CLOUDFLARE®

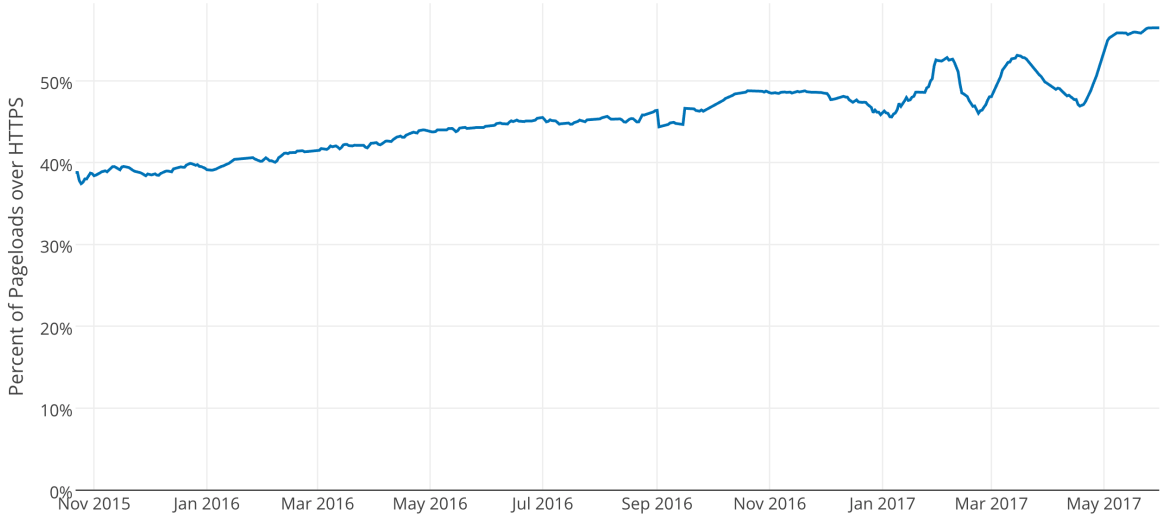
Policy Primer: The Encryption Conundrum

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Pervasive encryption is a reality

Encryption is already comprehensively embedded into our daily lives. It is an essential ingredient in online banking, checking the status of a health insurance claim, credit card transactions, watching satellite TV, or communicating via WhatsApp.

Millions of websites now routinely encrypt traffic in transit in order to protect data from being compromised and ensure user privacy. According to Mozilla's statistics, an encryption milestone was met in early 2017 when the average volume of encrypted traffic on the internet surpassed the average volume of unencrypted traffic.



Source: https://letsencrypt.org/stats/

The fact that this tipping point has been reached while the increased use of encryption has been largely imperceptible to users demonstrates the versatility of encryption technology. Security and data integrity in day-to-day life is of increasing importance and thanks to encryption capabilities, user trust in online services has rapidly increased and innovation, resulting in economic growth and consumer convenience, has thrived. In the not-too-distant future, it is likely that all data, whether data at rest or data in transit on a network, will be encrypted.

Tracing the steps

The desire to communicate discretely and securely traces as far back as Ancient Egyptian and Roman times. Modifications of the Egyptian hieroglyphic alphabet were found in ancient remains, and Julius Caesar used the rather simple 'Caesar Cipher', involving alphabet letter replacement, to protect his private communications.

At its core, **encryption involves a series of operations performed on information that renders it unreadable to all but the intended and authorized recipient.** Encrypted communications are, for example, used for government and military purposes and during World War II, the famous cipher Enigma was used by German armed forces arranging their military manoeuvres, until such time as the team at Bletchley Park in England successfully managed to break the code, and in doing so saved countless lives.

Modern encryption has moved on in its sophistication as a result of the growing volume of data and transactions taking place on the internet, and a need to ensure privacy for even non-threatening tasks such as online banking. Modern encryption algorithms rely on complex mathematical values and recipient keys to unlock the code, meaning that brute force or permission is really the only way to access what is needed or desired. Encryption is ultimately designed to be resilient against interference, although every encryption system will have its weaknesses.

