www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 3 March 2017, Page No. 20611-20613
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.38

Information Security: A Saga of Security Measures

Neha Tyagi[1], Ashish Agarwal[2], Anurag Katiyar[2], Shubham Garg[2], Shudhanshu Yadav[2]
[1]Assistant Professor, Department of Computer Science & Engineering,
G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India
[2]Student (B.Tech.), Department of Computer Science & Engineering,
G.L. Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India

Abstract: In the time of extreme proclivity of users towards internet and its services, it is almost implied to worry for the concerned security of highly confidential information. So, are the available safety trends and the continuous endeavor in this domain towards unfolding new techniques with enhanced features suggest pioneering concerns of the associated parties for preserving the integrity of underlying system(s). Having gone through some of the works available, we can easily gaze at the much talked issues in the field of network business (specifically communication) demanding the robust cryptosystems with adjusting feature(s) to safeguard the interest(s) of communicating parties. It is immaterial to talk about cryptosystems without touching the edges of famous algorithm i.e., R.S.A. algorithm. We, here, attempt to mention a few of the developing techniques that have/are gathering attention from masses associated with this field.

Keywords: Hybrid cryptography, Security threats, Private Key cryptography, Public key cryptography, Cryptography, Encryption, Key, R.S.A. algorithm.

1. Introduction

Information security is not just an issue to be discussed of forums but a domain of immense importance to deal with emerging threats imposing new challenges every moment specifically in the context of digital dream(s). As evident from past trends, mathematical tools have been adopted to generate safety and counter strategy to different malicious attacks aiming to steal away confidentiality of information and play with the integrity of the system. As an instance, the application of asymmetric techniques in the symmetric cryptosystems shows how two different classes being contrary in their approach still compatible to render the essence of their parent class i.e. Cryptography. The mixing of above mentioned too suggests the same instigating need to look differently not just newly which may be known as Hybrid Key Cryptography.
Cryptography, as has been defined as the branch that promotes the desired working application of any cryptosystem(s). It is mainly understood by showcasing into two sub divisions namely symmetric and asymmetric cryptography. Taking a direct orientation towards our concern, we here initiate the discussion with the proposed possible modification in the working of cryptographic algorithm. Though completely preservative in its approach, the proposed modification in the functional sketch of cryptographic algorithm may serve the challenge of facing suspected threats during the communication.

The methods of securing the channel in symmetric key cryptography may be of two types:

1. In the first method we have to apply security to the communicating channel and keeping the key same.
2. In the second method we have to apply security to the key and keeping the channel same.

To summarize all the concepts, first of all we talk about the cryptography process step by step where we try to find out all about cryptography, its applications, techniques, security and keys then we move to the essential security part where we can apply methods which would provide security to our private key [1] and make it secure against any invasion practices carried out by invaders.
Next step in the process of safeguarding the communication is selecting the method. The method selection creates the whole architecture on which the safeguarding process would be executed. The execution of each method varies tremendously but still it may provide the same degree of security to the cryptosystem.
With the advancement of technology and introduction of new attacks each day, the adaptation tendency of algorithms becomes by far the only important mean of defense for the victims of foreign interventions in their private lives.
There are several advancements in the algorithms being carried out as the day progresses which will increase the complexity of key present in the cryptosystem .While there are several key barriers that need to be crossed to make everything sustain and flourish, we can ensure that these goals will be reached.

2. Concept

The underlining principle which has to be worked on in order to achieve a secure communication mainly consists of the methods by which they are secured.
Here we look at some possible solutions to deal with the new brand of attacks made against the cryptosystems.

Method 1:

In order to secure the communication channel, we can apply protocols which will ensure the safety of cryptosystems from attacks like Man-in-the-Middle.
Some of these are PPTP (Point-to-Point tunneling protocol) and L2TP (Layer 2 Tunneling Protocol).

Method 2:
In this method, the focus lies on providing security to the key so that it becomes difficult to penetrate the cryptosystem.
Some possible solutions are mentioned below:

1. Modifications can be made on algorithms like R.S.A. algorithm [3] which would work on securing the key by increasing the complexity.
2. This process incorporates perceptions like 'Hybrid Cryptography' [2] – A technique in which both symmetric and asymmetric key cryptography is used to send the encrypted / cipher text to the receiver.

Refer to Figure 1 for block diagram.

