Journal of Applied Mathematics and Bioinformatics, Vol. x, No. xx, 2021, xxx-xxx
ISSN: 1792-6602(print), 1792- 6939(online)
Scientific Press International Limited

Evaluating the Security of Cryptographic Systems

George Marinakis [1]

Abstract

In this study, a method is proposed in order to evaluate the security of a cryptographic system, which besides of its cryptographic algorithm which is embedded into the system, includes other critical individual units and security mechanisms. If some of these security mechanisms are inadequate, they may reduce the initial security of the system which is provided by the strength of its cryptographic algorithm. The evaluation method combines the strength of the system's cryptographic algorithm with the strength of all the other security mechanisms and gives a final assessment for the security grade of the whole system. At the end of the study the necessary conditions are presented, for the validity and the duration of the evaluation, taking into account the expected evolution of technology.

Keywords: Cryptography, Data encryption, Communication security, Computer security, Data security, Information security.

1. Introduction

A cryptographic system, is a composite IT system which except of its cryptographic algorithm (which is embedded into the system and it is the core of its security), includes some other individual units and security mechanisms which affect its security. Therefore, as is the case for all systems, the security of a cryptographic system will be equal to the security of its weakest mechanism. For example, even if a cryptographic system has a very powerful algorithm, it cannot be considered secure if it has defects in its key management (because if the key is weak or it is compromised, all the security of the system collapses). For this reason, in the present study, an overall assessment of a cryptographic system security is made, which combines the security of its cryptographic algorithm with the security of its other security mechanisms. The most important of these security mechanisms are the following:

(a). Management of cryptographic keys.
(b). Cryptographic algorithm implementation.
(c). Access control mechanisms.
(d). Tamper proof mechanisms.
(e). Self-test mechanisms.
(f). Electromagnetic protection.

At the beginning of the evaluation of a cryptographic system, we must first take into account any existing certifications which are related to its operational security and are based on international and national standards. These certifications will show the major or minor vulnerabilities of the system or they may help to target some additional and specific security tests that must be done. The most important of these standards are the (FIPS 140-2, 2001) [1] and the

[1] Hellenic Army Academy. E-mail: gmari@tee.gr

Article Info: *Received:* …. .., 2022. *Revised*: …. .., 2022.
Published online: …. .., 2022.

ISO 15408 (ISO/IEC 15408, 2009) [2] which is also referred as Common Criteria (Common Criteria, 2006) [3].

At the end of this study, the necessary operating conditions of the cryptographic system will be examined, under which its evaluation remains to be valid, as well as the criteria for the time duration of the evaluation/certification. Also, the criteria for the expiration or renewal of the evaluation will be examined, as well as the criteria for conducting a new evaluation (periodic or extra-ordinary re-evaluation).

2. Security of an ideal cryptographic system

In order to estimate the security of a cryptographic system, we need to define a reference point. In the context of this study, as a reference point, we consider an ideal cryptographic system, in which all its security mechanisms are designed and implemented in a perfect (or very adequate) way. This means that the security of an ideal cryptographic system corresponds directly to the strength which is provided by its cryptographic algorithm. This is because that all the other security mechanisms of the cryptosystem (mentioned in the previous paragraph) do not reduce the initial security provided by its cryptographic algorithm. This correspondence is shown in Table 1.

However, in practice very few cryptographic systems are ideal, because in most of them there are some flaws or shortcomings in the design or in the implementation of their individual security mechanisms. For this reason, in the next paragraph we will describe a method for the evaluation of a cryptographic system, in which we will take into account all the shortcomings of its security mechanisms.

Table 1. Correspondence of the security grade of an ideal cryptographic system in relation to the strength grade of its cryptographic algorithm.

