ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Publisher and Subscriber Message Transaction Using Half-Key Security

[1]Dhinakaran, K., [2]Lakshmanaswamy, K., [3]Uma Priyadarsini, P.S.

[1,3]Department of Computer Science and Engineering, Assistant Professor, Saveetha School of Engineering, Saveetha University, Chennai, Tamil Nadu, India.
[2]Department of Computer Science and Engineering, UG Scholor, Saveetha School of Engineering, Saveetha University, Chennai, Tamil Nadu, India.

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Half-key, security, publisher, subscriber, transaction security, Bloom's taxonomy, key generation, authentication.

ABSTRACT

Nowadays, it has become a challenging task to provide security and confidentiality to the users from the view of both publisher and subscriber. Authentication and confidentiality of publisher and subscriber has become a question because loose interactions between them. This paper provides an approach to improve the authentication, security and confidentiality using half-key implementation. Authentication and confidentiality of users are ensured by using of Bloom's taxonomy to couple the publisher's and subscriber's data. This paper is implemented using three methods. The first method deals with publishing the content to appropriate subscriber by publisher, whereas the second method generation of three types of keys by the publisher the subscriber to access the content. The third method emphasizes on usage of key security parameters. The proposed methods and subsequent processes enable the messaging system to function efficiently in terms of Authentication, Security and Confidentiality.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Dhinakaran, K., Lakshmanaswamy, K., Uma Priyadarsini, P.S., Publisher and Subscriber Message Transaction Using Half-Key Security. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 671-676, 2015*

INTRODUCTION

The structure of publisher and subscriber interaction has gained a good and strong response because of its interactive nature and also it meets the necessity of the subscriber on time. The publisher sends the content to the common space where users can get it. Published events are sent to all subscribers. So irrelevant subscribers who do not want unnecessary information also gets irrelevant messages. But this irrelevancy of content is refined with the help of third party broker systems. Content or information based publishing and subscribing system is lot more expressive where the publishing and subscribing is based on content restriction. This structure of information transaction is one way where publisher can publish and subscriber can get it. This type of interaction is helpful in various fields. Content based publisher/subscriber (Anceaume, E., 2006) is the variant that provides the most expressive subscription model, where subscriptions define restrictions on the message content. Its expressiveness and asynchronous nature is particularly useful for large-scale distributed applications such as news distribution, stock exchange, environmental monitoring, traffic control, and public sensing. Not surprisingly, pub/sub needs to provide supportive mechanisms to full fill the basic security demands of these applications such as access control and confidentiality.

The Proposed work is designed in such a way that it gives a secure platform for the users in the view of both publisher and subscriber such that the data transaction in the form of subscription will not leak out since there is no intervention of third party brokers. The messages are being directly carried to the user with a help of self-sufficient server. This helps the user to avoid attacks like man in the middle, message manipulation etc.

Related Works:

In publisher/subscriber model the recipient receives only particular category or categories of message He or She wants. This process of sending or receiving a particular category of message is called filtering. The following are three common forms of filtering:

- Topic based
- Content based
- Hybrid

Corresponding Author: Dhinakaran, K., Department of Computer Science and Engineering, Assistant Professor, Saveetha School of Engineering, Saveetha University, Chennai, Tamil Nadu, India
Tel: +919710231842; E-mail: maildhina.k@gmail.com

Topic Based Filtering:

In topic based filtering the publisher publishes his message to a channel under some label. Publisher in topic based system will receive the message that is being posted under that particular label. All the users those who subscribe to that particular channel or those who are under that particular label receive the messages posted for that label. Publisher is the authority to define the category of message to which user can subscribe.

Content Based Filtering:

In content based filtering the messages sent by the publisher reach the user if and only if the content of the message matches the criteria selected by the subscriber. Otherwise the content does not even delivered to the user. Here the responsibility if defining the criteria of content is that of subscriber's. Here the subscriber is given the freedom to choose the criteria of message he wants so that he need not receive all the messages unnecessarily which helps the subscriber also to save lot of space in his inbox.

