© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Privacy Enhancing Identity Based Publisher Subscriber System

K.J. Sinduja, C. Kayalvizhi
Department of Computer Science, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

The provisioning of basic security mechanisms such as authentication and confidentiality is highly challenging in a content based publish/subscribe system. Authentication of publishers and subscribers is difficult to achieve due to the loose coupling of publishers and subscribers. Confidentiality of events and subscriptions conflicts with content-based routing. Hence, new mechanisms are needed to route encrypted events to subscribers without knowing their subscriptions and to allow subscribers and publishers authenticate each other without knowing each other. Our approach allows subscribers to maintain credentials according to their subscriptions. This project is adapted by the pairing-based cryptography mechanisms and symmetric key generation. In overall approach, provides fine-grained key management and the cost for encryption, decryption, and routing are in the order of subscribed attributes. Finally, the evaluations show that providing security is affordable.

Keywords: content based, publisher/subscriber, broker-less, security, identity-based encryption, paired based cryptography, symmetric key

I. INTRODUCTION

The publish/subscribe (pub/sub) communication paradigm has gained high popularity because of its inherent decoupling of publishers from subscribers in terms of time, space, and synchronization. Publishers inject information into the pub/sub system, and subscribers specify the events of interest by means of subscriptions. Published events are routed to their relevant subscribers, without the publishers knowing the relevant set of subscribers, or vice versa. This decoupling is traditionally ensured by intermediate routing over a broker network. In more recent systems, publishers and subscribers organize themselves in a broker-less routing infrastructure, forming an event forwarding overlay. Content-based pub/sub 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 fulfil the basic security demands of these applications such as access control and confidentiality. Access control in the context of pub/sub system means that only authenticated publishers are allowed to disseminate events in the network and only those events are delivered to authorized subscribers. Moreover, the content of events should not be exposed to the routing infrastructure and a subscriber should receive all relevant events without revealing its subscription to the system. Solving these security issues in a content-based pub/sub system imposes new challenges. For instance, end-to-end authentication using a public key infrastructure (PKI) conflicts with the loose coupling between publishers and subscribers, a key requirement for building scalable pub/sub systems. For PKI, publishers must maintain the public keys of all interested subscribers to encrypt events. Subscribers must know the public keys of all relevant publishers to verify the authenticity of the received events. Furthermore, traditional mechanisms to provide confidentiality by encrypting the whole event message conflict with the content-based routing paradigm. Hence, new mechanisms are needed to route encrypted events to subscribers without knowing their subscriptions and to allow subscribers and publishers authenticate each other without knowing each other.

II. METHODS AND MATERIAL

End-to-end authentication using a public key infrastructure (PKI) conflicts with the loose coupling between publishers and subscribers, a key requirement for building scalable pub/sub systems. Mechanisms to provide confidentiality by encrypting the whole event message conflict with the content-based routing paradigm.

Techniques

- ✓ Public key infrastructure (PKI)
- ✓ Triple Data Encryption (TDEA).
- ✓ A PKI is an arrangement that binds with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The third party validation authority (VA) can provide this information on behalf of CA. The binding is established through the registration and issuance process, which, depending on the assurance level of the binding, may be carried out by software at a CA or under human supervision. The PKI role that assures this binding is called the registration authority (RA), which ensures that the public key is bound to the individual to whom it is assigned in a way that ensures non reputation.
- ✓ Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) Symmetric-key algorithm, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Weak subscription confidentiality and loose coupling of publishers and subscribers are the drawbacks. Authentication of publishers and subscribers is difficult to achieve due to the loose coupling of publishers and subscribers.

The authentication of publishers and subscribers as well as confidentiality of events is ensured, by adapting the pairing-based cryptography mechanisms, to the needs of a publish/subscribe system. Publishers inject information into the pub/sub system, and subscribers specify the events of interest by means of subscriptions. Published events are routed to their relevant subscribers, without the publishers knowing the relevant set of subscribers, or vice versa. The content of events should not be exposed to the routing infrastructure and a subscriber should receive all relevant events without revealing its subscription to the system. Publishers must maintain the public keys of all interested subscribers to encrypt events. Subscribers must know the public keys of all relevant publishers to verify the authenticity of the received events.

Proposed system

This shows new mechanisms are route encrypted events to subscribers without knowing their subscriptions and to allow subscribers and publishers authenticate each other without knowing each other. For security, here the subscribers are clustered according to their subscriptions.

