Oct 30th, 1:30 PM - 4:15 PM

Importance of Cryptography in the Government

Gazmend Krasniqi
University for Business and Technology, gazmend.krasniqi@ubt-uni.net

Agnesa Pefqeli
University for Business and Technology - UBT, ap43088@ubt-uni.net

Importance of Cryptography in the Government

Agnesa Pefqeli[1] and Gazmend Krasniqi[2]

[1,2]UBT, Prishtina, Kosovo
ap43088@ubt-uni.net[1],
gazmend.krasniqi@ubt-uni.net[2]

Abstract. This paper first of all reflects the need for encryption and then the importance it has managed to accumulate over thousands of years of use. Various factors, mainly of a purpose; being powerful, have influenced the rapid development and stressed the importance of encryption in governing bodies. Depending on in which part of the world it is used and for what reasons it is developed, the importance of cryptography in different governments has shifted to the more powerful countries.
Governments have encountered conflicts due to its popularization, where users of encryption belonging to the non-governmental communities have declined government's requests to gain access to their private data. Cryptography is one of the most important solutions that governments use today to ensure that systems that hold their important data will be secure. It also helps to protect networks and national critical information systems against unauthorized access.
This paper aims to analyze and compare the most popular traditional cryptography approaches in government..

Keywords: Government, Encryption, Importance, Regulation, Algorithm, Security.

1 Introduction

Digitalization and the accessibility of the internet have significantly facilitated communication between two parties. This easing factor has led to an increase in the number of messages exchanged and thus to the need for data protection by other parties who are not intended to have access and who could potentially abuse that data or information.To safely exchange messages, meaning that in order for a readable and meaningful data to be transformed into an unreadable data so that it can travel from source to a target destination, it must undergo the process of encryption.

Various forms of encryption use date back to 1900 BC in Egypt, up to 100 BC to the time of Julius Caesar where encryption was used for war or military purposes so that a hidden and safe communication is established between two parties.These kinds of purposes have continued to be used increasingly by advancing and making the encryption process far more complex so that different states or governments keep their data secure and have inside knowledge of other states from which they are threatened, have interests and are aware of risks to them in general.

Governments have continuously shown interest in increasing encryption algorithms efficiency, so that the algorithms in use can provide integrity and confidentiality of

sensitive information while exchanging and storing. Possessing the right information represents power. World War II was a turning point for secret writing, where primitive computers were invented so that Britain and the United States could decode messages of Germany and Japan. Therefore besides the development of cryptography to encode the data, another branch has been developed alongside; cryptanalysis which is the process of breaking the codes and finding their weaknesses.

2 The Importance of Cryptography in different Countries

Most states define different sets of rules regarding encryption. This is because encryption is a dual-use technology; that is, it has commercial value and military value. In order to harmonize regulations on the export and import of dual-use technologies, many countries have agreed on a list of principles, such as the agreement known as the Wassenaar Arrangement[1].

One of the rules set in the agreement is the size of asymmetric and symmetric keys, where the size of the symmetric key can be as large as 56 bit whereas for the asymmetric key it can be up to 512 bit, while being excluded from export restrictions. In general this agreement defines general import and export parameters where the states participating oblige to.

[1] The 42 participating states in the Wassenaar Arrangement are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States.

2.1 Cryptography in the United States

The United States is currently the largest and leading manufacturer of information technology and security products, and also possesses the most advanced and detailed encryption laws. According to a study released by the NIST[2] department, it is proposed that America has had an economic gain of $ 250 billion during the development and sale of AES[3] systems in the last 20 years.

The United States has not enacted any regulations against the creation, sale or use of encryption products. The imposition of such rules is considered to be contrary to their constitution, although some state security agencies have attempted to prove otherwise. In terms of trade, the US has not imposed any restrictions on the import of cryptographic systems from other countries, but has set strict rules on their export. All exports of such systems are controlled by the Office of Industry and Security, part of the Department of Commerce.

The reluctance to sell them was based on the fact that the British and American systems after World War II were much more advanced, and their sale would make it more difficult to spy on US intelligence agencies in other countries. Lately exporting has started to become easier, unlike in the past when it was burdened with a lot of regulations and bans from the US government. However, even today, companies that have clients abroad are endangered by their placement.

2.2 Cryptography in the European Union

Cryptography under European Union jurisdiction bears a striking resemblance to that in the US in terms of trade policy. According to the regulations in use, the trade of cryptographic systems between member states is completely free from all prohibitions, while trade with non-member states may face some of them. The regulations set by the Council of the European Union (EC No. 1334-2000) follow the steps of the Wassenaar Agreement.

To facilitate trade with certain non-member countries, the EU has set up special trade zones, so that the sale of cryptographic systems goes with as few bans as possible. In terms of supporting these systems, the EU has on many occasions recommended the use of strong encryption systems, and has come out in defense of those systems. In some cases even opposing the government of the United States of America.

During the 1990s, under President Clinton, many proposals were made to enact laws requiring companies that create encryption systems to allow third-party to have access to their encryption keys in the event of their loss. The EU has come out firmly against these proposals in order to protect the privacy of parties using their encryption systems.

2.3 Cryptography in China

China is one of the countries with the most strict laws and regulations regarding the use of cryptography and trade in cryptographic systems. All acts of import and export of such systems that may be used by any individual, company or private or state agency, must go through and be licensed by the State Commission for Encryption Management.

Encryption products may not be sold or purchased without the approval of this commission. All encryption systems that can be used by any individual, company or private or state agency must be approved in advance for operation by the same commission. This rule applies to local and foreign entities operating in China. All of these entities, whether corporations or individuals, must report in detail the encryption systems they use, and be licensed to use them.

