ENISA's Opinion Paper on Encryption

Strong Encryption Safeguards our Digital Identity

DECEMBER 2016

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquiries about this paper, please use press@enisa.europa.eu.

Table of Contents

1. Purpose

The opinion paper gives an overview of cryptography in the context of proposals to reduce the strength of encryption to facilitate interception and decryption of communications by the Security Services.

The brief gives an overview of the history of cryptography and the different types of services and how internet services are now becoming reliant on strong encryption to protect communications from criminals and fraud. The brief outlines how technology is changing quickly and that the proposal to use backdoors has not worked in the past and is facing increasing technical challenges.

In section 7 the work of ENISA in this area including the work with Europol is described. The final section outlines ENISA's conclusions.

2. Key Messages

- The use of backdoors in cryptography is not a solution. Existing legitimate users are put at risk by the very existence of backdoors. The wrong people are punished.
- Backdoors do not address the challenge of accessing of decrypting material because criminals can already develop and use their own cryptographic tools.
- Judicial oversight may not be a perfect solution as different interpretations of the legislation may occur.
- Law Enforcement solutions need to be identified without the use of backdoors and key escrow. It is very difficult to restrict technical innovation using legislation.
- History has shown that technology beats legislation and criminals are best placed to capitalise on this opportunity.
- The perception that backdoors and key escrow exist can potentially affect and undermine the aspirations for a full embraced Digital Society in Europe.
- History has shown that Legal Controls are not always successful and may harm and inhibit innovation.
- The experience in the US that limiting the strength of encryption tools inhibited innovation and left the competitive advantage in this area with other jurisdictions.

3. Executive Summary

The two main aspects of Cryptography are encryption and digital signatures.

Many jurisdictions have taken slightly different approaches to regulating the use of Cryptography. Some jurisdictions have attempted to limit the effectiveness of encryption by the use of back doors, import export legislation and the requirement to provide clear text following judicial approval. Europe has recently adopted the eIDAS Regulation[1] on electronic identification and trust services including the use of Digital Signatures. The Regulation gives effect to the policy to facilitate and encourage the widespread adoption of digital signatures across the Single Market.

Digital Signatures often use the same technology as is used for encryption. However Digital Signatures are used to ensure the integrity (content remains unaltered) and authenticity (who wrote it) of documents and facilitate the equivalence of a binding written signature. Where encryption is concerned, the strength of the cipher is based on the mathematical algorithm used to protect the text and the size of the keys which manage the encryption and decryption process. Therefore, any reduction or limitation of the key size limits the strength of encryption process. Other approaches such as the use of back doors could have a similar reduction on the reliability and trust of both encryption and digital signatures.

Governments and citizens have been investing resources in developing and deploying digital content and services for decades. Our digital economy is seen as the way to improve efficiency, create wealth and to deliver a better quality of life for all.

The internet has facilitated this possibility as it is the only truly ubiquitous telecommunications network in the world. However, the designers of the internet designed the infrastructure to facilitate communications in a very technically efficient manner. As the reach of the internet developed and citizens and industry began to avail from the connectivity possibilities the need for personal and business privacy became important. Communications traffic has transferred from using standard telecommunications systems such as fixed phones and faxes to using the internet protocol standards that facilitate transmission of messages across the public internet.

In the past law enforcement once had relatively easy access to analogue and digital communications traffic at local telecommunications switches. The internet has changed this model in that the switching and transmission of communications messages is mainly in private sector hands and the routing of traffic can be diverted across nodes in many countries and continents at the press of a button. The ability to easily encrypt digital information has added increased challenges for law enforcement. The Digital internet and the deregulation of telecommunications has changed the business model, facilitated the introduction of disruptive business models in such a way that the old methods of doing business are no longer suitable, applicable or effective. It is against this background that the increasing challenge for law enforcement has emerged.