Techniques

- ✓ Pairing-based cryptography is the use of a pairing between elements of two cryptographic groups to a third group to construct cryptographic systems. If the same group is used for the first two groups, the pairing is called symmetric and is a mapping from two elements of one group to an element from a second group. In this way, pairings can be used to reduce a hard problem in one group to a different, usually easier problem in another group.
- ✓ Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

The main contributions of this paper are the following:

- ✓ Identity based encryption and Scalable in terms of number of subscribers and publishers are the advantages.
- ✓ The authentication of publishers and subscribers as well as confidentiality of events is ensured, by adapting the pairing-based cryptography mechanisms, to the needs of a publish/subscribe system. Nevertheless, security in broker-less

pub/sub systems, where the subscribers are clustered according to their subscriptions.

- ✓ A publisher associates each encrypted event with a set of credentials.
- ✓ We adapted identity-based encryption (IBE) mechanisms 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.
- ✓ Private keys assigned to the subscribers are labeled with the credentials.
- ✓ A publisher associates each encrypted event with a set of credentials.

Content based publisher/Subscriber

- ✓ We consider pub/sub 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

Implementation

We implement this project to enhance the privacy between Publisher and Subscribers. This is implemented by the broker-less concept and key concepts. Symmetric keys and the pairing based cryptographic techniques were mainly used to provide the secure data among publishers/subscriber. The Database used is MySQL which used the information storage about the pub/sub. At first the registration process is provided for both the publishers and subscribers. Both by using their Id's they are keep login. Then the publisher will be publisher their information in the server. To eliminate the memory occupying space and to find the subscriber interest as well as to provide the privacy this concept is used. Subscribers can subscriber their topics of their interest by using the subscriber button. Subscribed topics can be viewed by the key request given to the publisher. The response will be provided from the publisher then the information to be viewed to the corresponding subscriber. This is done by clustering the subscribers in order to provide the matching key i.e. symmetric key concepts.

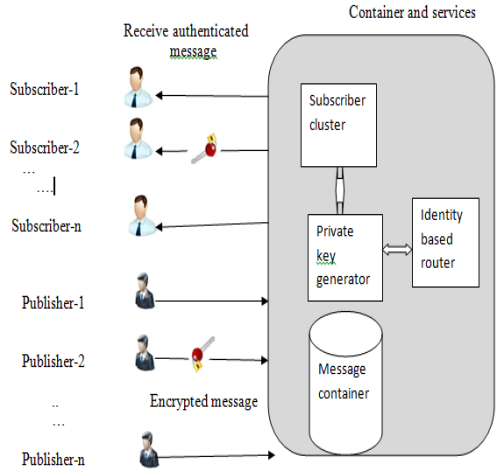


Figure 1: Architecture Diagram

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 [6] 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. 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.

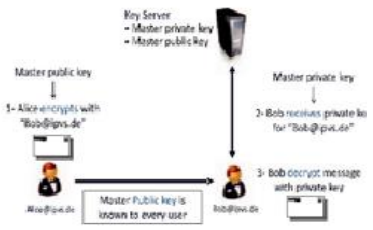


Figure 2: Identity-Based Encryption

Publisher/subscriber authentication and event confidentiality

The security methods describe in this section are built upon ciphertext-policy attribute-based encryption (in short CP-ABE) scheme proposed by Bethencourt et al. In particular, our modifications 1) allow publishers to sign and encrypt events at the same time by using the idea of the identity-based encryption proposed by Yu et al. 2) enable efficient routing of encrypted events (from publishers to subscribers) by using the idea of searchable encryption proposed by Boneh et al., and 3) allow subscribers to verify the signatures associated with all the attributes (of an event) simultaneously.

These can be done by the

- ✓ Security Parameter And Initialization
- ✓ Key Generation For The Publisher Subscriber
- ✓ Publishing Events
- ✓ Receiving Events

Subscription confidentiality

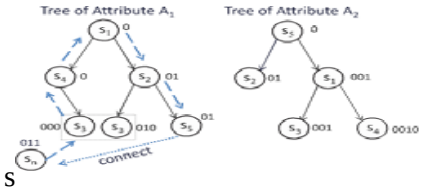
In this section, we address to achieve subscription confidentiality in a broker-less pub/sub system.

