Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 46(2), 2019, Pages 392–399
ISSN: 1223-6934

Impact factors involved in cryptoperiod computation in key compromise impersonation scenario

Nicolae Constantinescu

Abstract. Starting from the asymmetric encryption general protocols and vulnerability analysers, the present paper illustrate the most important factors, those owning the highest impact level on computation of cryptoperiod of keying data and material, as looked at in a key-compromise impersonation attack scenario. We support our researched list of such factors with mathematical principles and advanced computation techniques applied also on the cryptography theory of elliptic curves.

2010 Mathematics Subject Classification. Primary 14G50; Secondary 11T71.
Key words and phrases. cryptoperiod, key compromise computation.

1. Introduction

Asymmetric encryption represents the establishment factor for a multitude of network cryptographic protocols, such as Secure Shell (SSH), Transport Layer Security (TSL), Secure Socket Layer (SSL), digital signature algorithms such as The Elliptic Curve Digital Signature Algorithm (ECDSA), Diffie-Hellman scheme (ECDH), Elliptic Curve Integrated Encryption Scheme (ECIES) and many more. Public key encryption is, on large scale, deemed as responsible of granted secure communication over untrusted networks. Along this paper, we will use the term 'untrusted network' to refer to any communication channel, giving the fact that no communication connection is granted as being completely secure and protected from harm of all shapes of interception or attack. Having asymmetric encryption with such a great contribution in cyber-security and secured authentication manners for industry, business, government and many other heavily important fields, high protection techniques must be taken into consideration in case of system compromising situation.

As treated in [1, 2, 7], highest security for asymmetric encryption is provided by digital implementation of mathematical models of elliptic curves cryptography theory, which is used also on a similar mathematical model used in biochemical researches ([6, 16]) or applied physics ([11]). The protection brought above the authenticity and integrity of the keying data and encryption algorithm used for a certain session of elliptic curves implementations consists in the strength of the curves equations involved in the cryptographic session and the strength of assigned keys and encryption algorithm. Identical to each other, in manners of breaking resistance, cryptosystems and steel chains, for instance, are based on the same principle in case of attack: it is sufficient that only one element (weakest ring) to be compromised in order to destroy the integrity and escalate the vulnerability of the protected asset. By rising

Received September 15, 2019. Accepted October 8, 2019.

the strength of each involved individual, the overall security of the entire system is strengthened. Such an enforcement leads to infeasible costs of potential attack.

Subjects like the ones treated in [13, 17] describe and prove the advantages towards the usage of a third party (other than the direct entities involved in communication), entrusted with the key assigning. As having a general axiom enunciating that the value and integrity of information keeps its range just as long as it is owned by as few people as possible, we are entitled of willing to rise the protection in case of illicit ownership of information. By other words, most common type of active attacks against the integrity of a cryptosystem used trough a third party, problem also treated to [3], consists in security breaches that lead to eavesdropper's impersonation. The present illustrates most important factors that must be analysed and computed in case of key-compromise impersonation, along with mathematical computations demonstrating their importance.

2. Currently used computation considerations

Since elliptic curves provide highest security ratio and algorithm implementation feasibility, it is worth mentioning the computation considerations of the cryptoperiod of the keying material involved in cryptosystems that base on them. As mentioned in [7, 14], considerations of the elliptic curve domain parameter cryptoperiod are related to the number of elliptic curve key pairs. Therefore, having a single $\kappa(\rho, \varrho)$, pair of ρ public key and ϱ private key, where ρ, ϱ are large prime numbers and $\Theta(\kappa)$ being the individual pair's strength, the cryptoperiod ξ, defined as

$$\xi : \Theta_q \to T, \tag{1}$$

where T represents the set of time intervals and Θ_q being the codomain values of the function Θ, is directly related to the pair's strength. If only the parameter set of the function Θ enlarges its cardinal (situation that constrains function Θ to receive more than just one key pair as argument), the definition of the function ξ, updated with its new Θ_q domain, illustrates the cryptoperiod dependencies on the collective strength of the Θ's parameters.

