Encryption Key Distribution Applying Steganographic Techniques

Magdy Saeb,

Arab Academy of Science, Technology & Maritime Transport

Alexandria, Egypt

mail@magdysaeb.net

Abstract: The quondam problem of key distribution for symmetric ciphers has been, and still is, an essential element of secure information communications. In this proposed technique, we use ideas originated from steganography to hide the encryption key in the transmitted cipher text itself. The method begins by dividing the encryption key into an agreed-upon number of sub-keys. These sub-keys are concealed in the cipher text using a set of locations, known only to the sender and the receiver, as a shared secret. Then one transmits the resulting slightly longer message to the receiver where he or she can retrieve the key and decrypt the original message. We conjecture that since the ciphertext is a set of pseudorandom bits, embedding the pseudorandom bits representing the key will not be traceable. The proposed approach is suitable for both software and hardware implementations.

Key words: Cryptography, Encryption, Key distribution, Steganography.

I. Introduction

The quondam problem of key distribution for symmetric ciphers has been, and still is, an essential element of secure information communications [1-10]. Cryptography, in theory, uses security by design while Steganography uses security by obscurity. The majority of cryptographers often deals with the term "security by obscurity" with derision. Security by obscurity is a violation of Kerckhoffs' Principle, which holds that a system should be secure because of its design, not by hiding the design details to an adversary. The only allowed obscure element in this model is the encryption key. However, in Steganography, one can interpret hiding bits in a random vector is essentially a message scrambling technique [11-14]. That is, one can use Steganographic Techniques to encrypt messages. One can even visualize that reversing bits to hide a message is, in principle, an encryption technique. In this case, the key is the location pointer to the altered octets. Put differently, some cryptographic algorithms have used a bit-hiding technique to encrypt plain text messages. The basic premise of Kerckhoffs' Principle is that secrets do not remain secret for very long. Security by design versus security by obscurity is a risk management problem. The informed risk management decision, to take here, is to investigate the problem of the level of security required, the advantages and the disadvantages of the adopted key distribution technique. In this context, one conceives that the relation between Steganography and Cryptography is of a complementary nature. Therefore, security by design, and security by obscurity can adjoin together. Adopting this notion, we apply steganography to hide the encryption key in the ciphertext itself using the hiding locations as the shared secret between the communicating entities. Consequently, one can automate the encryption process for symmetric ciphers. One can even envision that the location keys have relatively longer life span as compared to the encryption keys. The method is suitable for machine-to-machine information security

applications. However, for high security applications we recommend using another secure channel for key distribution. In the following few sections we discuss the proposed protocol, provide some details of the hiding process and then give a summary and our conclusions.

II. The Protocol

In the following few lines, we summarize the proposed communications protocol between entities A and B:

Sender A:

1. Generate a random string, S_A
2. Hash this random string with a hash function of which output bits equal to agreed-upon key length, $K = h(S_A)$
3. Encrypt message, $E_K(m) = Enc_K(m)$
4. Hide the key in secret location(s) of the key in the ciphertext message using the shared secret **KL**, $M = \text{(K) in } E_K(m))$
5. Send the message with the hidden key, **M** to **B**
6. Destruct the key, (K)

Receiver B:

1. Obtain the message, **M**
2. Retrieve the key from the secret location(s) by removing it, $K = \text{(K) in } E_K(M))$, $Enc_K(m) = M - K$
3. Decrypt the message using the retrieved key, $m = Dec_K(Enc_K(m))$
4. Destruct the key, (K)
5. Halt.

The symbols , imply hiding, destructing and retrieving the key respectively.

In this protocol, we have not attempted to conceal the original message (m) length by adding a variable number of random bits to this message. However, if the user wishes to do that he or she can accomplish it by extending the key length and accordingly the shared secret locations KL. We provide the details of the embedding procedure $\text{(K) in } E_K(m))$ in the following section.

III. Details of the hiding Process (O

We summarize the concealment or hiding process as follows:

Procedure: EmbedKey

Objective: The aim of the procedure is hiding the bits of the encryption key (**K**) into the encrypted pseudorandom message of enciphered bits $Enc_K(m)$. The receiver retrieves the hidden key bits utilizing the location shared secret set [**KL**]. Number of entries in the set KL is >= n, where n = L /l, where L = Length of key K and l is the length of one sub-key. The smaller l, the larger number of sub-keys concealed (n) and the more secure is the key, however at the expense of increased processing time. In this implementation, we choose l to be equal to 16 bits.