Crypto-system / Crypto-algorithm	Relation of security and strength grades			
SECURITY OF AN IDEAL CRYPTO - SYSTEM	Low	Medium	High	Very High
STRENGTH OF ITS CRYPTO - ALGORITHM	Low	Medium	High	Very High

3. Cryptographic system evaluation process

In the flowchart of Figure 1, we show the steps of our method for the evaluation of a cryptographic system. The first step, which we must take as the starting point of the evaluation, is to determine the strength of the cryptographic algorithm of the system. The methods for the evaluation of a cryptographic algorithm were examined in three previous studies:

a). Estimation of the cryptographic algorithm strength (classified into four general categories) taking into account the cryptographic key length and the success rate of the randomness tests in the algorithm output samples, according the desired significance level and confidence interval (Marinakis, 2022) [4].

b). Study of the appropriate sampling methods for the statistical randomness tests, calculation of the necessary number and the appropriate size of the algorithm output samples and proposed methods for the reduction of the required time for the tests (Marinakis, May 2021) [5].

c). Study of the various methods for the selection of the sampling keys, combining the random sampling and the stratified sampling (Marinakis, July 2021) [6].

In Figure 1 we show the steps for the evaluation of a cryptographic system, in which we have assumed that the algorithm is evaluated and has a very high strength (top left of the figure). Then, we check one by one, the strength of the other security mechanisms of the system (which were mentioned in paragraph 1), in terms of the adequacy and the completeness of their design and the way that they are implemented.

3.1. Generation and Management of the keys

The most important security mechanism, which is examined first, concerns the Generation and Management of the cryptographic keys. According to what was mentioned in (Marinakis, 2015) [7] , in order for the cryptographic system to maintain the degree of security provided by its cryptographic algorithm, it is very important that its keys must be random and independent. Furthermore, the system must have the capability to produce and load the keys externally, so that the users can manage the keys according to their own security rules and procedures. Detailed recommendations for Cryptographic Key Management are given in (NIST.SP.800-57, 2016) [8] and the rest of the series NIST.SP.800 documents.

a. Evaluation of the Random Number Generator (RNG)

The generation of the keys is done with the use of Random Number Generators (RNGs), the evaluation procedures of which are mentioned in (Marinakis, 2015) [7]. In particular, the evaluation of the randomness of the digital sequences of an RNG, must be done with the same methods which are used for the evaluation of the randomness of the algorithm output samples, as described in (Marinakis, 2021) [5]. That is, we have to generate a large number of RNG output samples and submit them to specific statistical test for randomness. The number of samples *n,* the desired sampling error *e* and the maximum rejected number of samples *m* , must be the same as those used to test the outputs of the algorithm for which the RNG will produce the keys.

Regarding the length of the RNG samples, it is logical that it should not be as long as the length of the algorithmic output. This is because the RNG will produce much shorter outputs (in the order of 128 to 256 bits, which is the key length). As it is suggested in (FIPS 140-2, 2001) [1], when a TRNG is started, only four statistical tests (Monobit, Poker, Runs and Long Run) are applied to a sample of 20,000 bits (in order to reduce the required time). However, this sample length is not enough if we want to produce a long digital key sequence, as in One Time Pad cryptosystems. In these cases, more statistical tests and larger output samples should be used. Of course, this cannot be done during power up self-tests, but must be done in a separate time (off line). For the above reason, as an optimal practical solution, we propose that the size of the RNG output samples must be equal to the size of the algorithm output samples, i.e., in the order of 1Mbit. However, the final decision is up to the evaluator, which of course will depend on the computing power available.

For greater security, many users prefer to use their own RNG for the production of the keys. However, many cryptosystems offer optionally their own external Key Generation Unit (KGU), which is also referred as Key Generation Facility (KGF). If the user wishes to use the optional KGU, he will have to evaluate its RNG, according to what was mentioned above. However, the evaluation of the optional RNG should not necessarily affect the evaluation of the cryptographic system (as shown in Figure 1 with dotted lines), because the cryptosystem may be secure but its RNG may not be.

b. Production of keys from built-in RNG

If the cryptographic system does not have the capability to externally generate and import the keys (i.e., generates the keys with a built-in RNG and automatically enters them into the algorithm without user intervention), this must be considered as a drawback, because the users cannot generate and manage the keys according to their own security rules and procedures. In this case as it is shown in Figure 1, there are two sub-cases:

(1). If the embedded RNG is certified, then the security of the system may be reduced by one degree compared to the strength degree of its cryptographic algorithm. This reduction is at the discretion of the evaluator and depends on how detailed and documented is the certification of the RNG. Therefore, for the example of Figure 1, the cryptographic system may get the temporary security reduction of "High Security" and then the evaluation of its other security mechanisms will follow (which may further reduce its security).

