A Model of Anonymous cum Idiosyncratic Machiavellian Mailing System using Steganographic Scheme

Deo Brat Ojha
R.K.G. Institute of Technology,
5th K.M. Stone Delhi-Meerut, Road,
Gzb.U.P. (India)

Ramveer Singh
(Research Scholar Singhania University, Jhunjhunu, Rajsthan).
R.K.G. Institute of Technology,
5th K.M. Stone Delhi-Meerut, Road,
Gzb.U.P. (India)

Ajay Sharma
(Research Scholar Singhania University, Jhunjhunu, Rajsthan).
R.K.G. Institute of Technology,
5th K.M. Stone Delhi-Meerut, Road,
Gzb.U.P. (India)

Abhishek Shukla
(Research Scholar Singhania University, Jhunjhunu, Rajsthan).
R.K.G. Institute of Technology,
5th K.M. Stone Delhi-Meerut, Road,
Gzb.U.P. (India)

ABSTRACT

In this paper we show a model of an anonymous cum idiosyncratic Machiavellian mailing system 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, later which will become idiosyncratic. 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.

1. 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 [11], [10]. The most important feature of this steganography is that it has a very large data hiding capacity [9], [2]. It normally embeds 50% or more of a container image files 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 [5] 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. In the present paper we will show our basic model of an anonymous cum idiosyncratic Machiavellian e-mailing system. The interested reader may consult [1, 3, 4, 6, 7, 8 & 12].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 Anonymous cum idiosyncratic Machiavellian Mailing System.

2. 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.

3. A MODEL OF AN ANONYMOUS CUM IDIOSYNCRATIC MECHIAVELLIAN MAILING SYSTEM USING STEGNOGRAPHIC SCHEME

The authors' research group at Raj Kumar Goel Institute of Technology started to develop a secure and easy-to-use e-mailing system. We do not intend to develop a new "message reader and sender" or "message composer", but we are developing three system components that make an Anonymous cum Idiosyncratic Machiavellian Mailing System using Steganographic Scheme (AIMMS). 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.

3.1 Customization of an AIMMS

The Conjugacy Search Problem (CSP) asks to find a in Braid Group B_n satisfying $y = axa^{-1}$ for some a in B_n, CSP asks to find at least one particular element a like that. It is considered infeasible to solve CSP for sufficiently large braids. The probability for a random conjugate of x to be equal to y is negligible. For B_n, a pair $(x, y) \in B_n \det \times B_n$ is said to be CSP-hard if $x \sim y$ and CSP is infeasible for the instance (x, y) .If (x, y) is CSP-hard, so is clearly (y, x) .

In this section we describe two-pass Authenticated Key Agreement Protocol for Anonymous cum Idiosyncratic Machiavellian Mailing System (AKAPAIMMS) between two entities sender and receiver, and consider its security. For this scheme, the initial setup known to both sender and receiver is:

We denote by

x : Sufficiently complicated n-braid;

$r \in L B_n$: sender's long term private key;

$X_{sender} = rx\, r^{-1}$: sender's long term public key;

$s \in UB_{n_S}$: receiver's long term private key;

$X_{receiver} = sx\, s^{-1}$: receiver's long term public key.

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

Sender **Receiver**

$Y_{sender} = cxc^{-1}$ →

$K_{receiver} = sX_{sedner}s^{-1}$

$Y_{receiver} = K_{receiver}\, dY_{sender}\, d^{-1}K_{receiver}{}^{-1}$ ←

1. Sender choose $c \in L B_n$, computes $Y_{sender} = cxc^{-1}$. If Y_{sender} = I (Identity braid), terminates the protocol run with failure. Otherwise sender sends it to receiver.

2. Upon receiving Y_{sender}, Receiver choose $d \in UB_n$, computes $K_{receiver} = sX_{sender}s^{-1}$, and $Y_{receiver} = K_{receiver}\, dY_{sender}\, d^{-1}K_{receiver}{}^{-1}$.

3. If $K_{receiver}$ or $Y_{receiver} = I$, receiver terminates the protocol run with failure. Otherwise receiver sends it to sender.

4. Upon receiving $Y_{receiver}$, sender computes $K_{sender}(= K_{receiver}) = r\, X_{receiver}\, r^{-1}$, and the shared key $KE\, Y_{sender} = cK_{sender}{}^{-1}\, Y_{receiver}\, K_{sender}c^{-1}$.

