Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P) Vol.3 No.2, 2014, pp.56-59

DOI: https://doi.org/10.51983/ajes-2014.3.2.1921

A Review of Secure Pub Sub System

Padmavati N Kshirsagar[1], S Pratap singh[2] and Milindkumar V. Sarode[3]
[1]PG Student, Institute of Knowledge College of Engineering, Pimple Jagtap, Pune, Maharastra, India
[2]Asst.Prof. Institute of Knowledge College of engineering, Pune. Maharastra, India
[3]Jawaharalal Darda Institute of engineering & Technology,yavatmal, Maharastra
Email: padmavatisarode8@gmail.com, pratap.singh.s@gmail.com
(Received 5 October 2014; Revised 17 October 2014; Accepted 3 November 2014; Available online 8 November 2014)

***Abstract - In content-based publish subscribe system authentication and confidentiality are most challenging* security issues. This paper presents a novel way to provide confidentiality and authentications in a broker-less content-based publish subscribe system. The authentication of publishers and subscribers is done using pairing based cryptography. Confidentiality of events is also ensured, by adapting the pairing-based cryptography mechanisms. This paper contributes; secure communication between publisher and subscribers. Publisher use public key to encrypt message, publisher send that message along with its unique identity. To successfully decrypt the message; a receiver needs to obtain a private key for its identity from the key server. The overall approach provides fine-grained key management. Published events are routed to their corresponding subscribers. The evaluation of this project provides security respect to 1) authentication and confidentiality of event dissemination. 2) The overall approach provides fine-grained key management. Published events are routed to their relevant subscribers. The evaluation of this project provides security respect to throughput of the proposed cryptographic primitives.**
Keywords: **Content-based, publish subscribe, peer to peer, security, identity-based encryption**

I.INTRODUCTION

Recently in [1] new method is presented to provide authentication and confidentiality in broker-less publish subscribe system. These approaches allow subscribers to maintain credentials according to their subscriptions. Private keys assigned to the subscribers are labeled with the credentials. A publisher associates each encrypted event with a set of credentials. Authors adapted identity-based encryption (IBE) mechanisms 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 the key; and 2) to allow subscribers to verify the authenticity of received events. In this approach, publishers and subscribers interact with a key server. They provide credentials to the key server and in turn receive keys which fit the expressed capabilities in the credentials. But reliability of key server is a research problem whether it works under any kinds of network circumstances. Also as the number of subscribers or publishers increases, the response time of key server increases and this allows hackers to leak important information.

II.SCOPE FOR THE STUDY

An increasingly large number of Internet applications require information dissemination across different organizational boundaries, heterogeneous platforms, and a large, dynamic population of publishers and subscribers. A publish-subscribe overlay service is a wide-area communication infrastructure that enables data dissemination across potentially unlimited numbers of publishers and subscribers, scattered geographically across the wired and wireless Internet. In such an environment, publishers publish information in the form of event notifications and subscribers have the ability to express their interests in an event or a pattern of events by sending subscriptions to the pub-sub overlay network. The pub-sub overlay network uses content-based routing [1].

Schemes to dynamically match each publication to all the active subscriptions, and notifies the subscribers of any publication that matches their registered interest, ensuring that subscribers only receive notifications of those events that match their interests.

The routing of events from publishers to the relevant subscriber's content-based data model is used. Consider publisher subscriber in a setting where there exists no dedicated broker infrastructure. Publishers and subscribers contribute as peers to the maintenance of a self-organizing overlay structure. To authenticate publishers, we use the concept of advertisements in which a publisher announces beforehand the set of events which it intends to publish.

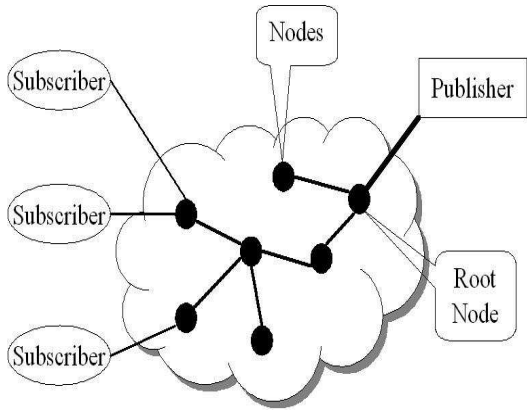

Fig. 1 Content based publisher subscriber system

As above figure:1 shows content based publisher subscriber system, publisher and subscribers interact with a key server that is root node[4]. They provide credentials to the key server and in turn receive keys which fit the expressed capabilities in the credentials. Subsequently, those keys can be used to encrypt, decrypt, and sign relevant messages in the content based publisher

subscriber system, i.e., the credential becomes authorized by the key server. A credential consists of two parts:

1. A binary string which describes the capability of a peer in publishing and receiving events, and
2. A proof of its identity.

The latter is used for authentication against the key server and verification whether the capabilities match the identity of the peer [1]. While this can happen in a variety of ways, for example, relying on challenge response, hardware support, and so on, we pay attention mainly at expressing the capabilities of a credential, i.e., how subscribers and publishers can create a credential. This process needs to account for the many possibilities to partition the set of events expressed by an advertisement or subscription and exploits overlaps in subscriptions and publications.

The term credential only for referring to the capability string of a credential. The keys assigned to publishers and subscribers, and the cipher texts, are labelled with credentials. In particular, the 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. Publishers and subscribers maintain separate private keys for each authorized credential. The public keys are generated by a string concatenation of a credential, an epoch for key revocation, a symbol SUB; PUB distinguishing publishers from subscribers. The public keys can be easily generated by any peer without contacting the key server or other peers in the system. Similarly, encryption of events and their verification using public keys do not require any interaction.

Due to the loose coupling between publishers and subscribers, a publisher does not know the set of relevant subscribers in the system. Therefore, a published event is encrypted with the public key of all possible credentials, which authorizes a subscriber to successfully decrypt the event. The overlay network is maintained according to the containment relationship between the subscriptions. Subscribers with coarser subscriptions are placed near the root and forward events to the subscribers with less coarser subscriptions. To maintain such a topology, each subscriber should know the subscription of its parent and child peers. When a new subscriber arrives, it sends the connection request (CR) along with its subscription to a random peer in the overlay network [1]. The connection request is forwarded by possibly many peers in the overlay network before it reaches the right peer to connect. Each forwarding peer matches the subscription in the request with the subscription of its parent and child peers to decide the forwarding direction. Maintaining a relationship between subscriptions clearly contradicts subscription confidentiality. Therefore, we show the approach to ensure a weaker notion of subscription confidentiality

III. SYSTEM OVERVIEW

It includes two entities in the system: publishers and subscribers. Both the entities are computationally bounded and do not trust each other. Moreover, all the peers (publishers or subscribers) participating in the publishers or subscribers overlay network are honest and do not deviate from the designed protocol. Likewise, authorized publishers only disseminate valid events in the system. However, malicious publishers may masquerade the authorized publishers and spam the overlay network with fake and duplicate events Authorized subscribers do not reveal the content of successfully decrypted events to other subscribers.

A. Goal

1. Privacy, confidentiality

This paper focus on the problem of subscriber and publisher privacy. As pointed out in privacy is expected to be a significant concern for acceptance of pervasive environments like CBPS systems [6]. Privacy from the subscriber point of view refers to the fact that subscribers do not want any other nodes, be it brokers, publishers, other subscribers or even nodes outside the CBPS infrastructure, to spy on their interests and be able to profile them in any way. There are several ways of ensuring privacy; one of the classical approaches is to guarantee data confidentiality with cryptographic primitives.