(2). If the embedded RNG is not certified, then we suggest to reduce the security of the system by one or two degrees compared to the strength degree of its cryptographic algorithm. Again, this reduction is at the discretion of the evaluator and depends solely on the level of trust he has in the RNG manufacturer. Therefore, for the example of Figure 1, the cryptographic system may get the temporary security reduction of "Medium Security" and then the evaluation of its other security mechanisms will follow (which may further reduce its security).

3.2. Other security mechanisms

After the evaluation of the cryptographic algorithm strength and the evaluation of the key generation and management system, the next step is to evaluate the strength of the other critical security mechanisms, which were listed as (b), (c), (d), (e), (f) in paragraph 1. The security evaluation of the above individual mechanisms is a separate subject of research and is outside the scope of the present study. However, we will make a brief of description of them, in order to give an overview before we proceed to the next paragraph:

Algorithm implementation: Generally, if the algorithm is implemented in hardware (i.e., in FPGA or ASIC) it will have a greater speed and security (integrity protection). However, a good software implementation can be quite fast, but can be also secure if strict configuration control measures are applied. As it is mentioned in (Marinakis, 2022) [4], the tests on the cryptographic algorithm outputs are usually performed using its software simulation. This means that after testing the software simulated model, the following procedures will be required:

a. Evaluate the implementation of the algorithm (in software, firmware or hardware) and confirm that the evaluated simulation model is identical to the implemented version of the algorithm.

b. Evaluate the way the algorithm is integrated into the cryptosystem, as well as the security measures against the authorized or unauthorized modifications of the algorithm.

c. Evaluate the option of modification/adaptation of the algorithm which is offered by some manufacturers (customization).

Access Control mechanisms: The Access Control include all the technical and procedural security measures which are used in order to use system resources, gain knowledge of the information the system contains, or to control system components and functions. These measures include software and hardware mechanisms (smart cards, biometric systems etc.), physical controls, operating procedures, management procedures, and various combinations of these, designed to detect and deny unauthorized access to the system. More information on Access Control can be found in (NIST.SP.800-162, 2014) [9] and (NIST.SP.800-205, 2019) [10].

Tamper Proof mechanisms: Tamper-Proof are mechanical or electronic technics which prevent unauthorized exploitation of critical technologies of a system, alter functions of a system or access sensitive information of a system. There are various hardware methods for Tamper Resistance, Tamper Prevention, Tamper Detection, Tamper Response and Tamper Evidence. Also, the Anti-Tamper software applications prevent attackers from modify them, using passive measures such as obfuscation against reverse engineering or active tamper-detection which makes a program to malfunction or to not operate if it is modified. More information on Tamper proof systems can be found in (Dubrova, 2018) [11] and (FIPS 140-2, 2001) [1].

Self-Test mechanisms: A cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required). A cryptographic module may perform other power-up or conditional self-tests in addition to the above tests. If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state. All data output via the data output interface shall be inhibited when an error state exists. More information on Self Tests can be found in (FIPS 140-2, 2001) [1].

Electromagnetic protection: All electrical and electronic equipment produce a small amount of electromagnetic radiation, which propagate through space (radiated emissions) and along conductive pathways (conducted emissions). If these undesired emissions are intercepted and analyzed, they could reveal sensitive data which are processed by the equipment (compromising emanations). The study, the signal interception and interpretation, as well as the shielding of the equipment in order not to radiate compromising emanations, are known under the codename TEMPEST. The NATO standards essentially define four security perimeters in terms of the risk for the signal interception: 0-20 meters (high risk), 20-50 (medium risk), 50-100 meters (low risk) and more than 100 meters (very low risk). More information about compromising emanations can be found in (Martin, Sunmola, Lauder 2022) [12] and (NCSC, 2021) [13].

