How to Thwart Rubber Hose Attacks

Magdy Saeb,

Arab Academy of Science, Technology and Maritime Transport, Alexandria, Egypt

Great Wall InfoSec Sdn. Bhd. Kuala Lumpur, Malaysia

mail@magdysaeb.net

Abstract: Cryptographic systems depend on the concealment of secret keys shared by the participants. However, in general, systems are not able to resist coercion attacks. In these attacks, the participant is forced by the adversary to surrender the key. This type of attacks, known as a rubber hose attack, is in many instances the least costly method, in time and effort, that are utilized to defeat cryptography. In this work, we present a procedure to thwart this kind of attacks. It is based on using the ciphertext as a lexicon to conceal the true secret message. If the participant is forced to surrender the key, the attacker will be able only to get a cover or decoy message, which is acting only as a diversion. The secret true message can be retrieved using a set of numbers that represent the locations of the ASCII code incorporated in the ciphertext of the cover or decoy message. Changing this set of numbers will generate a new secret message. The ciphertext of the decoy or cover message can be used to hide multiple true secret messages and it can be only sent once.

I. Introduction

We present a situation where a copy of an encrypted message was intercepted by an adversary who does not hold the decryption key. The adversary decides to capture the sender who possesses the secret decryption key. Using coercion, the adversary tries to acquire the key to decrypt the secret message. In this article, we present an approach to preventing this type of attacks that are known as “rubber hose attacks.”

In this approach a decoy message, we call it the cover message, is encrypted using a powerful encryption algorithm such as The Chameleon Polymorphic Cipher [1], shown in Figure 1, or any other algorithm. If the legitimate key holder is subject to this kind of attacks, which is less costly in terms of time and effort, he or she will surrender only the key of the cover message [2]. The true secret message is secured using YAEA-like encryption [3] which implementation program is shown in Figure 2. The ciphertext of the decoy cover message is utilized as a lexicon and the locations of ASCII code of the secret message characters are found and recorded as a set of numbers. This set of numbers is the correct decryption key of the true secret code. In the following sections, we discuss

the proposed procedure, provide a formal description, revisit the encryption methodology YAEA on which the procedure is based, and finally we give our summary and conclusions.

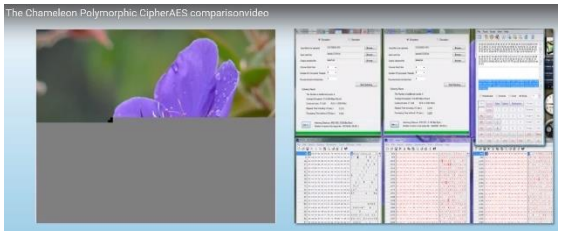

Figure 1: Implementation of The Polymorphic Cipher "Chameleon"

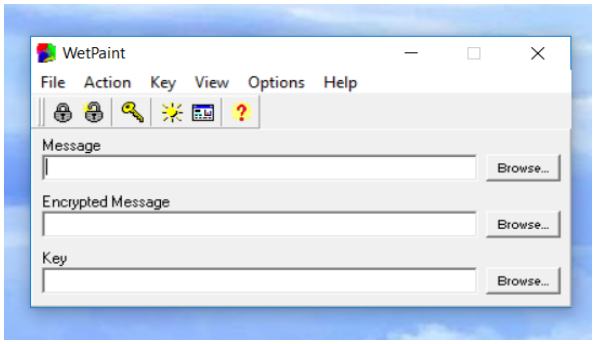

Figure 2: Implementation of YAEA, "Wet Paint"

II. Procedure

We describe the proposed procedure as follows:

A. At the sender end:

1. Choose a relatively large cover message M_c;
2. Encrypt M_c using a secure encryption algorithm such as the Chameleon Polymorphic Cipher [1] and key K_c to obtain cipher C_c;
3. Send C_c to the receiver;
4. Using a secure channel send K_c;
5. Hide the secret message M_{s1} using YAEA-like encryption and the key K_{s1};
6. "Hide", in step 5, indicates using the locations of the bits representing the secret message M_{s1} found in C_c and starting from a random location L_r that should appear at the beginning of the transmitted set of numbers representing the second encryption of the secret M_{s1} given by C_{s1};
7. For more than one secret message M_{si} repeat 5 using K_{si} where i = 1, 2, .., n ;
8. Using another secure channel send the set of numbers representing M_{s1};
9. HALT

B. At the receiver end:

1. If "Rubber Hose" attack occurs then surrender only K_c;
2. To retrieve secret message Ms_1, use C_c and K_{s1};
3. HALT.

III. Formal description

In the following few lines, we describe the proposed approach.