Hybrid Filtering:

In hybrid filtering, the filtering is done mixing both the above said types of filtering. This results in enabling the publisher free to post the messages to any type of label and subscriber is free to subscribe any type of label under defined criteria. Here Subscriber can subscribe to any number of categories.

Background:

Topologies:

In many publisher / subscriber structure of message transfer the message is sent to a middle man like message broker or event bus. The subscribers have to subscribe their messages from the brokers who are middle men. The broker or event bus does the work of filtering the message for subscribers. The event bus does the work of repository of messages from the publisher and makes it reach the appropriate subscribers .The event bus may keep the message in queue and give preference to whichever it has been programmed for. During the process of initialization, build time or run time the subscribers may register for messages of certain criteria.

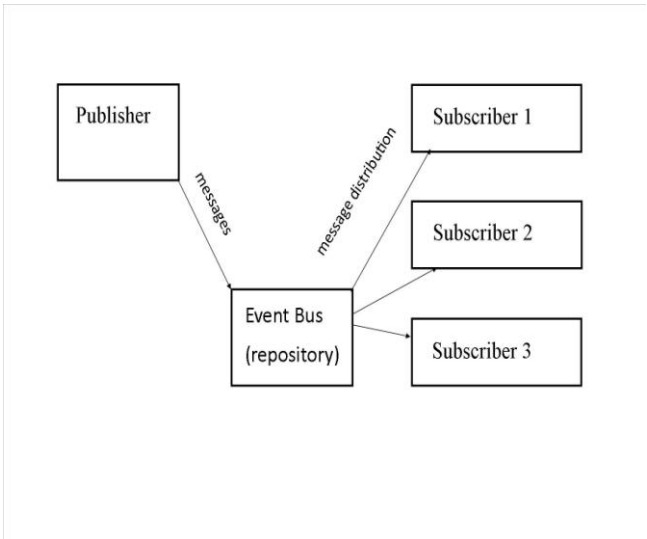
Inflexible Coupling with Subscriber Systems:

The framework of content published should fall under some well-established structure. But, this becomes difficult most times. If wrong data is published it is difficult to re do it. For redoing it You need to know the details of all the subscribers without which one cannot delete the information already sent and residing at subscribers system or subscribers space. There is also a complexity of maintaining the compatibility with older versions.

Security Threats:

The requirement of subscriber (Nabeel, M., 2012) changes from time to time. In such case if the structure of data is rigid and not compelling to use then this rigidity may end up in making the entire system outdated. So, This inflexibility issue has to be taken care of I order to make it more likely and easy to usable. There is a one stop solution for this issue and it is point backward compatibility which enables the publisher to take back whatever he has published.

Broker Architecture:



Architecture of broker system

In this figure, the broker architecture diagram explains how the system functions. The user publisher sends the message to the repository and the subscriber gets the information from the event bus which is a broker repository for distribution of messages.

Proposed Work:

In the proposed architecture the publisher sends the data to it's own server and processes it based on Bloom's Taxonomy to segregatte it based on the knowledge derived .The server sends the content to subscriber based on segreggation achieved and the ublisher sends a private key and a half key to the user. Based on the match of the private key and the half key the subscriber will be able to generate the public key. The public key and private key are input from the user to see their match and once it is verified and proved to be genuine then the user or subscriber is let to access the content (Bacon, J., 2008).

Goals:

Secure overlay maintenance protocol is designed to preserve the weak subscription confidentiality. The following methods are adopted to implement Secure Overlay Maintenance Protocol (SOMP)

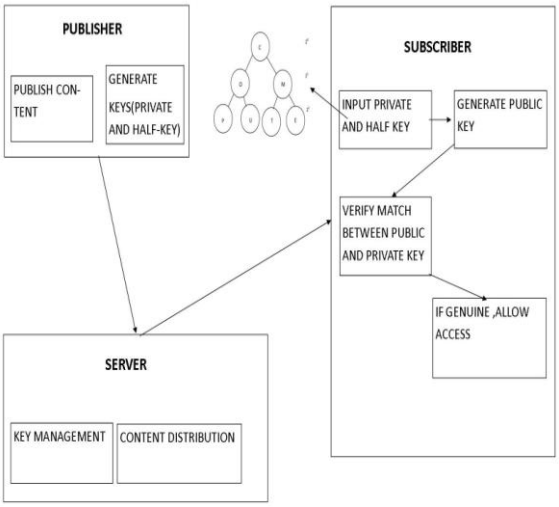
1) Extensions of the cryptographic methods to provide efficient routing of encrypted events by using the idea of searchable encryption.

2) Multi credential routing a new event dissemination strategy which strengthens the weak subscription confidentiality.
3) A thorough analysis of different attacks on subscription confidentiality

Advantages:

The approach is highly scalable in terms of number of subscribers and publishers in the system and the number of keys maintained by them. In particular, we have developed mechanisms to assign credentials to publishers and subscribers according to their subscriptions and advertisements.

Proposed Architecture:



Architecture of the proposed system

Implementation Methods:
Content Publishing:

For publishing any content on the web the publisher has to use a domain in which he/she have to register and become a publisher member to publish his/her content on the web .The publisher has to create his content and publish to the relevant users . This paper reduces the complexity and threat of content getting leaked by third party brokers. This is done by directly segregating the content in terms of subscribers interest .This is done using Bloom's taxonomy. Using Blooms taxonomy(BT) the interest of the user is determined and segregated based on their interest. This process involves six step processes which are listed below:

- Evaluation (E)
- Synthesis (S)
- Analysis(AN)
- Application(AP)
- Comprehension(C)
- Knowledge(K)

BT =∑ (E+S+AN+AP+C+K)

In Bloom's taxonomy each attribute has a relation with each other attribute.

Evaluation:

In the process of evaluation the ideas of subscription pattern of users interest are compared and identified by solving and judging it. It is the process where the opinions are presented and defended on variuos grounds by which they are predicted and judged. It is in this process where an idea or opinion is validated. This process can be classifies based on two methods. They are

A. Judgement By Internal Evidence:

Judgement by internal evidence is done on the basis of the understanding of the problem definition. From the understanding the evidence is derived. Based on the evidence the further process is carried out.

B. Judgement By External Criteria:

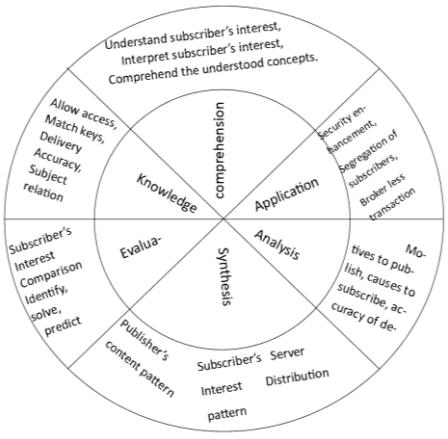
Judgement by external criteria is done on the basis of criteria posed. From this external criteria overal judgement is made.

Synthesis:

In the process of Synthesis Design (Jacobsen, H.A., 2010) for publishing the content based on subscribers interest based on evaluation is done. Basically synthesis is a process of deriving the pattern or structure from the elements of different kind. In this process to gain a whole product the parts or segments of it are combined. In this process of publisher's message is put together to make to make it easier for server to identify its category and deliver it to the subscriber based on subscription pattern.

Analysis:

In the analysis process ,The subscribers interest patterns are organized and the trends of their interest are related to make the delivery more accurate and precise. In this process the information is broken into pieces based on motives and causes and examined.



Data Interpretation

Application:

In the Application process the knowledge gained so far using evaluation ,synthesis and analysis are used

to solve the problems in conflict of interest in subscriber. It is the process where knowledge derived is implemented and this process helps in facing the unidentified or new problems.

Comprehension:

In the process of comprehension the trend so far analyzed is understood and comprehended to publish the content. In this process the basic understanding of problem definition is demonstrated by organizing ,translating, interpreting ,comparing, (Jelasity, M., 2013) stating main idea and giving descriptions. This process can be comprehended effectively based on translation, interpretation and extrapolation. Translation is a process of transforming data of one form to data of another form and interpretation is a process of garsping the meaning of the problem in a right way.

Knowledge:

In the process of knowledge ,all the knowledge gained are applied and implemented to segregate the users. Basically, In this process result of all the above seen processes are taken into consideration for the building of logic which helps the process of segregation of subscribers effectively**.**

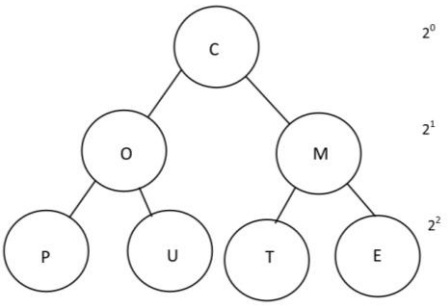
Keys Generation:

In order to implement the idea of this process there are three types of that has to be generated .They are 1.Public key (Miller, F.P., 2009), 2.Private key, 3.Half-key.This three tier security keys enhances the security and confidentiality of the content being published .public keys is publisher desired key and it is common for all of his users. Private key is the individual unique key and it is unique for each users and it is randomly generated by the automated systems meant for this purpose and half-key is part of key from the private key. This is decided based on publishers interest. It is implemented based on tree structure. For example, let us assume that the private key is "COMPUTE" .It will be implemented in the tree structure as follows.

Starting fromm the primary root node of the tree which is a single node each character of the key is arranged.The expression for the Chosen Nth level is as follows:

No of characters for n^{th} level = 2^{n-1}

Based on this the Publisher can select the order of Half-key and send it to the subscriber



Generation of half-key

From the above mentioned tree the user can select half-key of any one order. If order is 2^0 then half-key is "C". If order is 2^1 then half-key is " OM" .If order is 2^2 then half-key is "PUTE". Once the publisher publishes his/her content the subscriber need all the three keys to access the contents.

Authentication:

Authentication is the process of checking the genuinity of the publisher and subscriber .Only legitimate publisher should publish content and only intended subscribers should get the intended content based on their interest .This helps to maintain the data confidentiality(Bethencourt, J., 2007). Authentication is a primary process to verify your genuinity to access content.

Data Confidentiality:

Data confidentiality (Barker, W.C. and E.B. Barker, 2012) is the parameter to maintain the secrecy of the subscribers content. publisher's message should reach the intended subscriber opaquely without other subscribers knowing it .This helps the secure transaction (Ion, M., 2010) of data.

Scalability:

Scalability (Khurana, H., 2005) is the parameter to check the ability of system to deliver the content effectively and accurately. This ensures that the subscribers are getting the right message at the right time.

Robustness:

Robustness (Boneh, D. and M.K. Franklin, 2001) of the system is the parameter to check the ability, interpretation, understandability , adaptability etc.. These processes together makes the system to check its correctness and efficiency so that no mistake occurs with the confidentiality of the content where it is needed at most.

Proposed Algorithm for Message Transaction:

Based on the analysis and consideration of the critical parameters and security keys, the new algorithm is devised which is not only robust but also provides segregation of the subscribers.

Algorithm For Publisher and Subscriber Message Transaction

```
/*Publisher side process module */
Step 1:Content Creation
Step 2:Key Generation
Step 3:  Private Key(Pr) ,Half Key(Hf) generation  from server side.
/*Server side process module */
Step 4:Segeregation of subscriber based on interest
Step5:Distribution of cotent based on subscriber's interest
Step 6:Distribution of Private key(Pr),Half key(Hf) to subscriber
/*Subscriber side process module */
Step 7:Subscriber inputs the Private key(Pr) and Half  key(Hf).
Step 8:Public key (Pu) generated based on match of  half key and private key
Step 9:Subscriber inputs Public key(Pu) and Private key(Pr)
Step 10:If Public key(Pu) matches Private key(Pr) then user is allowed to access.
Step 11:Else Access denied
```

Pseudo code for proposed algorithm:

```
Publisher side:
Create content
Publish content
Generate Private key , Public key and Half key
If subscriber's interest matches the content
        Send keys to subscriber
Else
        Move to next subscriber to know his interest

Subscriber side:
If Private key matches Half key
        Generate public key
        Print public key
        If private key matches public key
                Print access granted
        Else
                Print access denied
Else
        Access denied
```

The above algorithm gives an effective way to segregate the subscribers based on bloom's taxonomy to make the segregation more accurate and see to that the users are getting relevant subscriptions based on their interest. This avoids the need of third party brokers which empowers us in terms of security, authenticity and data confidentiality.