3.3. Evaluation procedure

As it was mentioned in previous paragraphs, in order to conduct a reliable and secure evaluation of a cryptographic system, it is very important to evaluate the strength of all its individual security mechanisms. This means that, concerning the general diagram of Figure1, we will have the following three general cases:

a. All security mechanisms are adequate: If all the mechanisms are adequate (indications "YES" in the flowchart of Figure 1), then the security of the cryptographic system corresponds to the strength degree of its cryptographic algorithm (as it is referred in paragraph 2). That is, for the example of Figure 1, the cryptographic system will have finally a Very High Security grade (bottom right of the figure).

b. All security mechanisms are inadequate: If all the mechanisms are inadequate (indications "NO" in the flowchart of Figure 1), then the security of the cryptographic system must be reduced by one or two degrees compared to the strength degree of its cryptographic algorithm. That is, for the example of Figure 1, the cryptographic system will have a security grade between Medium and High Security, depending on the judgement of the evaluator. In addition, the condition is added, that stricter physical and procedural safety measures must be taken (per mechanism), in order to address the risks due to the insufficiency of the mechanisms.

c. Some of the security mechanisms are inadequate: If only some of the mechanisms are inadequate, then the security grade of the cryptographic system may not be reduced compared to the strength degree of its cryptographic algorithm. Depending on the judgment of the evaluator and depending on the degree of inadequacy of some of its mechanisms, it can maintain the Very High Security due to the strength of its algorithm (example of Figure 1), with some special physical and procedural security measures (per mechanism), in order to address the risks due to the insufficiency of the mechanisms. It is obvious that the evaluators can set a different security weighting factor for each mechanism.