Given the now widespread use of encryption, it is incorrect to assume that it is used for nefarious purposes and, as illustrated above, it is equally wrong to assume that all efforts to break or bypass encryption are ill-intended.

Forms of encryption

Encryption used in communication, otherwise known as **encryption for data transit**, can take many forms, and is frequently managed with a 'key' - a random string of bits created to scramble and unscramble data. With *symmetric encryption*, both the sender and the recipient have access to the same key for decryption, while in *asymmetric encryption* the information secured with a public key can only be decrypted with a matching private key. *End-to-end encryption* is used for WhatsApp communications, and is the most secure form of encryption in that only the sender and specified recipient can access the communication. Key components of encryption in data transit are the digital 'handshake' between the two parties exchanging the messages, and the authentication of both the source and destination of the message.

Encryption for data at rest (data in storage) is also critical. Data that is not actively moving from device to device or network to network, such as data stored on a hard drive, server or in a data centre, is sometimes considered to be less vulnerable but is equally open to attack and can be compromised.

Encryption as an enabler of human rights

At a time when the public is (rightly) concerned about cyber-attacks, the privacy and security protections offered by encryption may be taken for granted. However, encryption also offers a vital means to communicate privately and without undue interference. The principle of confidentiality of communications is codified in Article 19 of the Universal Declaration[1] of Human Rights, even if it is not yet recognized in all societies and not all citizens enjoy the freedom of opinion and expression.

Encryption is therefore essential for political activists and journalists, allowing them to communicate and express themselves freely, and in particular impart information in territories where the freedom of expression is frowned upon. And as noted in a 2015 report[2] by the United Nations Special Rapporteur for the Freedom of Expression, **any restrictions on encryption and anonymity, as enablers of the right to freedom of expression, should meet a well-known three-part test:** any limitation on expression must be provided for by law; may only be imposed for legitimate grounds, and must conform to the strict tests of necessity and proportionality.

The European Data Protection Supervisor has gone as far to say[3] that the use of end-to-end encryption should be encouraged and when necessary, mandated, in accordance with the principle of data protection by design. This support for encryption has also been echoed by the EU Article 29 Working Party, which has stated[4] that it would welcome new obligations to use algorithms and standards that have proven to be secure, to respect the confidentiality of encrypted communications and to prohibit the decryption, reverse engineering or other monitoring of those communications protected by encryption.

The good, the bad, the ugly

Organisational support[5] for encryption from entities such as the Internet Architecture Board (IAB), the Internet Engineering Task Force (IETF) and the Internet Society (ISOC) have helped advance the case for encryption in recent years. However, the now pervasive use of encryption means that while it has many laudable uses, public sentiment can focus disproportionately on nefarious uses. In the very same way that a kitchen knife can be used both by a chef and a murderer, it is the case that criminals can sometimes leverage the anonymity and security offered by encrypted communications for their actions. This poses a challenge for law enforcement officials and the intelligence community, who sometimes need access to information to pursue a criminal case. Undeniably, the work of law enforcement has become increasingly complex as technology has advanced.

Particularly in cases involving terrorism, there is an almost inevitable assumption at the outset that there is an online component to the crime and so an approach is usually made by a law enforcement agency towards a provider of communication services. Even in the absence of any evidence of necessity or accuracy, the communications service provider may be asked to provide a workaround in the form of backdoor access, in order to allow encrypted messages to be decrypted without the knowledge of the sending or receiving party. However, while such access *may* be technically possible in principle, it would effectively trigger a vulnerability and these weak points could be exploited by criminal or State actors. Furthermore, the existence of a backdoor

1 http://www.un.org/en/universal-declaration-human-rights/

2 http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

3 https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

4 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

5 https://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default

would put legitimate users at risk as their communications/data could be indiscriminately targeted. **Intentionally compromising encryption, even for a legitimate purpose such as fighting crime, weakens everyone's security online and the collateral damage is unmeasurably large.**

In February 2016, a federal magistrate judge in the U.S. District Court for the Central District of California ordered Apple to assist the Federal Bureau of Investigation (FBI) in obtaining encrypted data from an iPhone related to a 2015 shooting in San Bernardino, California. Apple resisted the order, and published an open letter to its customers [6] expressing its concern. While this case involved data at rest as opposed to data in transit, the underlying premise remains the same: there is no way to completely guarantee control and the isolation of specific data in cases where security is bypassed and a backdoor is created.

