Security Analysis of the Power Based Key Hopping (PBKH) Technique

Magdy Saeb,

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

Great Wall Information Security (GWIS), Kuala Lumpur, Malaysia

mail@magdysaeb.net

Abstract: In a previous work, we showed that Key Hopping based on packet or message power (PBKH) tremendously increases the key space and consequently the cipher security. In the present work, we provide security analysis of this technique computing the required minimum times, in computer cycles, to break all or one of the sequence keys.

Key words: Cipher, Key, Hopping, Power-based, Sequence Key

1. Introduction

In a previous work [1], we discussed a Power Based Key Hopping protocol. This is a key hopping methodology that is founded on utilizing the theme of power based dynamic frequency hopping. PBKH utilizes four keys; one key acts as the authentication master key and the power of a cipher text packet are used for deciding to keep or change the key in a pseudo random fashion. In this work, we provide a security analysis of the method and show that the key space is increased tremendously using this approach. We also introduce the notion of the minimum adversary trial time for a successful attack. Finally, we provide a summary and our conclusions.

2. The PBKH Technique [1]

It is a well-known fact that the cipher security depends on the key size, the block size, the number of rounds, the round function and the round key generation algorithm. Increasing the key size, the block size and the number of rounds, in general, require larger computational and communication costs. The alternative technique to increase the cipher security is to use multiple keys to encrypt the plaintext. As shown in [1], the authors proposed dividing the plaintext file into n packets, generate a sequence of n keys to encrypt each packet separately. The sequence of these keys is performed by using a master user key, a hash function (h), a counter and changing the initial value (IV) of this hash function. In the following analysis, without loss of generality, we use one master key and three packet keys. The method discussed in [1], is summarized here as follows:

It uses a discrete form of signal analysis where the signal power is measured as the mean of the signal encountered. In this case, the power of discrete signal with length is determined by the mean of x_i:

$$\text{Power} = \frac{\sum_i^L |x_i^2|}{L}$$

In other words, the power of a packet of binary sequence with length L can be determined by the number of ones in that packet compared with the number of zeros. In this respect, the power based key hopping (PBKH) has its roots in the method that is called Dynamic Frequency Hopping (DFH) [5]. The PBKH method utilizes four keys. Each two communicating entities maintain four secret keys, one of them will be an authentication key and the first key will be used as the default key at each time the communication session is started. The communicating entities use the first key to encrypt and decrypt the first plaintext packet. Then the sender and receiver utilize the hash function, the counter and the IV to generate locally the other sequence keys. This technique [1] is summarized as shown in Figure 1.

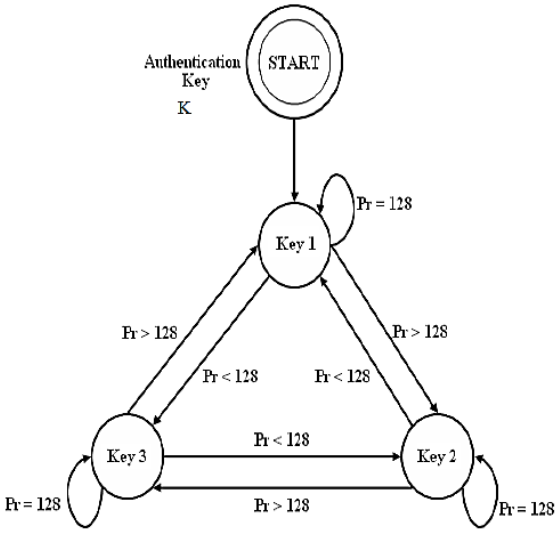

Figure 1. *The Power Based Key Hopping Technique [1]*

3. Analysis of the PBKH Technique

Now to analyze this technique, we take k as the number of bits in each of these keys. In this approach, the probability of brute force attack on the resulting key sequence to decrypt n packets comprising the plaintext file is given by:

Pr {Successful Brute Force Attack}

$$= 1/2^{(n+1)\,k} \qquad (1)$$

In other words the key space has been increased from 2^k to $2^{k\,(n+1)}$. As an example assuming k = 256 bits and n = 3 then the new key space is 2^{1024} without the added computational and communications overheads. Now assuming that a skillful adversary requires a probability of a successful attack greater than that of brute force, say this probability is equal to P_{adv}.

Then $P_{adv} \geq 1/2^{(n+1)\,k}$ that is:

$$(1 / P_{adv}) \leq 2^{(n+1)\,k}$$

Then,

$$\log_2 (1/ P_{adv}) \quad \leq (n+1)\,k \qquad (2)$$

Now suppose that the adversary is performing y trials to break the key sequence, then the probability of successful attack is reduced to

Pr {Successful Attack with y Trials}

$$= 1/ [2^{(n+1)\,k} – y] \qquad (3)$$

If we call this probability the adversary probability with y trials P_{yadv}, then

$$P_{yadv} = 1/ [2^{(n+1)\,k} – y] \qquad (4)$$

And

$(1/P_{yadv}) + y = 2^{(n+1)\,k}$ (5)

Then,

$\log_2 [(1/P_{yadv}) + y] = (n+1)\,k$ (6)

In other words the number of packets or sequence keys n, for an adversary who can perform y trials, is at least should be

$n = \{(1/k) \log_2 [(1/P_{yadv}) + y]\} - 1$ (7)

If each trial consumes c computer cycle time, then the time required to launch an attack by the adversary is T, where T = c.y

Then y = T/c

Replacing for the value of y in the above equation, we get

$n = \{(1/k) \log_2 [(1/P_{yadv}) + T/c]\} - 1$ (8)

Where n is the number of messages for an adversary trial time T.

On the other hand, to find T, we rearrange the above equation as follows:

$\log_2 [(1/P_{yadv}) + T/c] = k\,(n+1)$ (9)

And

$T = c\,(2^{\,k\,(n+1)} - 1/P_{yadv})$ (10)

Obviously, this is the time spent in the y trials. If this trial time is manageable, say the adversary found some key in 2^{32} trials then this time is approximately 1.43 seconds for a 3 GHz processor.

The Probability of find the i-th sequence key is given by:

Pr {Finding the i-th Sequence Key}

$= 1/\,(2^k - y)$

Assuming the maximum value of this probability is equal to P_{max}, then

$1/\,(2^k - y) \le P_{max}$ (11)

And

$(2^k - y) \le 1/\,P_{max}$ (12)

Consequently,

$y \ge 2^k - 1/\,P_{max}$ (13)

And the trial time T = c.y

That is, $T \ge c\,(2^k - 1/\,P_{max})$ (14)

In other words, the minimum required time to break one sequence key is T_{min} is given by:

$T_{min} = c.\,(2^k - 1/\,P_{max})$ (15)

Therefore, the sequence keys should be changed before T_{min} or else the adversary has a serious chance of successful attack.

Summary and Conclusions

In this short correspondence, we have provided an insightful account of the security of the PBKH technique. We have shown that the technique tremendously increases the key space without additional communication costs since the key sequence is locally generated. We have provided a closed-form set of equations to estimate the required times to change one or all of the sequence keys to avoid key-related adversary attacks. In addition, we have provided an estimate of the expected lifespan for each sequence key.

References:

1. Rabie Mahmoud, Magdy Saeb, "Power-based Key Hopping (PBKH) and Associated Hardware Implementation," International Journal of Computer Science & Information Security (IJCSIS), VOL.8 No.9, Dec. 2010. http://sites.google.com/site/ijcsis/vol-8-no-9-dec-2010.

2. W. Ying, "Key Hopping – A Security Enhancement Scheme for IEEE 802.11 WEP Standards," NextComm Inc, USA, 2002.

3. K. Srinivasan, and S. Mitchell, "State Based Key Hop (SBKH) Protocol," Sixteenth International Conference on Wireless Communications Wireless 2004, Alberta, Canada, 2004.

4. A. M. Kholaif, M. B. Fayek, H. S. Eissa, and H. A. Baraka, "DRKH: Dynamic Re-Keying with Key Hopping," McMaster University, Hamilton, Canada, 2005.

5. H. Bli, and H. Salim, "Performance Enhancement of GSM Cellular Phone Network using Dynamic Frequency Hopping," Engineering & Technology Journal, Vol. 26, No.3 (2008), University of Technology, Baghdad, Iraq, 2008.

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 in the Department of Computer Engineering, Arab Academy of Science, Technology & Maritime Transport, Alexandria, Egypt; He was on leave working as a principal researcher in the Malaysian Institute of Microelectronic Systems (MIMOS). Now he is the CTO of Great Wall Information Security, Kuala Lumpur, Malaysia. His current research interests include Cryptography, FPGA Implementations of Cryptography and Steganography Data Security Techniques, Encryption Processors, Mobile Agent Security.

www.magdysaeb.net