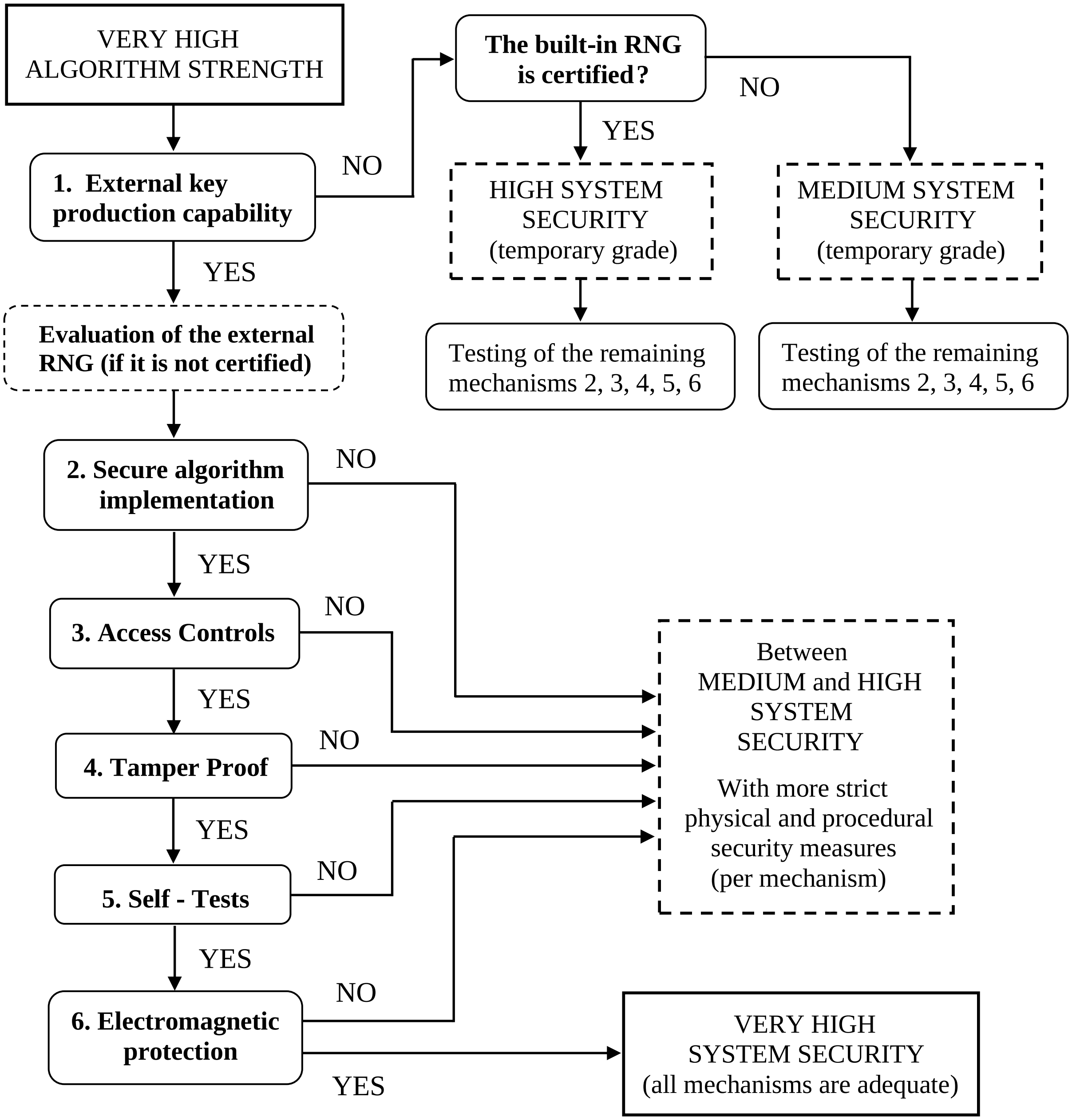
VERY HIGH ALGORITHM STRENGTH
1. External key production capability
NO
YES
The built-in RNG is certified?
NO
YES
HIGH SYSTEM SECURITY (temporary grade)
MEDIUM SYSTEM SECURITY (temporary grade)
Testing of the remaining mechanisms 2, 3, 4, 5, 6
Testing of the remaining mechanisms 2, 3, 4, 5, 6
Evaluation of the external RNG (if it is not certified)
2. Secure algorithm implementation
NO
YES
3. Access Controls
NO
YES
4. Tamper Proof
NO
YES
5. Self - Tests
NO
YES
6. Electromagnetic protection
NO
YES
Between MEDIUM and HIGH SYSTEM SECURITY
With more strict physical and procedural security measures (per mechanism)
VERY HIGH SYSTEM SECURITY (all mechanisms are adequate)

Figure 1. Evaluation example of a cryptographic system with a very high strength algorithm, taking into account the strength of its individual security mechanisms 1,2,3,4,5,6.

Notes:

1. The limits within which the cryptographic system will be determined are at the discretion of the evaluator. For example, the cryptographic system can be a single stand-alone computer or can be a Local Area Network (which except the Communication Server may include an Encryption-Decryption Server and a Key Management Server, which will affect the cryptographic security of the whole LAN).

2. In the case of the temporary grades of the High and Medium Security of the system (upper right part of Figure 1), the testing of the other security mechanisms 2, 3, 4, 5, 6, can further reduce the final security. E.g., if the security mechanisms are not sufficient, the temporary grade of High Security may be reduced to Medium Security and the temporary grade of Medium Security may be reduced to Low Security.

3. The answers to the flowchart in Figure 1 may not be an absolute YES (sufficient strength) or NO (insufficient strength), but an intermediate state. In this case, the assessment of the strength of each security mechanism is at the discretion of the evaluator.

4. For the strength of the security mechanisms, the certification of the cryptographic system according to the FIPS 140-2 and ISO 15408 standards will play an important role. We suggest that the security mechanisms must be considered adequate if the cryptosystem has a security level of 3 or higher (Security Level 3 for FIPS 140-2 and EAL 3 for ISO 15408), and insufficient if the cryptosystem has a security grade of 2 or lower (Security Level 2 for FIPS 140-2 and EAL 2 for ISO 15408).

