International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secured Brokerless Identity-Based Publisher Subscriber System

Sayaram N. Shingote[1], Prof. Syed Akhter[2]

[1]Computer Engineering Department, Computer Engineering Department,

[2]Aditya Engineering College, Beed(M.S) Aditya Engineering College, Beed (M.S)

Abstract: ***The most challenging task is to provide basic security mechanism as authentication and confidentiality in any system. Publisher is one who publish the document and subscriber is a authenticated user who use access that publisher provided documents. Authentication of both publisher and subscriber is one of the difficult task to achieve due to the loose coupling between publisher and subscriber. Similarly confidentiality of event and subscription conflicts with existing system. My paper presents a new method to provide confidentiality and authentication in a broker-less content-based publish/subscribe system by introducing identity based encryption Technique. The authentication of publisher and subscriber as well as confidentiality of events is ensured, by adapting the public and private key cryptography mechanisms, to the needs of a publish/subscribe system. Also algorithm to cluster subscriber based on their subscription preserves a weak notion of subscription confidentiality. This paper also contributes1)use of search encryption to enable efficient routing of encrypted event, 2)multi-credential routing a new event dissemination strategy make strong to the weak subscription confidentiality, and 3) thorough analysis of different attacks by hackers on subscription confidentiality. The proposed approach provides fine grained key management and the less cost for encrypt, decrypt, and routing is in the order of subscribed attribute. The evaluations show that providing security is affordable with respective to1) throughput of the proposed cryptographic primitive, and 2) delay occurred during the construction of the publish-subscribe overlay and the event dissemination. The proposed approach is highly scalable in terms of increasing number of subscribers and publishers in the system and the number of keys maintained by both of them.***

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

1. Introduction

The publisher/subscriber (pubs/subs) communication paradigm has obtained more popularity because of its inherent decoupling of publisher from subscriber in terms of space, time, and synchronization. Publisher inject information into the publish/subscribe system, and subscriber specify the event of interest by making of subscriptions. Published events are routed to their relevant subscribers, the publisher unknowing the relevant set of subscriber, or vice versa. This decoupling is traditionally ensured by intermediate routing over a broker network [10]. In more recent systems, publisher-subscriber organize themselves in a brokerless routing infrastructure, forming an event forwarding overlay [14]. Identitybased publish/subscribe is the variant that provides the most expressive subscription model, where subscription define restrictions on the message content. Its expressive-ness and asynchronous nature is particularly useful for largescale distributed applications such as stock exchange, news distribution, traffic control, environmental monitoring, and public sensing.publish/subscribe needs to provide supportive mechanisms to fulfill the basic security requirements of these applications such as accesscontrol and confidentiality.

Access control in terms of publish/subscribe system means that only authenticated publisher is allowed to disseminate events in the network and only those events are delivered to authorized subscribers. Moreover, the content of events should not be provide to the routing infrastructure and a subscriber should receive all relevant events without revealing its subscription to the system. To solve these security issues in a content based pubsher/subscriber system imposes new challenges for PKI. In proposed system Public Key Infrastructure (PKI) , publisher must maintain the public key of interested subscribers to encrypt events. Subscriber must know the public keys of all related 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 basedrouting. Hence, new mechanisms are needed to route encrypted events to subscribers without knowing their subscriptions to allow subscribers and publishers authenticate each other without knowing each other through key server.

2. System Model

We consider publish/subscribe in a setting where there not exists dedicated broker infrastructure. Publisher and subscriber contribute as peers to the maintenance of a self-organizing overlay structure. To authenticate publisher, we use the term of advertisements in which a publisher announces before-hand the set of events which it wants to publish.

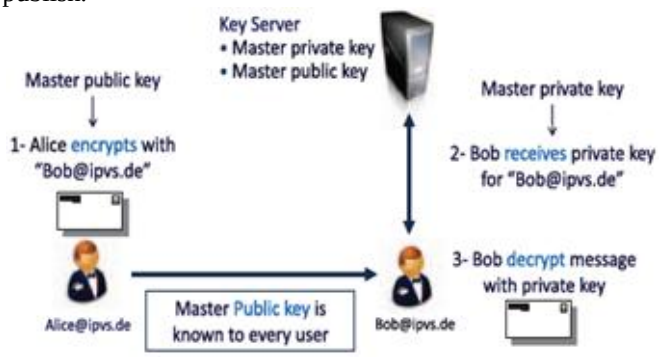

Figure 1: Identity Based Encryption.

In our proposed approach, publishers-subscribers interact with a key distribution server. Both provide credentials to the key distribution server and receive keys which fit the expressed capabilities in the credentials. Those keys can be used to encryption, decryption, and sign relevant messages in the content-based pub/sub system, i.e., the credential becomes authorized by the key distribution server. A credential consists of following two parts: 1) a binary string describes the capability of a peer in publishing and receiving event and 2) a proof of its identities. The latter is used for authentication against the key distribution server and verification whether the capabilities match the identity of the peer.We pay our attention mainly on expressing the capabilities of a credentials, i.e., how subscriber and publisher can create a credentials. This process needs to address the many possibilities to partition the set of events described by an advertisement or subscription and exploits overlaps in subscriptions and publications. Subsequently, here we use the term credentials only for referring to the capability string of a credentials.

3. Publish/Subscribe Authentication and Event Confidentiality

3.1 Security Parameters and Initialization:

Let GG1 and GG2 denote the bilinear groups of prime order q, i.e., |GG1|= |GG2| = q, e : GG1 × GG1 →GG2 denote an admissible bilinear map, and g denote a generator in GG1. Moreover, let H1 : {0,1}*→{0,1}^nu , H2 :{0,1}*→{0,1}^nm,H3:{0,1}→GG1, and H4 : GG2→{0,1}^log q designate collusion resistant cryptographic hash functions. The initialization algorithm:

1) chooses α.¥ € Zq,
2) computes g1= g^ α and h=g^¥,
3) chooses g2.u',a'€ G1, and
4) select vectors ū=(ui) and ā=(ai) of length nu and na, respectively, with every element chose nonformly at random from GG1.

The Master Public Key MPu is composed of (e,g,g1,g2,h,u',a',ū,ā).This master public key is known to every peer in the system and is used for encryption and signature verification. The Master Private key MPris (¥,g^α2), and is only known to the key server. The master private key is used for generating private keys for publishers and subscribers.

3.2 Key Generation for Publishers

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. Let Credi;j denote the credential with label j for the attribute Ai,for example, CredTemp,0 denotes credential 0 of attributeTemp. The public key of a publisher p for credential Credi,jis generated as:

$Pu^{p}_{i,j}$= ($Cred_{i,J}$ || Ai || PUB || Epoch)

The key server will generate the corresponding private keys as follows: For each credential Credi;j and a publisher p, let,vp=H1(Pup i;j) be a bit string of length nu and let vp[k]denote thekth bit. Let Γi;jC_{1,2, . . . ; nu} be the set of all kfor which vp[k] = 1. The key server chooses γi;j €Zqatrandom and computes

$Pr^{p}_{i,j:=}$(g^α($u' \prod_{k \in \Gamma i,j} uk$^γi,j,g^γi,j)=:$Pr^{p}_{i,j[1]}.Pr^{p}_{i,j[2]}$

3.3 Key Generation for Subscribers

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 Ai. In case of subscribers, the public key for a credential Credi,j is given as:

$Pu^{p}_{i,j}$= ($Cred_{i,J}$ || Ai || PUB || Epoch)

A different symbol SUB is used to differentiate the keys used for the verification of valid events from the ones used to provide event confidentiality. The private keys are generated as follows: The key server chooses γs€Zqat random. The same γs is used for all credentials associated with a subscription. For each credential Credi;j, it calculates Γi;jsimilar to the publisher's case, chooses γi;j€ Zqand computes,

$Pr^{s}_{i,j}$=:(g2^γs ($u' \prod_{k \in \Gamma i,j} uk$)^γi,j,g^γi,j, H3($u' \prod_{k \in \Gamma i,j} uk$)^¥)=:$Pr^{s}_{i,j[1]}.Pr^{s}_{i,j[2]},Pr^{s}_{i,j[3]}$

4. Secure Overlay Maintenance

We propose a secure protocol to maintain the desired pub/sub overlay topology without violating the weak subscription confidentiality. For simplicity and without loss of generality, here we discuss the overlay maintenance w.r.t. a single tree associated with a numeric attribute

Ai and each of the subscribers owns a single credential. 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 credentials, for example, a subscriber with credential 00 can only connect to the subscribers with credentials 0 or 00. A new subscriber s generates a random key SW and encrypts it with the public keys Pubi,j for all credentials that cover its own credential. The generated cipher text 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.

Filling the security gaps. By looking at the number ofcipher-text in the connection request, a peer can detect the credential of the requesting subscriber s.In the worst case, a subscriber has a credential ofthe finest granularity. This can be covered by log2bZip othercredentials, and therefore, a connection request contains inthe worst case that many cipher-text. To avoid any informationleak, cipher-texts in the connection request are alwayskept in Olog2 Zip by adding random cipher-text if needed. Furthermore, the cipher-textare shuffled to avoid any information leak from their order.

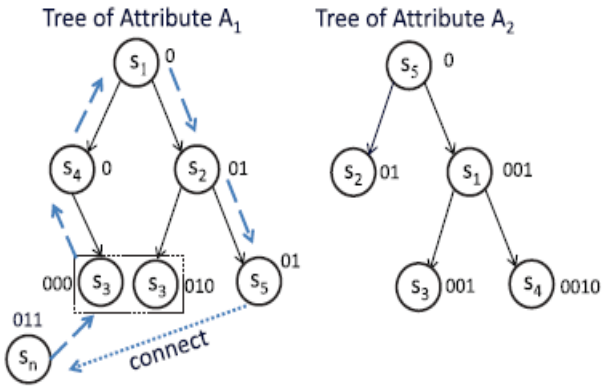

Figure 2: Publish/Subscribe system with two numericattributes

A different random key SW is used for the generation ofeach cipher-text to avoid any information leak to the peerwho has successfully decrypted one of the cipher-text and,thus, has recovered the random key SW. Otherwise, thepeer can try to generate cipher-text by encrypting the(recovered) SW with public keys for Olog2Zip credentials and can easily determine the random cipher-text in the connection request and, thus, the credentials of the requesting subscriber s. Finally, to avoid an attacker to generate arbitrary connection request messages and try to discover the credential of other peers in the system, the connection request is signed by the key server. This step needs to be performed only once, when a newly arriving subscriber authorizes itself to the key server in order to receive private keys for its credentials.

Algorithm 1. Secure overlay maintenance protocolat peer sq.
1: upon event Receive (CR of s new from sp) do
2: if decrypt request (CR)= = SUCCESS then
3: if degree (sq) == available then //can have child peers
4: connect to the s new
5: else
6: forward CR to {child peers and parent} - sp
7: if decrypt request (CR)= = FAIL then
8: if sp = =parent then
9: Try to swap by sending it own CR to the snew.
10: else
11: forward to parent

A child peer sq receives CR (of subscriber snew) from the parent sp only if the parent cannot accommodate more children. If sq cannot be the parent of snew, i.e., snew's credential is coarser than that of sq, then it tries to swap its position with snew by sending its own connection request (cf. Algorithm 1, lines 7-9). However, if none of the children of parent sp can connect or swap with snew, then there is no containment relationship between the credentials of the children and snew. In this case, a parent should disconnect one of its children to ensure the new subscriber is connected to the tree.

5. Conclusions

In this research paper, I have presented a new method to provide authentication and confidentiality in a broker-less identity 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 cipher-text are labeled with credentials. I 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 keysand 2) to allow subscribers to verify the authenticity of received events. Further more, 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] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, "PeerSim: APeer-to-Peer Simulator," http://peersim.sourceforge.net/, 2013.
[2] W.C. Barker and E.B. Barker, "SP 800-67 Rev. 1. Recommendationfor the Triple Data EncryptionAlgorithm (TDEA) Block Cipher,"technical report, Nat'l Inst. of Standards & Technology, 2012.
[3] M. Nabeel, N. Shang, and E. Bertino, "Efficient Privacy PreservingContent Based Publish Subscribe Systems," Proc. 17th ACM Symp.Access Control Models and Technologies, 2012.
[4] M.A. Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel,"Meeting Subscriber-Defined QoS Constraints in Publish/SubscribeSystems," Concurrency and Computation: Practice andExperience, vol. 23, pp. 2140-2153, 2011.
[5] M. Srivatsa, L. Liu, and A. Iyengar, "EventGuard: A SystemArchitecture for Securing Publish-Subscribe Networks," ACMTrans. Computer Systems, vol. 29, article 10, 2011.
[6] 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.
[7] S. Choi, G. Ghinita, and E. Bertino, "A Privacy-EnhancingContent-Based Publish/Subscribe System Using Scalar ProductPreserving Transformations," Proc. 21st Int'l Conf. Database andExpert Systems Applications: Part I, 2010.
[8] M. Ion, G. Russello, and B. Crispo, "Supporting Publication andSubscription Confidentiality in Pub/Sub Networks," Proc. SixthInt'l ICST Conf. Security and Privacy in Comm. Networks SecureComm),2010.
[9] 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 DistributedEvent-Based Systems. IGI Global, 2010.
[10] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with VerySmall Private Keys," Proc. IEEE Symp. Security and Privacy, 2010.

[11] B. Lynn, "The Pairing-Based Cryptography (PBC) Library,"http://crypto.stanford.edu/pbc/, 2010.
[12] F.P. Miller, A.F. Vandome, and J. McBrewster, Advanced EncryptionStandard. Alpha Press, 2009.
[13] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges forSecurity, Privacy and Trust, 2009.
[14] Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based SigncryptionScheme without Random Oracles," Computer Standards & Interfaces,vol. 31, pp. 56-62, 2009.
[15] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access Controlin Publish/Subscribe Systems," Proc. Second ACM Int'l Conf.Distributed Event-Based Systems (DEBS), 2008.

Author Profile

Sayaram Shingote received the B.E. degree First Class with Distinction in Information Technology and M.E. in Software Engineering from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad. Area of interest is Information security.

Prof. Syed Akhter, Head of Department of Computer Engineering & M.E. Coordinator in Aditya Engineering College, Beed (Maharashtra).