In order to attempt a KCI (Key Compromise Impersonation) attack on a cryptographic system holding data accessed and protected by multiple pairs of keys, the assailant must consider the theoretical costs of its trial, addressed to cracking the security of one desired key on whose identity the attacker wants to acquire; suppose having a system that involves η pairs of keys, resulting to a total of $\gamma = 2 \times \eta$ keys, all large prime numbers. The cost of breaking a set K of γ keys is represented by the formula

$$\varpi(K) = \gamma^{\frac{1}{2}} \times \varpi(K_i) = (2 \times \eta)^{\frac{1}{2}} \times \varpi(K_i), \tag{2}$$

where ϖ(K) represents the cost of breaking the set K of γ keys, and $\varpi(K_i)$, where $K_i \in K$, i $\in \overline{0, \gamma - 1}$ represents the cost of breaking a single key of the set.

This general computation of the KCI attack costs is also related to a subset of factors such as those regarding hardware configuration of the attacker's machine, the time interval in which the revealed information is valuable, the chosen field and bit representation of the elliptic curve key pairs etc. If the costs are acceptable for the attacker and if the attack succeeds, then any data transferred or encrypted using the cracked pairs of keys is compromised. Also, an attacker being in possession of one or many pairs of keys is entitled to not only intercept the data, but also impersonate one entity and alter transfers and data. If an attacker impersonates one entity which is considered trusted by the authorised users of the cryptosystem, then those users can easily respond to fake requests of private data that can be initiate by the attacker in the name of the trusted entity.

The time period available for an attacker to develop and initiate malicious actions in case of potential succeeded attack may be defining for the amount of compromised data and communication. Other than hardware failure considerations, the variable that dictates the amount of time available to the impersonator to harm the cryptographic protocol and data is represented by the cryptoperiod of the keying material that serve as the cryptosystem's base.

3. Proposed computation considerations

The present illustrates the most meaningful factors that must be considered in order to preserve the highest security rate in cryptosystems based on public-key cryptography, along with mathematical computation meant to describe the assignment of cryptoperiods, sustained by the factor importance rate.

Looked at from the perspective of Alice and Bob, (where Alice and Bob are the only parties that are eligible for using the cryptosystem) the Key-Compromised Impersonation scenario counts down to few important terms that dictate the behavior of key pairs' existence. In real life application of cryptosystems, Alice and Bob might not represented by two single entities, but by two groups of entities entitled to securely use the cryptosystem. Having this statement, Alice represent a set of authorised persons of which cardinal is σ and Bob be another set with a cardinal of ς. The sum of these two cardinals represent the entire number of entities that are allowed to having access of the cryptosystem usage. To maintain computations less complicated, along the present we will refer to the standard meaning of Alice and Bob, similar to those presented in [2, 15], therefore let σ and ς each have a value of 1. Computation for other cardinals may be adapted by replacing the simplified values with more precise ones.

Each accepted entity use a pair of keys, leading, in the scenario treated in the present, to having

$$\gamma = 2 \times (\sigma + \varsigma) \tag{3}$$

number of keys. It is sufficient for an attacker participating in a KCI scenario, to break only one of the keys, in order to compromise the entire security of the cryptosystem, theory treated in papers like [9, 4, 12, 5].

Establishing these basic circumstances, we now proceed with the factors that we consider to be most important in computation of the cryptoperiod of a cryptosystem. It is worth to mention that the importance of each factor differs from scenario to scenario, therefore we will not treat them in order of their importance.

The factors we propose to mainly be taken into consideration:

- Life span of protected data
- Importance of protected data
- Additional security layers
- Attacker affordability in front of the raised attack costs

Having the enumerated factors, we should further analyse their role in the computation of the cryptoperiod.

