افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــــاد   بدین بوم وبر زنده یک تن مـــباد
همه سر به سر تن به کشتن دهیم   از آن به که کشور به دشمن دهیم

www.afgazad.com   afgazad@gmail.com

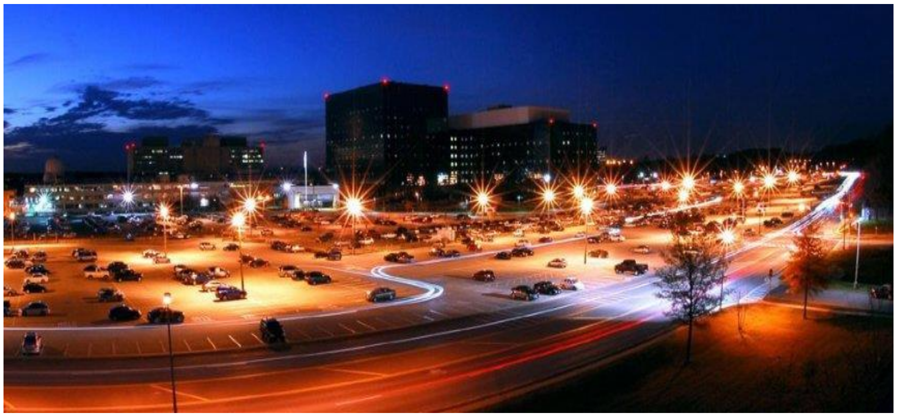
European Languages	زبان های اروپائی

http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361-druck.html

Inside the NSA's War on Internet Security

By SPIEGEL Staff

12/28/2014



The NSA's headquarters in Fort Meade, Maryland: The US foreign intelligence agency views all encrypted communications as a "threat" to its operations.

US and British intelligence agencies undertake every effort imaginable to crack all types of encrypted Internet communication. The cloud, it seems, is full of holes. The good news: New Snowden documents show that some forms of encryption still cause problems for the NSA.

When Christmas approaches, the spies of the Five Eyes intelligence services can look forward to a break from the arduous daily work of spying. In addition to their usual job -- attempting to crack encryption all around the world -- they play a game called the "Kryptos Kristmas Kwiz," which involves solving challenging numerical and alphabetical puzzles. The proud winners of the competition are awarded "Kryptos" mugs.

Encryption -- the use of mathematics to protect communications from spying -- is used for electronic transactions of all types, by governments, firms and private users alike. But a look into the archive of whistleblower Edward Snowden shows that not all encryption technologies live up to what they promise.

One example is the encryption featured in Skype, a program used by some 300 million users to conduct Internet video chat that is touted as secure. It isn't really. "Sustained Skype collection began in Feb 2011," reads a National Security Agency (NSA) training document from the archive of whistleblower Edward Snowden. Less than half a year later, in the fall, the code crackers declared their mission accomplished. Since then, data from Skype has been accessible to the NSA's snoops. Software giant Microsoft, which acquired Skype in 2011, said in a statement: "We will not provide governments with direct or unfettered access to customer data or encryption keys." The NSA had been monitoring Skype even before that, but since February 2011, the service has been under order from the secret US Foreign Intelligence Surveillance Court (FISC), to not only supply information to the NSA but also to make itself accessible as a source of data for the agency.

The "sustained Skype collection" is a further step taken by the authority in the arms race between intelligence agencies seeking to deny users of their privacy and those wanting to ensure they are protected. There have also been some victories for privacy, with certain encryption systems proving to be so robust they have been tried and true standards for more than 20 years.

For the NSA, encrypted communication -- or what all other Internet users would call secure communication -- is "a threat". In one internal training document viewed by SPIEGEL, an NSA employee asks: "Did you know that ubiquitous encryption on the Internet is a major threat to NSA's ability to prosecute digital-network intelligence (DNI) traffic or defeat adversary malware?"

