Securing Brokerless Publish/Subscribe Systems Using Identity Based Encryption

Avinash Yalla

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. Likewise, confidentiality of events and subscriptions conflicts with content-based routing. This paper presents a novel approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. 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. Furthermore, an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality. In addition to our previous work this paper contributes 1) use of searchable encryption to enable efficient routing of encrypted events, 2) multicredential routing a new event dissemination strategy to strengthen the weak subscription confidentiality, and 3) thorough analysis of different attacks on subscription confidentiality. The overall approach provides fine-grained key management and the cost for encryption, decryption, and routing is in the order of subscribed attributes. Moreover, the evaluations show that providing security is affordable w.r.t. 1) throughput of the proposed cryptographic primitives, and 2) delays incurred during the construction of the publish/subscribe overlay and the event dissemination.**

Keywords: **security mechanisms, publish/subscribe system, authentication.**

1. INTRODUCTION

EXISTING SYSTEM:

In the past, most research has focused only on providing expressive and scalable pub/sub systems, but little attention has been paid for the need of security. Existing approaches toward secure pub/sub 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 pub/sub systems, where the subscribers are clustered according to their subscriptions, has not been discussed yet in the literature.

PROPOSED SYSTEM:

Proposed System presents a new approach to provide authentication and confidentiality in a broker-less pub/sub system. Our approach 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. We 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. Furthermore, we address the issue of subscription confidentiality in the presence of semantic clustering of subscribers. A weaker notion of subscription confidentiality is defined and a secure overlay maintenance protocol is designed to preserve the weak subscription confidentiality.

PROBLEM STATEMENT:

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 pub/sub 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. 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. SCOPE

The pub/sub overlay proposed is similar to DPS system with modifications to ensure subscription confidentiality. In this paper, we, therefore, evaluate performance and scalability of the proposed pub/sub system only with respect to the security mechanisms and omit other aspects. In particular, we evaluate the performance of our system the overlay construction time and the event dissemination delays. 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. It shows that the average connection time (delay) increases with the number of peers in the system because of the increase in the height of the attribute tree (each new hop increases the network delay as well as time to apply security methods).

3. MODULE DESCRIPTION

Number of Modules:

After careful analysis the system has been identified to have the following modules:

1. **Content-Based Publish/Subcriber Module.**
2. **Identity Based Encryption Module.**
3. **Key Generation for Publisher/Subscriber Module.**
4. **Secure Overlay Maintenance Module.**

1. Content-Based Publish/Subscriber Module:

The routing of events from publishers to the relevant subscribers, we use the content-based data model. 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.

2. Identity Based Encryption Module:

In our 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. Subsequently, those keys can be used to encrypt, decrypt, and sign relevant messages in the content based pub/sub system, i.e., the credential becomes authorized by the key server. The keys assigned to publishers and subscribers, and the ciphertexts, are labeled with credentials. In particular, the identity-based encryption ensures that a particular key can decrypt a particular ciphertext only if there is a match between the credentials of the ciphertext and the key. Publishers and subscribers maintain separate private keys for each authorized credential.

3. Key Generation For Publisher/Subscriber Module:

Publisher keys: Before starting to publish events, a publisher contacts the key server along with the credentials for each attribute in its advertisement. If the publisher is allowed to publish events according to its credentials, the key server will generate separate private keys for each credential. The public key of a publisher p for credential is generated.

Subscriber keys: Similarly, to receive events matching its subscription, a subscriber should contact the key server and receive the private keys for the credentials associated with each attribute A.

4. Secure Overlay Maintenance Module:

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. 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 ciphertexts 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.

4. SOFTWARE REQUIREMENTS

Operating System	: Windows
Technology	: Java and J2EE
Web Technologies	: Html, JavaScript, CSS
IDE	: My Eclipse
Web Server	: Tomcat
Tool kit	: Android Phone
Database	: My SQL
Java Version	: J2SDK1.5

5. HARDWARE REQUIREMENTS

Hardware	:	Pentium
Speed	:	1.1 GHz
RAM	:	1GB
Hard Disk	:	20 GB
Floppy Drive	:	1.44 MB
Key Board	:	Standard Windows Keyboard
Mouse	:	Two or Three Button Mouse
Monitor	:	SVGA

6. CONCLUSION

In this system, we have presented a new approach to provide authentication and confidentiality in a broker-less content based pub/sub system. The approach is highly scalable in terms of number of subscribers and publishers in the system and the number of keys maintained by them. In particular, 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 ciphertexts are labeled with credentials. We adapted techniques from identity based encryption 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 its private keys and 2) to allow subscribers to verify the authenticity of received events. Furthermore, we developed a secure overlay maintenance protocol and proposed two event dissemination strategies to preserve the weak subscription confidentiality in the presence of semantic clustering of subscribers. The evaluations demonstrate the viability of the proposed security mechanisms and analyze attacks on subscription confidentiality.

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 andSubscription 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.

[11] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, “PeerSim: A Peer-to-Peer Simulator,” http://peersim.sourceforge.net/, 2013.

[12] H. Khurana, “Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems,” Proc. ACM Symp. Applied Computing, 2005.

[13] .A. Lewko, A. Sahai, and B. Waters, “Revocation Systems with Very Small Private Keys,” Proc. IEEE Symp. Security and Privacy, 2010.

[14] B. Lynn, “The Pairing-Based Cryptography (PBC) Library,” http://crypto.stanford.edu/pbc/, 2010.

[15] F.P. Miller, A.F. Vandome, and J. McBrewster, Advanced Encryption Standard. Alpha Press, 2009.

[16] M. Nabeel, N. Shang, and E. Bertino, “Efficient Privacy Preserving Content Based Publish Subscribe Systems,” Proc. 17th ACM Symp. Access Control Models and Technologies, 2012.

[17] L. Opyrchal and A. Prakash, “Secure Distribution of Events in Content-Based Publish Subscribe Systems,” Proc. 10th Conf. USENIX Security Symp., 2001.

[18] 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.

[19] P. Pietzuch, “Hermes: A Scalable Event-Based Middleware,” PhD dissertation, Univ. of Cambridge, Feb. 2004.

[20] C. Raiciu and D.S. Rosenblum, “Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures,” Proc. IEEE Second CreatNet Int’l Conf. Security and Privacy in Comm. Networks (SecureComm), 2006.

[21] . A. Shikfa, M. O ¨ nen, and R. Molva, “Privacy-Preserving Content- Based Publish/Subscribe Networks,” Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[22] 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.

[23] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, “Providing Basic Security Mechanisms in Broker-Less Publish/ Subscribe Systems,” Proc. ACM Fourth Int’l Conf. Distributed Event- Based Systems (DEBS), 2010.

[24] 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.

[25] 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, 200.