Europe has taken the lead in the world as an advocate for protecting personal information. This protection is given the level of a personal right and has been enshrined in law in the Lisbon Treaty[2], the Charter for

[1] Regulation 910 /2014
[2] Article 16 "Everyone has the right to the protection of personal data concerning them"

Fundamental Rights[3] and more recently in Data Protection legislation[4] and the eIDAS Regulation[5]. The right to privacy is seen as a differentiator for Europe, an approach that will accelerate the adoption of the Digital Single Market and the generator of jobs and wealth of the future.

As with any right and privilege, there are cases where a right has to be balanced against a competing right and restricted for the public good. This approach could be referred to as the tight rope of privacy against security.

One solution that has been put forward by law enforcement to address their diminished operational capability to lawfully intercept communications has been to suggest the implementation of back doors to allow digitally encrypted messages to be decrypted. The principle of the backdoor is that another third party could have a mechanism to independently and without the knowledge of the sending or receiving party decrypt the communication. In an attempt to protect privacy and unlawful use of the back door the concept of key escrow where the covert cooperation of independent parties with law enforcement would be required to facilitate the use of the backdoor to decrypt the communication.

While this is technically possible, ENISA is of the opinion that the risks to the effective operation of the Digital ecosystem could be undermined by this approach. The very existence of backdoors provides an opportunity for criminals or state actors to undermine the privacy of communications and for users to believe that their communications are not secure.

Another argument against the provision of backdoors is that the criminal operators may resort to developing their own independent encryption systems which would leave law enforcement with the additional challenge of identifying the encryption system being used and then setting about breaking the encryption algorithm. The expertise to build new encryption tools is readily available and at present strong encryption products are available on the internet free of charge.

There is already evidence of custom made digital products for use on the internet being designed and marketed specifically for the criminal community. There is little doubt that undermining the privacy of commercially of freely available encrypted tools will generate a new market for new private encrypted products to serve the criminal community.

Ultimately the risk benefit analysis is a political judgement.

[3] Article 8 Under the Charter every citizen has the right of personal data protection. Personal data should be processed fairly for specified purposes, and with the owner's consent, or some other legitimate basis laid down by las supervised by an independent body

[4] General Data Protection Regulation 679/2016

[5] Regulation 910/2014

4. Background

4.1 Historical Context

The desire to protect communications content dates back to 1900 BC where the Egyptians used hieroglyphs in a non-standard way to conceal their messages. The Greeks concealed their messages by wrapping a tape around a stick and writing a message. The receiver of the message needed a similar diameter stick to decrypt the message. The Romans used a method where they shifter the letters by a pre agreed amount. This is known as the Caesar Shift.

Today encryption is often achieved using a method call public key cryptography. This involves two keys a public and private key together. This known as PKI. The two keys are linked mathematically in a way that it is difficult with today's computing power to link the two keys.

When a document is encrypted with the public key of the receiver by the sender the receiver uses their private key to decrypt the cyphered text. While this works in theory a more practical application involves the use of symmetric keys as well as PKI.

A digital signature can be created when a document is encrypted with the sender's private key which can then be verified that it came from that person using the sender's public key. While this works in theory Digital signatures are usually created by calculating from a document a small value that characterises it in the same way a fingerprint characterises a person. This is known as a hash code or message digest. The hash code is then protected using the sender's private key. The hash code, protected in this way, is the digital signature.

When both of the above approaches are used together the document can be encrypted and signed to ensure confidentiality and authenticity together.

Therefore any reduction in the strength of encryption by the use of backdoor technology potentially undermines both digital secrecy and the integrity derived from digital signatures.

5. The increasing importance of cryptography for the Digital society - the tightrope of security vs privacy

While human resources are often considered the most important asset of a company, its information is considered a close second. Today most information is digital. While digital information has many advantages it also has one main disadvantage in that the digital information is harder to protect. As increasing amounts of digital information is transmitted across the internet and the challenge of protecting this information from unlawful use has increased. This challenge has been addressed by the use of encryption. Every day an increasing amount of services and information transmitted on the internet is encrypted. A prerequisite for the successful adoption of the Single Digital Market is the ability to maintain confidential communications between sender and receiver.