Publish/Subscribe Overlay

The pub/sub overlay is a virtual forest of logical trees, where each tree is associated with an attribute. A subscriber joins the trees corresponding to the attributes of its subscription. Similarly, a publisher sends an event on all the trees associated with the attributes in the event. Within each attribute tree, subscribers are connected according to the containment relationship between their credentials associated with the attribute. The subscribers with coarser credentials (e.g., the ones mapped to coarser subspaces in case of numeric attributes) are placed near the root of the tree and forward events to the subscribers with finer credentials. A subscriber with more than one credentials can be handled by running multiple virtual peers on a single physical node, each virtual peer maintaining its own set of tree links, as shown. To connect to an attribute tree, a newly arriving subscriber sn sends the connection request along with its credential to a random peer sr in the tree. The peer sr compares the request credential with its own; if the peer's credential covers the request credential and the peer can accommodate more children, it accepts the connection. Otherwise, the connection request is forwarded to all the children with covering credentials and the parent peer with the exception of the peer from which it was received.

Weak Subscription Confidentiality

It is infeasible to provide strong subscription confidentiality in a broker-less pub/sub system because the maintenance of the overlay topology requires each peer to know the subscription of its parent as well as its children. To address this issue, a weaker notion of subscription confidentiality is required.



s

1. The credential of s1 is either coarser or equal to the credentials of s2.
2. The credential of s1 is either finer or equal to the credentials of s2.
3. The credentials of s1 and s2 are not in any containment relationship.

Applications: Publish-Subscribe Notification for Web services

The Event-driven, or Notification-based, interaction pattern is a commonly used pattern for inter-object communications. Examples exist in many domains, for example in publish/subscribe systems provided by Message Oriented Middleware vendors, or in system and device management domains. This notification pattern is increasingly being used in a Web services context. This document introduces the notification pattern, sets the goals and requirements for the WS-Notification family of specifications and describes each of the specifications that make up this family. It also defines a set of terms and concepts used in the specifications, provide some examples, and include a discussion of security considerations.

- ✓ Message sharing system in police department
- ✓ Health care message services

This schema can be implemented in any concepts of the publisher and subscriber system.

III. RESULTS AND DISCUSSION

Cryptographic Primitives

All of our measurements were made on a 2-GHz Intel Centrino Duo with 2-GB RAM, running Ubuntu 9. This table shows the computation times for Pub/sub. All reporting values are averaged over 1,000 measurements. In our system, pairing-based encryption is used to encrypt a random key SK, which is later used to decrypt the actual event using symmetric encryption.

Table 1: Computation Times for Publishers and Subscribers

Operation	Time(msec)
Encryption(E)	$6.9 + d \times 5.4$
Signature(S)	$d \times 6.32$
Decryption(D)	$6.2 + d \times 6.1$

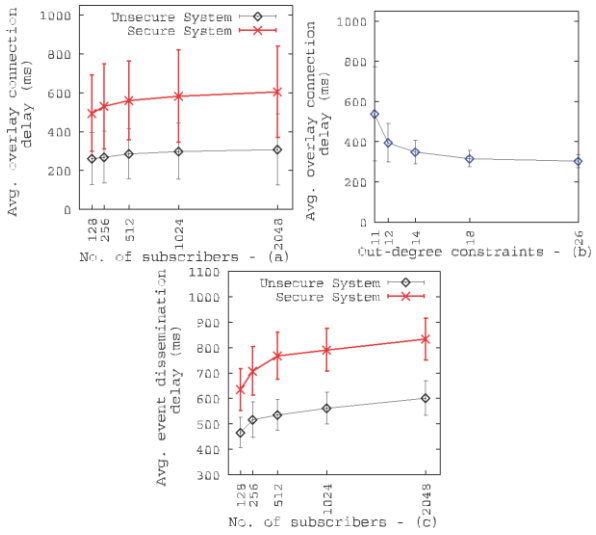


Figure 3: The Graph of Average overlay/event vs. number of subscribers

IV. CONCLUSION

In this paper, we evaluate performance and scalability of the proposed pub/sub system only with respect to the security mechanisms and omit other aspects. , we measure the average delay experienced by each subscriber to connect to a suitable position in an attribute tree. Delay is measured from the time a subscriber sends connection request message to a random peer in the tree till the time the connection is actually established. The evaluations are performed only for a single attribute tree. These papers conclude that the Private keys assigned to publishers and subscribers, and the cipher texts are labelled with credentials. 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 to allow subscribers to verify the authenticity of received events.

V. REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

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