Berner Fachhochschule
Technik und Informatik
Informatik

Christian Grothoff

Höheweg 80
2502 Biel

Telefon 032 321 64 88

christian.grothoff@bfh.ch
www.ti.bfh.ch

BFH | Höheweg 80 | 2502 Biel

12. Februar 2020

To Gareth Peirce,

I am Professor of Computer Science at the University of Applied Sciences in Bern. My main area of research is network security, including peer-to-peer networks and applied cryptography. I have a PhD from UCLA, was Assistant Professor at the University of Denver, and lead research groups in the area of network security at the Technical University of Munich and INRIA.

I was asked by the legal team of Julian Assange (Birnberg Peirce) to explain the following technical details to the court, and to do an investigation of information in the public domain on the first origins of the unredacted cables. I will present my findings in chronological order, interspersing the reconstructed history of events with related technical explanations.

(1) Summer 2010: ***Wikileaks shares access to the diplomatic cables with David Leigh using an obscure file on a website. This file is protected by a strong passphrase that serves as the key for decryption.[1] David Leigh, a reporter for The Guardian, is given the passphrase to decrypt the documents, together with extensive security instructions for how to handle the documents safely to prevent accidental disclosure.[2]***

In cryptography, we define a *key* as a short information asset. By encrypting documents to a key we obtain ciphertext. This ciphertext can be transmitted, shared, and stored with the assurance that only those in possession of the key can decrypt the ciphertext and access the original document. Basically, encryption allows us to focus our effort to guard the secrecy of the document on the (short) key, instead of the (large) document.

The key required for decryption is fixed at the time of encryption. Once the ciphertext has been generated, the key never changes.

[1] https://www.spiegel.de/international/world/leak-at-wikileaks-accidental-release-of-us-cables-endangers-sources-a-783084.html

[2] David Leigh and Luke Harding, "WikiLeaks: Inside Julian Assange's War on Secrecy", ISBN 978-0-85265-239-8

To the best of our scientific knowledge today, the specific encryption chosen for the documents in question was secure, and the only way to decrypt the documents was by being given the passphrase. Thus, distributing the ciphertext via the Web site was a safe choice under the assumption that the passphrase would be adequately protected. However, once the passphrase was disclosed, there was equally no way to prevent anyone who had access to the ciphertext and the passphrase from decrypting the information.

(2) 28.11.2010: ***The Guardian, El Pais, Le Monde, Der Spiegel, and The New York Times begin publishing redacted cables they obtained from Wikileaks.[3] At the same time, a Distributed Denial-of-Service (DDoS) attack begins on Wikileaks.[4]***

In a DDoS attack, an attacker attempts to overwhelm the resources of the victim by automatically sending a large number of requests. DDoS attacks often involve using a botnet to both hide the actual origin of the attack and to minimize the cost to the attacker by abusing third party resources for the attack. As the victim's server cannot distinguish between requests made by legitimate users and requests made by the attacker, resulting in legitimate users often being unable to reach the service or at least being frustrated by long delays. DDoS attacks, especially weaker ones, can be costly to the victim. However, they usually do not directly cause any loss of data; the data merely becomes less available for third parties.

DDoS attacks are generally considered criminal acts and are sometimes used to target human rights groups. For example, there are various reports of DDoS attacks against Hong Kong from China relating to the recent protests there.[5]

(3) 2.12.2010: ***The DDoS attack against Wikileaks raises to the point that EveryDNS.net terminates DNS hosting for Wikileaks as the attack impacts its other users.[6]***

DNS provides name resolution. Name resolution is the first step performed by browsers when accessing a Web site. While DNS is sometimes involved in DDoS attacks, in ordinary operations DNS is never the bottleneck for Web sites due DNS's inherent support for decentralized caching of DNS replies.

This demonstrates that the attack was not easily compensated by providing more computing resources, and that the style of attack makes clear that the attacker does not care about causing collateral damage to unaffiliated third parties.