The Snowden documents reveal the encryption programs the NSA has succeeded in cracking, but, importantly, also the ones that are still likely to be secure. Although the documents are around two years old, experts consider it unlikely the agency's digital spies have made much progress in cracking these technologies. "Properly implemented strong crypto systems are one of the few things that you can rely on," Snowden said in June 2013, after fleeing to Hong Kong.

The digitization of society in the past several decades has been accompanied by the broad deployment of cryptography, which is no longer the exclusive realm of secret agents. Whether a person is conducting online banking, Internet shopping or making a phone call, almost every Internet connection today is encrypted in some way. The entire realm of cloud computing -- that is of outsourcing computing tasks to data centers somewhere else, possibly even on the other side of the globe -- relies heavily on cryptographic security systems. Internet activists even hold crypto parties where they teach people who are interested in communicating securely and privately how to encrypt their data.

German officials suggest "consistent encryption"

In Germany, concern about the need for strong encryption goes right up to the highest levels of the government. Chancellor Angela Merkel and her cabinet now communicate using phones incorporating strong encryption. The government has also encouraged members of the German public to take steps to protect their own communication. Michael Hange, the president of the Federal Office for Information Security, has stated: "We suggest cryptography -- that is, consistent encryption."

It's a suggestion unlikely to please some intelligence agencies. After all, the Five Eyes alliance -- the secret services of Britain, Canada, Australia, New Zealand and the United States -- pursue a clear goal: removing the encryption of others on the Internet wherever possible. In 2013, the NSA had a budget of more than $10 billion. According to the US intelligence budget for 2013, the money allocated for the NSA department called Cryptanalysis and Exploitation Services (CES) alone was $34.3 million.

Last year, the Guardian, New York Times and *ProPublica* reported on the contents of a 2010 presentation on the NSA's BULLRUN decryption program, but left out many specific vulnerabilities. The presentation states that, "for the past decade, NSA has led an aggressive, multipronged effort to break widely used Internet encryption technologies," and "vast amounts of encrypted Internet data which have up till now been discarded are now exploitable." Decryption, it turns out, works retroactively - once a system is broken, the agencies can look back in time in their databases and read stuff they could not read before.

The number of Internet users concerned about privacy online has risen dramatically since the first Snowden revelations. But people who consciously use strong end-to-end encryption to protect their data still represent a minority of the Internet-using population. There are a number of reasons for this: Some believe encryption is too complicated to use. Or they think the intelligence agency experts are already so many steps ahead of them that they can crack any encryption program.

Still Safe from the NSA

This isn't true. As one document from the Snowden archive shows, the NSA had been unsuccessful in attempts to decrypt several communications protocols, at least as of 2012. An NSA presentation for a conference that took place that year lists the encryption programs the Americans failed to crack. In the process, the NSA cryptologists divided their targets into five levels corresponding to the degree of the difficulty of the attack and the outcome, ranging from "trivial" to "catastrophic."

Monitoring a document's path through the Internet is classified as "trivial." Recording Facebook chats is considered a "minor" task, while the level of difficulty involved in decrypting emails sent through Moscow-based Internet service provider "mail.ru" is considered "moderate." Still, all three of those classifications don't appear to pose any significant problems for the NSA.

Things first become troublesome at the fourth level. The presentation states that the NSA encounters "major" problems in its attempts to decrypt messages sent through heavily encrypted email service providers like Zoho or in monitoring users of the Tor network*, which was developed for surfing the web anonymously. Tor, otherwise known as The Onion Router, is free and open source software that allows users to surf the web through a network of more than 6,000 linked volunteer computers. The software automatically encrypts data in a way that ensures that no single computer in the network has all of a user's information. For surveillance experts, it becomes very difficult to trace the whereabouts of a person who visits a particular website or to attack a specific person while they are using Tor to surf the Web.