As with all rights there are competing interests. Law enforcement have a legitimate right to intercept communications in certain circumstances.

The balance of these rights together with the need to protect confidential communications is known as the tight rope of security v privacy.

This brief outlines the nature of services that are provided over the internet where secrecy and encryption are becoming the norm. The brief also outlines some of the attempts that have been made to meet the requirements of law enforcement while protecting the confidentiality of the communications.

6. Use of Encryption

6.1 E-mail

Electronically communications is quickly replacing the need for paper and the use of traditional postal services. Increasing use is being made of email for general communications, making contracts and managing our personal affairs. In the last few years email service providers have begun to encrypt their services in order to give security to privacy of communications between the end users and the service provider. Any undermining of the privacy of these communications by the use of backdoor encryption could undermine the efficiency and effectiveness of this part of the email service.

Encryption is also used on the servers that store the information. In the event of unauthorised access it would be necessary to decrypt the information before any use could be made of the data. The presence of backdoor technology could undermine the security of the stored data

Where the email involves communication with a third party beyond the service provider the communication is generally sent in the clear text format. Special technical solutions are required where end user to end user encrypted is required and generally there has to be agreement on the encryption standards between the end users.

6.2 Accessing web sites

An increasing number of web site operators are now engaged in ecommerce. Indeed many EU Governments had adopted strategies to encourage the take up by SMEs of web sites that facilitate ecommerce.

In recent years the search engine operators have switched to using secure connection between the end user and the search engine operator. This approach means that when the end user switches on their computer and the start up menu defaults to a search engine, the communications to the Internet is immediately encrypted. If the end user then decides to do online banking another level of encryption operates between the end user and the bank. This approach prevents a person monitoring the communicating and is a defence to what is commonly known as "a man in middle attack". The man in the middle will not be able to see the search engine activity or the subsequent banking activity thanks to the encryption being used.

Encrypted web traffic is signalled to the end user by a lock sign on the browser and or the use of a "https" link on the address field of the browser. End users have been encouraged to look for the "https" text to indicate a secure connection over the traditional "http" text in the address bar of the browser. Currently the use of the https technology is considered secure.

However the existence of a backdoor undermines this confidence will have for the use and take up of new services.

Everyday services where this is important include banking, purchasing and selling online, email access and e-government services.

These examples also illustrate the need for a common approach between different countries to encryption as there is often an international dimension as the telecommunications circuits being used may cross different jurisdictions i.e. the end user could be located in Germany and the server processing the electronic transaction could be located in Ireland or in the US. To ensure secure communication the same standards or at least comparable standards and legislative approaches need to be in force.

In this regard and in order to protect personal information of EU citizens the European Court of Justice (ECJ) set down the operation of the Safe Harbour Principles as being inadequate to protect the data protection required by EU law. This has been subsequently been replaced by the EU US Privacy Shield. While this case does not address encryption directly the principles for the need to adequately protect personal information is the same. In the event that deliberate weakening mechanisms to data protection are introduced the ECJ may question its application in the context of EU data protection law.

6.3 Internet Services

Where initially computer power and storage were centrally located in large mainframe computers, the last few decades have seen a shift to computing power residing on the end user PC and data being stored locally on the same PC or a server owned and operated by the end user.

In the last few years this trend is reversing again with the increased use of "Cloud Computing". This approach is a move back to original days of computing where the end user has little information or computing power and the end user accesses the Cloud for both services and data storage. This model is predicated on the delivery of secure communications between the Cloud and the end users. If the confidentiality of this communication is breached the business of the end user is undermined. The confidentiality of the communication is maintained by the appropriate encryption on the telecommunications access path between the end user and the Cloud provider. In many cases the end user and the cloud provider may be different jurisdictions.