Two confidentiality issues, defined as follows:

2. Publication confidentiality

Can publishers control which subscribers may receive particular publications? Subscription confidentiality is obviously a must to preserve subscriber's privacy but it is not sufficient: we also need to take information confidentiality into consideration; otherwise adversaries could infer the subscription filter by analyzing the information which matches it. From a publisher's perspective privacy may not be as crucial. Publishers publish some content which is meant to be received by some nodes, hence they often do not require a full-fledged privacy but they require publication confidentiality that we mentioned earlier. Publication confidentiality is an access control rather than privacy issue: publishers want to be able to authorize certain subscribers to be able to access the content they publish while preventing unauthorized ones from learning valuable information about it. Since publication confidentiality is not necessary to ensure privacy, we do not consider it in the sequel of the paper, especially those orthogonal solutions can be developed to ensure it [6].

3. Subscription confidentiality

This is the dual problem of information confidentiality. Here, subscribers do not want to reveal

their interests either to brokers or publishers or other subscribers but they still want to receive the content they are interested in and only this one. So the challenge in this case is to match content with an encrypted subscription without disclosing the subscription filter. In the stock quotes example, this requirement corresponds to the ability to find which events match which filter without accessing it in clear; it is a problem of secure function evaluation, where a broker has to evaluate a hidden function (the filter which was encrypted by the subscriber) [6].In summary, information and subscriber confidentiality in CBPS call for new mechanisms to achieve secure routing of encrypted data with the capability of matching encrypted event notifications against encrypted subscription filters in order to ensure end-users privacy.

B. Existing system

In the past, most research has focused only on providing expressive and scalable publish subscribe systems, but little attention has been paid for the need of security. Existing approaches toward secure publish subscribe systems mostly rely on the presence of a traditional broker network. These either address security under restricted expressiveness, for example, by using only keyword matching for routing events or rely on a network of (semi-)trusted brokers. Furthermore, existing approaches use coarse-grain epoch based key management and cannot provide fine-grain access control in a scalable manner. Nevertheless, security in broker-less publish subscribe systems, where the subscribers are clustered according to their subscriptions, has not been discussed yet in the literature.

C. Identity based encryption

While a traditional PKI infrastructure requires maintaining for each publisher or subscriber a private/public key pair which has to be known between communicating entities to encrypt and decrypt messages, identity-based encryption [10] provides a promising alternative to reduce the amount of keys to be managed. In identity-based encryption, any valid string which uniquely identifies a user can be the public key of the user. A key server maintains a single pair of public and private master keys. The master public key can be used by the sender to encrypt and send the messages to a user with any identity, for example, an e-mail address. To successfully decrypt the message, a receiver needs to obtain a private key for its identity from the key server. Figure. 2 shows the basic idea of using identity-based encryption. We want to stress here that although identity-based encryption at the first glance appears like a highly centralized solution, its properties are ideal for highly distributed applications. A sender needs to know only a single master public key to communicate with any identity. Similarly, a receiver only obtains private keys for own identities. Furthermore, an instance of central key server can be easily replicated within the network. Finally, a key server maintains only a single pair of master keys and, therefore, can be realized as a smart card, provided to each participant of the system. Although identity-based encryption has been proposed some time ago, only recently pairing-based cryptography (PBC) has laid the foundation of practical implementation of identity-based encryption. Pairing-based cryptography establishes a mapping between two cryptographic groups by means of bilinear maps. This allows the reduction of one problem in one group to a different usually easier problem in another group. We utilize bilinear maps for establishing the basic security mechanisms in the pub/sub system and, therefore, introduce here the main properties [1].

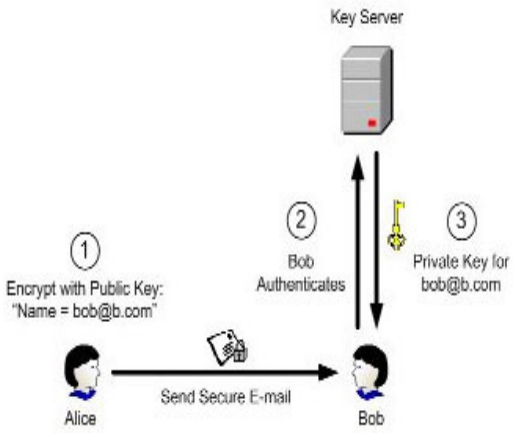

Fig.2 Identity Based Encryption

Step 1:

Alice encrypts the email using Bob's e-mail address, "bob@b.com", as the public key.