5. It should be taken into account that some of the security mechanisms are complementary and interdependent. For example, if a system has very strict access control measures and different authorization levels for the users (simple user, administration user, technical user etc.), the tamper proof measures may not be strictly necessary.

Examples:

1. If in a cryptographic system the algorithm is implemented in software, but is to be installed in a safe place, with strict physical protection measures, strict control measures of incoming staff, and automatic self-checks of the integrity of the algorithm at system startup, then it can successfully pass the test no. 2 of Figure 1.

2. If a cryptographic system does not have adequate built-in tamper-proof measures, but is to be installed in a very secure place (with very strict physical protection measures and very strict control measures of incoming staff, etc.), then it successfully passes the test no. 4 of Figure 1.

3. If a cryptographic system does not use sufficient built-in electromagnetic protection technics against compromising emanations, but it will be installed in a shielded chamber with a very good grounding (Faraday cage), then it can successfully pass the test no. 6 of Figure 1.

4. If a cryptographic system does not use sufficient built-in electromagnetic protection technics against compromising emanations, but it will be installed in a place which has a security perimeter more than 100 meters, then it can successfully pass the test no. 6 of Figure 1.

3.4. Evaluation, Certification and Accreditation

After what has been said, it is important to clarify the different terms of evaluation, certification and accreditation, which are relevant to the content of the present study.

Evaluation is the detailed technical testing of the security mechanisms of an information system or product (IT system), in order to investigate any existing problems and vulnerabilities.

Certification is the issuing of an official document, which is based on the results of an evaluation and which states the extent to which an information system or product meets specific security requirements, i.e. states the level of the security it provides.

Accreditation is the operating authorization given to a complex information system, so that it can process classified information within its particular operational environment (various network connections, various computers and peripherals, different classification levels of the processed information, different authorization of the users, different installation premises, etc.).

Therefore, in the context of the present study, after the technical evaluation of the cryptographic system which was described in the previous paragraphs, a certificate must be issued by the competent authority, based on the technical report of the evaluation. And when the system will be ready for operation, the process of the security accreditation must follow, which must take into account all the technical, physical and human particularities of the environment in which the system will operate. Detailed guidelines about the certification and accreditation processes can be found in (NIST.SP.800-100, 2006) [14].

4. Conditions for the validity of the evaluation

After conducting an evaluation, there are some basic conditions that must be met during the operation of the cryptographic system, in order for its evaluation and the corresponding certification which is given to it to be valid. The most important conditions concern the following three security measures for the management of cryptographic keys:

a. Randomness of the keys: The keys must be produced from a RNG which has a certified randomness and which has an entropy at least equal to the entropy of the cryptographic algorithm.

b. Secure key management: Strict physical and technical measures must be followed in order to protect the cryptographic keys (from leakage, theft, deterioration, destruction etc.) throughout their life cycle.

c. Frequent key change (small cryptoperiod): The cryptoperiod should be as smaller, as grater are the threats and vulnerabilities of the cryptographic system. For this reason, a very strict risk analysis of the cryptographic system must be done.

Recommendations and details for the above measures can be found in (NIST.SP.800-57, 2016) [8] and the rest of the series NIST.SP.800 documents.

4.1. Duration of evaluation and re-evaluation

The time period during which an evaluation will be valid, in addition to the strict application of the aforementioned measures for the security of the keys, also depends on the appearance over time of some cryptanalytic threats against the cryptographic system (e.g., increase of computer power which can shorten the time of the Exhaustive Key Search). These threats can be addressed either by an emergency re-evaluation (urgent) or by a regular re-evaluation (preventive or periodic).

4.1.1. Extraordinary re-evaluation

An emergency re-evaluation of the cryptographic algorithm should be performed immediately when any of the following three serious cryptanalytic threats occur:

a. A method of cryptanalytic attack against the algorithm has become known (in case that the algorithm is published).

b. There is an indication or certainty that the algorithm or some elements of its structure have been leaked (in case that the algorithm is secret).

c. A serious malfunction or a successful intrusion attack has happened to a security mechanism of the system.