In addition to providing connectivity the Cloud Industry provides for the safe storage of the end users data. The safe storage of data can be ensured by the data being securely encrypted on the servers being used by the end user. The end user has a requirement that his data will remain secure and that it cannot be read or modified by any other person. These two requirements can only be satisfied by the use of strong encryption and strong digital signatures without backdoors.

Weakening of encryption standards potentially weaken the security of the transmission of the digital information and the storage of information on the Cloud's servers.

6.4 Darknet

Darknet generally relates to an arbitrary number of unregistered computers connected to each other in a distributed way where each computer can act as a server for the others. This approach avoids the need for a central server through which all traffic would pass. The approach raises difficulties for law enforcement as the route that a targeted communication would take varies in time and depends on the availability of other connected computers. While this type of infrastructure was initially used for file sharing in a manner that would make the identity of the source difficult to determine, these types of networks are now being used for voice and small amounts of data transfer. When this model is combined with encrypted communications and the absence of records of the communications routes and contents the difficulty for law enforcement increases. Therefore the provision of backdoors technology will not adequately address the requirements for the identity of the plain text as the route of the traffic may be unknown to Law Enforcement.

6.5 New open source

New open source software such as that available from Open Whisper systems which has been according to press articles been adopted by large social media operators[6] and telephone and data operators[7] raise additional challenges for lawful interception. This technology uses a different key for each communication. This technology allows the private keys to be generated and stored on the user's devices. Therefore there is no central repository where the keys can be accessed or stored. This technology is also known as perfect forward secrecy and is an example of the increasing challenge is accessing and decrypting data by third parties.

6.6 Next generation telephone networks

A similar transition is taking place with the provision of next generation telephone services. The model for next generation networks (NGN) is that the intelligence for the management of telephone traffic will be located in a few key servers and that the end user device will have very little intelligence. Once again the effective operation of this business model requires privacy and security on the digital communications links by way of strong encryption. The existence of backdoors potentially undermines the effectiveness of this business model.

[6] Facebook as per www.techworld.com accessed 24th November 2016
[7] Whats App as per www.techworld.com accessed 24th November 2016

7. Technical Solutions that have been considered to address Law Enforcement issues

7.1 Domestic control

There has been no widespread banning of the use of encryption products in Western countries. However more subtle approaches have been considered such as the operation of key recovery or key escrow. The principles behind these approaches involve the ability to recover or the holding of a key to facilitate decryption by an independent third party or parties. These third parties are often referred to as Trusted Third Parties (TTP). Who are the third parties or how the decryption is

released has been the subject of different approaches. One approach is that the TTPs only release the information on the basis of judicial oversight. Another approach which has been put forward in the UN model laws (UNCITRAL) is that legislation be adopted that, subject to Judicial Order, the plain text be made available to law enforcement. In this case the decryption key is not made available to Law Enforcement unless the operation of the Judicial Order is not successful. Another approach is that following a Judicial Ord

Whatever the detail of the method for obtaining the unencrypted communication privacy advocates would claim that the existence of any of these models push the balance of rights too far towards the side of Law Enforcement. The cost and supervision of any of these models would also need to be addressed.

Other technical arguments against the approach of having TTPs is that criminals may use multiple layers of encryption and or develop their own so that multiple different third parties in different jurisdictions may be required to cooperate to give effect to a successful decryption of the communication.er the decryption keys are handed over to Law Enforcement.

7.2 One example of an attempted domestic control in the US

In 1993, the US Government developed the Escrowed Encryption Standard. This initiative became known as "Clipper Chip". The Standard proposed that communications equipment operated in the US would have to have a Clipper Chip installed. The Clipper Chip operated key escrow technology where a special key would allow law enforcement access to the decrypted documents. The special key would be divided into two parts, one part with the US Justice Department and the second

part with the National Institute of Standards and Technology. Following securing a Court Order the two parts of the key could be retrieved thereby facilitating the decryption of the data. While the necessary legislation required to introduce the "Clipper Chip" was never enacted the principles behind Clipper continue to be considered by Law Enforcement in Europe.