The NSA also has "major" problems with Truecrypt, a program for encrypting files on computers. Truecrypt's developers stopped their work on the program last May, prompting speculation about pressures from government agencies. A protocol called Off-the-Record (OTR) for encrypting instant messaging in an end-to-end encryption process also seems to cause the NSA major problems. Both are programs whose source code can be viewed, modified, shared and used by anyone. Experts agree it is far more difficult for intelligence agencies to manipulate open source software programs than many of the closed systems developed by companies like Apple and Microsoft. Since anyone can view free and open source software, it becomes difficult to insert secret back doors without it being noticed. Transcripts of intercepted chats using OTR encryption handed over to the intelligence agency by a partner in Prism -- an NSA program that accesses data from at least nine American internet companies such as Google, Facebook and Apple -- show that the NSA's efforts appear to have been thwarted in these cases: "No decrypt available for this OTR message." This shows that OTR at least sometimes makes communications impossible to read for the NSA.

Things become "catastrophic" for the NSA at level five - when, for example, a subject uses a combination of Tor, another anonymization service, the instant messaging system CSpace and a system for Internet telephony (voice over IP) called ZRTP. This type of combination results in a "near-total loss/lack of insight to target communications, presence," the NSA document states.

ZRTP, which is used to securely encrypt conversations and text chats on mobile phones, is used in free and open source programs like RedPhone and Signal. "It's satisfying to know that the NSA considers encrypted communication from our apps to be truly opaque," says RedPhone developer Moxie Marlinspike.

Too Robust for Fort Meade

Also, the "Z" in ZRTP stands for one of its developers, Phil Zimmermann, the same man who created Pretty Good Privacy, which is still the most common encryption program for emails and documents in use today. PGP is more than 20 years old, but apparently it remains too robust for the NSA spies to crack. "No decrypt available for this PGP encrypted message," a further document viewed by SPIEGEL states of emails the NSA obtained from Yahoo.

Phil Zimmermann wrote PGP in 1991. The American nuclear weapons freeze activist wanted to create an encryption program that would enable him to securely exchange information with other like-minded individuals. His system quickly became very popular among dissidents around the world. Given its use outside the United States, the US government launched an investigation into Zimmermann during the 1990s for allegedly violating the Arms Export Control Act. Prosecutors argued that making encryption software of such complexity available abroad was illegal. Zimmermann responded by publishing the source code as a book, an act that was constitutionally protected as free speech.

PGP continues to be developed and various versions are available today. The most widely used is GNU Privacy Guard (GnuPG), a program developed by German programmer Werner Koch. One document shows that the Five Eyes intelligence services sometimes use PGP themselves. The fact is that hackers obsessed with privacy and the US authorities have a lot more in common than one might initially believe. The Tor Project*****, was originally developed with the support of the US Naval Research Laboratory.

Today, NSA spies and their allies do their best to subvert the system their own military helped conceive, as a number of documents show. Tor deanonymization is obviously high on the list of NSA priorities, but the success achieved here seems limited. One GCHQ document from 2011 even mentions trying to decrypt the agencies' own use of Tor -- as a test case.

To a certain extent, the Snowden documents should provide some level of relief to people who thought nothing could stop the NSA in its unquenchable thirst to collect data. It appears secure channels still exist for communication. Nevertheless, the documents also underscore just how far the intelligence agencies already go in their digital surveillance activities.

Internet security comes at various levels -- and the NSA and its allies obviously are able to "exploit" -- i.e. crack -- several of the most widely used ones on a scale that was previously unimaginable.

VPN Security only Virtual

One example is virtual private networks (VPN), which are often used by companies and institutions operating from multiple offices and locations. A VPN theoretically creates a secure tunnel between two points on the Internet. All data is channeled through that tunnel, protected by cryptography. When it comes to the level of privacy offered here, virtual is the right word, too. This is because the NSA operates a large-scale VPN exploitation project to crack large numbers of connections, allowing it to intercept the data exchanged inside the VPN -- including, for example, the Greek government's use of VPNs. The team responsible for the exploitation of those Greek VPN communications consisted of 12 people, according to an NSA document SPIEGEL has seen.