3.1. Life span of protected data. The so named "data life span" represents the period of time in which data is considered valuable. The value of the data is applied to both eavesdropper (Eve) and Alice and Bob sides. Even though we refer to the same data from both sides of the cryptosystem, it might own different levels of value for each part involved, depending on each one's considerations and desire. The more valuable an asset, the more determinate the efforts to own it are. Along the present we will refer to Alice and Bob's value system but will also consider Eve having large interest in illicit ownership of the data.

Let the life span of protected data be μ time units , with μ>0. The life span, μ is directly proportional with the amount of time an attacker has to fulfil its malicious actions. This statement leading to the urge of appliance of good computation tactics and value assignments that will later make the subject of debate.

3.2. Importance of protected data. In the previous section we mentioned the value the of life spam, to protect the data. This can also be referred to as the 'importance of protected data'. For both Alice and Bob's and Eve's sides, the value of the data is translated to the amount or importance of harm illicit ownership of the data that can be produced to Alice and Bob.

Let the importance of protected data be υ, a positive number. The larger the value of υ is, the more important the protected data is.

3.3. Additional security layers. A cryptosystem's usage may also be protected by additional security layers in order to provide higher defence in front of a potential attack. For instance, Alice and Bob might be authorized to try to use the cryptosystem x times per one unit time, or they might be able to use it only from a certain location, or, as papers like [8] suggest, they might be required to use biometrical authentication before their access is granted to the cryptosystem etc. These extra security precautions will be treated in this paper as being a set ϖ with a cardinal of ϱ entities, each $\varpi_{[i]}$ (with i $\in \overline{0, (\varrho - 1)}$) representing a security layer. We will involve in following computations only the cost of breaking the additional security layers. Let that cost be $\chi(\varpi)$.

3.4. Attacker affordability in front of the raised attack costs. The success rate of any potential attack also relies on the competence of the machine from which the attack is maintained. For Alice and Bob's worst case scenario and best of Eve's, we will consider Eve to be able to afford an attack with a total power of $\eta \times n$, where η is the greatest known computation power of the best configurations known to exist and n is a large number of physical machines involved in the attack. This suppositions leads Eve to afford a cost of attack $\chi(attack) \approx 0$.

4. Mathematical theory appliance

Having the most important terms previously enunciated, the present illustrates all of potential cases that grant their influence in the cryptoperiod computed value. The following scenarios are presented as an outlined computation whereas advanced mathematical demonstrations are admitted to be modified in order to suit a particular individual's needs or tasks in terms of KCI situations.

Let cryptoperiod be λ, where $\lambda \in \mathbb{Q}_{>0}$, expressed in same time units measurement as μ. Several circumstances are then possible:

(1) $\mu \to +\infty$ and $\upsilon \to 0$: Consider a positive non-zero constant k. In order to ensure the reliability of the involved cryptosystem, λ should then have a value of

$$\lambda = \left(\frac{\upsilon}{k}\right)$$

granting the two a relation of $\lambda \propto \upsilon^{-1}$.

(2) $\mu \to +\infty$ and $\upsilon \to (\xi/2)$, where ξ represents the maximum, positive non-zero value importance grade can express.
This situation involves two different cases, having the cost $\chi(\rho)$ as principal factor, where $\rho \in \{\mathrm{E}_1, \mathrm{E}_2\}$, where E_1 represents the event of losing the integrity of ownership authorisation of involved data and E_2 represents the event of new keys assignment in the involved cryptosystem, expressed by the following:

(a) $\chi(E_1) \geq \chi(E_2)$
In this situation, an accepted computation of each keying material new assignment cryptoperiod is the one computed having the following

$$\sum_{i=0}^{n-1} \chi_i(E_2) < q + \chi_i(E_1), \tag{4}$$

where n represents the number of times new keys are assigned and $q \in \mathbb{N}$ represents a very large number in order to assure the feasibility of the event E_2.