[3] **See, for example,** https://www.spiegel.de/international/world/wikileaks-faq-what-do-the-diplomatic-cables-really-tell-us-a-731441.html

[4] https://www.wired.com/2010/11/wikileaks-attack/

[5] https://www.theverge.com/2019/6/13/18677282/telegram-ddos-attack-china-hong-kong-protest-pavel-durov-state-actor-sized-cyberattack,
https://www.zdnet.com/article/china-resurrects-great-cannon-for-ddos-attacks-on-hong-kong-forum/

[6] https://web.archive.org/web/20101206221243/http://www.everydns.com/news.php

(4) **December 2010:** *In a collective effort to defeat the DDoS attack, third parties globally begin to mirror the information from the Wikileaks Web site and a repository of past publications on hundreds of alternative locations, setting up additional Web sites and BitTorrents with the data in an attempt to make the data broadly available.*[7] *Some of these mirrors include the encrypted copy of the encrypted archive of the cables given to Leigh under the filename "xyz_z.gpg".*

BitTorrent is a common technique employed by organizations world-wide to cope with situations where their own bandwidth is insufficient to serve demand. By enlisting computers of other participants, the load is shared and data remains reasonably available even if the primary source is overloaded. The basic technique has been used in the past by Microsoft to distribute updates to its operating system, and the popular Debian operating system uses it today to distribute its installation medium. When facing denial of service attacks on static resources (like files) using BitTorrent is thus an established defense technique to scale one's bandwidth.

In general, mirroring information, that is making a copy of the information available at another location, is a widely used technique to preserve availability of information.

Setting up such a mirror or BitTorrent is often done for servers serving a large number of files. Here, the people creating the mirrors rarely look at the individual files, and instead simply use a computer program to make a copy of everything. Given that Cablegate involved a very large number of files and that mirrors were setup quickly, it is very likely that this case of blindly mirroring everything was the case here. Once the copy has been made, the data source no longer matters and the data can be kept available without its involvement.

However, as noted under (1), the xyz_z.gpg file remains entirely useless without the proper passphrase.

(5) 1.02.2011: ***David Leigh's book on "WikiLeaks: Inside Julian Assange's War on Secrecy" (ISBN 978-0-85265-239-8) is published. In it, Mr. Leigh discloses the passphrase.***

As David Leigh writes in the book, "He (David Leigh) asked Assange to stop procrastinating, and hand over the biggest trove of all: the cables." (...) In return he would give Assange a promise to keep the cables secure, and not to publish them until the time came.". David Leigh writes that "(Assange) had instructed him that he must never allow his memory stick to be connected to any computer that was exposed to the internet".

By itself, the passphrase disclosed by Mr. Leigh is useless, just like a physical house key found in the street. It opens some house. Without knowing which house, the key is useless.

Wikileaks itself cannot rectify the situation. It is not in control of the many mirrors of xyz_z.gpg already online. The published book has provided the key.

[7] https://web.archive.org/web/20190302104117/zen65898.zen.co.uk/wikileaks/

(6) 25.8.2011*: Der Freitag reports that it discovered an encrypted copy of the full archive "on the Internet" and was able to decrypt it using a passphrase they also found "on the Internet". This therefore could draw public attention to David Leigh's information leak.*[8]

(7) 31.8.2011*: Cryptome.org and others report on the specific passphrase and which file it decrypts.*[9] *On the same day (before 8pm) someone else makes a first searchable copy of the cables available at http://cables.mrkva.eu/. At 23:44 GMT Wikileaks makes its first public statement on the information breach in David Leigh's book.*[10]

(8) 1.9.2011: *A user "droehien" creates a BitTorrent with the decrypted Cables at The Pirate Bay.*[11] *The Pirate Bay is well-known for people sharing copyrighted information without the consent of the owner. Just like the movie industry has found it difficult to restrict the illegal sharing of their movies online, it is now virtually impossible for Wikileaks to limit the distribution of the archive.*

(9) 2.9.2011, 1:20 am GMT: *The information already published by others is re-published on the WikiLeaks site.*[12]

In conclusion, at the time when the Wikileaks site republished the unredacted cables, the information was already easily available to any technically competent person, for example from the cryptome.org site.

Best regards,

Christian Grothoff
Professor für Informatik

Berner Fachhochschule
Technik und Informatik

Berner Fachhochschule
Haute école spécialisée bernoise
Technik und Informatik
Technique et informatique
Fachbereich Informatik / Section d'informatique
Postfach / Case postale
CH-2501 Biel/Bienne

[8] https://www.freitag.de/autoren/steffen-kraft/leck-bei-wikileaks

[9] https://web.archive.org/web/20111130103442/http://nigelparry.com/news/guardian-david-leigh-cablegate.shtml

[10] https://twitter.com/wikileaks/status/109048944943841280

[11] https://thepiratebay.org/torrent/6644172

[12] https://twitter.com/wikileaks/status/109435393639849986, https://twitter.com/wikileaks/status/109579374839345152