Solving semantic problems in" chaff and winnowing" problem by using cryptography

Sara Mohamadrezaei[a*], Bahram Sadeghi Bigham [a†]

[a]*Department of Applied Mathematics, Faculty of Mathematics and Computer Science,*
Amirkabir University of Technology, No. 424, Hafez Ave., Tehran, Iran

[a]*Department of Information Technology,*
Institute for Advanced Studies in Basic Sciences, Zanjan, Iran

SAM'07- The 2007 International Conference on Security and Management

February 20, 2007

Abstract

The need to secure the Internet is clear to everyone consequently more and more mechanisms to provide security and enhance it at different layers and different applications are being developed. Thus we want to introduce a new and secure method in network security. In this article at first we will survey "chaff and winnowing" method and cryptography method. Then we will discuss about their advantages and disadvantages and we will introduce a new method which it can solve the "chaff and winnowing" method's semantic challenges and make cryptography method safer. This new method uses the advantages of both methods and tries to omit the disadvantages of before methods to make a secure method for general using. Also this method is efficiency in confidentially and authentication problems.

Keywords: Steganography, Encryption, Confidentially, Authentication, Water mark.

Introduction

During these years using Internet for transmitting personal information is increasing. Thus making a safe structure for healthy transition is very important. In this paper we will present a new method to make this process safe. For protecting information from adversaries attack we have two strategies which are steganography and cryptography. It is important to keep in mind the differences between steganography, cryptography, confidentiality and authentication.

Steganography is the art of hiding a secret message within a larger one in such a way that the adversary can not discern the presence or contents of the hidden message. For example, a message might be hidden within a picture by changing the low-order pixel bits to be the message bits [12].

Encryption is the main way of achieving confidentiality using computers. Encryption transforms a message into a ciphertext using an encryption key. The ciphertext can only be transformed back into the original message using the encryption key and therefore can only be read by someone who has the key. The person who encrypts the message (the sender) and the person who decrypts the message (the receiver) may use the same keys (private key encryption) or different keys (public key encryption) [13], [5], [7]. DES, RSA, and IDEA are examples of encryption schemes

Confidentiality is the exchanging information between two parties without a third party being able to understand it[13].

Authentication is the process of verifying that a message was sent by a given person. A message is authenticated by computing a Message Authentication Code (MAC), which is a function of a secret key and

[*] E-mail address: `S_Mohamadrezaei@iasbs.ac.ir Corresponding author(S.Mohamadrezaei).`

[†] E-mail address: `b_sadeghi_b@aut.ac.ir (B. Sadeghi B.).`

the message. This MAC is then appended to the message. A MAC is similar to private key encryption because the sender and receiver both share the same secret key. When using encryption, the secret key allows the receiver to read the message. However, when using authentication, the receiver uses the secret key to decide if the message was sent by the person who claims to have sent it (the only other person with the secret key). If the message was changed or the wrong secret key was used, the MAC will be wrong. This tells the receiver that the message is not authentic. [8], [13].

1 Background

In this section we want to present some fundamental information about two major methods that are ”chaff and winnowing” and Cryptography in network security.

1.1 Chaff and winnowing problem:

In this part we want to present some before methods which have been used until know. Until know we have two group of secure approach, steganography and cryptography which we explain them.
One technique for providing confidentiality using authentication is called “chaffing and winnowing” it was first implemented by Ronald Rivest of MIT's Laboratory for Computer Science [10]. The scheme works by sending incorrect messages (chaff) that can only be differentiated from the real message (wheat) by the intended receiver who winnows the stream. Winnowing means to separate useless parts and is derived from. Chaffing and winnowing is easy to implement. As you see in figure 1, The sender authenticates the real message by adding a serial number which named MAC to it. Then the sender adds chaff (with incorrect MACs) to confuse any eavesdroppers. The recipient knows which MAC is correct and which MAC is incorrect.(as he also has the secret key) and throws away all chaff messages to obtain the original message. Figure 2 illustrates ”chaff and winnowing” method's configuration. In a simple example of this, Alice sends a message to Bob. Before sending her message, she authenticates it, and computes a MAC and adding it to the end of the message. A secret authentication key can be agreed upon at the beginning by using a method. [3], [2].

