International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Review: Securing Broker-Less Public/Subscribe Systems Using Identity-Based Encryption

Minakshi B. Shingan[1], Sanchika A. Bajpai[2]

[1]JSPM's Bhivrabai Sawant Institute of Technology and Research, Wagholi, Pune

[2] Professor, JSPM's Bhivrabai Sawant Institute of Technology and Research, Wagholi, Pune

Abstract: ***Publish/subscribe systems has evolved as an striking communication model for building Internet-wide distributed systems by decoupling senders of messages from receivers. So far most of the research on publish/subscribe has focused on other areas such as efficient event routing, event filtering etc. Very trivial research has been published regarding securing publish/subscribe systems. In content based public subscribe systems authentication and confidentiality are basic security issues. In this paper we presents a new approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. By using pairing based cryptography mechanism, authentication and confidentiality for public subscribe event is ensured. Additionally, an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality .To enable efficient routing of encrypted events searchable encryption is provided. To support weak subscription confidentiality, multi credential routing a new event distribution method is provided. Also comprehensive analyses of different attacks on subscription confidentiality are provided. The overall methodology provides Key management for identity based encryption, cost for encryption decryption and routing based on subscription of attributes.***

Keywords: Publish/subscribe, Identity-based encryption

1. Introduction

The publish/subscribe model evolved from last few years as an efficient tool for distributed applications in which information has to be dispersed from event producers to event consumers i.e. from publishers to subscribers. Users receive certain types of events by applying filters on event contents called subscription. For each new event published the Pub/sub system checks all events beside all present subscriptions and deliver it to all users for their matched subscription. Traditionally they were using broker networks for routing of events from publishers to subscribers. In more recent systems, broker-less routing infrastructure is used by making event forwarding overlay. [1]

In content based public subscribe systems information concerning an event (i.e. content of message) determines where the message is delivered. Senders send messages without knowing the destination address, with only some message content visible to network. Receivers declare a query which is matched against published message content. Then the message is transmitted to all receivers whose query is matched by the content of the message. This method is useful for different distributed applications like stock exchange, traffic control, publish sensing. Pub/Sub systems need to provide security to these applications such access control and confidentiality.

In Pubs/sub system access control means only authenticated publishers are allowed to distribute events and only authorized subscribers are allowed to receive that events .Contents of events are kept as confidential and subscribers receive that events without informing their subscriptions for the system. Both publication and subscription confidentiality is required to reduce risk of leakage of events in systems. For that purpose publisher and subscriber need to share secret key, by using public key infrastructure, which is not desirable because it would weaken the decoupling property of the model. In PKI, publishers maintain public keys of all subscribers for encryption of events. Similarly, subscribers must know the public keys of publishers to check authenticity of received events. Traditional methods of encrypting all message violates the approach of content based system. Hence new method is needed to route events to subscribers without knowing their subscriptions and authenticating them.

Public subscribe systems are provided by most researchers but less consideration is given on security of public subscribe systems. Existing approach depends on conventional broker network. This either deal with security under limited perspicuity, for example, by using only keyword matching for routing events [2], [10] or depends on semi-trusted broker network. [9], [6], [5]. In keyword search method, events are routed based on keyword in the message contents. This approach provides key management but does not provide access control in scalable manner. Yet, in security issues of public subscribe systems how the subscribers are clustered is not mentioned.

In this paper we present new approach to provide authentication and confidentiality in public subscribe systems. The credentials are maintained based on subscriptions of subscribers. For encryption of events we requires keys, private keys allocated to the subscribers are labeled with credentials. A publisher is having set of credentials. In public key encryption a public key can be any arbitrary string. In such a scheme there are four phases. In first setup phase, global system parameters and a master-key are generated. In second, i.e. extraction, private keys are extracted from master keys. In third, encryption, events are encrypted using public keys. In fourth, decryption, messages are decrypted by using relative private keys. [4]

We develop an identity based encryption in which, relative subscribers can decrypt event only if there is match between credentials and key. Also it allows subscribers to check authenticity of received events. [3] In addition we tackle issues regarding subscription confidentiality for semantic clustering of events. A secure overlay maintenance protocol is designed to preserve the weak subscription confidentiality.

Additionally, we propose a extended cryptographic methods for routing of events and "Multi credential Routing", new event distribution method.

2. Related Research

From last few years, Internet is growing day by day and most of the applications requires information distribution between different entities. As the millions of entities distributed globally their locations and behavior may vary. A large scale, running, geographically distributed features requires scalable, more efficient and reliable techniques for information distribution. The synchronous point to point communication models are not able to satisfy these requirements. So publish subscribe systems has received large attention for asynchronous nature of interaction for large systems.

A public subscribe system allows information distribution from event producers i.e. publishers to event consumers i.e. subscribers. These publics subscribe system having different types of infrastructure including topic based systems and content based systems.

In topic based systems, communication infrastructure maintains a logical channel also called as topics. A publisher publishes messages to topic. The subscriber subscribes to topics of their interests. They receive messages coming from their subscribed topic. Different subscribers subscribing to same topic will receive same messages. The enhancement in the logical channel changed the way to implement public subscribe systems.

