IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 98-101
www.iosrjournals.org

The Pairing-Based Cryptography Mechanism to Provide Confidentiality and Authentication for Broker-Less Content-Based Publish/Subscribe System

[1]Vinit Malpure
[1]*Department of Computer technology, Rajarshi Shahu College of Engineering, Pune, India.*

Abstract: *Publish–subscribe system is a messaging system, which consists of different types agents where these agents are classified based on their roles. These agents can be the information producers or information consumers. In Publish subscribe system, publishers publish messages and these messages or the subscribers based on their subscriptions receive events. Event subscribers describe the kind of events that they want to receive with an event subscription, which acts as a filter on the message or event contents. In the content based publish/subscribe system, publishers and subscribers are loosely coupled and they do not trust each other; so providing the basic security mechanisms like authentication and confidentiality in the publish/subscribe system is a difficult task. As publisher does not need to know all subscribers that receive an event and, similarly, subscribers do not know the identity of publishers that send events to them, all the communication between them is handled by the publish/subscribe system. In the existing broker architecture of most messaging systems, they have a messaging server i.e. broker in the middle. Every application is been connected to the central broker and there is no direct communication between applications. All the communication is been done through the broker. As all the messages have to be passing through the broker, it becomes bottleneck of the whole system. In the event of broker failure, it results in the breakdown of the entire system. To address this issue there is an approach is to provide confidentiality and authentication in a broker-less content-based publish/subscribe system by using the pairing-based cryptography mechanisms.*

Keywords: *Content-based, publish/subscribe, peer-to-peer, broker-less, security, identity-based encryption*

I. Introduction

The publisher/subscriber messaging system has been very popular due to its built in capability in decoupling of publishers from subscribers in terms of time, space, and synchronization. Publisher's passes information into the pub/sub system, and subscribers describe the events of interest by means of subscriptions. Published events are forwarded to those subscribers whose subscriptions are matched against the publish event. In the traditional systems, this decoupling is been achieved by the intermediate routing over a broker network. All the communication is been done through the broker. It became a single point of failure in the traditional broker architecture. So to overcome these issues, in current systems, publishers and subscribers are using a broker-less routing environment. Even if there is a failure of publisher or subscriber, it will not bring down the entire system. There are two types of subscription models for specifying the subscriptions: 1) topic-based. 2) Content based. In the topic based model, a single topic is specified and all the events or messages related to that topic are delivered to the related subscribers. The subscribers cannot specify any restrictions on the message contents. Content-based pub/sub is the most expressive subscription model; by using this model subscribers will define the subscriptions that will provide restrictions or constraints on the message content. This expressiveness and asynchronous nature is helpful for large-scale distributed applications like news distribution, stock exchange, environmental monitoring, traffic control, and public sensing. Pub/sub has to support the mechanisms that are used to provide the basic security requirements of such applications like access control and confidentiality. Access control with reference to the pub/sub system means that only authenticated publishers are allowed to publish events in the network and only those events are delivered to authorized subscribers and the content of events should not be disclosed to the routing infrastructure and a subscriber should receive all relevant events without exposing its subscription to the system. Addressing these security issues in the context of content-based pub/sub system produces new challenges. For example, end-to-end authentication by using a public key infrastructure (PKI) will not maintain the loose coupling between publishers and subscribers. In the PKI, publishers must organize the public keys of all interested subscribers to encrypt events. Subscribers must have the knowledge of the public keys of all related publishers to verify the authenticity of the received events. It will not maintain the decoupling between publisher and subscriber.

Therefore, new mechanisms are required to route encrypted events or messages to the subscribers without knowing their subscriptions allow subscribers and publishers authenticate each other without knowing each other. In the past, most research that has been done focused only on providing expressive and scalable pub/sub systems, but little attention was given for the need of security. All the existing approaches for secure publisher/subscriber systems mainly depend on the presence of a traditional broker network. So to provide a better security in the broker-less

Publisher/subscriber systems, a new approach is proposed that will provide authentication and confidentiality in a broker-less pub/sub system. In this approach, all subscribers are allowed to maintain credentials according to their subscriptions. Private keys that are assigned to the subscribers are also labeled with the credentials. A publisher maps each encrypted event with a set of credentials. Here, identity-based encryption (IBE) mechanisms are used to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and the key; and also to allow subscribers to verify the authenticity of received events.

II. Literature Survey

Here we have considered some of the related previous research work about the traditional broker oriented architectures. These work mostly focused on the scalability and expressiveness of the system and little attention is given to the security. The work is been presented as follows:

J. Bethencourt, A. Sahai, and B. Waters[2], they have presented in their work a system for the complex access control strategy on encrypted data that is called as Ciphertext-Policy Attribute-Based Encryption. By using this technique encrypted data is being kept secret even if the storage server is is not secured. In the previous research work Attribute-Based Encryption systems used attributes to describe the encrypted data and specify the policies into user's keys, while in this system attributes are used to describe a user's credentials, and a party that is encrypting the data determines the policy for who can decrypt the encrypted data.S. Choi, G. Ghinita, and E. Bertino[3], have presented a system in which every user submits a list of subscriptions to a broker, and after that broker routes data items from publishers to the subscribers. When a broker receives a notification from the publisher that contains a value from apublisher, it will forward that only to the subscribers whose subscriptions match the value in the publication. However, in many applications, the data that published is confidential, and its contents must not be revealed to the brokers. In addition, a user's subscription may contain sensitive information that must be protected from the brokers. Therefore, there is a difficult challenge arises that is how to route publisher data to the appropriate subscribers without the intermediate brokers learning the plain text values of the notifications and subscriptions.M. Ion, G. Russello, and B. Crispo[4], have presented a pub/sub system that are loosely coupled where applications interact indirectly and asynchronously. Publisher generates events that are sent to interested subscribers through a network of brokers. Subscriber specifies its interest by specifying filters that is been used by the brokers for the routing of events. So, it is desirable that any mechanism that is used for protecting the confidentiality of both the events and the filters should not require the publishers and subscribers to share their secret keys. In addition, such a mechanism should not restrict the expressiveness of filters and it should allow the broker to perform event filtering to route the events to the interested subscribers. Existing solutions do not fully address these issues, so here they propose a mechanism that will address all these issues.M. Srivatsa, L. Liu, and A. Iyengar[5], have presented a framework called as Event Guard for the construction of secure wide area pub-sub systems. The purpose of the Event Guard mechanisms is to provide the security guarantees at the same time maintaining the system's over all simplicity, scalability and performance. Event Guard architecture consists of three main components. First one is a suite of security guards that is plugged-into a content based pub-sub system, second component is a scalable key management algorithm that will be used to enforce access control on subscribers, and the third component is a pub sub network design that is capable of recovering quickly from the difficult situations.

A. Shikfa, M. O¨nen, and R. Molva[6], in their work they have suggested a set of security mechanisms that will allow for privacy-preserving forwarding of the encrypted contents based on subscribers interests. The main advantages of this scheme are that it ensures both data confidentiality with respect to the publishers and the privacy of the subscribers with respect to their interests in a model where the publishers, the subscribers and the intermediate nodes i.e. brokers in charge of data forwarding do not trust each other. The scheme depends on a multi-layer encryption that allows intermediate nodes to manage forwarding tables and to perform content forwarding using encrypted content and based on encrypted subscriber messages without accessing the plaintext of the data. This scheme also avoids key sharing among the end-users and targets an enhanced CBPS model where brokers can also be subscribers at the same time. H.-A. Jacobsen, G. Li, A.K.Y. Cheung, V. Muthusamy,

R.S. Kazemzadeh, B. Maniymaran, [7], in their work have conducted a detailed overview of the "PADRES" which is a content-based publish/subscribe system. PADRES has a capability that is helpful in correlating events, accessing data that is produced in the past and that will be produced in the future, balance the traffic load among brokers, and handle network failures. It can also filter, aggregate, correlate and project any combination of historic and future data. They have also presented the several applications in detail that can benefit from the content-based nature of the publish/subscribe system and take advantage of its scalability and robustness features. When we are developing large-scale distributed systems that are going to be used on the Internet, it should have a proper middleware support, which handles the communication needs of those application clients in a scalable and efficient way, and without compromising traditional middleware features. P. Pietzuch[8], in his work have described "Hermes", that is a distributed, event-based middleware that provides peer-to-peer communication techniques for scalable and robust event transmission. Hermes uses peer-to-peer techniques for managing its network of event brokers and also adding fault-tolerance to its event transmission algorithms in the pub/sub systems. Y. Yu, B. Yang, Y. Sun, and S. l. Zhu [9], in their work have proposed the first identity based sign encryption scheme. However, they show that their scheme still has some security weaknesses and further, propose a corrected version of the scheme and prove its security under the existing security model for identity-based sign encryption.