At the sender end:

1. $E_{Kc}(M_c) \rightarrow C_c$; \\ Kc is the shared key for the cover message M_c
2. $C_c \rightarrow$ receiver; \\ Transmit C_c to receiver
3. $E_{Ks1}(m_{s1}) <=> C_{s1}$; \\ The symbol <=> represents getting the locations of

octets representing the corresponding to characters of the secret message M_{s1} found in C_c and starting from a random location L_r;

4. L_r and K_{s1} → receiver; \\Transmit L_r and K_{s1} using another secure channel;
5. HALT.

At the receiver end:

Surrender K_c; //If rubber hose attack occurs, then surrender key K_c

1. $D_{Kc}(C_c) \rightarrow M_c$; //If required, decrypt the cover ciphertext to get a decoy message;
2. $D_{Ks1}(C_{s1})$ >=< ms1 //Other secret messages can be retrieved using K_{si} for i =1,2 , .. n using L_r and K_{s1} , whenever another key is received, the corresponding message is retrieved. The symbol >=< represents replacing the received locations by their ASCII code;
3. HALT. //If No more keys received then HALT.

IV. Discussion

Based on the previous sections, one can easily recognize the following points:

- The ciphertext of the message M_c, given by C_c, is utilized as a binary lexicon for substituting the secret message ASCII codes with their respective locations in this dictionary. One can immediately understand that the cover message M_c can be transmitted only once and then used multiple times.
- Since the encrypted cover message C_c can be used multiple times, it should be relatively large to provide a large number of different locations for the same ASCII character.
- It is preferable that the cover message would be a multimedia file since it contains a large number of varying octets. This large number, it was found, through different experimentations, to be of the order of thousands of locations for the same character. Thus, eliminating the possibility of some dictionary attacks.
- "The best false statements are based on some actual events." Therefore, the cover message should contain some actual events to convince the rubber hose attacker that he or she has obtained the correct message.
- The YAEA-like procedure, discussed before, can be repeated for other secret messages. Whenever a new key is transmitted, the receiver gets a new secret message.

V. Summary & Conclusion

It is partly true that strong, nonstandard, encryption algorithms invite trouble. One can immediately visualize that a determined establishment with enough resources to intercept an encrypted message, is also capable of excruciating and extracting the key from their opponents. These physical attacks, as discussed before, save both time and financial resources as compared to advanced cryptoanalysis techniques. The issue has motivated cryptographer to think

how to thwart forcible attacks on the key holder.

I have presented an approach for protecting against coercion attacks through hiding other secret messages in the ciphertext of a decoy message. In this case, the ciphertext acts as an encryption lexicon.

I have described the adopted procedure in detail and provided a discussion of its potential application as an encryption dictionary. The method is based on the YAEA encryption and the polymorphic cipher Chameleon. I believe, if the proposed technique is employed correctly, it will save a secret message from an aggressive organization willing to violate some rules of engagement.

References

[1] Magdy Saeb, " The Chameleon Cipher-192(CC192): A Polymorphic Cipher, "SECRYPT2009, International Conference on Security & Cryptography, Milan, Italy; 7-10 July 2009 http://secrypt.icete.org/Abstracts/2009/SECRYPT_2009_Abstracts.htm

[2] Hristo Bojinov Daniel Sanchez, Paul Reber Dan Boneh Patrick Lincoln, “Neuroscience Meets Cryptography: Designing Crypto
Primitives Secure Against Rubber Hose Attacks,” Stanford University North-western University Stanford University SRI, 2012.
https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final25.pdf

[3] Magdy Saeb, Ramy Zewail, Ahmed Seif, "A Micro-architecture Implementation of YAEA Encryption Algorithm Utilizing VHDL and Field Programmable Gate Arrays," Proceedings of the Third International Conference on Electrical Engineering ICEENG 2002, Military Technical College, Cairo, Egypt, May 2002. www.magdysaeb.net

Magdy Saeb received the BSEE, School of Engineering, Cairo University, in 1974, the MSEE, and Ph.D. degrees in Electrical & Computer Engineering, University of California, Irvine, in 1981 and 1985, respectively. He was with Kaiser Aerospace and Electronics, Irvine California, and The Atomic Energy Establishment, Anshas, Egypt., He is a professor emeritus & former chairman of the Department of Computer Engineering, Arab Academy for Science, Technology & Maritime Transport, Alexandria, Egypt; He was on-leave working as a principal researcher in the Malaysian Institute of Microelectronic Systems (MIMOS). While in MIMOS, he obtained five US/International Patents in Cryptography. Currently, he is the CTO, Great Wall InfoSec Sdn. Bhd., Malaysia. His current research interests include Cryptography, FPGA Implementations of Cryptography and Steganography Data Security Techniques, Encryption Processors, Mobile Agent Security.
mail@magdysaeb.net
www.magdysaeb.net