The emergency re-evaluation is performed in order to determine if the cryptographic algorithm is still secure and if all the information which were encrypted with it are at risk. In case that the re-evaluation shows that the algorithm no longer provides the same level of security, it should be replaced as soon as possible with a stronger one. Also, for precautionary reasons and if it is possible, all the stored information which were encrypted with the old algorithm should be re-encrypted with the new algorithm and re-stored.

Depending on the case, as an alternative or temporary solution until a new and more powerful algorithm is selected, the old algorithm may continue to be used, by increasing the frequency of its key changes (reduction of the cryptoperiod) or by re-encrypting its output by another algorithm (double encryption).

Over time, in addition to the cryptanalytic threats against the algorithm, it is possible that may appear some new methods of attacking the security mechanisms of the cryptographic system, (which were mentioned in paragraph 3.2). In this case, an emergency re-evaluation should also be carried out on the security mechanisms which are under risk.

4.1.2. Regular re-evaluation

As mentioned in the previous paragraph, the emergency re-evaluation of the cryptographic system is carried out when the existence of a serious threat is detected. However, this finding can be made late and so there may have already been some damage to the security (e.g., algorithm cryptanalysis and decryption of classified information). For this reason, a regular re-evaluation of the cryptographic system should be carried out periodically, in order to prevent any attacks against it in a timely manner. The process of the regular re-evaluation is the same as the process of the initial evaluation (described in paragraph 3). During this re-evaluation, the following factors should be investigated and taken into account:

a. The evolution of technology in the field of power (speed) of computers. Such an evolution could drastically reduce the time of the attack with Exhaustive Key Search.

b. The evolution of analytical cryptanalytic attacks on the cryptographic algorithm, as well as attacks on other security mechanisms of the cryptographic system.

c. The evolution in the evaluation methods of cryptographic systems.

It is obvious that research should be constantly carried out in order to find new improved evaluation methods and practices (e.g., adding new statistical tests, increasing computing power in order to test more and larger samples, etc.). And it is very important, in any re-evaluation (regular or extraordinary) to take into account these improved methods and practices, because they may reveal some new vulnerabilities in the evaluated cryptographic system.

Regarding the frequency with which the regular (periodic) re-evaluation should be carried out, it depends on the evolution that the above three factors (a), (b) and (c) will have over time. However, the only factor which can be predicted with a satisfactory approach is the first (evolution of the computer power). According to the study which is presented in (Marinakis, 2013) [15], if we want to compensate for the constant evolution of computer power due to Moore's law, the cryptographic key must increase by one bit each year in order to be safe from the Exhaustive Key Search (Brute Force Attack). As a result of this, in Table 2 we show the key lengths that must be valid every 5 years for cryptographic algorithms in order to be secure against the Exhaustive Key Search, according to the expected technological development.

From Table 2 it can be seen that, a cryptographic algorithm which has a key of 128 bits while today is considered to have high strength (year 2022), after 5 years will have medium strength (year 2027) and after 20 years will have low strength (year 2042).

Table 2. Correspondence between the key length K (in bits) and the strength of cryptographic algorithms every 5 years, according to the expected technological evolution.

YEAR	EVOLUTION OF CRYPTOGRAPHIC ALGORITHMS STRENGTH			
	LOW	MEDIUM	HIGH	VERY HIGH
2022	$80 \leq K \leq 112$	$112 < K < 128$	$128 \leq K \leq 192$	$192 < K \leq 256$
2027	$85 \leq K \leq 117$	$117 < K < 133$	$133 \leq K \leq 197$	$197 < K \leq 261$
2032	$90 \leq K \leq 122$	$122 < K < 138$	$138 \leq K \leq 202$	$202 < K \leq 266$
2037	$95 \leq K \leq 127$	$127 < K < 143$	$143 \leq K \leq 207$	$207 < K \leq 271$
2042	$100 \leq K \leq 132$	$132 < K < 148$	$148 \leq K \leq 212$	$212 < K \leq 276$

From what has been said, we believe that the optimal period for the conduction of a regular re-evaluation of a cryptographic algorithm, should be 5 years. This is because as shown in Table 2, the theoretical strength of the cryptographic algorithm is degraded by 5 bits every 5 years. This is of course valid, if in the meantime some unexpected cryptanalytical and technological developments have not occurred, which will greatly speed up the Exhaustive Key Search (e.g., the evolution of quantum computers).