Input: Random String S_A, user message **m**, random vector **KL** of secret locations such that the Length of KL is >= Length of key K/16, hash function **h**

Output: Encrypted message **M** with the encryption key hidden in it.

Procedure Body:

1. Divide the user key into (n) 16-bit sub-keys;
2. For i =1 to n
   Read i-th location entry from the shared secret set KL;
   Embed i-the sub-key into the encrypted message in this location, resulting in the larger message **M**;
3. End Embedding.

IV. Summary and Conclusions

In this article, we are using steganography, as a type of security by obscurity, to hide the encryption key in the pseudorandom ciphertext itself. Knowing the fact that for good ciphers, the probability of bits changed is from 0.46 to 0.48, the cipher presents a valid and suitable medium for hiding the pseudo-randomly generated key with a low probability of detection. The shared secret between the communicating entities is the set of hiding locations. The number of entries in this set should be greater or at least equal to the number of sub-keys used depending the sizes of the key and the sub-keys. The user can extend the method to hide the message size as well. The method is simple and practical, however, we conjecture, it is secure for machine-to-machine applications. Other high security applications should rely on other key distribution techniques.

References:

[1] R. M. Needham, M. D. Schroeder, "Using Encryption in Large Networks of Computers," Communication ACM21, pp.993-999, 1978.
[2] R. K. Bauer, T. A. Berson, R. J. Freietag, "A Key Distribution Protocol Using Event Markers," ACM Transactions on Computer Systems, Vol. 1 Number 3, pp. 249-255, August 1983.
[3] M. Bellare, P. Rogaway, "Entity Authentication and key Distribution," Advances in Cryptology, Crypto93, Proceedings, Springer Verlag, 1993.
[4] M. Bellare, R. Canetti, H. Krawczyk, "A Modular Approach for the Design and Analysis of Authentication and Key Exchange protocols," Proceedings of the 30 th Annual Symposium On the Theory of Computing, ACM, 1998.
[5] H. Huang, "A Pairwise key Pre-distribution for Wireless Sensor networks," ISI 2008 Workshops, LNCS 5075, pp. 77–82, 2008.
[6] C. Chang, C. Lin, C. Chen, "A Conference Key Distribution Scheme Using Interpolating Polynomials," International Journal of Security and its Applications, Vol. 1, No. 2, October 2007.
[7] D. Liu, P. Neng, W. Du, "Group-Based Key Pre-distribution in Wireless Sensor Networks," WiSE'05, Cologne, Germany. September 2, 2005.
[8] M. R. Wahiddin, N. S. Noor Sham, M. Saeb, M. Hamdan, "A Protocol for Secret Key Infusion from Satellite Transmissions," International Journal of Computer and Network Security (IJCNS), Vol.2, No.7, July 2010.
[9] I. Cervesato, C. Meadows, and D. Pavlovic, "An Encapsulated Authentication Logic for Reasoning About Key Distribution Protocol," Eighteenth Computer Security Foundations Workshop, IEEE Computer Society, Press, CSFW-18, pages 48–61, Aix-en-Provence, France, 2005.
[10] H. Sun, H. Yeh, "Password-based authentication and key distribution protocols with perfect forward secrecy," Journal of Computer and System Sciences 72, 1002–1011, 2006.
[11] H. Farouk and Magdy Saeb, "An Improved FPGA Implementation of the Hybrid Hiding Encryption Algorithm (HHEA) for Data Communication Security," DATE, ICM, MEESE, Munich, Germany, 7-11, March 2005.
[12] Magdy Saeb, H. Farouk, "Design and implementation of a Secret Key Steganographic Micro-Architecture Employing FPGA," DATE2004, Designer Forum C-lab, Paris, France, 2004.
[13] Mahmoud Shaar, Magdy Saeb, Usama Badawi, "A Hybrid Hiding Encryption Algorithm (HHEA) For Data Communication Security," Proceedings of the IEEE Midwest 2003 Symposium on Circuits, Systems, & Computers, Dec. 2003.
[14] Mahmoud Shaar, Magdy Saeb, Usama Badawi, "A Multi-bit Replacement Algorithm (TSF) for Steganography," Proceedings of the IEEE Midwest2003 Symposium on Circuits, Systems, & Computers, Dec. 2003.