Volume 1, No. 3, Sept-Oct 2010
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Model of e-mailing system using Braid Group and Steganographic scheme

Deo Brat Ojha
Department of Mathematics
R.K.G. Institute of Technology
Ghaziabad ,U.P. India
ojhabrat@gmail.com

Abhishek Shukla*
(Research Scholar Singhania Univ., Jhunjhunu,Rajsthan)
College of Computer Application,R.K.G. I.T.
Ghaziabad ,U.P. India
abhishekknit@gmail.com

Meenu Sahani
Department of Mathematics
Bhagwati Institute of Technology
Ghaziabad,U.P., India
mnu.sahni@rediffmail.com

Abstract: In this paper we show a model of e-mailing system in braid group using steganographic scheme for Internet communication. It is the model of a real-life secure mailing system for any organization. In this model a sender can send a secret message even to a unacquainted person in an anonymous way. The users of this model are assumed to be may or may not be the members of a closed organization.

Keywords: Steganography; e-mailing system; Braid Group; Envelope Producer (EP);Message Inserter (MI) ; Envelope Opener (EO).

I. INTRODUCTION

Human beings have long hoped to have a technique to communicate with a distant partner anonymously but later on distinctive and must be secure. We may be able to realize this hope by using steganography.

Modern steganography has a relatively short history because people did not pay much attention to this skill until Internet security became a social concern. Most people did not know what steganography was because they did not have any means to know the meaning. Even today ordinary dictionaries do not contain the word "steganography." Books on steganography are still very few [1], [2]. The most important feature of this steganography is that it has a very large data hiding capacity [3], [4]. It normally embeds 50% or more of a container image file with information without increasing its size. Steganography can be applied to variety of information systems. Some key is used in these systems when it embeds/extracts secret data. One natural application is a secret mailing system [7] that uses a symmetric key. Another application pays attention to the nature of steganography whereby the external data (e.g., visible image data) and the internal data (any hidden information) cannot be separated by any means. We will term this nature as an "inseparability" of the two forms of data. For more details [5,6,8,9,10,11,12].

In the present paper we will show our basic model of e-mailing system in braid group using steganographic scheme. The structure of the present paper is as follows. In Section 2 we will make a short discussion on the problems of an encrypted mailing system. Section 3 describes the scheme of the e-mailing system in braid group using steganographic scheme.

II. PROBLEMS OF AN ENCRYPTED MAILING SYSTEM

There are two types of cryptography scheme: Symmetric key schemes and asymmetric key schemes.

In a symmetric system a message sender and receiver use a same encryption/decryption key. In this scheme, however, the sender and the receiver must negotiate on what key they are going to use before they start communication. Such a negotiation must be absolutely secret. They usually use some second channel (e.g., fax or phone). However, the second channels may not be very secure. There is another problem in this situation in that if the sender is not acquainted with the receiver, it is difficult to start the key-negotiation in secret. Furthermore, the more secure the key system is, the more inconvenient the system usage is. An asymmetric system uses a public key and a private key system. The public key is open to the public, and it is used for message encoding when a sender is sending a message to the key owner.

III. A MODEL OF E-MAILING SYSTEM IN BRAID GROUP USING STEGANOGRAPHIC SCHEME

We do not intend to develop a new "message reader-and-sender" or "message composer", but we are developing three system components that make e-mailing system in braid group using Steganographic scheme(EBSS). A message sender inserts (actually, embeds) a secret message in an envelope using steganography and sends it as an e-mail attachment. The receiver receives the attached envelope and opens it to receive the message. An "envelope" in this system is actually an image file that is a container, vessel, cover, or dummy data in the terminology of steganography. This system can solve all the problems mentioned above.

The following items are the conditions we have set forth in designing the system.

1. The name of the message sender may or may not be anonymous, as depends upon their wish.
2. The message is hidden in the envelope and only the designated receiver can open it.
3. Sender can send a secret message even to an unaccustomed person.

