www.ijecs.in

International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18309-18313

Publish/Subscribe Systems Security through Distinct Identity Encryiption

#1 R. Kiranmayi, #2 P. Pothuraju
Mtech Pursuing,
Assistant Professor,
Department Of Computer Science And Engineering,
Vasireddy Venkatadri Institute Of Technology (Vvit) Guntur

Abstract:

The publish/subscribe communication paradigm has gained high popularity. Publishers inject information into the pub/sub system and subscribers specify the events of interest by means of subscription. Traditional Content based pub/sub provide expressiveness and asynchronous nature but gives little attention to security. Existing approaches rely on traditional broker network that address security under restricted expressiveness or rely on network of semi-trusted brokers. This paper shows a new approach to provide authentication and confidentiality in BROKER_LESS pub/sub system by allowing subscribers to maintain credentials. Additionally we present Extensions of cryptographic methods, Multi credential routing that strengthens the weak subscription confidentiality.

1. INTRODUCTION

Security is essential for any system. The requirement for security must be extremely high. It is one of the important requirements among to provide or control any kind of failures. Several mechanisms are available to provide security for any system, among these mechanisms encryption is one of the major important mechanism. In this process plain text is converted into cipher text which is unreadable from unauthorized users can be said as cryptography encryption process. This cryptography mechanism is essential for publish/subscribe system. Evolution of this publish/subscribe system over the times has proven to be an efficient tool between the publishers and subscribers. Broker networks were used in traditional times between the publishers to subscribers for routing of events. Published events were routed to relevant subscribers without knowing to the publishers to the set of subscribers or vice versa. In this type of systems the access control can be done only by authorized users. The personal details of the subscribers should be hidden from other subscribers and any subscriber should receive events only by subscription to that system. Only by means of subscription any subscriber can get all the relative events. This system has gained high popularity by means of this type of relation from publishers to the subscribers.

The information concerning an event by content based public subscribe systems determines where the message is delivered. Senders send messages without knowing the destination address, with only some message content visible to network. The matched published message content will be declared by receivers. The message is transmitted to all the receivers whose query is matched by the content of the messages. In different distributed applications like stock exchange, publish sensing, traffic control this method is very useful. In order to provide control and confidentiality publish/subscribe systems need to have security. Only authenticated publishers were allowed to distribute events and only authorized subscribers were allowed to receive events in a publish/subscribe system. The contents of the events were kept confidential and subscribers receive the events without informing their subscriptions for the system. Confidentiality is required for both the publication and subscription for the risk of leakage reduction of events in a system. By using public key infrastructure, the publisher and subscriber need to share the secret key for this purpose. This method may not be desirable as it may weaken the decoupling property of models. Here it should be noted that the published content should not expose to the routing infrastructure and the content should be received by customers without subscription leaking to the system. Solving these issues in a security system, content based publish/subscribe system imposes new challenges. New method of authenticating the needed route events to subscribers without knowing the subscriptions results in preventing misusage of data.

Most researches have focused on scalable and expressive pub/sub systems, but less consideration is given to the need of security. Traditional approaches deals with conventional broker networks. This may deals with either security by limited perspicuity using only keyword matching for routing events. This may also depends on semi-trusted broker networks. This method does not provide access control in a scalable manner as it provides key management. Yet, security is an issue to be considered here. To overcome these problems, a new approach is used which helps in mapping of end parties, called pairing-based cryptography mechanism. In this, end parties are called cryptographic groups. In this mechanism Identity Based Encryption Technique (IBE) is used. This new method provides authentication and confidentiality throughout the network. This approach permits users to secure the credentials based on the subscriptions. The secret keys provided will be labeled with credentials to the users. In this approach we adopted Identity-based encryption (IBE) mechanisms 1) the subscriber can decrypt key only if there is a match between credentials with the key and content; and 2) to allow the subscribers to check the validity of the received content. This type of approach helps in providing effective encryption and decryption operations and routing, fine-grained key-management in subscribed attributes.

2. RELATED WORK

Publishers and subscribers are the two entities in the system, though they are computationally bounded but they do not trust each other. All the publishers/subscribers participating in a pub/sub system network were honest and do not deviate from designed protocol. On other hand, in a system authorized publishers only allows valid events. Malicious publishers may pretence authorized publishers and could spam the overlay network with duplicate or fake events. We do not intend to solve the digital copyright problem; therefore, authorized subscribers do not reveal the content of successfully decrypted events to other subscribers.

2.1.PUBLISHER SUBSCRIBER TECHNIQUE

The publishers and subscribers will interact with a key server and provides credentials in it, receives keys which fit the expressed capabilities in the credentials. These keys can be used to encrypt/decrypt or sign the relevant messages in a content based pub/sub system. Then, the credential becomes authorized by the key server. It consists of two parts i.e., 1) binary string- describes the capabilities of a peer in publishing and receiving events, 2) proof of its identity.

2.2. IDENTITY BASED ENCRYPTION IDENTITY (ID)

ID-based public based cryptosystem enables a set of two users to communicate public key certificates securely without exchanging, without using the online third party and without keeping the public key directory as well as a trusted key generation center issues a private key to each user when they joins in an network.

2.3. IDENTITY HANDLING

Identification is needed in distributed information systems; it provides an essential building block for a large number of services and functionalities. In a simple manner, it is used to uniquely denote computers on the internet by IP address in combination with the Domain Name Systems (DNS) as mapping service between symbolic names and IP addresses. Thus the symbolic names of the computers can be referred, whereas, the IP addresses must be used in the routing process. X.500/LDAP which are higher level directories, consistently map their properties to the objects which are uniquely identified by distinguished name(DN) which means their position in that X.500 tree.

2.4. CONTENT BASED PUBLISH/SUBSCRIBE

The generalization of the content based publish/subscribe model is content based networking. To the communication end-points the messages are no longer addressed in the content-based networking. They are instead published to a distributed information space and routed to the ‘interested’ communication end-points by the networking substrate. For realizing binding, naming, and actual content delivery the same substrate is used in most cases.

2.5. SECURE KEY EXCHANGE

In a network of interconnected parties a key exchange (KE) protocol is run, where a instance of protocol is run by activating a party, which is called session. A party can be activated within a session to initiate a session or to respond to an incoming message. The party creates and maintains session state, generates outgoing messages, and by outputting a session-key and erasing the session state it eventually completes the session.

3. PROPOSED WORK

Publishers will be interacted by the subscribers. Publishers are provided by credentials by the subscribers and in turn receive keys which fit the expressed capabilities in the credentials. By using the checksum algorithm the keys are generated and it is distributed to the publisher and subscriber. Within the encryption decryption algorithm the publisher will encrypt the data and embedded the key with data. As the publisher sends the acknowledgement by means of email the subscriber will login. To decrypt the data in the email the subscriber gets the private key. Various data sharing techniques by which the data will get shared by the publisher to the subscriber are:

-NUMERICALS ATTRIBUTE

The data is distributed in the form of spaces in this type of attribute. These spaces are decomposed into sub-spaces, which serves the limited range of enclosure between the publisher and subscriber. These sub-spaces are denoted by 0&1.For instance, an event 0010 is enclosed by the five subspaces 001,0010,00,0 hence the cipher text must be generated according to the events of the subspaces.

-ALPHASTRING ATTRIBUTE

By using the process of prefixing the node using a trie, credentials for alpha-string string operations are performed. A particular string will be given to a root, and using different prefixes the same string is given to the descendents. A single credential assigned to each peer, which is same as its subscription or advertisement.

-RANGE ATTRIBUTE

Subscriber receives separate attribute and keys for each attribute for a range attribute. In the network the particular range is described. In the limited range of subscriber the data is send.

4. CONCLUSION

By increasing the number of subscribers scalability is achieved. Publisher can distribute the private keys to the subscribers once the credentials are submitted using the public-key cryptography. To maintain the authenticity in the system cipher text are labeled with the credentials. To ensure that, a particular subscriber can decrypt an event only if there is a match between the event’s credentials and its private keys to maintain the subscribers confidentiality we have adapted a technique from identity-based encryption.

DOI: 10.18535/ijecs/v5i10.13

5. REFERENCES

[1]Muhammad adnan Tariq, Boris Koldehofe and kurt Rothermel" Securing Broker-less Publish/subscribe Systems Using "*Identity-based Encryption*" IEEE transactions on parallel and distrubuteds systems,vol. 25,no.2, February 2014.

[2]Ms.Meenal Bhoyar,Ranjana Shende "Credential based publisher/subscriber technique using Identity based encryption" ISSN:2277128X vol 4,issue 11, November 2014.

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

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

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

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

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

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

[9] S. Choi, G. Ghinita, and E. Bertino, "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, 2010.

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