International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Data Security for Email System in XML Format using Graceful Code and Graphical Password

Rutika S. Ingole†* and V. B. Bhagat†

†Computer Science and Engineering, P.R.Patil COET, Amravati, Maharashtra, India

Accepted 07 March 2015, Available online 19 March 2015, **Vol.5, No.2 (April 2015)**

Abstract

In a real world scenario, email has become the most widely communication way in daily life. The main intention for proposing this paper is to enhance the security of email system, as there are various standards such as secure multipurpose mail extension(s/mime), pretty good privacy(pgp) etc. but they have a significant drawback that there headers are unauthentic. Because of unauthenticity of headers there are possibilities of impersonation attack, profiling of the email communication and can also lead to a spam and phishing activities. Here, we provide a technique to encrypt a data using graceful code and text based graphical password scheme using color combination for email system.

Keywords*: Graceful code, Elgamal cryptography, RGB color model, XML (Extensible Markup Language).*

1. Introduction

Email is one of the most crucial and regarded network services. In recent years, data security in email system plays a dynamic role. Thus, nowadays it is a difficult task to communicate via email. This is because cyber terrorist are becoming more active. Theirfore, there is great need for security innovation regarding email system.

Email security is a broad term that incorporates multiple techniques used to secure an email service. One of them technique is a cryptography which is used for secure data communication. It involves the maintenance of basic security services such as integrity, confidentiality, availability and authentication. A large number of email security standards are already developed but they also need a refinement over security issues. We describe a solution which is resistant the shoulder surfing attack for that we provide a text based graphical password scheme which leads to a desirable security for the email system.

1.1 Objectives

- A narrative solution that unifies strengths of previous approaches and provide additional attractive features for higher flexibility of the email communication in a secure manner.
- To provide a complete data security in email system.
- To resist shoulder surfing attack.

*Corresponding author **Rutika S. Ingole** is a Student

2. Literature review

There are various cryptanalysis techniques available to break most of the encryption algorithms at one point of time like linear cryptanalysis, n-gram analysis, brute force attack, man in the middle attack etc. [Berouz Forouzan]. Furthermore in recent past, there was some famous algorithms have been developed like RSA, DES or the AES. These algorithms look secure. But these algorithms have a significant drawback that, they are not able to eliminate the repetition of data values in the cipher text which is called as patterns [G. Usha Devi, Ipsita Rana, Sutanu Nandi, (2012)]. Besides these some multilevel encryption system have been developed using the existing cryptographic algorithms to provide more security [Sairam Natarajan, Manikandan Ganesan, Krishnan Ganesan (2011)]. But the disadvantage of this kind of multilevel system is that it is relatively slow compared to other cryptographic algorithms because of multiple levels and multiple algorithms. In recent past some multilevel encryptions using graceful code have also been developed. They eliminate the patterns [G. Usha Devi, Ipsita Rana, Sutanu Nandi, (2012)] but the disadvantage is that one character is encrypted into fixed number of data values [Sairam Natarajan, Manikandan Ganesan, Krishnan Ganesan (2011)]. So they can be vulnerable to the attackers.

Many system uses RSA but from the analysis between RSA and Elgamal cryptography, RSA is highly power consumption as compared to elgamal cryptosystem. Also in terms of hardware and software implementation RSA is not very efficient whereas

elgamal is faster and efficient. Theirfore the proposed scheme uses elgamal cryptosystem for the encryption and decryption purpose. Existing system having the following architecture in fig1:

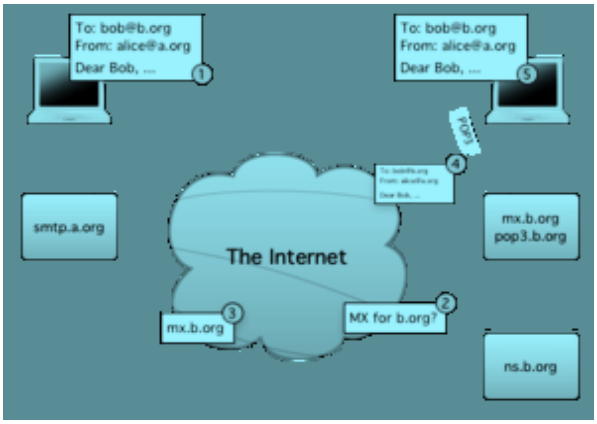

Fig 1: Overview of the existing email system architecture

3. Proposed Approach

We model the architecture to interchange an email in xml scheme. Web services allow the two applications running on two different servers to communicate with each other. Our proposed scheme achieves the features of both xml and email. It provides efficient way for code processing, archiving and searching, also provides end to end security of complete message simple implementation of clients, readability of the signature and encryption for a natural person, multiple signatures over different contents, and transport via the existing systems. In this authentication is done using color combination of RGB model.

3.1 Authentication

The authentication is done with text based graphical password using RGB color model. The RGB color model is an additive color model in which red, green and blue lights are added in a different ways. To verify the authenticity, the first step is to assign a unique color for each receiver. By using appropriate combination of red, green and blue lights various colors can be represented.

3.2 Encryption and Decryption

Phase 1: The process of encryption

1. Produce a digital signature of message content using SHA-1 hashing algorithm.
2. Encrypt message content using elgamal cryptography. To encrypt a message elgamal uses public key of the receiver which is already stored on the server.
3. Register sender's color: For the receiver to confirm the authenticity of sender, register senders color on the server.