4. It is easy to use for both sender and receiver.

A. Customization of an EBSS

In this section we describe our two pass e-mailing system in braid group using Steganographic scheme (EBSS) between two entities $EBSS_{first}$ and $EBSS_{second}$, and consider its security. For this scheme, the initial setup known to both $EBSS_{first}$ and $EBSS_{second}$ braid group B_n For a,b in B_n, it is hard to guess *a* and *b* from *ab*.We assume that n is even, and denoted by LB_n (resp. UB_n) is:

We denote by

s : Sufficiently complicated n -braid;

$a_1, a_2 \in LB_n$: $EBSS_{first}$'s long term private key pair;

$a_1^e s a_2^e = X_a$: $EBSS_{first}$'s long term public key ;

$b_1, b_2 \in UB_n$: $EBSS_{second}$'s long term private keypair;

$b_1^e s b_2^e = X_b$: $EBSS_{second}$'s long term public key.

Following the above mentioned notations, we describe the EBSS below. The protocol works in the following steps.

$EBSS_{first}$ $EBSS_{second}$

$x_1^e s x_2^e = Y_a \longrightarrow K_b = b_1^e X_a b_2^e$

$Y_b = K_b^e y_1^e s y_2^e K_b^e$

$\longleftarrow$

1. $EBSS_{first}$ choose $a_1, a_2 \in LB_n$,computes $x_1^e s x_2^e = Y_a$. If Y_a = I (Identity braid), A terminates the protocol and restarts x_1 and x_2, $EBSS_{first}$ then sends *h* (Y_a) to $EBSS_{first}$ sends it to $EBSS_{second}$.

2. Upon receiving Y_a, $EBSS_{second}$ randomly chooses $y_1, y_2 \in UB_n$, computes $K_b = b_1^e X_a b_2^e$, and $Y_b = K_b^e y_1^e s y_2^e K_b^e$.

3. If K_b or $Y_b = I$, $EBSS_{second}$ terminates the protocol and restarts with new y_1 and y_2. otherwise $EBSS_{second}$ sends it to $EBSS_{first}$.

4.Upon receiving

Y_b, $EBSS_{first}$ computes $K_b = a_1^e X_b a_2^e = K_a$,and the shared key $KEY_a = x_1^e K_a^{-e} Y_b K_a^{-e} x_2^e$.

5. $EBSS_{second}$ also computes the shared key

$KEY_b = y_1^e Y_a y_2^e$.

6. In each step 4 and 5, if KEY_a or KEY_b is I, then the protocol run is terminated with failure.

7. After regular protocol running, $EBSS_{first}$ and $EBSS_{second}$ share the secret $K = KEY_a = KEY_b$.

Customization of an EBSS for a member $EBSS_{first}$ takes place in the following way. $EBSS_{first}$ and $EBSS_{second}$ first agree to generate a key ($K = KEY_{first} = KEY_{second}$). Then $EBSS_{first}$ types in his name ($NAME_{first}$) and e-mail address ($e-mail_{first}$). Key is secretly hidden (according to a steganographic method or some other method) in $EBSS_{first}$ envelope (E_{first}). This *Key* is eventually transferred to a message sender's MI_{second} in an invisible way. $NAME_{first}$ and $e-mail_{first}$ are printed out on the envelope surface when $EBSS_{first}$ produces E_{first} by using EP_{first}. *Key* is also set to EO_{first} for the initialization. $NAME_{first}$ and $e-mail_{first}$ are also inserted (actually, embedded) automatically by MI_{first} any time $EBSS_{first}$ inserts message ($MESSAGE_{first}$) in envelope (E_{second}). The embedded $NAME_{first}$ and $e-mail_{first}$ are extracted by a message receiver ($EBSS_{second}$) by EO_{second}.

B. Components of the system

EBSS is a steganography application .It makes use of the inseparability of the external and internal data. The system can be implemented differently according to different programmers or different specifications. Different EBSS' are incompatible in operation with others.

An EBSS consists of the three following components.

1. Envelope Producer (EP)
2. Message Inserter (MI)
3. Envelope Opener (EO)

In this scheme we have two communicating parties first and second. We denote first's EBSS as $EBSS_{first}$ So, it is described as $EBSS_{first} = EP_{first}, MI_{first}, EO_{first}$.

EP_{first} is a component that produces MI_{first}'s envelope E_{first}. E_{first} is the envelope (actually,an image file) which is used by all, when they send a secret message to $EBSS_{first}$. EO_{first} is produced from an original image EO. $EBSS_{first}$ can select it according to his preference. E_{first} has both the name and e-mail address of $EBSS_{first}$ on the envelope surface (actually, the name and address are "printed" on image E_{first}). It will be placed at downloadable site, so that anyone can get it freely and use it any time.