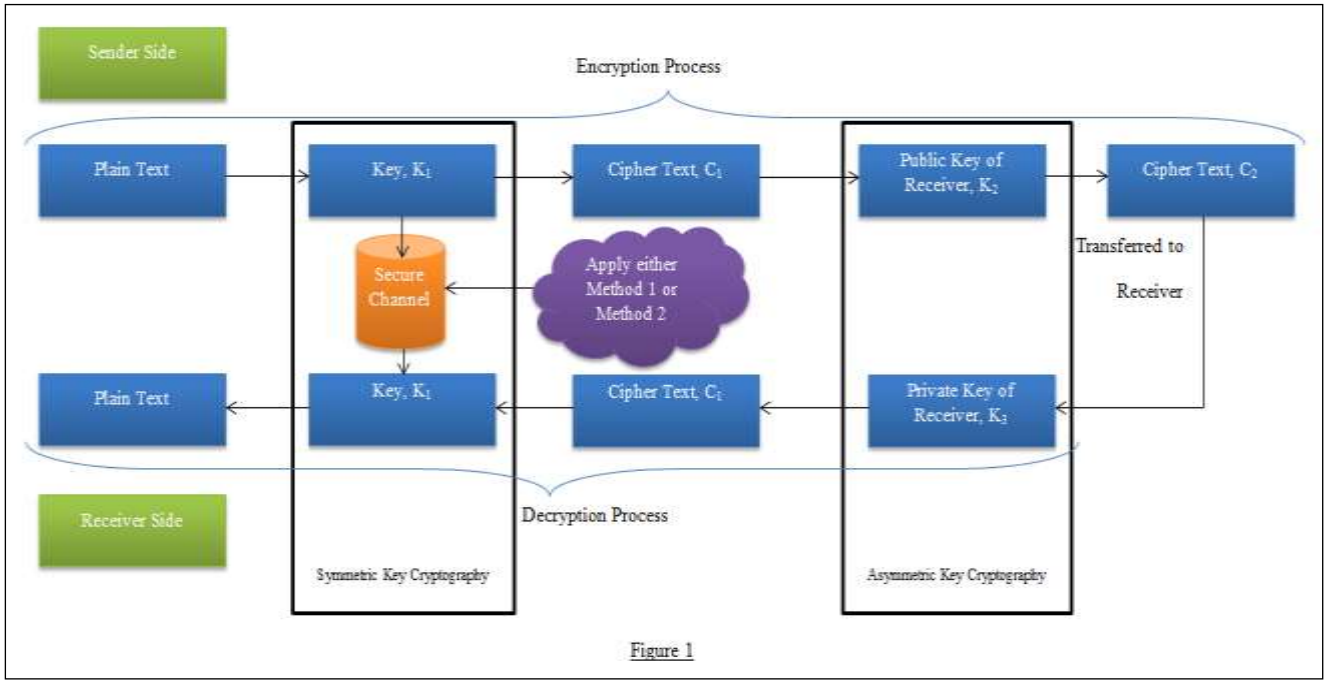

Figure 1

3. Example

For the better understanding of method, we have considered a brief example representing the working of Hybrid cryptography.

Two friends Diane and Barbara have to share secret information regarding their private party.

Before sending the message to Barbara , Diane executes following

1. Attain Barbara's Public key from her,
2. She now generates a new Symmetric key for the data encapsulation procedure.
3. Then she encrypts the message under the data encapsulation procedure using the newly generated key.
4. Then she generates the symmetric key under the key encapsulation procedure using Barbara's public key.
5. Send both these encryptions to Barbara.

At receiver's end Barbara executes the following steps to decrypt message,

1. Barbara first uses her private key to decrypt the key present in the key encapsulation segment.
2. Then she uses the retrieved key to decrypt the data encapsulation segment.

4. Future Scope

The possibilities that the works accepted as standards carry, by allowing to extend them define the scope of further enhancements. As discussed above, utilizing some of the basic mathematical functionalities do offer opportunities to think different meanwhile maintaining the basic framework. The emergence of new contenders in the race amongst threats to the information and its security do pose challenge(s) to come up with equally strong tools/techniques that are worth strong to nullify their impacts and demolish their intents. Developing newer tools or introducing modifications in the existing methodologies, at the same time, poke the concerned people to control the complexities and compatibilities in terms of technologies and feasibilities. Attempts to bring down the reading on complexity scale with equal increment on the measure of efficiency are the requirements need to be looked

for and served keeping challenges of attacks at the bay. The motive, at a glance is same for all concerned with information security i.e., to ensure easy and confidential mode of communication.

5. Conclusion

Encouraging allowances in terms of widely acceptance for the works that have been in practice for past many years do present a wide range of possibilities in the field to try something further. R.S.A. algorithm is surely one of the powerful tools that gather attention of excellence's before they look for alternatives. Combining the practices of asymmetric key cryptography with the symmetric key cryptographic tools is not new but doing it differently is certainly promoting, if done properly. The strengthening of underlying systems can be accomplished only if the basic idea of cryptography i.e., confidentiality, is kept at the heart of attempts. Problems such as going dark problem, proposed techniques such as split key cryptography, all come up with instigating features in this area to look for. Therefore, complexities controlled with multifarious features in terms of ease of use present the domain of carrying out inquisitive research work(s).

6. References

[1] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Protection of Key in Private Key Cryptography" published by "International Journal of Advanced Research", Volume 5, Issue 2, Feb 2017.

[2] Arpit Agrawal, Gunjan Patankar,"Design of Hybrid Cryptography Algorithm for Secure Communication" published by "International Research Journal of Engineering and Technology", Volume 3 Issue 1, Jan 2016.

[3] Meenakshi Shankar, Akshay.P, "Hybrid Cryptographic Techniques Using RSA Algorithm and Scheduling Concepts" published by "International Journal of Network Security & Its Application", Volume 6, Issue 6, Nov 2014.