(b) $\chi(E_1) < t \times \chi(E_2)$, where t $\in \mathbb{N}$ represents a very large number.
Consider a positive non-zero constant k. In order to ensure the reliability of the involved cryptosystem, λ should then have a value of

$$\lambda = \left(\frac{\upsilon}{k}\right),$$

granting the two a relation of $\lambda \propto \upsilon^{-1}$.

(3) $\mu \to +\infty$ and $\upsilon \to +\infty$
In this situation, Alice and Bob must ensure an cryptoperiod assignment that obeys the following:

$$\sum_{i=0}^{p-1} \lambda_i < \mu,$$

where p represents the number of times new values are assigned to λ. Having $\chi(E_1)$, $\chi(E_2)$ previously described, λ assignment should also respect

$$\sum_{i=0}^{p-1} \chi_i(E_2) < t + \chi_i(E_1), \tag{5}$$

where p represents the same as declared above and and $t \in \mathbb{N}$ represents a very large number in order to assure the feasibility of the event E_2.
In addition to that, let θ be defined as $\theta : \mathbb{N} \to \mathbb{Q}_{>0}$, expressed in same time units measurement as μ as the representation of the amount of time Eve's computations and operations require in order to break the security of $\overline{\kappa}$ keys of the

cryptosystem, where κ represents a set of keys that fulfil the cryptosystem's mathematical requirements . λ should then also obey

$$\lambda < \theta(\overline{\kappa}),$$

where $\overline{\kappa}$ is considered to have a value of 1.

(4) $\mu \to \mathit{0}$ and $\upsilon \to \mathit{0}$:
Consider a positive non-zero constant k. In order to ensure the reliability of the involved cryptosystem, λ should then have a value of

$$\lambda = \mu \times k$$

granting the two a relation of $\lambda \propto \mu$.

(5) $\mu \to \mathit{0}$ and $\upsilon \to (\xi/\mathit{2})$, where ξ represents the maximum, positive non-zero value importance grade can express.
Consider a positive non-zero constant y. In order to ensure the reliability of the involved cryptosystem, λ should then have a value of

$$\lambda = \left(\frac{\mu}{y}\right)$$

granting the two a relation of $\lambda \propto \mu^{-\mathit{1}}$.

(6) $\mu \to \mathit{0}$ and $\upsilon \to +\infty$
Consider a positive non-zero constant k. In order to ensure the reliability of the involved cryptosystem, λ should then have a value of

$$\lambda = \mu \times k$$

granting the two a relation of $\lambda \propto \mu$.

It is essential to be mentioned that, along the present, the $\pm\infty$ symbols are used to describe the maximum and minimum value which a defined measure can have.

5. Conclusions

As an opposite to first impressions' foreground, Key-Impersonation Scenario impose authorised entities to compute and assign different values for cryptoperiod having the importance of the protected data as a leading character, rather than the malicious entities' best time of action regarding key breaking.

We mainly proposed this data specification as the major factor of computations for its general appliance and utility in real life situations and its functionality was probed on a medical application from [10]. Considering the asset to be vulnerable to any malicious attempt and also to be approachable by any theoretical attack manners, a feasible and cogent methodology has left to lead solely to a procedure of costs analysis applied to the level of data's importance and, additional, to the period in which it owns the specific level of significance.

A more coherent method of data protection in systems that involve keying material is the one that fulfils a specific situation dictated by worse and worse (leading to the worst) scenarios on the side of authorised and entrusted entities, on behalf of the assumptions of potential hypothesis having the entities' characterised by malice best possible provided attack time.

If a cryptosystem's security assure a strong resistance in front of worst case scenarios (regardless their plausible chances of occurrence), it is more likely for it to succeed in case of facing more probable manifestations that also own high impact factor.

Real life demonstrations provide a valid representation of the variety of constituents and situations that interfere the presented general broad-spectrum computations. This is one of the foremost reasons that promise to supply our future work concerning the cryptoperiod computations in KCI scenarios. As future work with focus on this subject, we desire to attain more accurate computation formula suitable for both enterprise and academic fields, along with specific cases annotations and restrictions computations.

