intercepted nearly 100,000 keys for mobile phone users in Somalia. By June, they'd compiled 300,000. "Somali providers are not on GCHQ's list of interest," the document noted. "[H]owever, this was usefully shared with NSA."

The GCHQ documents only contain statistics for three months of encryption key theft in 2010. During this period, millions of keys were harvested. The documents stated explicitly that GCHQ had already created a constantly evolving automated process for bulk harvesting of keys. They describe active operations targeting Gemalto's personalization centers across the globe, as well as other major SIM card manufacturers and the private communications of their employees.

A top-secret NSA document asserted that, as of 2009, the U.S. spy agency already had the

capacity to process between 12 and 22 million keys per second for later use against surveillance targets. In the future, the agency predicted, it would be capable of processing more than 50 million per second. The document did not state how many keys were actually processed, just that the NSA had the technology to perform such swift, bulk operations. It is impossible to know how many keys have been stolen by the NSA and GCHQ to date, but, even using conservative math, the numbers are likely staggering.

GCHQ assigned "scores" to more than 150 individual email addresses based on how often the users mentioned certain technical terms, and then intensified the mining of those individuals' accounts based on priority. The highest-scoring email address was that of an employee of Chinese tech giant Huawei, which the U.S. has repeatedly accused of collaborating with Chinese intelligence. In all, GCHQ harvested the emails of employees of hardware companies that manufacture phones, such as Ericsson and Nokia; operators of mobile networks, such as MTN Irancell and Belgacom; SIM card providers, such as Bluefish and Gemalto; and employees of targeted companies who used email providers, such as Yahoo and Google. During the three-month trial, the largest number of email addresses harvested were those belonging to Huawei employees, followed by MTN Irancell. The third largest class of emails harvested in the trial were private Gmail accounts, presumably belonging to employees at targeted companies.

## [redacted] "People were specifically hunted and targeted by

**intelligence agencies, not because they did anything wrong, but because they could be used."**

The GCHQ program targeting Gemalto was called DAPINO GAMMA. In 2011, GCHQ launched operation HIGHLAND FLING to mine the email accounts of Gemalto employees in France and Poland. A top-secret document on the operation stated that one of the aims was "getting into French HQ" of Gemalto "to get in to core data repositories." France, home to one of Gemalto's global headquarters, is the nerve center of the company's worldwide operations. Another goal was to intercept private communications of employees in Poland that "could lead to penetration into one or more personalisation centers" — the factories where the encryption keys are burned onto SIM cards.

As part of these operations, GCHQ operatives acquired the usernames and passwords for Facebook accounts of Gemalto targets. An internal top-secret GCHQ wiki on the program from May 2011 indicated that GCHQ was in the process of "targeting" more than a dozen Gemalto facilities across the globe, including in Germany, Mexico, Brazil, Canada, China, India, Italy, Russia, Sweden, Spain, Japan and Singapore.

The document also stated that GCHQ was preparing similar key theft operations against one of Gemalto's competitors, Germany-based SIM card giant Giesecke and Devrient.

On January 17, 2014, President Barack Obama gave a major address on the NSA spying

scandal. “The bottom line is 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,” he said.

The monitoring of the lawful communications of employees of major international corporations shows that such statements by Obama, other U.S. officials and British leaders — that they only intercept and monitor the communications of known or suspected criminals or terrorists — were untrue. “The NSA and GCHQ view the private communications of people who work for these companies as fair game,” says the ACLU’s Soghoian. “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.”

## [edit] Other

Gemalto Yuaawaa - secure file sharing service identified. apparently used by gemalto employees- maybe just as testers?

- Findings from [redacted]

JTRIG research identified [redacted] as a Gemalto Technical Consultant in Prague. Searching in UDAQ revealed an item in which an email was sent from sharing@yuuwaa.com to a number of @gemalto.com email addresses, including [redacted] and [redacted] (who is already known to us as a Tech Consultant). Investigation on the internet revealed that Yuuwaa (www.yuuwaa.com) is a device for storing and sharing files sold by Gemalto. It consists of a USB stick and associated management software. The device also provides access to online storage using a subscription model. It claims to use 128-bit SSL to encrypt the traffic to the online storage location. The device is aimed at the general consumer market, so presumably Gemalto is encouraging its employees to use it. Amusingly, the quotes from "customers" on the website all appear to be from Gemalto employees!