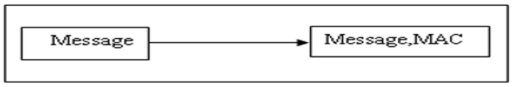

Figure 1: adding MAC to message

Chaffing confidentially depends on: 1) the MAC algorithm, 2) on how the original message is broken into packets, 3) on how the chaffing is done. A good MAC algorithm [8], [6], [4], [9]. will enhance the security. In such cases the adversary can not differentiate wheat and chaff. If the adversary or eavesdropper sees only one packet with a given serial number, then he sure that packet is probably wheat, not chaff. So a good chaffing process should add at least one chaff packet for each serial number used in the message. The second problem is, the adversary may also distinguish wheat from chaff by the contents of each packet. If the wheat packets have English sentences and the chaff packets have random bits, then the adversary will have no difficulty in winnowing and separating wheat from chaff. However, if wheat packets have a single bit and there are chaff packets with the same serial numbers but complementary bits, the adversary will find it virtually impossible to find the wheat packet. To obtain the original message, the adversary would have to break the MAC algorithm or know the secret authentication key. With a good MAC algorithm, the adversary hasn't ability to winnow, so chaffing provides confidentiality [13].

1.2 cryptography problem:

Controlling the flow of information in the information age is important and necessary. The critical tool for protecting information is using cryptography. In recent years, encryption has shifted from the obscure obsession of generals and mathematicians to a very important issue for all citizens, with impact on crime, civil

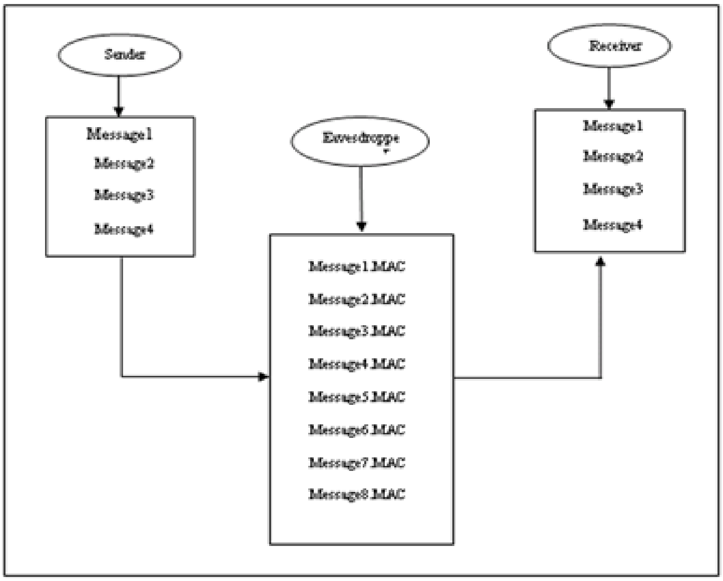

Figure 2: the process of "chaff and winnowing" and the access of every party to data

rights, national defense and economic competitiveness. Encryption makes information systems trustworthy in different ways. First, encryption protect information confidentiality. If information is encrypted before it is transmitted across a telephone network or stored in a database, eavesdroppers, hackers and adversary may capture the cipher text, but they won't understand it. Second, encryption can be used for authentication, i.e. to verify the identity of receiver. For example, if only sender holds the key to encrypt a message, then by performing this operation on an encrypted message, sender will prove her identity. This is the basis of a digital signature, which can be used to authorize payments or sign contracts and other secure transactions. Third, encryption can be used to protect the integrity of information. Consider a case where only legal recipient can encrypt a message, but anyone can decrypt it. Recipient records the message and an encrypted version of the message. If decrypting the latter still produces the former, then the message could not have been altered by any one except legal recipient. Using cryptography system that has been compromised is worse than using none at all, so much of the policy debate is about the availability of strong encryption. Given enough time, codes would be broken, which means an unauthorized observer can guess or calculate the secret key. The question is whether breaking a code will take a month, or a decade, or a billion years. The more possible values for that key, the longer it takes. So, a common measure for the strength of a code should be the number of bits (1's or 0's) in the key. Increasing the number of bits should increase the decrypting time . The time it takes to break or decrypt a code depends on the processing speed of computers as the number of bits in a key. For over five decades, computer processing speeds have doubled every 1.5 to 2.5 years. So, a code that took a thousand years to break with the computers available in 1960 would take 1 year to break with the computers available in 1980, and a few hours to decrypt with the computers available in 2000. It is necessary to increase the strength of encryption systems on a regular basis [5].