In content based system, subscription to subscribers is given based on the message content. If the attributes are matched from the published messages then only subscribers can subscribe to them. The proposition of this approach is that messages are intelligently routed to their destination. A greater flexibility is provided when deciding routing logic in content based public subscribe systems. While implementing pub/sub systems messages, integrated applications and communicating infrastructure gets affected.

First for receiving applications contents of interests are identified. Message types are partitioned into different subsets. Next, the information is added to identify content specific information. Then communication infrastructure must be extended so that messages are delivered to subscribers according to their subscription. The approach used here depends on different topologies used. Finally the integrated applications are modified. For each message that is published by publisher, it adds topic related information. For ex. If topic is specified as header element, this information must be included into proper element by publisher. Similarly, topics of interests must be specified by subscriber.

Subscriptions of subscriber can be of two types, Fixed or dynamic. For fixed subscriptions, communication infrastructure sets the topics that are used by applications. Subscriptions are not controlled by application. When the applications are added to communicating infrastructure subscriptions are defined. Whereas in dynamic subscriptions, applications are able to control their own subscriptions by using set of control messages. Applications can edit existing subscriptions by sending messages to communicating infrastructure. New applications are added to communicating infrastructure forming subscription list.

Authorized publishers distribute only valid events in the system. Conversely, masquerade publishers may overload network with fake events. Some subscribers are interested in discovering subscriptions of other subscribers and published events for which they are not authorized. Some passive attackers may listen communication actively to find contents events. So secure channel is required for the distribution of public keys.

3. System Workflow and Algorithm

The classical cryptosystems uses same keys for encryption and decryption. Both keys are kept are kept secret. The problems of this traditional cryptosystems were distribution of keys and key management. A paradigm is shifted towards public key cryptosystem. In which different keys are used for encryption and decryption. One key being public and other as private. These schemes also possess some operational issues. For management of keys Public key infrastructure is maintained. But traditional PKI needs to maintain large number of keys. IBE provides alternative to reduce amount of keys to store.

The private key generator is used as trusted third party. It is also called as key server. At the start first PKG generates pair of keys, public keys and private key. The public key is available users. These keys are called master public keys and master private keys.

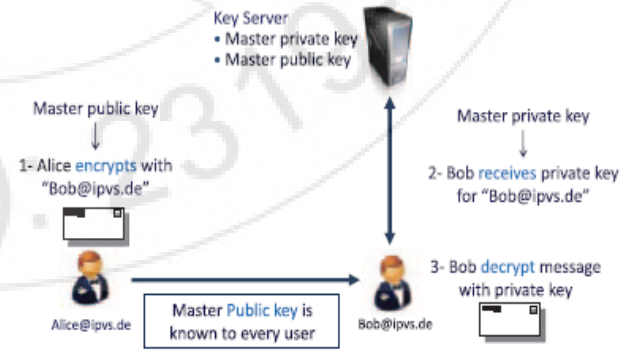

Figure 1.1: System Workflow

1) Sender, Alice in this case, creates plaintext message for receiver, bob. The message is sent from sender to receiver. Alice uses some credentials for encrypting

message that includes Bob's identity, public key of PKG, and cipher text is encrypted.

2) Bob receives cipher text from Alice. While transmitting cipher text some plaintext information is also sent with that. This information is used for receiving private key from PKG to decrypt message. Bob also required authenticating with PKG by sending credentials such as Identity of Bob. After that PKG transmits Bob's private key over a secure channel.
3) For ex. E-mail address can be used as public key.
4) Bob decrypts cipher text using his private key to recover plaintext message.
5) As PKG maintains single Master public keys and Master Private Keys, so it can be used as smart card. A pairing based cryptography is used for implementation of IBE. A mapping is established between to cryptographic groups by means of bilinear maps.

Let G1 and G2 be cyclic group of order q, where q is some large prime
E: G1 x G1 → G2
This bilinear graph satisfies Bilinearity, Nondegeneracy and Computability properties.

4. Conclusion

We have proposed a new approach to provide authentication and confidentiality in a broker-less content based pub/sub system. 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. The paper demonstrates the feasibility of the proposed security mechanisms and analyzes attacks on subscription confidentiality.

References

[1] E. Anceaume, M. Gradinariu, A.K. Datta, G. Simon, andA. Virgillito, "A Semantic Overlay for Self- Peer-to-Peer Publish/Subscribe," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2006.
[2] Antonio Carzaniga, Michele Papalini, Alexander L. Wolf "Content-Based Publish/Subscribe Networking and Information-Centric Networking".
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.
[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2001.
[5] H. Khurana, "Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems," Proc. ACM Symp. Applied Computing, 2005.
[6] L. Opyrchal and A. Prakash, "Secure Distribution of Events in Content-Based Publish Subscribe Systems," Proc. 10th Conf. USENIX Security Symp., 2001.
[7] L.I.W. Pesonen, D.M. Eyers, and J. Bacon, "Encryption-Enforced Access Control in Dynamic Multi-Domain Publish/Subscribe Networks," Proc. ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2007.
[8] P.Pietzuch,"Hermes: A Scalable Event-Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 2004.
[9] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.
[10] 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.

Author Profile

Minakshi B. Shingan received the B.E degree in Information Technology from Dr. Daulatrao Aher College Of Engineering, Karad in 2012. She is currently pursuing her master's degree in computer engineering from Bhivrabai Sawant Institute of Technology and Research, Wagholi, Pune