[redacted] is a Gemalto employee in Singapore. His job title is "Sales – Telecom Solutions and Services". He will shortly (Feb/March 2011) be moving to Paris (still with Gemalto)

[redacted] is described as a "Consumer Device – Product Marketing Manager" at La Ciotat (France). He appears to be some sort of administrator for Yuuwaa, and we have not seen any indication that he will have any data of interest, so he is unlikely to be worth following up.

[redacted] is "Technical Account Manager METNA-Telecom" and is based in Dubai (from previous knowledge). We did not see any interesting data in collection, and since we have good coverage of the Dubai office, further investigation is probably unnecessary at this time.

[redacted] is "CITO T&I Servers Software/Cloud Computing Innovation WG Chairman" and is not likely to be of interest.

[redacted] is Account Manager (Middle East) and is based in Dubai (see [redacted])

[redacted] appears to be Sales Manager for Gemalto (Thailand). We saw him sending PGP-encrypted output files in XKEYSCORE. Again, if we ever become more interested in this area, he would certainly be a good place to start.

All other names (other than [redacted] who was already known about) did not have any useful information or any details of their role.

For a full list of names, see the CMAPS ([redacted] contacts) under OP HIGHLAND FLING.

- Hopefully some of this information will be useful in future efforts against Gemalto.

**THERE ARE TWO** basic types of electronic or digital surveillance: passive and active. All intelligence agencies engage in extensive passive surveillance, which means they collect bulk data by intercepting communications sent over fiber-optic cables, radio waves or wireless devices.

Intelligence agencies place high-power antennas, known as "spy nests," on the top of their countries' embassies and consulates, which are capable of vacuuming up data sent to or from mobile phones in the surrounding area. The joint NSA/CIA Special Collection Service is the lead entity that installs and mans these nests for the United States. An embassy situated near a parliament or government agency could easily intercept the phone calls and data transfers of the mobile phones used by foreign government officials. The U.S. embassy in Berlin, for instance, is located a stone's throw from the Bundestag. But if the wireless carriers are using stronger encryption, which is built into modern 3G, 4G and LTE networks, then intercepted calls and other data would be more difficult to crack, particularly in bulk. If the intelligence agency wants to actually

listen to or read what is being transmitted, they would need to decrypt the encrypted data.

Active surveillance is another option. This would require government agencies to "jam" a 3G or 4G network, forcing nearby phones onto 2G. Once forced down to the less secure 2G technology, the phone can be tricked into connecting to a fake cell tower operated by an intelligence agency. This method of surveillance, though effective, is risky, as it leaves a digital trace that counter-surveillance experts from foreign governments could detect.

Stealing the Kis solves all of these problems. This way, intelligence agencies can safely engage in passive, bulk surveillance without having to decrypt data and without leaving any trace whatsoever.

"Key theft enables the bulk, low-risk surveillance of encrypted communications," the ACLU's Soghoian says. "Agencies can collect all the communications and then look through them later. With the keys, they can decrypt whatever they want, whenever they want. It's like a time machine, enabling the surveillance of communications that occurred before someone was even a target."

Neither the NSA nor GCHQ would comment specifically on the key theft operations. In the past, they have argued more broadly that breaking encryption is a necessary part of tracking terrorists and other criminals. "It is longstanding policy that we do not comment on intelligence matters," a GCHQ official stated in an email, adding that the agency's work is conducted within a "strict legal and policy framework" that ensures its activities are "authorized, necessary and proportionate," with proper oversight, which is the standard

response the agency has provided for previous stories published by *The Intercept*. The agency also said, "[T]he UK's interception regime is entirely compatible with the European Convention on Human Rights." The NSA declined to offer any comment.

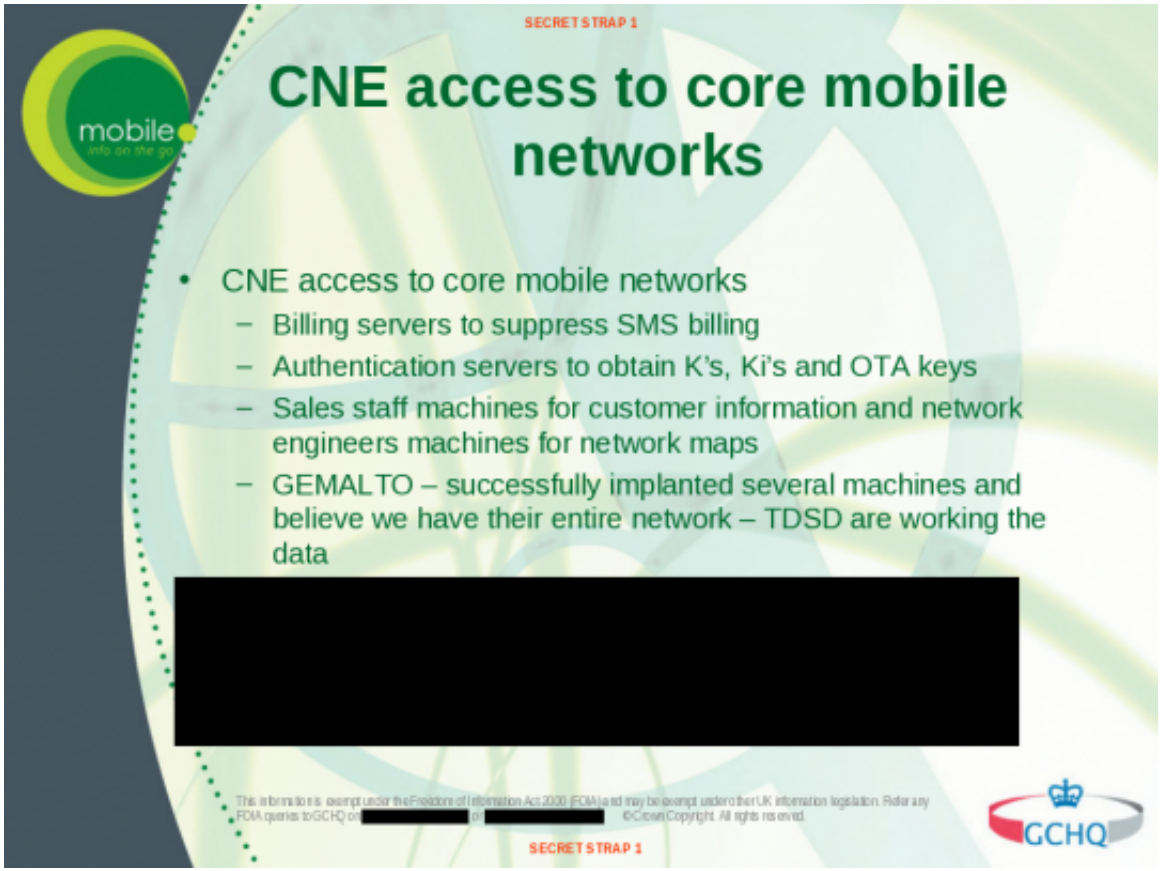
It is unlikely that GCHQ's pronouncement about the legality of its operations will be universally embraced in Europe. "It is governments massively engaging in illegal activities," says Sophie in't Veld, a Dutch member of the European Parliament. "If you are not a government and you are a student doing this, you will end up in jail for 30 years." Veld, who chaired the European Parliament's recent inquiry into mass surveillance exposed by Snowden, told *The Intercept*: "The secret services are just behaving like cowboys. Governments are behaving like cowboys and nobody is holding them to account."

*The Intercept*'s Laura Poitras has previously reported that in 2013 Australia's signals intelligence agency, a close partner of the NSA, stole some 1.8 million encryption keys from an Indonesian wireless carrier.

A few years ago, the FBI reportedly dismantled several transmitters set up by foreign intelligence agencies around the Washington, D.C. area, which could be used to intercept cellphone communications. Russia, China, Israel and other nations use similar technology as the NSA across the world. If those governments had the encryption keys for major U.S. cellphone companies' customers, such as those manufactured by Gemalto, mass snooping would be simple. "It would mean that with a few antennas placed around Washington, D.C., the Chinese or Russian governments could sweep up and decrypt the communications of members of Congress, U.S. agency heads, reporters, lobbyists and everyone else involved

in the policymaking process and decrypt their telephone conversations," says Soghoian.

"Put a device in front of the U.N., record every bit you see going over the air. Steal some keys, you have all those conversations," says Green, the Johns Hopkins cryptographer. And it's not just spy agencies that would benefit from stealing encryption keys. "I can only imagine how much money you could make if you had access to the calls made around Wall Street," he adds.




GCHQ slide.

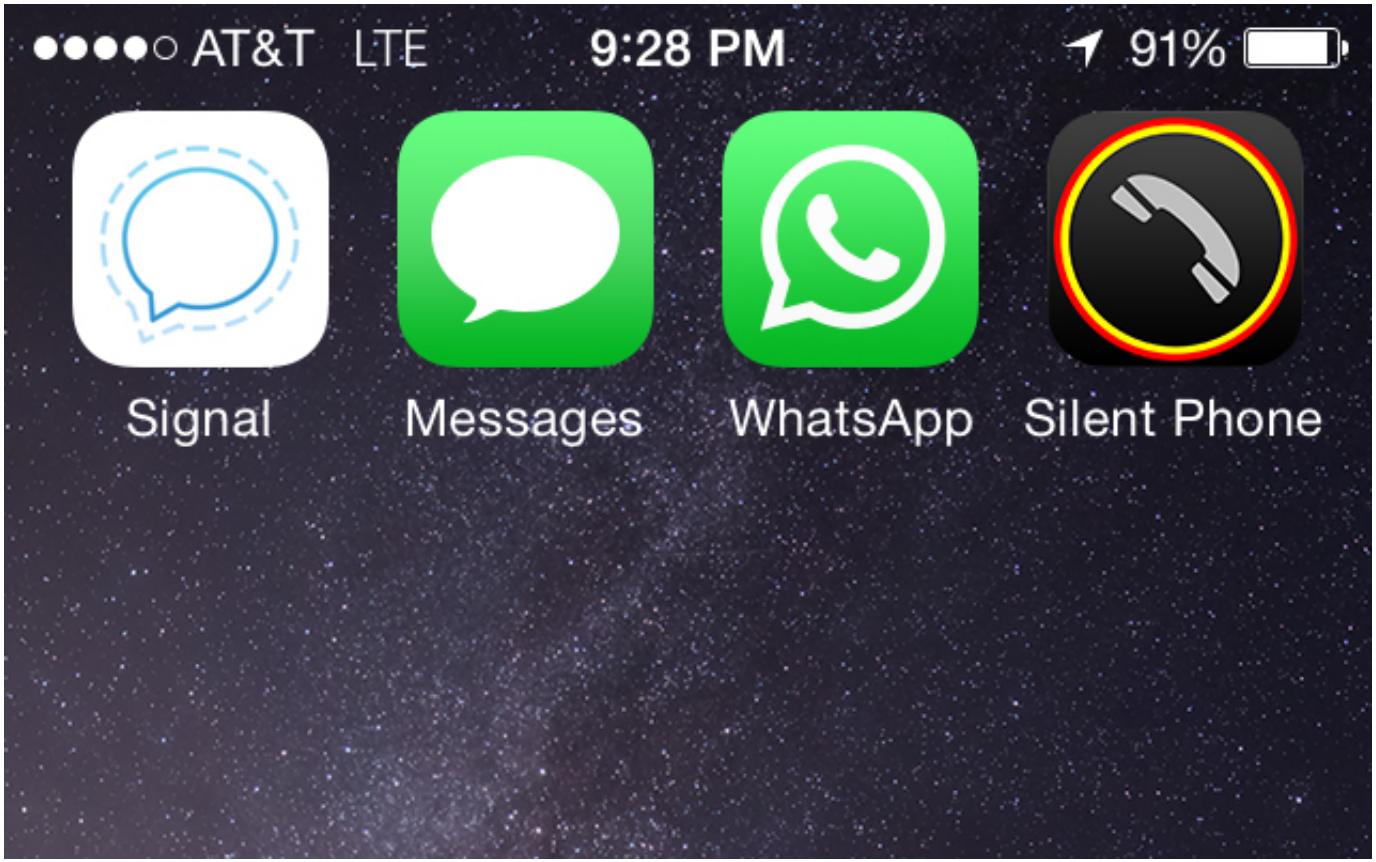
**THE BREACH OF** Gemalto's computer network by GCHQ has far-reaching global implications. The company, which brought in $2.7 billion in revenue in 2013, is a global leader in digital security, producing banking cards, mobile payment systems, two-factor authentication devices used for online security, hardware tokens used for securing buildings and offices, electronic passports and identification cards. It provides chips to Vodafone in Europe and France's Orange, as well as EE, a joint venture in the U.K. between France Telecom and Deutsche Telekom. Royal KPN, the largest Dutch wireless network provider, also uses Gemalto technology.

In Asia, Gemalto's chips are used by China Unicom, Japan's NTT and Taiwan's Chungwa Telecom, as well as scores of wireless network providers throughout Africa and the Middle East. The company's security technology is used by more than 3,000 financial institutions and 80 government organizations. Among its clients are Visa, Mastercard, American Express, JP Morgan Chase and Barclays. It also provides chips for use in luxury cars, including those made by Audi and BMW.

In 2012, Gemalto won a sizable contract, worth $175 million, from the U.S. government to produce the covers for electronic U.S. passports, which contain chips and antennas that can be used to better authenticate travelers. As part of its contract, Gemalto provides the

personalization and software for the microchips implanted in the passports. The U.S. represents Gemalto's single largest market, accounting for some 15 percent of its total business. This raises the question of whether GCHQ, which was able to bypass encryption on mobile networks, has the ability to access private data protected by other Gemalto products created for banks and governments.

As smart phones become smarter, they are increasingly replacing credit cards and cash as a means of paying for goods and services. When Verizon, AT&T and T-Mobile formed an alliance in 2010 to jointly build an electronic pay system to challenge Google Wallet and Apple Pay, they purchased Gemalto's technology for their program, known as Softcard. (Until July 2014, it previously went by the unfortunate name of "ISIS Mobile Wallet.") Whether data relating to that, and other Gemalto security products, has been compromised by GCHQ and the NSA is unclear. Both intelligence agencies declined to answer any specific questions for this story.




Signal, iMessage, WhatsApp, Silent Phone.

**PRIVACY ADVOCATES** and security experts say it would take billions of dollars, significant political pressure, and several years to fix the fundamental security flaws in the current mobile phone system that NSA, GCHQ and other intelligence agencies regularly exploit.

A current gaping hole in the protection of mobile communications is that cellphones and wireless network providers do not support the use of Perfect Forward Secrecy (PFS), a form of encryption designed to limit the damage caused by theft or disclosure of encryption keys. PFS, which is now built into modern web browsers and used by sites like Google and Twitter, works by generating unique encryption keys for each communication or message, which are then discarded. Rather than using the same encryption key to protect years' worth of data, as the permanent Kis on SIM cards can, a new key might be generated each minute, hour or day, and then promptly destroyed.

Because cellphone communications do not utilize PFS, if an intelligence agency has been "passively" intercepting someone's communications for a year and later acquires the permanent encryption key, it can go back and decrypt all of those communications. If mobile phone networks were using PFS, that would not be possible — even if the permanent keys were later stolen.

The only effective way for individuals to protect themselves from Ki theft-enabled surveillance is to use secure communications software, rather than relying on SIM card-based security. Secure software includes email and other apps that use Transport Layer Security (TLS), the mechanism underlying the secure HTTPS web protocol. The email clients included with Android phones and iPhones support TLS, as do large email providers like Yahoo and Google.

Apps like TextSecure and Silent Text are secure alternatives to SMS messages, while Signal, RedPhone and Silent Phone encrypt voice calls. Governments still may be able to intercept communications, but reading or listening to them would require hacking a specific handset, obtaining internal data from an email provider, or installing a bug in a room to record the conversations.

"We need to stop assuming that the phone companies will provide us with a secure method of making calls or exchanging text messages," says Soghoian.

— — —

*Documents published with this article:*

- CNE Access to Core Mobile Networks
- Where Are These Keys?
- CCNE Successes Jan10-Mar10 Trial
- DAPINO GAMMA CNE Presence Wiki
- DAPINO GAMMA Gemalto Yuaawaa Wiki
- DAPINO GAMMA Target Personalisation Centres Gemalto Wiki
- IMSIs Identified with Ki Data for Network Providers Jan10-Mar10 Trial
- CCNE Stats Summaries Jan10-Mar10 Trial
- CCNE Email Harvesting Jan10-Mar10 Trial
- CCNE Email Addresses Jan10-Mar10 Trial
- PCS Harvesting at Scale

– – –

*Additional reporting by Andrew Fishman and Ryan Gallagher. Sheelagh McNeill, Morgan Marquis-Boire, Alleen Brown, Margot Williams, Ryan Devereaux and Andrea Jones contributed to this story. Erin O'Rourke provided additional assistance.*

*Top photo: Shutterstock*

## CONTACT THE AUTHOR:

Jeremy Scahill

jeremy.scahill@theintercept.com

@jeremyscahill

Josh Begley

josh.begley@theintercept.com

@joshbegley

406 Comments (closed)