5. Receiver also computes the shared key $KE\, Y_{receiver} = d\, Y_{sender}\, d^{-1}$.

6. In each step 4 and 5, if $KE\, Y_{sender}$ or $KE\, Y_{receiver}$ is I, then the protocol run is terminated with failure.

7. After regular protocol running, Sender and Receiver share the secret $K = KE\, Y_{sender} = KE\, Y_{receiver}$.

Customization of an AIMMS for a member $AIMMS_{first}$ takes place in the following way. $AIMMS_{first}$ and $AIMMS_{second}$ first agree to generate a key ($K = KE\, Y_{first} = KE\, Y_{second}$). Then $AIMMS_{first}$ 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 $AIMMS_{first}$ 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 $AIMMS_{first}$ 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 $AIMMS_{first}$ inserts message ($MESSAGE_{first}$) in envelope (E_{second}). The embedded $NAME_{first}$ and $e - mail_{first}$ are extracted by a message receiver ($AIMMS_{second}$) by EO_{second}.

3.2 Components of the system

AIMMS 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 AIMMS are incompatible in operation with others.

An AIMMS 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 AIMMS as $AIMMS_{first}$ So, it is described as $AIMMS_{first} = EP_{first}, MI_{first}, EO_{first}$.

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 $AIMMS_{first}$. EO_{first} is produced from an original image EO. $AIMMS_{first}$ can select it according to his preference. E_{first} has both the name and e-mail address of $AIMMS_{first}$ 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 $AIMMS_{first}$ to send it directly to him/her. MI_{first} is the component to insert (i.e., embed according to the steganographic scheme) $AIMMS_{first}$'s message into another member's (e.g., $AIMMS_{second}$)'s envelope (E_{second}) when $AIMMS_{first}$ 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 $AIMMS_{first}$ received from someone as an e-mail attachment. The sender ($AIMMS_{second}$) of the secret message ($MESSAGE_{second}$) is not known until $AIMMS_{first}$ opens the envelope by using EO_{first} .

4. HOW IT WORKS

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

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

5. REFERENCES

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

[2]. 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.

[3]. 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.

[4]. 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.

[5]. 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)

[6]. 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), LNCS 1880, pp. 166-183, Springer- Verlag, 2000.

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

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

[9]. 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.

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

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

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

AUTHOR PROFILE

Dr. Deo Brat Ojha, Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (U.P.), INDIA in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. . He is working as a Professor at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. He is the author/co-author of more than 50 publications in International/National journals and conferences.

Ramveer Singh, Bachelor of Engineering from Dr. B.R. Ambedkar university, Agra (U.P.), INDIA in 2003. Master of Technology from V.M.R.F. Deemed University, Salem (T.N.), INDIA in 2007. Persuing Ph.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. The major field of study is Cryptography and network security. He has more than eight year experience in teaching and research as ASSOCIATE PROFESSOR. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network security. Mr. Singh is the member of LMCSI, LMIAENG, LMIACSIT, LMCSTA. He is the author/co-author of more than 17 publications in International/National journals and conferences.

Ajay Sharma, He did his Master of Technology(CSE) from Guru Jambheswar University of Science and Technology, Hisar (Haryana), India in 2004 and pursuing Ph.D. from Singhania University, Pacheri Beri, (Rajasthan), India . His major field of study is Cryptography and network security. His current research area is cryptographic protocol, symmetric encryption, asymmetric encryption and biometric template security. He has more than six years teaching experience. He is working as Associate Professor in the Department of Information Technology, Raj Kumar Goel Institute of Technology, Ghaziabad, (U.P.) India. Mr. Sharma is the life-time member of IAENG, IACSIT and CSTA. He is the author/co-author of more than 14 publications in International/National journals and conferences.

Abhishek Shukla, He did his Master of Computer Application (MCA) from Dr. Ram Manohar Lohia Avadh University, Faizabad, U.P., India in 2007 and pursuing Ph.D. from Singhania University, Pacheri Beri, (Rajasthan), India . His major field of study is Cryptography and network security. His current research area is secure mailing protocol and application.
He has more than three year experience. He is working in College of Computer Application, Raj Kumar Goel Institute of Technology, Ghaziabad, (U.P.) India. Mr. Shukla is the life-time member of IAENG. He is the author/co-author of more than 04 publications in International/National journals and conferences.