Furthermore, as noted by the European Agency for Network and Information Security (ENISA) in its paper [7] on encryption, there is little doubt that in the face of backdoor facilitation, criminal operators would simply resort to developing their own independent encryption systems, and a game of whack-a-mole would ensue.

Encryption workarounds, whatever form they take (e.g compelling third parties to provide access, exploiting a technology flaw or brute force) are inherently problematic, and often raise complex legal questions, practical and technical issues aside. Moreover, there is uncertainty around the success of any workaround, and what may be produced as a result.

In addition, there is as yet **no conclusive empirical evidence to suggest that the growing use of encryption is significantly impacting the ability of law enforcement agencies to solve criminal cases,** or that it is contributing in a negative way to society. Furthermore, it remains largely unknown if data accessed has successfully contributed to an investigative case. While this is clearly a very sensitive and difficult issue, it is one that must be addressed as the risks are high in terms of potential human rights violations.

The solution to such a complex problem, one combining technology, human rights and the evolving rule of law in this area (including jurisdictional issues), is not so easily found. It is evident, however, that any solution must be a multi-stakeholder one.

In late 2016, the U.S House Judiciary Committee and House Energy and Commerce Committee issued a report on encryption [8] that was striking because of the strong statements made on a complex issue, signed by the bipartisan leadership of both committees. The report was clear in its recommendation that the U.S Congress should not weaken encryption technology because doing so works against the national interest.

Specifically, the report's findings were as follows:

- Any measure that weakens encryption works against the national interest.
- Encryption technology is a global technology that is widely and increasingly available around the world.
- The variety of stakeholders, technologies, and other factors create different and divergent challenges with respect to encryption and the "going dark" phenomenon, and therefore there is no one-size-fits-all solution to the encryption challenge.
- Congress should foster cooperation between the law enforcement community and technology companies.

6 https://www.apple.com/customer-letter/

7 https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

8 https://judiciary.house.gov/wp-content/uploads/2016/12/20161220EWGFINALReport.pdf

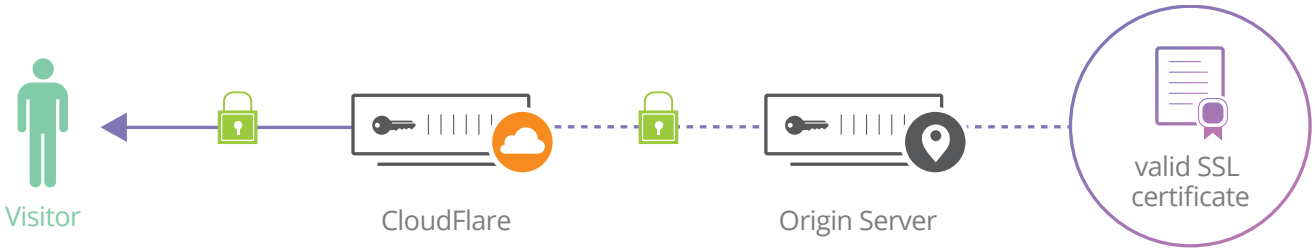
On the last point, regarding pursuance of stakeholder collaboration, there may be opportunities here to reduce any knowledge and capability gaps, and improve law enforcement's effectiveness while also exploring and addressing legitimate civil liberties concerns. A multi-stakeholder approach is also the best way to ensure that a reasonable and proportionate approach, including any burden put on third parties, is found.

Cloudflare's encryption offering

Cloudflare sits between a third party website and the internet and acts as a shield, intelligently protecting against Denial of Service (DDoS) attacks while helping accelerate and improve the speed and performance of that website. Cloudflare is neither a hosting provider nor an ISP but rather a "reverse proxy service".