Or someone may ask $EBSS_{first}$ to send it directly to him/her. MI_{first} is the component to insert (i.e., embed according to the steganographic scheme) $EBSS_{first}$'s message into another member's (e.g., $EBSS_{second}$)'s envelope (E_{second}) when $EBSS_{first}$ is sending a secret message ($MESSAGE_{first}$) to $AIMMS_{second}$. One important function of MI_{first} is that it detects a key (KEY_{second}) that has been hidden in the envelope (E_{second}), and uses it when inserting a message

($MESSAGE_{first}$) in E_{second}. EO_{first} is a component that opens (extracts) E_{first} 's "message inserted" envelop E_{first} ($MESSAGE_{second}$) which $EBSS_{first}$ received from someone as an e-mail attachment. The sender ($EBSS_{second}$) of the secret message ($MESSAGE_{second}$) is not known until $EBSS_{first}$ opens the envelope by using EO_{first} .

C. How it works

When some member ($EBSS_{second}$) wants to send a secret message ($MESSAGE_{second}$) to another member ($EBSS_{first}$),whether they are acquainted or not, $EBSS_{second}$ gets (e.g., downloads) the $EBSS_{first}$'s envelope (E_{first}), and uses it to insert his message ($MESSAGE_{second}$) by using MI_{second} . When $EBSS_{second}$ tries to insert a message, $EBSS_{first}$'s key is transferred to MI_{second} automatically in an invisible manner, and is actually used. $EBSS_{first}$ can send E_{first} $MESSAGE_{second}$ directly, or ask someone else to send it to $EBSS_{first}$ as an e-mail attachment.

$EBSS_{second}$ can be anonymous because no sender's information is seen on E_{first} $MESSAGE_{second}$. $MESSAGE_{second}$ is hidden, and only $EBSS_{first}$ can see it by opening the envelope. It is not a problem for $EBSS_{second}$ and $EBSS_{first}$ to be acquainted or not because $EBSS_{second}$ can get anyone's envelope from downloadable site. EBSS is a very easy-to-use system because users are not bothered by any key handling.

IV. REFERENCES

[1] Stefan Katzenbeisser and Fabien A.P. Petitcolas (eds) "Information hiding techniques for steganography and digital watermarking", Artech House, 2000.

[2] Neil F. Johnson, Zoran Duric and Sushil Jajodia "Information Hiding", Kluwer Academic Publishers, 2001 .

[3] M. Niimi, H. Noda and E. Kawaguchi "An image embedding in image by a complexity based region segmentation method", Proceedings of International Conf. on Image Processing'97, Vol.3, pp.74-77, Santa Barbara, Oct., 1997.

[4] E. Kawaguchi and R. O. Eason "Principle and applications of BPCS-Steganography", Proceedings of SPIE: Multimeda Systems and Applications,Vol.3528, pp.464-463, 1998.

[5] URL:http://www.know.comp.kyutech.ac.jp/BPCSe/Dpenv/DPENVe- pro_ down. html.

[6] E. Kawaguchi, et al "A concept of digital picture envelope for Internet communication" in Information modeling and knowledge bases X,IOS Press, pp. 343-349,1999.

[7] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Lee, "New signature scheme using conjugacy problem." (http://eprint.iacr.org/2002/168).

[8] K.H.KO, S.J.Lee, J.H.Cheon, J.W.Han,J. S. Kang, and C Park, "New public- key cryptosystem using braid groups," in Advances in Cryptology (Crypto'00), LNCS1880,pp,166-183,Springer-Verlag, 2000.

[9] Menezes, M. Qu, and S. Vanstone, "Key agreement and the need for authentication," in Proceed-ings of PKS'95, pp. 34-42, 1995.

[10] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, An Efficient Protocol for Authenticated Key Agreement, Technical Report CORR98-05, Department of CO, University of Waterloo, 1998.

[11] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key-agreement," Design, Codes and Cryptography, vol. 28, no. 2, pp. 119-134, 2003.

[12] Eiji Kawaguchi, Hideki Noda, Michiharu Niimi and Richard O. Eason, A Model of Anonymous Covert Mailing System Using Steganographic Scheme, Information modelling and knowledge bases X,IOS Press, pp.81-85,2003.