The NSA also targeted SecurityKiss, a VPN service in Ireland. The following fingerprint for Xkeyscore, the agency's powerful spying tool, was reported to be tested and working against the service:

fingerprint('encryption/securitykiss/x509') = $pkcs and (($tcp and from_port(443)) or ($udp and (from_port(123) or from_por (5000) or from_port(5353)))) and (not (ip_subnet('10.0.0.0/8' or '172.16.0.0/12' or '192.168.0.0/16'))) and 'RSA Generated Server Certificate'c and 'Dublin1'c and 'GL CA'c;

According to an NSA document dating from late 2009, the agency was processing 1,000 requests an hour to decrypt VPN connections. This number was expected to increase to 100,000 per hour by the end of 2011. The aim was for the system to be able to completely process "at least 20 percent" of these requests, meaning the data traffic would have to be decrypted and reinjected. In other words, by the end of 2011, the NSA's plans called for simultaneously surveilling 20,000 supposedly secure VPN communications per hour.

VPN connections can be based on a number of different protocols. The most widely used ones are called Point-to-Point Tunneling Protocol (PPTP) and Internet Protocol Security (Ipsec). Both seem to pose few problems for the NSA spies if they really want to crack a connection. Experts have considered PPTP insecure for some time now, but it is still in use in many commercial systems. The authors of one NSA presentation boast of a project called FOURSCORE that stores information including decrypted PPTP VPN metadata.

Using a number of different programs, they claim to have succeeded in penetrating numerous networks. Among those surveilled were the Russian carrier Transaero Airlines, Royal Jordanian Airlines as well as Moscow-based telecommunications firm Mir Telematiki. Another success touted is the NSA's surveillance of the internal communications of diplomats and government officials from Afghanistan, Pakistan and Turkey.

Ipsec as a protocol seems to create slightly more trouble for the spies. But the NSA has the resources to actively attack routers involved in the communication process to get to the keys to unlock the encryption rather than trying to break it, courtesy of the unit called Tailored Access Operations: "TAO got on the router through which banking traffic of interest flows," it says in one presentation.

Anything But Secure

Even more vulnerable than VPN systems are the supposedly secure connections ordinary Internet users must rely on all the time for Web applications like financial services, e-commerce or accessing webmail accounts. A lay user can recognize these allegedly secure connections by looking at the address bar in his or her Web browser: With these connections, the first letters of the address there are not just http -- for Hypertext Transfer Protocol -- but https. The "s" stands for "secure". The problem is that there isn't really anything secure about them.

The NSA and its allies routinely intercept such connections -- by the millions. According to an NSA document, the agency intended to crack 10 million intercepted https connections a day by late 2012. The intelligence services are particularly interested in the moment when a user types his or her password. By the end of 2012, the system was supposed to be able to "detect the presence of at least 100 password based encryption applications" in each instance some 20,000 times a month.

For its part, Britain's GCHQ collects information about encryption using the TLS and SSL protocols -- the protocols https connections are encrypted with -- in a database called "FLYING PIG." The British spies produce weekly "trends reports" to catalog which services use the most SSL connections and save details about those connections. Sites like Facebook, Twitter, Hotmail, Yahoo and Apple's iCloud service top the charts, and the number of catalogued SSL connections for one week is in the many billions -- for the top 40 sites alone.

Hockey sites monitored

Canada's Communications Security Establishment (CSEC) even monitors sites devoted to the country's national pastime: "We have noticed a large increase in chat activity on the hockeytalk sites. This is likely due to the beginning of playoff season," it says in one presentation.

The NSA also has a program with which it claims it can sometimes decrypt the Secure Shell protocol (SSH). This is typically used by systems administrators to log into employees' computers remotely, largely for use in the infrastructure of businesses, core Internet routers and other similarly important systems. The NSA combines the data collected in this manner with other information to leverage access to important systems of interest.