This paper also formulates the pseudo code for the proposed algorithm and can be seen in forthcoming parts.

Conclusion:

This paper concludes the idea by generating the series of keys by the publisher and make the user to use it in different combinations in order to access the document to ensure the confidentiality of the content. We have presented a new approach to provide authentication and confidentiality in a broker-less content based pub/sub system. The approach is highly scalable in terms of number of subscribers and publishers in the system and the number of keys maintained by them. In particular, we have developed mechanisms to assign credentials to publishers and subscribers according to their subscriptions and advertisements. Private keys assigned to publishers and subscribers, and the cipher texts are labeled with credentials. We adapted techniques from identity based encryption 1) to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and its private keys and 2) to allow subscribers to verify the authenticity of received events. Furthermore, we developed a secure overlay maintenance protocol and proposed two event dissemination strategies to preserve the weak subscription confidentiality in the presence of semantic clustering of subscribers. Further evaluations should be conducted to demonstrate the viability of the proposed security mechanisms against the third party broker system and analyze the attacks on subscription confidentiality. There are multiple research avenues exists in order to test the efficiency of the proposed half-key message transaction system and algorithms with other related works.

REFERENCES

Anceaume, E., M. Gradinariu, A.K. Datta, G. Simon and A. Virgillito, 2006. "A Semantic Overlay for Self- Peer-to-Peer Publish/ Subscribe," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS).

Bacon, J., D.M. Eyers, J. Singh and P.R. Pietzuch, 2008. "Access Control in Publish/Subscribe Systems," Proc. Second ACM Int'l Conf. Distributed Event-Based Systems (DEBS).

Barker, W.C. and E.B. Barker, 2012. "SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," technical report, Nat'l Inst. of Standards & Technology.

Bethencourt, J., A. Sahai and B. Waters, 2007. "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy.

Boneh, D. and M.K. Franklin, 2001. "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology.

Boneh, D., G.D. Crescenzo, R. Ostrovsky and G. Persiano, 2004. "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT).

Choi, S., G. Ghinita and E. Bertino, 2010. "A Privacy-Enhancing Content-Based Publish/Subscribe System Using Scalar Product Preserving Transformations," Proc. 21st Int'l Conf. Database and Expert Systems Applications: Part I.

Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006. "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM 13th Conf. Computer and Comm. Security (CCS).

Ion, M., G. Russello and B. Crispo, 2010. "Supporting Publication and Subscription Confidentiality in Pub/Sub Networks," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm).

Jacobsen, H.A., A.K.Y. Cheung, G. Li, B. Maniymaran, V. Muthusamy and R.S. Kazemzadeh, 2010. "The PADRES Publish/ Subscribe System," Principles and Applications of Distributed Event-Based Systems. IGI Global.

Jelasity, M., A. Montresor, G.P. Jesi and S. Voulgaris, 2013. "PeerSim: A Peer-to-Peer Simulator," http://peersim.sourceforge.net/.

Khurana, H., 2005. "Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems," Proc. ACM Symp. Applied Computing.

Lewko, A., A. Sahai and B. Waters, 2010. "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy.

Lynn, B., 2010. "The Pairing-Based Cryptography (PBC) Library," http://crypto.stanford.edu/pbc/.

Miller, F.P., A.F. Vandome and J. McBrewster, 2009. Advanced Encryption Standard. Alpha Press.

Nabeel, M., N. Shang and E. Bertino, 2012. "Efficient Privacy Preserving Content Based Publish Subscribe Systems," Proc. 17th ACM Symp. Access Control Models and Technologies.