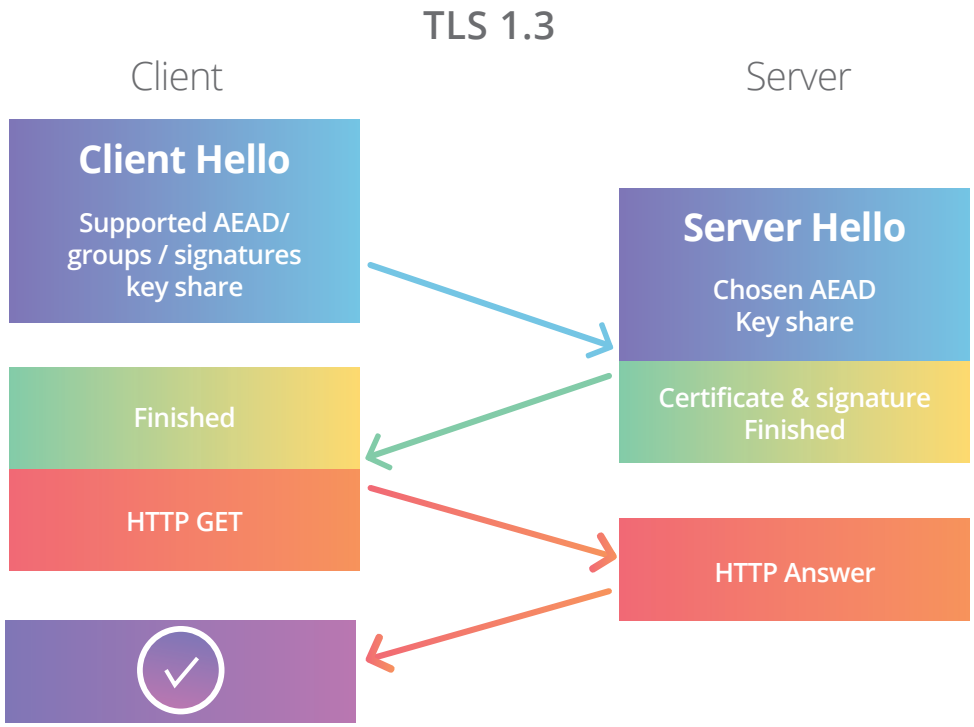
Cloudflare has offered some form of encryption as a default to all its customers since September 2014, and it now supports encryption from the web client (e.g web browser) to the Cloudflare 'edge' (the Cloudflare network) and from the edge to the origin server. The initial Cloudflare encryption offering, called "Universal SSL", allowed the connection between the browser and Cloudflare's edge to be encrypted with a protocol called SSL/TLS, and laid the groundwork for Cloudflare to later roll out encryption optimizations.

Cloudflare now [9] leverages the latest web security technology - TLS (Transport Layer Security) 1.3 - to protect web communication. Cloudflare also offers "opportunistic encryption" by encrypting the connection between a user's web browser and Cloudflare, even in situations where a site has not enabled HTTPS (a communications protocol for secure communication).



To send a message to an encrypted site, you must first establish shared cryptographic keys via a cryptographic handshake which requires special messages to be sent back and forth between the browser and the website. The TLS handshake happens behind the scenes whenever a user connects to an encrypted site with a browser.

9 https://blog.cloudflare.com/introducing-tls-1-3/



Cloudflare's policy position

Cloudflare fully supports encryption as a tool to ensure the privacy and security of communications, and Cloudflare's goal is to move towards a version of the web where secure, encrypted channels are the norm.

Encryption is a fundamental and essential tool for cybersecurity and data integrity, as well as being an enabler of human rights.

While recognizing the challenges that law enforcement agencies face today, **it is important to have an evidence-based debate insofar as encryption is part of the picture.** Policy solutions should never be imposed without due consideration of facts, and the rule of law.

Cloudflare believes that **any government requests to weaken encryption and facilitate backdoor access are at best shortsighted and at worst, detrimental to society at large.**

A multi-stakeholder dialogue is recommended to help find a balanced, proportionate and workable approach to the policy and societal challenges faced today, and Cloudflare is committed to engaging in such debate.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com