Weakening Cryptographic Standards

But how do the Five-Eyes agencies manage to break all these encryption standards and systems? The short answer is: They use every means available.

One method is consciously weakening the cryptographic standards that are used to implement the respective systems. Documents seen by SPIEGEL show that NSA agents travel to the meetings of the Internet Engineering Task Force (IETF), an organization that develops such standards, to gather information but presumably also to influence the discussions there. "New session policy extensions may improve our ability to passively target two sided communications," says a brief write-up of an IETF meeting in San Diego on an NSA-internal Wiki.

This process of weakening encryption standards has been going on for some time. A classification guide, a document that explains how to classify certain types of secret information, labels "the fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable" as Top Secret.

Cryptographic systems actively weakened this way or faulty to begin with are then exploited using supercomputers. The NSA maintains a system called Longhaul, an "end-to-end attack orchestration and key recovery service for Data Network Cipher and Data Network Session Cipher traffic." Basically, Longhaul is the place where the NSA looks for ways to break encryption. According to an NSA document, it uses facilities at the Tordella Supercomputer Building at Fort Meade, Maryland, and Oak Ridge Data Center in Oak Ridge, Tennessee. It can pass decrypted data to systems such as Turmoil -- a part of the secret network the NSA operates throughout the world, used to siphon off data. The cover term for the development of these capabilities is Valientsurf. A similar program called Gallantwave is meant to "break tunnel and session ciphers."

In other cases, the spies use their infrastructure to steal cryptographic keys from the configuration files found on Internet routers. A repository called Discoroute contains "router configuration data from passive and active collection" one document states. Active here means hacking or otherwise infiltrating computers, passive refers to collecting data flowing through the Internet with secret NSA-operated computers.

An important part of the Five Eyes' efforts to break encryption on the Internet is the gathering of vast amounts of data. For example, they collect so-called SSL handshakes -- that is, the first exchanges between two computers beginning an SSL connection. A combination of metadata about the connections and metadata from the encryption protocols then help to break the keys which in turn allow reading or recording the now decrypted traffic.

If all else fails, the NSA and its allies resort to brute force: They hack their target's computers or Internet routers to get to the secret encryption -- or they intercept computers on the way to their targets, open them and insert spy gear before they even reach their destination, a process they call interdiction.

A Grave Threat to Security

For the NSA, the breaking of encryption methods represents a constant conflict of interest. The agency and its allies do have their own secret encryption methods for internal use. But the NSA is also tasked with providing the US National Institute of Standards and Technology (NIST) with "technical guidelines in trusted technology" that may be "used in cost-effective systems for protecting sensitive computer data." In other words: Checking cryptographic systems for their value is part of the NSA's job. One encryption standard the NIST explicitly recommends is the Advanced Encryption Standard (AES). The standard is used for a large variety of tasks, from encrypting the PIN numbers of banking cards to hard disk encryption for computers.

One NSA document shows that the agency is actively looking for ways to break the very standard it recommends - this section is marked as "Top Secret" (TS): "Electronic codebooks, such as the Advanced Encryption Standard, are both widely used and difficult to attack cryptanalytically. The NSA has only a handful of in-house techniques. The TUNDRA project investigated a potentially new technique -- the Tau statistic -- to determine its usefulness in codebook analysis."

The fact that large amounts of the cryptographic systems that underpin the entire Internet have been intentionally weakened or broken by the NSA and its allies poses a grave threat to the security of everyone who relies on the Internet -- from individuals looking for privacy to institutions and companies relying on cloud computing. Many of these weaknesses can be exploited by anyone who knows about them -- not just the NSA.

Inside the intelligence community, this danger is widely known: According to a 2011 document, 832 individuals at GCHQ alone were briefed into the BULLRUN project, whose goal is a large-scale assault on Internet security.