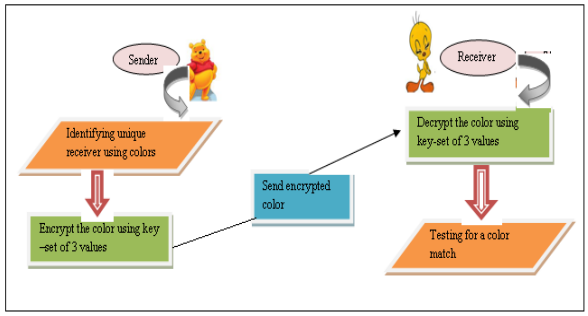

Fig 2: The architecture for authentication using color model

4. Add G-code: Graceful code is added with the encrypted message.
5. Upload data.

Phase 2: The process of decryption

1. Download the message.
2. Decrypt the graceful code: G-code is removed from the encrypted message.
3. Check the authenticity of the receiver.
4. Decrypt the message using the receiver's private key.
5. Verify the digital signature: to verify the message integrity, the digital signature of the decrypted message is produced and compared with the received digital signature.

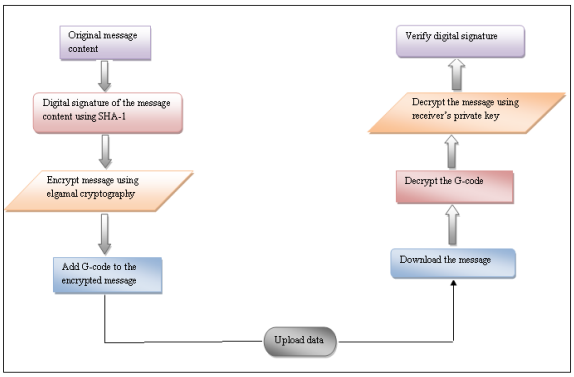

Fig 3: Architecture for encryption and decryption of message content

3.3 Illustration for the Graceful Code

Once the email is downloaded on the sender's system instead of storing it in the original format the data are encrypted in the following way and then stored it in the system. To implement a relatively fast and secured encryption scheme we used a technique called as graceful code. Here, we design two levels for an encryption. The main thing for doing this approach is to remove any patterns in the cipher text.

Following steps shows the process of encryption

1. First level encryption

In this first we have to remove all the blank spaces from the original content. Thus now we obtain a contiguous number of characters. Then next stage is to represent each character in its ASCII value. This ASCII value is then encrypted into a set of prime numbers using the prime factors. This set of prime numbers may contain an iteration of values, thus there is a possibility for an attacker to guess that pattern. Theirfore, there is need to go with the second level of encryption for to eliminate this pattern.

2. Second level encryption

In order to remove this repeating pattern, we proceed with the second level of encryption. In this level, it renovates the random prime numbers into a graceful code. Technically, graceful code is called as G-code by representing them into graceful tree. This G-code must need to be satisfying all the conditions of the graceful graph. The G-code set that we obtain must be unique for all the characters in the content i.e. the values in this set are not repeating for all the characters. And the number of data values in it also differs from each other. At this instant the cipher text is almost impossible to break.

Following figure shows the working of graceful code and how the code is generated

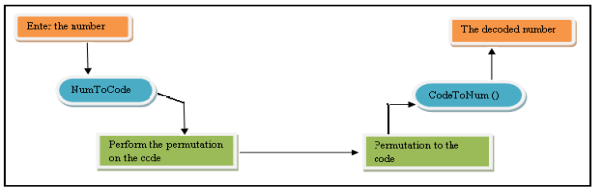

Fig 4: Generation of the Graceful code

Conclusion

1) We give the prime importance for the data security in email system which is widely used in day to day life.
2) Thus, we address the problem of security regarding unauthentic headers in the email.
3) For this, we had used a textual password using color combination of RGB model and for encryption and decryption of message content we had used elgamal cryptography which is efficient in terms of software and hardware implementation.
4) As our proposed scheme uses advanced authentication technique and is well adapted to any possible future technology.

References

Atul Kahate, Cryptography and Network Security, *Tata McGraw Hill Publications.*

S. PavithraDeepa, S. Kannimuthu, V. Keerthika (2011), Security using colors and Armstrong Numbers, *Proceeding of the National Conference on Innovations in Emerging Technology.*

S. A. Saoji, Nikita B. Agarwal, Mrunal B. Bokil, Ashwini V. Gosavi (2013), Securing Emails in XML format using colors and Armstrong numbers, *International Journal of Scientific & Engineering Research.*

G. Usha Devi, Ipsita Rana, Sutanu Nandi, (2012) Multilevel Encryption System using Graceful Codes, *International Journal of Advanced Research in computer science and software Engineering*

Berouz Forouzan, Cryptography and Network Security, 2nd edition, TMH, ISBN: 9780070702080.

Bandawane Reshma B., Gangadhar Mahesh M., Kumbhar Dnyaneshwar B. (2014), Data Security using Graphical Password and AES algorithm for E-mail system, *IJEDR.*

Annapoorna Shetty, Shravya Shetty K, Krithika K (2014), A review on Asymmetric Cryptography-RSA and ELGamal algorithm,*International Journal of Innovative Research in Computer and Communication Engineering.*

Sairam Natarajan, Manikandan Ganesan, Krishnan Ganesan (2011), A Novel Approach for Data Security Enhancement Using Multilevel Encryption Scheme, *International Journal of Computer Science And Information Technologies,* Vol. 2 (1), 469-473.

Lijun Liao, Jorg Schwenk, Secure Emails in XML Format Using Web Services, *Fifth European Conference on Web Services.*

Nina Godbole, Information Systems Security, *Wiley India Pvt Ltd*, ISBN -978-81-265-1692-6.

Gautam Shroff, Enterprise Cloud Computing Cambridge, *ISBN*: 978-0-521-13735-5.

Restful Web Services, O'Reilly Media, *ISBN*: 978-0-596-52926-0.