7.3 Export Control

The Wassenaar framework has provided a mechanism to control Dual Use goods. By Dual Use it is meant that something that has the capability for civil and military use. In Europe the principles have been given effect by the Dual Use legislation[8]. Some Cryptographic products can be considered to fall into this category. One effect of this approach that depending on the Cryptograhy strength of the product a licence is required before being exported. This is in effect a method of limiting the strength of cryptography products being available in Third Country markets. How effective the restriction of cryptographic products in the fight against crime has never been clear. It can only be assumed that the continued request for back doors means that the restrictions have not been very effective.

7.4 Key Recovery approached can affect the effectiveness of Digital Signatures

The purpose of a digital signature is to address the authenticity of data as oppose to concealing its content. It is not considered that this matter is of prime interest to Law Enforcement. However the same technology is generally used to encrypt the data as well as provide the digital signature. The existence of back doors / key recovery mechanisms can also potentially undermine the authenticity of a document. This is probable an unintended consequence of the provision of backdoors/ key recovery technology.

[8] Regulation No 1382/2014 of 22nd October 2014

8. ENISA work in this area

On the 20th May 2016 ENISA and Europol held a joint conference to discuss lawful criminal investigation that respects 21st Century data protection. The text of the joint declaration produced at the end of the meeting can be found at https://www.enisa.europa.eu/news/enisa- news/enisa-europol-issue-joint-statement.

ENISA is working with Europol to discuss technical options to meet the needs of law enforcement while protecting the needs to maintain strong cryptography. This expert group is called the "The Impact of cryptography on Law Enforcement Agencies". The Terms of Reference of this Group are currently being prepared.

In November 2015 ENISA produced a technical report entitled "2015 algorithms, key sizes and parameter report". This report was only circulated to the Management Board Members of ENISA.

In November 2014 ENISA produced a technical report entitled "algorithms, key sizes and parameter report -2014" https://www.enisa.europa.eu/publications/algorithms-key-size-and- parameters-report-2014

Study on cryptographic protocols, ENISA, 2014 available at:
https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols

Algorithms, Key Sizes and Parameters Report – 2013, 2013, ENISA, available at:
https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report

Securing personal data in the context of data retention, 2013, ENISA, available at:
https://www.enisa.europa.eu/publications/securing-personal-data-in-the-context-of-data-retention

The Use of Cryptographic Techniques in Europe, ENISA, 2011, 54 pages, available at:
https://www.enisa.europa.eu/publications/the-use-of-cryptographic-techniques-in-europe

9. ENISA's conclusions

1. There is a legitimate need to protect communications among individuals and between individuals and public and private organisations. Cryptography provides the electronic equivalent of letter cover, seal or rubber stamp and signature. In the light of terror attacks and organised crime, law enforcement and intelligence services have requested to create means to circumvent these protection measures. While their aims are legitimate, limiting the use of cryptographic tools will create vulnerabilities that can in turn be used by terrorists and criminals, and lower trust in electronic services, which will eventually damage industry and civil society in the EU.

2. If backdoor and trusted third party solutions are legislated for, the overhead and cost for the provision of a proper secure service needs to be taken into account.

3. Technology is changing at a very fast pace. It is questionable if solutions such as backdoors will be effective given that criminals can develop their own encryption technologies.

4. New technologies which generate once off encryption keys between end users are now being deployed. These keys are not stored centrally by the operator. These types of technologies make lawful interception in a timely manner very difficult. There is every reason to believe that more technology advances will emerge that will continue to erode the possibility of identifying or decrypting electronic communications.

5. The weakening of encryption technology may have the unintended consequences of weakening other aspects of cryptology such as digital signatures.

6. An analysis should be carried out to analyse the benefit to law enforcement of the introduction of backdoor weakened encryption technology as against the potential damage to the take up and operation of the Digital Single Market before any legislation is introduced.

7. Other procedural approaches should be explored that focus on the power of the judicial process to find solutions.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu