INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY SCHEME FOR WIRELESS NETWORK BASED ON SECRET SHARING

PRIYA BARDE, PROF. MS. SUNITA PARIHAR

1. Student (M tech communication), PIET, Nagpur, INDIA.
2. Asst. Prof. PIET, Nagpur, INDIA.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Password

Security

Corresponding Author

Ms. Priya Barde

Abstract

If a secret key or a password is to be used in an application, where multi users are involved, then it is better to share the key or the password to all the authorized users in such a way that a minimum or all the shares of the users put together must result in the key or the password. This method avoids the unauthorized access to the information by a single user without the knowledge of the other users. So this can protect the important information and also protect the key by sharing. If the key is not shared, then always there may be a threat of key being compromised intentionally or unintentionally. If the key is shared among the authorized users, at the time of requirement to use the information, few authorized users can use their shares to reconstruct the key and use it. This avoids the drawbacks of the single user having the key. Also it is necessary to authenticate the shares given by the users during reconstruction of the key.

To achieve the confidentiality of the key we can use threshold cryptography, secret sharing deals with such difficulty. This approach shares a highly sensitive secret among a group of n users so that only when a sufficient number k (k<= n) of them come together, the secret can be reconstructed. Well known secret sharing schemes (SSS) in the literature include Shamir based on polynomial interpolation, Blakley based on hyper plane geometry[3] and Asmuth-Bloom based on Chinese Remainder theorem[4].All these approaches lead to high computational complexity during both sharing and reconstructing the information. Our scheme employs simple graphical masking method, done by simple ANDing for share generation and reconstruction can be done by simple ORing the qualified set of shares. This makes the computational complexity very minimal compared to the earlier proposed schemes. This makes it effective for addressing energy saving distributed environment where battery driven low end processors are used and security is also a major challenge. To achieve the confidentiality of the key we are using the threshold secret sharing method where the key will be divided in to number of shares depending on the number of authorized users and to provide authentication we are using SHA-1 algorithm. The key can be text data, image.

Introduction:

Secure transmission of information in wireless environment is an important concern. If a secret key or a password is to be used in an application, where multi users are involved, then it is better to share the key or the password to all the authorized users in such a way that a minimum or all the shares of the users put together must result in the key or the password. There are two aspects in the area of information security. One is the actual information which is supposed to be very confidential. Example in any business organization the business related information stored in a database needs confidentiality only the authorized user can access that information. Second one is the key or the password needed to enter in to the database must also be confidential. If the key or the password is not protected properly, definitely there will be a threat for the database where the sensitive information is stored. This is true in other areas like military, banking, medical, government organizations etc where sensitive information is being maintained. There will not be any problem if the information is allowed to be accessed by only one authorized user, and then the key is known only to that user. But if the information needs to be accessed by multiple users' utmost care must be taken so that both the key as well as the information stored in the system must be safe. But in a multi user system it is very difficult to achieve confidentiality, since maintaining the key itself is very difficult. A single user can not be given the key, because if that user doesn't turn up then there is no way that the information can be accessed, and also there can always be a threat of compromising the key to the unauthorized users, losing the key, forgetting the key. On the other hand if the key is given to all the authorized users, then any of the users can access the system without the knowledge of the other users. A method known as secret splitting can be used, where the key will be shared among all the users. When the key is required, it is necessary to get all the shares from all the users. Even if one share is missed due to some reason it is not possible to reconstruct the key. So to avoid all these a technique devised by Shamir known as threshold secret sharing (m,n) which is interpolation can be used so that the key can be shared to all the authorized users by the administrator. Where n is the number of authorized users and m is the minimum number of shares required to construct the key. When the key is required, the user who needs the key will request other users to send their shares. In this method m or more than m shares are required to construct the key. With less than m shares it is not possible to construct the key, this ensures the minimum number of users required to access the system. This overcomes the misuse of key, compromising the key, forgetting the key, etc. Also it indicates the users who participated in the construction of the key. At any point of time no user will have the complete key, and with the knowledge of the partial key he cannot access the system.

THRESHOLD SECRET SHARING:

First secret sharing (m,n) was proposed by shamir[1], which is based on the polynomial interpolation. There are other secret methods proposed by many people but Shamir's is very simple. This method can be used for the key of text, image, and integers also. In this method a polynomial of order m-1 will be used. The polynomial is used to share the secret by considering the coefficients.

$F(x) = S + C1x + C2x2 \ldots\ldots.. + Cmxm$

Where S is the secret to be shared, C1, C2 … Cm are coefficients. The coefficients can be any random integer values. When it is necessary to use the key/secret to access the system, the user requiring the key can send a request for shares to other users. When a user receives m or more number of shares he can reconstruct the required key.

The reconstruction of the key is based on Lagrange's interpolation as shown below.

$$F(X) = \frac{(X-x1)(x-x2)\ y0}{(X0-x1)(X0-x2)} + \frac{(x-x0)\ (x-x2)\ y1}{(X1-x0)(X1-x2)} + \frac{(X-x0)(x-x1)\ y2}{(X2-x0)(X2-x1)}$$

This approach lead to high computational complexity during both sharing and reconstructing the information

GRAPHICAL MASKING METHOD:[5]

As an example a possible set of masks for 5 shares with threshold of 3 shares is shown below:

Mask 1: 0 0 0 0 1 1 1 1 1 1

Mask 2: 0 1 1 1 0 0 0 1 1 1

Mask 3: 1 0 1 1 0 1 1 0 0 1

Mask 4: 1 1 0 1 1 0 1 0 1 0

Mask 5: 1 1 1 0 1 1 0 1 0 0

One can easily check that O Ring any three or more shares we get all 1's but with less than three shares some positions still have 0's i.e. remain missing.

