Encryption: a successful digital security strategy?

Leandro Maglianella

Kingston University

1. Introduction

The advent of the modern digital era has brought a huge amount of information into everyone's lives, which travels perpetually across the entire globe. When the first personal computers in the history of computing came about in the early 1970s, the security of these primordial computing systems was not yet considered necessary and their fundamental importance was understood only starting from the birth of the World Wide Web and from the public use of the Internet (SentinelOne, 2019).

The ultimate goal of security is to effectively protect anything that a company values, be they services, infrastructure, users, physical and digital data: all these elements at risk of a potential attack by an adversary are defined as "assets". A security strategy or policy is developed by a team of experts, through which it is possible to clarify the system weaknesses that could be exploited to threaten and violate the information it contains. Subsequently, the best security measures to be applied to minimise these vulnerabilities are established (Stallings, 2017).

In this report, we will analyse cryptography, one of the multiple security mechanisms used today in data protection. We will cover the encryption techniques, which will be defined and studied in the following section, to then establish how effective encryption is as a security tool and if it will continue to be so in the future, despite the ever faster development of the technologies that surround us.

2. Cryptography fundamentals: encryption

All digital data in our possession are constantly in danger: for instance, they could be both physically compromised by the theft of a computer or smartphone that stores them, or virtually intercepted in their transit on the Internet.

Cryptography concerns all the dynamics that convert information (generally defined as "plaintext" when it is unencrypted) into a "ciphertext", a non-random code impossible to read, transmuting the bytes that form it to hide its true meaning. Cryptography is composed of the encryption and decryption phases: in the first, the data is hidden while in the second it is restored to a readable message; therefore, cryptography simply deals with obscuring a message and making it uninterpretable, but it does not concern the hiding of a message itself (Salomon, 2006).

The encryption process uses an algorithm or cipher to encode the message, using different variables (i.e. different keys) in these algorithms makes their output unique. The recipient of the hidden message, or an intruder who intercepted it, in order to decode it needs the specific keys and it is therefore of primary importance that they are not simply obtainable by anyone (Rouse, 2014).

The most well-known encryption algorithms fall into the following two categories of approach:

2.1 Symmetric (or shared key) encryption

Symmetric encryption uses only one key, which must be kept secret and shared only with those who are authorised to decrypt the messages: because of this, it is necessary that the parties involved in the exchange of the message trust each other (Stallings, 2017). This method is considerably faster than asymmetric encryption, however it is usually more problematic to use as protected key distribution is complex to perform; to deal with this difficulty, a symmetric algorithm is often used for exchanging messages and an asymmetric algorithm for exchanging the key (Rouse, 2014).

2.2 Public key (or asymmetric) encryption

Unlike symmetric encryption, this second approach encrypt messages using two different keys, one public and one private; obviously, these keys are not random but logically linked to each other. Both parties involved in the exchange generate a pair of keys and make the public key accessible by anyone: to send a message now just encrypt it using the recipient's public key, the ciphertext thus obtained will be decryptable only through the use of the recipient's private key (Stallings, 2017). Since the private key is never sent to anyone but only kept locally by the sender, there is no need to trust the recipients (Stallings, 2017).

3. The encryption effectiveness

Let us now analyse the extent to which encryption supports the security of a system by observing how much it ensures a secure exchange of information. For instance, the security goals of confidentiality, according to which information must be accessible only by those authorized, is obtained in asymmetric encryption because only the owner of the private key can read the message; similarly the authenticity of the message can be verified, in this way ensuring that a message was necessarily sent by a specific person and also, if necessary, preventing a sender from denying of being the origin of a malicious message (Rouse, 2014). The integrity (which monitors whether the message has been modified during its path) is guaranteed through a message digest, which stores the initial state of the information and allow to understand if tampering or errors have occurred by comparing it with the message digest produced by the information once it reaches the recipient (Stallings, 2017).

The reason for the great effectiveness of asymmetric encryption lies in the mathematical difficulty of establishing the private key, which is calculated from three prime numbers, two of which are particularly very high and multiplied with each other. The product and the third prime number form the public key. To obtain the private key, it is "simply" necessary to obtain the two starting prime numbers by breaking down the product and, although this may seem like an easy task for a computer to perform, it is not at all. Searching very large prime numbers is in fact one of the most time consuming activities to carry out; for example, NatWest Bank uses a 617-digit number as a public key and it is estimated that several decades are required to break down such a number (Numberphile, 2012). However, due to the evolution of computers, this time is gradually decreasing, making these keys less and less secure. Will this be the end of encryption as a security practice? No, absolutely, it will be enough to replace the old keys with others made up of even more digits to increase their confidentiality exponentially.

4. Conclusion

Encryption and some of its major characteristics have been defined, described and analysed. Encryption has proven to be a particularly advantageous and reliable security mechanism, the use of which is beneficial in any area where some data protection is required. Finally, it has been shown that, excluding some technological discoveries that are currently unpredictable, the level of protection offered by encryption will remain high and easy to increase in the future.

References

- Numberphile (2012) *Encryption and HUGE numbers - Numberphile.* 9 December. Available at: https://www.youtube.com/watch?v=M7kEpw1tn50 (Accessed: 6 January 2020).

- Rouse, M. (2014) *encryption.* Available at: https://searchsecurity.techtarget.com/definition/encryption (Accessed: 6 January 2020).

- Salomon, D. (2006) *Foundations of computer security*. Springer London.

- SentinelOne (2019) *The History of Cyber Security - Everything You Ever Wanted To Know.* Available at: https://www.sentinelone.com/blog/history-of-cyber-security/ (Accessed: 6 January 2020).

- Stallings, W. (2017) *Network security essentials: applications and standards.* 6th edition. Harlow, Essex: Pearson.