5. Conclusion

When there is a need to evaluate the security of a cryptographic system, besides its cryptographic algorithm, the adequacy of all its critical security mechanisms must also be evaluated. The most important of these security mechanisms are the management of cryptographic keys, the cryptographic algorithm implementation, the access control mechanisms, the tamper proof mechanisms, the self-test mechanisms and the protection against compromising emanations. If some of these mechanisms are inadequate, they may reduce the initial security grade of the system which is provided by the strength grade of its cryptographic algorithm. The evaluation method combines the assessment of all the critical security mechanisms and gives a final assessment for the security grade of the whole system. That is, when there are significant defects in some security mechanisms, the initial grade of the system security may be reduced by one or more grades depending on the judgment of the evaluator. Therefore, the method includes the basic procedures for the evaluation of a cryptographic system, but also gives the flexibility to rate the final security of the system according to the specific security policy and the operational environment of the users. Finally, the method analyzes the necessary conditions for the validity of the evaluation, as well as the conditions for the duration of the evaluation, the regular re-evaluation and the extraordinary re-evaluation, according to the new cryptanalytic risks and the expected technology evolution.

References

[1]. NIST FIPS 140-2, “Security Requirements for Cryptographic Modules”, May 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

[2]. ISO/IEC 15408-1:2009 “Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model”. https://www.iso.org/standard/50341.html

[3]. “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model”, Version 3.1, Revision 1 (CCMB-2006-09-001), September 2006. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

[4]. George Marinakis, “Rating the Security Strength of Cryptographic Algorithms” February 2022. https://www.scienpress.com/journal_focus.asp?main_id=57&Sub_id=IV&volid=512

[5]. George Marinakis, “Sampling methods for cryptographic tests”, May 2021. https://www.scienpress.com/journal_focus.asp?main_id=57&Sub_id=IV&Issue=2143151

[6]. George Marinakis, “Selection of sampling keys for cryptographic tests”, July 2021. https://www.scienpress.com/journal_focus.asp?main_id=57&Sub_id=IV&Issue=2202191

[7]. George Marinakis, “Design and evaluation of random number generators”, September 2015. http://www.scienpress.com/journal_focus.asp?main_id=57&Sub_id=IV&Issue=1608

[8]. NIST.SP.800-57pt1r4 “Recommendation for Key Management-1”, 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[9]. NIST.SP.800-162, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”, January 2014 - February 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[10]. NIST.SP.800-205, “Attribute Considerations for Access Control Systems”, June 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf

[11]. Elena Dubrova, “Anti-Tamper Techniques”, Royal Institute of Technology, Stockholm, Sweden, 2018. https://people.kth.se/~msmith/is2500_pdf/Anti-Tamper%20Techniques_elena.pdf

[12]. M.Martin, F.Sunmola, D.Lauder, “Unintentional Compromising Electromagnetic Emanations from IT Equipment: A Concept Map of Domain Knowledge”, Elsevier B.V., 2022. https://www.sciencedirect.com/science/article/pii/S1877050922003532

[13]. NCSC, “TEMPEST and Electromagnetic Security”, National Cyber Security Centre, November 2021. https://www.ncsc.gov.uk/information/tempest-and-electromagnetic-security

[14]. NIST SP. 800-100, “Information Security Handbook: A Guide for Managers”, October 2006, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

[15]. George Marinakis “Minimum key length for cryptographic security”, March 2013. http://www.scienpress.com/journal_focus.asp?main_id=57&Sub_id=IV&Issue=597