Mask Designing Technique [5]

The algorithm for designing the masks for **n** shares with threshold **k** is as follows.

Step 1: List all row vectors of size **n** having the combination of **(k-1)** nos. of **0's** and **(n-k+1)** nos. of **1's** and arranges them in the form of a matrix. Obvious dimension of the matrix will be **nCk-1** × **n.**

Step 2: Transpose the matrix generated in Step-1. Obvious dimension of the transposed matrix will be **n** × **nCk-1.** Each row of this matrix will be the individual mask for **n** different shares. The size of each mask is **nCk-1** bits, i.e. the size of the mask varies with the value of **n** and **k**.

(It may be noted that the masking patterns are not unique. Different arrangements of the row vectors in Step-1 leads to different sets of masks but for a particular set, the masks are unique and they satisfy the requirements)

Let us consider the previous example where **n**=5 and **k**=3.

Step 1: List of row vectors of size 5 bits with 2 numbers of 0's and 3 nos. of 1's.

0 0 1 1 1

0 1 0 1 1

0 1 1 0 1

0 1 1 1 0

1 0 0 1 1

1 0 1 0 1

1 0 1 1 0

1 1 0 0 1

1 1 0 1 0

1 1 1 0 0

Dimension of the matrix is **5C2 × 5** i.e. **10 × 5**

Step 2: Take the transpose of the above matrix and we get the desired masks for five shares as listed above in the form of matrix of dimension **5** × **5C2** i.e. 5 x 10. There are five masks each of size 10 bits

SHA (SECURE HASH ALGORITHM):[6]

Encryption protects against passive attack where as message authentication protects against active attack. So it is necessary to protect the data against active attacks like modification of data, masquerade, and replay etc.SHA-1 provides message authentication. It provides a message digest of 160 bits for any length of input stream. For a given input of any length this algorithm generates a unique value called hash value or code. If any of the bits in the input is changed then the hash code will also be changed. But this is a one way function, by knowing the hash code it is not possible to generate the input data. This property can be used to authenticate the shares. During the reconstruction of the key one can check whether he/she has got the legitimate shares only or not by generating the hash code for the received share and compare the new and the old hash code, if they are different it indicates that that particular share has been unauthorizedly changed.

Characteristics of SHA-1:

Every bit of the hash code is a function of every bit of the input. Due to the complex operations bits are well mixed and, rare chance of producing the same hash code for 2 messages with similar patterns. 2 messages having same code is on the order of 2256 operations. Difficulty of finding a message with a given hash value is on the order of 2512 operations. Using this, one can prove the integrity of the message

Example :

Dealer generates 5 shares s1, s2, s3, s4, s5 and their corresponding hash values h1, h2, h3, h4,h5

He distributes the shares to 5 participants in the following way

P1 s1, h1,h2,h3,h4,h5

P2 s2, h1,h2,h3,h4,h5

P3 s3, h1,h2,h3,h4,h5

P4 s4, h1,h2,h3,h4,h5

P5 s5, h1, h2, h3, h4, h5

When the participants receive these they store their share and others hash value in the memory. It also verifies if the received share is the actual one or the modified one by calculating the hash value and compares that with the corresponding received hash value. If the values are same it will retain all the information else it can reject and inform the same to the dealer.

For example if the participant P1 received s1, h1, h2, h3, h4, h5 It calculates hash value for s1, and compares that with the corresponding received hash value h1. If they match then the P1 can store the secret and hash values in its memory else it can discard. Like this all the participants can verify their shares when they receive from the dealer. When a user wants to reconstruct the secret, he will request the other participants, when he receives the shares; he will generate the hash values and compares that with the stored hash values of the users. Thus the verification of the shares will be done by any user. This method can be applied to any type of data text, numeric, or image.

SECURITY ANALYSIS:

This method certainly gives security for the key in general. First of all the key is divided into number of shares, so no single share reveals any information about the key. And also even if one share is not available still it is possible to reconstruct the key if m number of shares is available. Second since for each share the hash code is generated by the dealer and sent along with the respective shares to each of the users, the users can verify the shares before accepting the corresponding shares. Third when a user requests for shares to reconstruct the key he can also verify the shares he obtained from other users. Only if the received shares hash code match with the stored hash code of the users then only the receiver can construct the key. Otherwise he can reject those shares and inform the same to the dealer. This verifies the points of vulnerabilities.

CONCLUSION:

This work has proved that specified number of threshold shares is sufficient to reconstruct the key; also we have used a new method (Graphical masking method) to reduce complexity. A very few have worked on authentication. Here we have used one of the strongest and simple algorithms to generate hash code for verification of the shares. Using this user can verify the shares when they receive it from the dealer and also, users can verify the shares received from other users during reconstruction process. This clearly indicates which user is creating a fake share or which communication channel is vulnerable. So this work has proved both confidentiality and authentication of the key without using encryption and decryption which requires processing time.

REFERENCES:

1. A. Shamir, "How to share a secret, Comm.ACM" **22**(1979).

2. T.S. Rappaport, Wireless Communications: Principles and Practice, Prentice Hall, Upper Saddle River, NJ, Oct. 1995

3. G. Blakley : "Safeguarding cryptographic keys "Proc. of AFIPS National Computer Conference, 1979

4. C. Asmuth and J. Bloom:" A modular approach to key safeguarding" IEEE transaction on Information Theory, 29(2): pp 208-210, 1983.

5. A Novel Security Scheme for Wireless Adhoc Network "*Abhijit Das, Soumya Sankar Basu, Atal Chaudhuri* Kolkata, India (2011).

6. A Novel Way Of Providing Confidentiality TO Shared Secret Key And Authenticate The Shares During Reconstruction "*P Devak*, G Rghavendra Rao, India(2012).