Step 2:

When Bob receives the message, he contacts the key server. The key server contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements.

Step 3:

After authenticating Bob, the key server then returns his private key, with which Bob can decrypt the message. This private key can be used to decrypt all future messages received by Bob.

Note that private keys need to be generated only once, upon initial receipt of an encrypted message. All subsequent communications corresponding to the same public key can be decrypted using the same private key, even if the user is offline. Also, because the public key is generated using only Bob's email address, Bob does not need to have downloaded any software before Alice can send him a secure message[11].

The mathematical foundation of Identity based encryption

The mathematical foundation of IBE is a special type of function called a "bilinear map." A bilinear map is a pairing that has the property:

Pair*(aoX, boY) = Pair(boX, aoY)*

The operator "**o**" is multiplication of a point on an elliptic curve by integers. While multiplication itself (e.g., calculating aoX) is easy, the inverse operation (finding a

given X and aoX) is practically impossible. Two examples of bilinear maps are the Weil Pairing and the Tate Pairing. The IBE algorithm consists of four operations:

1. Setup, which initializes a key server
2. Encrypt, which encrypts a message for a given user
3. Key Generation, which generates a private key for a given user
4. Decrypt, which given a private key, decrypts a message

IV. SECURE OVERLAY MAINTENANCE PROTOCOL

The secure overlay maintenance protocol is based on the idea that in the tree, subscribers are always connected according to the containment relationship between their credential [2]. A new subscriber s generates a random key SW and encrypts it with the public keys for all credentials that cover its own credential, for example, a subscriber with credential will generate cipher texts by applying the public keys. The generated cipher texts are added to a connection request (CR) and the request is forwarded to a random peer in the tree. A connection is established if the peer can decrypt any of the cipher text using its private keys.

V.APPLICATION

A. Police infrastructure

A number of county-level police domains need support for intra- and inter-domain messages. Incident reports may be sent within and between domains for real-time response and may also be stored as part of an audit or record-keeping process. Databases for court records and the licensing of drivers of vehicles are accessible from all domains [5].

B. Healthcare systems

The communication infrastructure of a national health service is shared by many independent hospitals, clinics, primary-care practices, etc. Caring for a patient in their home involves carers from many domains. This includes sharing information with various care providers making aspects of patient information persistent in centralised health record services and auditing data owns, to monitor compliance with procedures, and to investigate anomalies [5].

C.Environmental monitoring

Traffic, noise, pollution, and weather conditions are monitored in a city to provide real-time information for citizens. All data is recorded for historical analysis to aid prediction and for use by Local Government for planning purposes [5].

VI.CONCLUSION

Broker Less publisher subscriber system is secure system. It uses Identity Based Encryption to secure publisher subscriber system. This paper implements IBE to improve system reliability, scalability and security. Secure overlay maintenance protocol implements tree structure in which subscriber always connected according to the relationship between their credential. A dynamic server will give security to server .Dynamic Backup Key Server of main key sever based on number of current subscribers. When System Exceeds threshold of accessing number of subscriber, server will require a backup. This not only achieves system reliability but also improves the time requirement and security. Paper will improve system reliability, security with time performances.

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 Distributed Systems, VOL. 25, NO. 2, FEBRUARY 2014

[2] 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

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

[4] 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.

[5] 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.

[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] M.A. Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel, “Meeting Subscriber-Defined QoS Constraints in Publish/Subscribe Systems,” Concurrency and Computation: Practice and Experience, vol. 23, pp. 2140-2153, 2011.

[8] Ahmet Burak and Bharat Bhargava,” SORT: A Self-Organizing Trust Model for Peer-to-Peer Systems”, IEEE transactions on dependable and secure computing, vol. 10, no1, Jan/Feb 2013.

[9] 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

[10] D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology, 2001.

[11] http://www.voltage.com/technology/identity-based-encryption