Around the year 2000 the Chinese government had issued an order exempting from these rules all products whose main purpose was not encryption, although encryption could be offered as an option within that particular product. In addition to restricting imports, the Chinese government has been proactive in encouraging local companies and agencies to use encryption systems designed and manufactured in China. An example of following policy has been the case when China did not follow the international 802.11 standard created by the IEEE. In addition to failing to comply with the 802.11 standard, China in 2003 established its own WAPI standard and has established regulations that stipulate that every wireless LAN device sold in China must comply with this standard. The WAPI standard was opposed by outsiders on the grounds that it could be insecure and could open the door to wiretapping by the Chinese government on encrypted communications.

3 Relationship between The Government and Commercial Encryption

The relationship between world governments and private companies that provide data encryption platforms has not been very transparent so far. The U.S. government and major tech companies have clashed with each other several times in public. This conflict originates from the government requesting access to private and personal data. The Washington Post reports that federal law enforcement agencies and other government organizations have argued that technology companies should give the government access through a "secret door" to computers, telephone equipment and other systems where information can be stored. Through this "door" federal agencies would bypass encryption protocols so that they have knowledge of email communications, phone calls, messages and other communications performed by users on their platforms that are encrypted.

For the government to achieve its (above) goals, companies that store encrypted data must share their secret key with the government or not encrypt the data at all. Both options are risky and unacceptable for companies which can have significant losses as a result of distrust on the part of users. The moment these companies do not provide their data then all the information they possess is at risk of cyber attacks where the information can be made accessible to the public and that this part of the public may

[2] National Institute of Standards and Technology
[3] Advanced Encryption Standard

have criminal intentions or motives. If companies offer "split key" access then they will not only open the "door" for the government but also for cybercriminals.

The reasons behind these government intentions lie in the belief that technologies such as encryption put the state at risk of terrorist attacks and hinder investigations related to national security. To reduce this risk, many companies want to be contributors in this regard, respectively to give access to the government but without opening the risk to themselves, which is not possible, at least nowadays. Among the strongest arguments presented were through the FBI agency, when they asked Apple to open the iPhone devices of some terrorist attackers, to find more information about the people they had contacted.

Technology companies including Apple, Microsoft and Google have begun to increase encryption of their data and their users data, after it was noticed by the Snowden scandal that the NSA along with other similar agencies had hacked private companies to store data or had intercepted their digital communications. Snowden during his career was a contractor for US intelligence agencies and had spent time within the CIA and NSA. In late May 2013, Snowden left the U.S. after leaking to the media details of extensive surveillance of the Internet and telephone signals by U.S. intelligence agencies. Snowden, who has been granted temporary asylum in Russia, faces espionage charges for his actions during his time in the US.

This event has been a strong announcement for all internet users and has opened the eyes of many companies but also of ordinary users who have used it for personal needs. As a result of the scandal, inter-state relations were also affected and the discussion focused on under whose jurisdiction the information exchanged on the Internet falls. This incident has also affected the relationships between companies that use commercial encryption with the government, especially in terms of reliability.

During 2020 in the US Congress came several proposals, EARN IT act (Eliminating Abusive and Rampant Neglect of Interactive Technologies) being the most important for security activists on the Internet. This proposal has been heavily unwelcomed by many human rights organizations as it allows the government to open the secret "door" and eavesdrop on online communications.

4 AES

AES (Advanced Encryption Standard) is a specification or standard used to encrypt and decrypt electronic information. This standard was approved by the US government or NIST in 2001 and is now widely used worldwide. Also, AES is available in various encryption packages, and is the first publicly accessible encryption which is approved by the US NSA for top secret information.

The original name of AES is Rijndael where it originates from the two Belgian cryptographers Vincent Rijmen and Joan Daemen. Rijndael is a family of ciphers with different sizes of blocks and switches.

Security is a strong pillar of AES encryption. Cryptographers agree that given the current state of technology, it would take billions of years for hackers to penetrate even if a 128-bit key was used. This fact gives great comfort to all those who rely on AES encryption to secure their personal files. Although this standard offers considerable convenience to users, it does not mean that hackers will stop trying to find any way to

penetrate AES encryption. This fact should not be a particular concern because it applies to any other algorithm.

5 Conclusion

Considering all the components in which cryptography has a significant impact, the consequences of cryptography being used by the government, and the continuous development of technology, we can say that the importance of cryptography in government is undoubtedly increasing. Historical events have shown that the vast majority of the population sometimes is not aware of the actions taken by the government, so we must ask ourselves what position we are in, how safe we are and who to trust for sharing our personal data. Every so often we are not able to control the things around us and especially the things over which we have no control or power, it is important to take sufficient care of our security, and in this case, cyber security.

References

1. Huergo, J. (2018). "NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study".
2. (2017). "Government backdoor: The basics of the plan to bypass encryption". Available at : cloudmask.com/blog.
3. (2017). "Why the government isn't a fan of commercial encryption". Available at : cloudmask.com/blog.
4. Perlroth, N. (2015). "Security Experts Oppose Government Access to Encrypted Communication".
5. (2013). "The Importance of Cryptography". Available at : quotium.com/resources
6. Schneier, B. (2016). "The Importance of Strong Encryption to Security".
7. Saper, N. (2013). "International Cryptography Regulation and the
8. Global Information Economy".
9. Flamm, K (1997). "Deciphering the Cryptography Debate".
10. Sidhpurwala, H (2013). "A Brief History of Cryptography".
11. Rembert, L (2020). "What is AES Encryption? A Beginner Friendly Guide".
12. NIST, (2001). "Announcing the ADVANCED ENCRYPTION STANDARD (AES)".
13. n.a, (n.d). "Wassenaar participating states". Available at : Wassenaar.org/participating-states