theguardian

Revealed: how US and UK spy agencies defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products
- Security experts say programs 'undermine the fabric of the internet'

- Q&A: submit your questions for our privacy experts

James Ball, **Julian Borger** and **Glenn Greenwald**
Guardian Weekly, Thursday 5 September 2013

Through covert partnerships with tech companies, the spy agencies have inserted secret vulnerabilities into encryption software. Photograph: Kacper Pempel/Reuters

US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the privacy of their personal data, online transactions and emails, according to top-secret documents revealed by former contractor Edward Snowden.

This story has been reported in partnership between the New York Times, the Guardian and ProPublica based on documents obtained by the Guardian.

For the Guardian: James Ball, Julian Borger, Glenn Greenwald

For the New York Times: Nicole Perlroth, Scott Shane

For ProPublica: Jeff Larson

Read the New York Times story here

The files show that the National Security Agency and its UK counterpart GCHQ have broadly compromised the guarantees that internet companies have given consumers to reassure them that their communications, online banking and medical records would be indecipherable to criminals or governments.

The agencies, the documents reveal, have adopted a battery of methods in their systematic and ongoing assault on what they see as one of the biggest threats to their ability to access huge swathes of internet traffic – "the use of ubiquitous encryption across the internet".

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.

The files, from both the NSA and GCHQ, were obtained by the Guardian, and the details are being published today in partnership with the New York Times and ProPublica. They reveal:

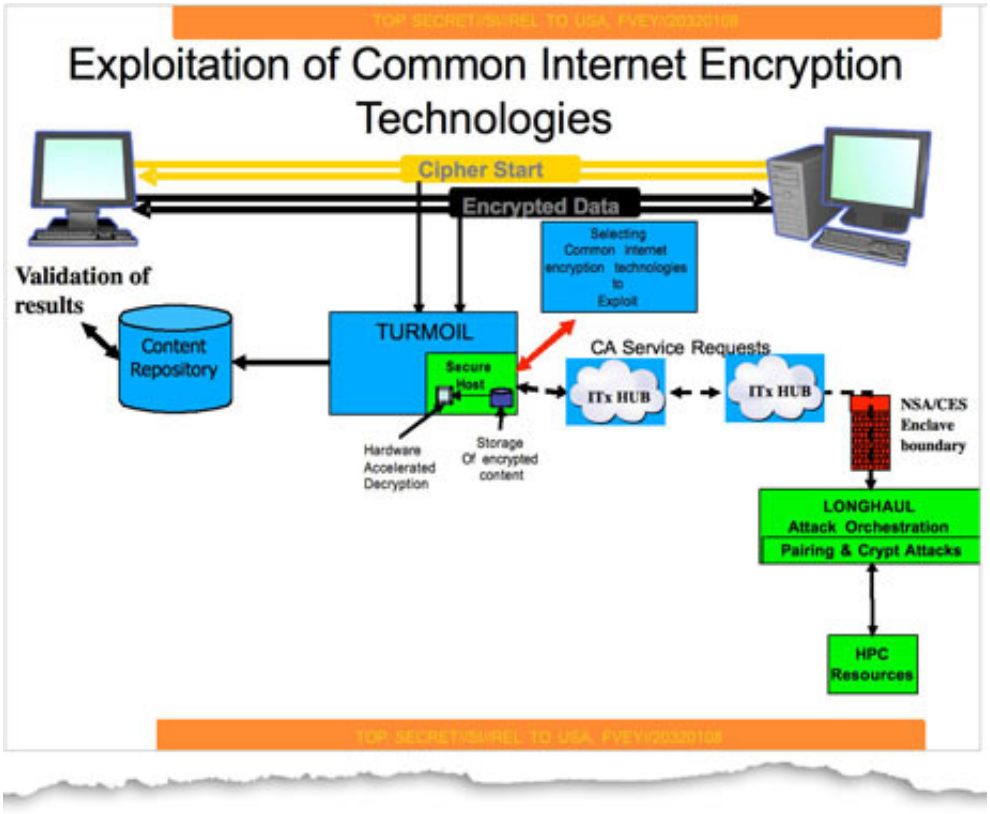
• A 10-year NSA program against encryption technologies made a breakthrough in 2010 which made "vast amounts" of data collected through internet cable taps newly "exploitable".

• The NSA spends $250m a year on a program which, among other goals, works with technology companies to "covertly influence" their product designs.

• The secrecy of their capabilities against encryption is closely guarded, with analysts warned: "Do not ask about or speculate on sources or methods."

• The NSA describes strong decryption programs as the "price of admission for the US to maintain unrestricted access to and use of cyberspace".

• A GCHQ team has been working to develop ways into encrypted traffic on the "big four" service providers, named as Hotmail, Google, Yahoo and Facebook.



This network diagram, from a GCHQ pilot program, shows how the agency proposed a system to identify encrypted traffic from its internet cable-tapping programs and decrypt what it could in near-real time. Photograph: Guardian

The agencies insist that the ability to defeat encryption is vital to their core missions of counter-terrorism and foreign intelligence gathering.

But security experts accused them of attacking the internet itself and the privacy of all users. "Cryptography forms the basis for trust online," said Bruce Schneier, an encryption specialist and fellow at Harvard's Berkman Center for Internet and Society. "By deliberately undermining online security in a short-sighted effort to eavesdrop, the NSA is undermining the very fabric of the internet." Classified briefings between the agencies celebrate their success at "defeating network security and privacy".

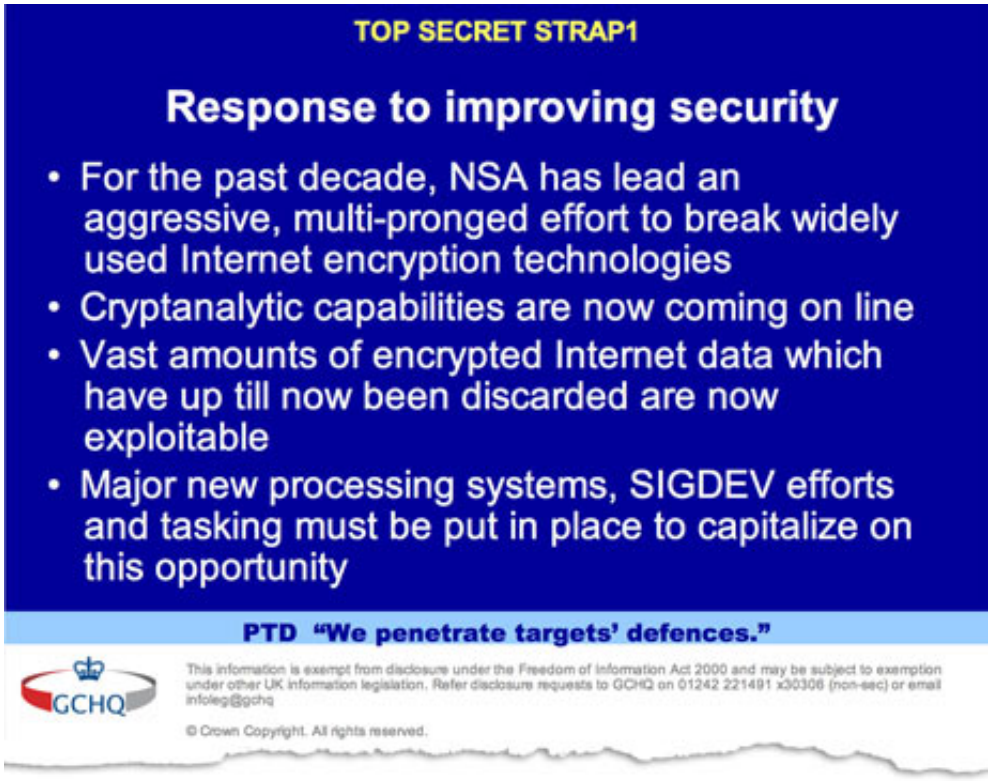
"For the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies," stated a 2010 GCHQ document. "Vast amounts of encrypted internet data which have up till now been discarded are now exploitable."

An internal agency memo noted that among British analysts shown a presentation on the

NSA's progress: "Those not already briefed were gobsmacked!"

The breakthrough, which was not described in detail in the documents, meant the intelligence agencies were able to monitor "large amounts" of data flowing through the world's fibre-optic cables and break its encryption, despite assurances from internet company executives that this data was beyond the reach of government.

The key component of the NSA's battle against encryption, its collaboration with technology companies, is detailed in the US intelligence community's top-secret 2013 budget request under the heading "Sigint [signals intelligence] enabling".



Classified briefings between the NSA and GCHQ celebrate their success at 'defeating network security and privacy'. Photograph: Guardian

Funding for the program – $254.9m for this year – dwarfs that of the Prism program, which operates at a cost of $20m a year, according to previous NSA documents. Since 2011, the total spending on Sigint enabling has topped $800m. 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; these details are guarded by still higher levels of classification.

Among other things, the program is designed to "insert vulnerabilities into commercial encryption systems". These would be known to the NSA, but to no 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 sets out in clear terms the program's broad aims, including making commercial encryption software "more tractable" to NSA attacks by "shaping" the worldwide marketplace and continuing efforts to break into the encryption used by the next generation of 4G phones.

Among the specific accomplishments for 2013, the NSA expects the program to obtain access to "data flowing through a hub for a major communications provider" and to a "major internet peer-to-peer voice and text communications system".

Technology companies maintain that they work with the intelligence agencies only when legally compelled to do so. The Guardian has previously reported that Microsoft co-operated with the NSA to circumvent encryption on the Outlook.com email and chat services. The company insisted that it was obliged to comply with "existing or future lawful demands" when designing its products.

The documents show that the agency has already achieved another of the goals laid out in the budget request: to influence the international standards upon which encryption systems rely.

Independent security experts have long suspected that the NSA has been introducing weaknesses into security standards, a fact confirmed for the first time by another secret document. It shows the agency worked covertly to get its own version of a draft security standard issued by the US National Institute of Standards and Technology approved for worldwide use in 2006.

"Eventually, NSA became the sole editor," the document states.

The NSA's codeword for its decryption program, Bullrun, is taken from a major battle of the American civil war. Its British counterpart, Edgehill, is named after the first major engagement of the English civil war, more than 200 years earlier.

A classification guide for NSA employees and contractors on Bullrun outlines in broad terms its goals.

"Project Bullrun deals with NSA's abilities to defeat the encryption used in specific network communication technologies. Bullrun involves multiple sources, all of which are extremely sensitive." The document reveals that the agency has capabilities against widely used online protocols, such as HTTPS, voice-over-IP and Secure Sockets Layer (SSL), used to protect online shopping and banking.

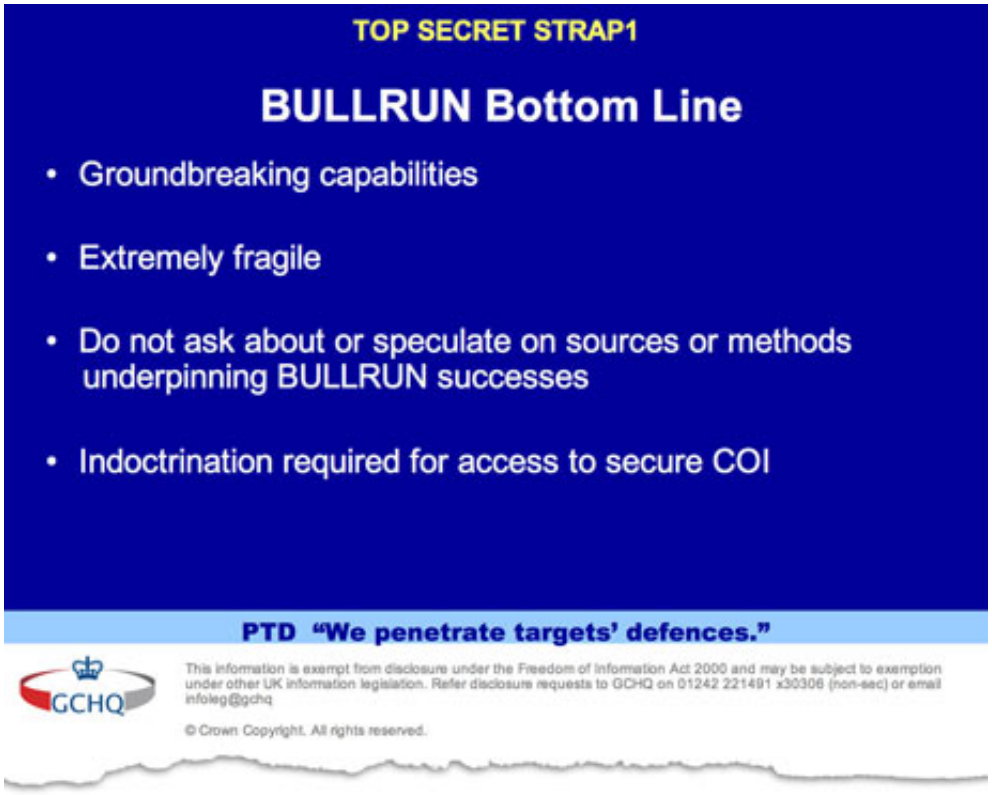
The document also shows that the NSA's Commercial Solutions Center, ostensibly the body through which technology companies can have their security products assessed and presented to prospective government buyers, has another, more clandestine role.

It is used by the NSA to "to leverage sensitive, co-operative relationships with specific industry partners" to insert vulnerabilities into security products. Operatives were warned that this information must be kept top secret "at a minimum".

A more general NSA classification guide reveals more detail on the agency's deep partnerships with industry, and its ability to modify products. It cautions analysts that two facts must remain top secret: that NSA makes modifications to commercial encryption software and devices "to make them exploitable", and that NSA "obtains cryptographic details of commercial cryptographic information security systems through industry relationships".

The agencies have not yet cracked all encryption technologies, however, the documents suggest. Snowden appeared to confirm this during a live Q&A with Guardian readers in June. "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on," he said before warning that NSA can frequently find ways around it as a result of weak security on the computers at either end of the communication.

The documents are scattered with warnings over the importance of maintaining absolute secrecy around decryption capabilities.



A slide showing that the secrecy of the agencies' capabilities against encryption is closely guarded. Photograph: Guardian

Strict guidelines were laid down at the GCHQ complex in Cheltenham, Gloucestershire, on how to discuss projects relating to decryption. Analysts were instructed: "Do not ask about or speculate on sources or methods underpinning Bullrun." This informaton was so closely guarded, according to one document, that even those with access to aspects of the program were warned: "There will be no 'need to know'."

The agencies were supposed to be "selective in which contractors are given exposure to this information", but it was ultimately seen by Snowden, one of 850,000 people in the US with top-secret clearance.A 2009 GCHQ document spells out the significant potential consequences of any leaks, including "damage to industry relationships".

"Loss of confidence in our ability to adhere to confidentiality agreements would lead to loss of access to proprietary information that can save time when developing new capability," intelligence workers were told. Somewhat less important to GCHQ was the public's trust which was marked as a moderate risk, the document stated.

"Some exploitable products are used by the general public; some exploitable weaknesses are well known eg possibility of recovering poorly chosen passwords," it said. "Knowledge that GCHQ exploits these products and the scale of our capability would raise public awareness generating unwelcome publicity for us and our political masters."

The decryption effort is particularly important to GCHQ. Its strategic advantage from its Tempora program – direct taps on transatlantic fibre-optic cables of major telecommunications corporations – was in danger of eroding as more and more big internet companies encrypted their traffic, responding to customer demands for guaranteed privacy.

Without attention, the 2010 GCHQ document warned, the UK's "Sigint utility will degrade as information flows changes, new applications are developed (and deployed) at pace and widespread encryption becomes more commonplace." Documents show that Edgehill's initial aim was to decode the encrypted traffic certified by three major (unnamed) internet companies and 30 types of Virtual Private Network (VPN) – used by businesses to provide secure remote access to their systems. By 2015, GCHQ hoped to have cracked the codes used by 15 major internet companies, and 300 VPNs.

Another program, codenamed Cheesy Name, was aimed at singling out encryption keys, known as 'certificates', that might be vulnerable to being cracked by GCHQ supercomputers.

Analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project. A quarterly update from 2012 notes the project's team "continue to work on understanding" the big four communication providers, named in the document as Hotmail, Google, Yahoo and Facebook, adding "work has predominantly been focused this quarter on Google due to new access opportunities being developed".

To help secure an insider advantage, GCHQ also established a Humint Operations Team (HOT). Humint, short for "human intelligence" refers to information gleaned directly from sources or undercover agents.

This GCHQ team was, according to an internal document, "responsible for identifying, recruiting and running covert agents in the global telecommunications industry."

"This enables GCHQ to tackle some of its most challenging targets," the report said. The efforts made by the NSA and GCHQ against encryption technologies may have negative consequences for all internet users, experts warn.

"Backdoors are fundamentally in conflict with good security," said Christopher Soghoian, principal technologist and senior policy analyst at the American Civil Liberties Union. "Backdoors expose all users of a backdoored system, not just intelligence agency targets, to heightened risk of data compromise." This is because the insertion of backdoors in a

software product, particularly those that can be used to obtain unencrypted user communications or data, significantly increases the difficulty of designing a secure product."

This was a view echoed in a recent paper by Stephanie Pell, a former prosecutor at the US Department of Justice and non-resident fellow at the Center for Internet and Security at Stanford Law School.

"[An] encrypted communications system with a lawful interception back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users," she states.

Intelligence officials asked the Guardian, New York Times and ProPublica not to publish this article, saying that it might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read.

The three organisations removed some specific facts but decided to publish the story because of the value of a public debate about government actions that weaken the most powerful tools for protecting the privacy of internet users in the US and worldwide.

;