References

[1] R. Alsaedi, N. Constantinescu, V. Rădulescu, Nonlinearities in Elliptic Curve Authentication, *Entropy* **16** (2014), no. 9, 5144–5158.

[2] N. Constantinescu, *Criptografie*, Ed. Academiei Române, Bucharest, 2009.

[3] N. Constantinescu, Security system vulnerabilities, *Proceedings of Romanian Academy Series A-Mathematics Physics Technical Sciences, Information Science* **13** (2012), no. 2, 175–179.

[4] N. Constantinescu, G. Stephanides, The GN-authenticated key agreement, *Journal of Applied Mathematics and Computation* **170** (2006), 531–544.

[5] N. Constantinescu, G. Stephanides, M. Cosulschi, M. Gabroveanu, RSA-Padding Signatures with Attack Studies, *Proceedings of International Conference on Web Information Systems and Technologies: Internet Technology/Web Interface and Applications*, Portugal, ISBN 978-972-8865-46-7 (2006), 97–100.

[6] L. Duica, E. Antonescu, M. Pirlog, T. Purnichi, J. Szakacs, M. Totan, B. Vintila, M. Mitariu, S. Mitariu, A. Stetiu, Clinical and Biochemical Correlations of Aggression in Young Patients with Mental Disorders, *Revista de Chimie* **69** (2018), no. 6, 1544–1549.

[7] D. Hankerson, A.J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2003.

[8] I. Iancu, N. Constantinescu, Intuitionistic fuzzy system for fingerprints authentication, *Applied Soft Computing* **13** (2013), no. 4, 2136–2142.

[9] R.A. Mollin, *RSA and Public-Key Cryptography*, CRC Press, 2002.

[10] M. Mutica, A. Ciubara, L. Duica, D. Alexandru, C. Plesea, M. Pirlog, M. Cara, Elderly schizophrenic patients - clinical and social correlations, *Proceedings of European Neuropsychopharmacology* **26** (2016), no. 2, 5512–5512.

[11] C. Silisteanu, L. Mitariu, R. Ranga, E. Antonescu, L. Duica, M. Racheriu, M. Totan, M. Manea, Potentiating the Effect of Treatment with Voltaren Gel Using Ultrasonic Frequencies of 1 MHz, *Revista de Chimie* **69** (2108), no. 7, 1749–1751.

[12] E. Simion, N. Constantinescu, Complexity Computations in Code Cracking Problems, *Proceedings of Concurrent Engineering in Electronic Packaging-ISSE*, IEEE Communication, May 05-09 (2001), 225–232.

[13] O.A. Ticleanu, N. Constantinescu, D. Ebanca, Intelligent data retrieval with hierarchically structured information, *In Intelligent Interactive Multimedia Systems and Services - Proceedings of the 6th International Conference on Intelligent Interactive Multimedia Systems and Services-IIMS*, Sesimbra, Portugal, 26-28 June (2013), 345–351.

[14] O.A. Ticleanu, Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography, *Electronic Journal of Differential Equations* **2015** (2015), no. 214, 1–9.

[15] O.A. Ticleanu, Differential operators over particular elliptic curves spaces with cryptographic applications, *Electronic Journal of Differential Equations* **2015** (2015), no. 303, 1–9.

[16] M. Totan, E. Antonescu, G. Catana, M. Mitariu, L. Duica, C. Filip, R. Comaneanu, C. Mitariu, C-Reactive Protein - A Predictable Biomarker in Ischemic Stroke, *Revista de Chimie* **70** (2019), no. 6, 2290–2293.

[17] S.Y. Yan, *Quantum Attacks on Public-Key Cryptosystems*, Springer Science Business Media, 2014.

(Nicolae Constantinescu) Department of Computer Science, University of Craiova, 13 A.I. Cuza Street, Craiova, 200585, Romania
E-mail address: `nikyc@central.ucv.ro`