III. Proposed System

In our proposed system to provide the confidentiality and authentication in the broker-less content-based publisher/subscriber system, we will be using the identity-based encryption. In the identity-based encryption, any valid string that uniquely identifies a user can be the public key of that particular user. The proposed system consists of publishers, subscribers and a key server, which maintains a single pair of public and private master keys. The master public key is known to every user in the system and it is used by the sender i.e. publisher to encrypt the messagesand send them to a user with any identity. To decrypt that message successfully, receiver i.e. subscriber needs to get a private key for its identity from a key server. Our proposed system allow subscribers to have credentials according to their subscriptions, private keys that are assigned to the subscribers are also labeled with a credentials. Identity based encryption ensures that a subscriber can decrypt an event only if there is a match between the credentials associated with the event and the key to avoid the unauthorized publications. It also ensures that only the authorized publishers should be able to publish events in the system and similarly subscribers should only receive those events to which they have subscribed. To provide confidentiality, it ensures that the events are visible to only authorized subscribers and are protected from unauthorized modifications.

A. Phase 1: Publishing Events

In this phase, publisher will publish the events in the system. Publisher is authenticated by using the advertisements in which a publisher tells in advance the set of events which it intends to publish. This notification is forwarded to all the subscribers in the system and the subscribers those are interested in that particular event will send respond to the publisher.

B. Phase 2: Key Generation

Before publishing an event, a publisher will contact the key server along with the credentials that is been assigned by the key server for each attribute that are present in its advertisement. If the publisher is been authenticated to publish events according to its credentials, then the key server will generate separate private keys for each credential. In the same way, to receive events that are matching to its subscription, a subscriber should also contact the key server and receive the private keys for the credentials that are associated with each attribute in the subscription.

C. Phase 3: Identity Based Encryption

In this phase, publishers and subscribers contact the key server. They provide credentials to the key server and receive keys, which fit the capabilities in the credentials. After that, those keys are used to encrypt, decrypt, and sign the relevant messages in the content-based pub/sub system. The keys that is been assigned to the publishers and the subscribers, and the cipher texts, are labeled with the credentials. Identity-based encryption ensures that a particular key can decrypt a particular cipher text only if there is a match between the credentials of the cipher text and the key.

IV. Conclusions

Confidentiality and authentication in the content-based publisher/subscriber systems is not easy to achieve due to the loose coupling between the publisher and the subscribers. Therefore, we have proposed a new approach to provide authentication and confidentiality in a broker-less content-based pub/sub system. This approach is highly scalable in number of subscribers and publishers in the system and the number of keys that is been maintained by them. It will assign credentials to publishers and subscribers according to their subscriptions and advertisements. Private keys assigned to publishers and subscribers, and the cipher texts assigned with the credentials. So that the subscribers can only decrypt an event when there is a match between the credentials of the cipher text and the key.

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 distri buted systems, vol. 25, no. 2, Februar y 2014.
[2]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.
[3]. 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.
[4]. M. Ion, G. Russello, and B. Crispo, "Supporting Publication and Subscription Confidentiality in Pub/Sub Networks," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), 2010.
[5]. M. Srivatsa, L. Liu, and A. Iyengar, "EventGuard: A System Architecture for Securing Publish-Subscribe Networks," ACM Trans. Computer Systems, vol. 29, article 10, 2011.
[6]. A. Shikfa, M. O¨ nen, and R. Molva, "Privacy-Preserving Content- Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.
[7]. H.-A . J acobsen, A.K.Y. Cheung, G . Li, B. Ma niymaran, V . Muthusa my, and R.S. Ka zemzadeh, "The PADRES Publi sh/ Subscribe System," Principl es and Applications of Distributed Event-Based Systems. IGI Global, 2010.
[8]. P. Pietzuch, "Hermes: A Scalable Event-Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 2004.
[9]. Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based Signcryption Scheme without Random Oracles," Computer Standards & Interfaces, vol. 31, pp. 56-62, 2009.
[10]. Handore Jayshree Shrikant et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7532-7535.