2 What do we want to do?

In this section we want to talk about the advantages and disadvantages of before methods and introduce you our new method. We will find each method's pros and merge them together and use them in our method. At the end we will discuss about feature of our method

2.1 Pros and cons of "chaff and winnowing"

In the chaff and winnowing part we discuss about sending pockets without any encryption and authenticating it by a serial number which call it MAC number. Then we add some chaff pockets to the sending data.

The receiver separates chaff and wheat by MAC algorithm and analyzes the MAC numbers. The best and optimize number of adding chaff to wheat is(2*wheat)[13].This is a very good idea, but the eavesdropper knows the half of the no related data is chaff and will omit them, and then give some information which shouldn't received. With this information he can guess the sending data and it is harmful for personal and critical information The second one is for adding chaff. Because if the addition chaffs are not related to wheat. So the clever eavesdroppers can recognize and separate the wheat and chaff. To avoid such problem and make this model safe in the sending part we should use artificial intelligence and some semantic sensors to make related chaff which not to be understandable for the eavesdropper. This method is very simple, But implementing it, is very hard and it is very time and cost consuming. But the most interesting idea here is that, the first and last packet isn't known for Eavesdropper so the sequence of packets is irregular. Because of this feature we have some methods like" all or nothing" [11]. The sequence is calculated by the MAC algorithm in the receiver's part. This idea is very interesting approach for having secure systems, because if we use this method we will make the adversary confused. We should use some functions which aren't ascending or descending functions. We would rather use no monotone functions.

2.2 Advantages and disadvantages of cryptography:

Transforming the message to a cipher text such that an eavesdropper who overhears the cipher text can not determine the message sent. The recipient possesses a secret decryption key that allows him to reverse the encryption transformation and retrieve the message. The sender might have used the same key to encrypt the message (with symmetric encryption schemes) or used a different, but related key (with public-key schemes). DES and RSA are familiar examples of encryption schemes.[13] Ideally, it should not be possible to perform one or both of these operations without knowing some secret key, which generally takes the form of a string of 1's and 0's. One way in which a cryptosystem may be attacked is by brute force search an adversary tries decrypting an intercepted cipher text with all possible keys until the plaintext makes sense or until it matches a known target plaintext our primary motivation is to devise means to make brute force search more difficult by appropriately pre processing a message before encrypting it.[11] All the encryption methods use confidentiality for providing their security .The confidentiality based on decrypting the encrypted pocket to right form. It provides security by using many models about key recovery which there are many articles about it. The main problem in using net cryptography is its sequence .because it is distinctive for receivers. So the adversary can easily find the regulation of pockets. This will decrease the security of our approach. Thus we can use authentication and hide the sequence of packets for adversary and eavesdropper so we can make a barrier in front of eave.

2.3 Mixture of chaff and encryption:

As we mentioned in part 1 Steganography is a method for hiding a message in a larger massage. We want to use this method in our approach. What articles had talked about until know is using this method for protecting images which they called it water mark [1] .This method used images for protecting data, this data can be an image or text. But in all these methods the sending data is meaningful and it is not optimized. According to 3.1 and 3.2, the mentioned problems of chaff and winnowing, need using artificial intelligence so if we go through this problem and find a new idea we can get new approach to enhance security in the networks. We want to apply this approach by cryptography. When we encrypt data we just have a pile of symbols which doesn't have meaning without its special key so this feature helps us to build chaffs without any need to use artificial intelligence or paying attention to its meaning. The second step for security enhancement, is adding authentication to the encrypted packets and changing the regulation of packet sequence. So we can mix chaff packet with wheat packets and it needs no extra works to make chaff packets, symbols are unknown and using this method make eavesdropper and adversary confuse.Figure 3 shows the sequence of "chaff and winnowing" and cryptography's mixture:

2.4 Feature of chaffs:

In this mixture adding chaffs theory is simple and it hasn't any semantic or artificial intelligence problems. It just uses the known symbols from wheat packets(it can find them random) and it doesn't need any calculating or any attention to it's concept. So this method can make eavesdropper confuse and he can't

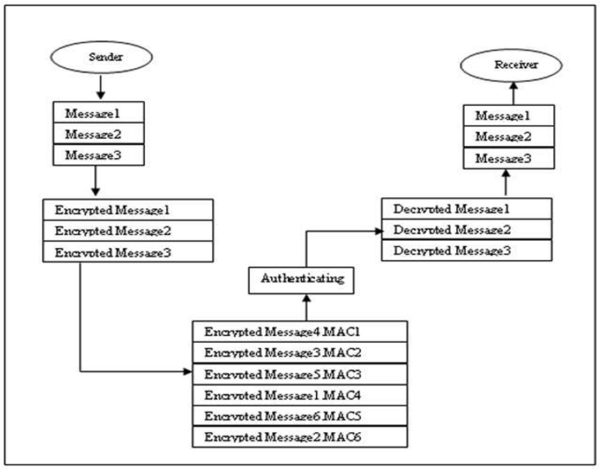

Figure 3: The mixture model sequence

find the context of sent data and the encryption key. About the number of chaffs which we should add , It depends to sender. Because of decrypting there isn't any obligation on number of sending chaffs. with using this method guessing encryption rule is difficult because the symbols in chaffs haven't any rule and they destroy the regulation of wheat.Thus no one can break it easily.

3 Conclusion:

In this paper we present a new method for enhancing the security for confidentiality and authentication. This approach can solve the semantic problem of chaff and winnowing method. Also the new presented method use the "chaff and winnowing" and "encryption" advantages to enhance the security level. Breaking, forgery and eavesdropping in this method is very hard

References

[1] A.Tanenbaum" Computer networks", .Fourth edition, ISBN: 0-13-066102-3.

[2] Barker, E. B, (The Keyed-Hash Message Authentication Code (HMAC)) , Federal Information Processing Standards Publication (FIPS 198) - March 01, 2002.

[3] Bart Preneel "THE PAST AND THE FUTURE OF CRYPTOGRAPHIC RESEARCH IN EUROPE" , Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium.

[4] B.preneel and P.C van Oorschot. On the security of iterated Message Authentication Codes.IEEE Transactions on Information Theory, 45: 188-199,1999.

[5] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, S. Yoo, Secure Key Issuing in ID-based Cryptography , In proceedings of the Second Australian Information Security Workshop-AISW 2004.

[6] Don Coppersmith "Key recovery and forgery attacks on the MacDES MAC algorithm" Electronics Letters, 35:1626-1627, 1999.

[7] Hugo Krawczyk" SKEME AVersatile Secure Key Exchange Mechanism for Internet" , Ny 10598, 1996 IEEE.

[8])Jon M. Peha" Encryption Policy Issues ", 1998.

[9]) Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-hashing for Message Authentication," RCF2104, February 1997.

[10] L. R. Knudsen and B. Preneel. MacDES "MAC algorithm based on DES. " Electronics Letters, 34: 871-873, 1998.

[11] Ronald L Rivest" All Or Nothing Encryption and The Package Transform", Lecture Notes in Computer Science, volume 1267, 210 , 1997.

[12] Ronald L. Rivest" Chaffing and Winnowing: Confidentiality without Encryption" CryptoBytes (RSA Laboratories), volume 4, number 1 (summer 1998), 12–17.

[13] Robert Schlaff" Confidentiality Using Authentication" Crossroads, November 1998 Location: www.acm.org/crossroads/xrds5-2/confide.html.