Optimization of security systems facing vulnerability stakes

A. ELALIMI[1] and H. HACHIMI [2]

1. Ibn Tofail University, National School of Applied Sciences.
University Campus, PO Box 241, Kenitra, Morocco.
GS laboratory ADSI team
alim.issam@gmail.com

2. Ibn Tofail University, National School of Applied Sciences.
University Campus, PO Box 241, Kenitra, Morocco.
GS laboratory ADSI team
hanaa.hachimi@univ-ibntofail.ac.ma

Keywords: Optimization, cryptographic algorithms, metaheuristics, linear programming.

Abstract

With their adoption of measures meant at minimizing costs and increasing gains, corporations have opted for "cloud computing" and "BYOND[1]" services as key systems that would enable them to address such challenges. However, this kind of choices has blurred the once clear-cut *-thou hostile-* digital boundaries between these corporations and the outside world. In this context, their ITs remain more than ever vulnerable and exposed to different types of attacks and threats. In fact, these attacks can range from the simple gathering of economic information to causing a total paralysis of the targeted computing system with the potential loss of all its data.
Such a pressing situation has prompted several corporations to adopt different security policies with the aim of preventing themselves from the targeting of their confidential data. Consequently, the encryption of such data through the use of robust algorithms has become an obligation.
With this goal in mind, this humble research tries to bring a worked solution meant at minimizing the potential risks inherent to the use of computing systems through the optimization of a number of cryptographic algorithms.
In this perspective, our adopted approach is founded on the use of a number of mathematical optimisation methods that will be applied on ciphering algorithms. Such algorithms are currently used by several operators during the encryption process of their respective sensitive data. Thus, these steps would enable us to solve, efficiently and correctly, not only the required time reduction for ciphering/deciphering operations problematic but also the necessity of guarantying maximum security to concerned data.
In relation to our chosen optimisation methods used for the purpose of this research, we have opted for the following:

- Genetic algorithm (A.G) ;
- Particle Swarm Optimization(P.S.O) ;
- Hybridization of A.G and P.S.O.

Our choice is mainly meant at concluding which of the above-proposed methods would be the most suitable way for the achievement of the first target of our research i.e. reducing the required time for the completion of ciphering/deciphering operations through the use of the most widely spread symmetric algorithms; DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

[1] BYOD: Bring your own device refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace,

References

[1] L. Granboulan (2003) “la sécurité à l’ère numérique” editor : Lavoisier, 51-71.
[2] J. Crampton, Sushil Jajodia,Keith Mayes (Eds.) (2013)“Computer Security - ESORICS ” editor: springer, 646-710.
[3] Ali Ismail Awad, Aboul Ella Hassanien, Kensuke Baba(2013) “Advances in Security of Information and Communication Networks” editor: springer, 196-240.
[4] Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss (2013) “Cyber Security Policy Guidebook” editor: wiley, 15-84.
[5] Alfred Menezes, Paul van Oorschot, Scott Vanstone (1996) “Handbook of Applied Cryptography” Publisher: CRC-Press, 385-420.
[6] Mark Talabis, Jason Martin (2012) “Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis” 63-140.
[7] John Vacca, Renowned “Computer and Information Security Handbook” editor: elsivier, 25-66.