ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Protecting Trader Distribute Systems Using Similitude-Stationed Cipher

P.Keerthi
M-Tech Student
Department of CSE,
Bharath Institute of Technology And Science for Woman
Mangalpally Village, Ibrahimpatnam Mandal,
Telangana 501510, India.

Parimala
Guide
Department of CSE,
Bharath Institute of Technology And Science for Woman
Mangalpally Village, Ibrahimpatnam Mandal,
Telangana 501510, India.

ABSTRACT: ***The provisioning of basic security mechanisms such as authentication and confidentiality is highly challenging in a contentbased publish/subscribe system. Authentication of publishers and subscribers is difficult 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.***

Index Terms—***Content-based, publish/subscribe, peer-to-peer, broker-less, security, identity-based encryption***

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 fulfill the basic security demands of these applications such as access control and confidentiality.

EXISTING SYSTEM: Content-based publish/subscribe is the variant which pro-vides 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 with high-volume data streams.
Access control in the context of publish/subscribe system means that only authenticated publishers are allowed to disseminate events in the network and only those events are delivered to authorized subscribers. Similarly, 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. These security issues are not trivial to solve in a content-based pubish/subscribe system and pose new challenges.

DISADVANTAGES OF EXISTING SYSTEM: It is very hard to provide subscription confidentiality in a broker-less publish/subscribe system, where the subscribers are arranged in an overlay network according to the containment relationship between their subscriptions. In this case, regardless of the cryptographic primitives used, the maximum level of attainable confidentiality is very limited.

The limitation arises from the fact that a parent can decrypt every event it forwarded to its children. Therefore, mechanisms are needed to provide a weaker notion of confidentiality. Do not intend to solve the digital copyright problem.

PROPOSED SYSTEM: In this paper, we present a new approach to provide authentication and confidentiality in a broker-less publish/subscribe system. Our approach allows subscribers to maintain credentials according to their subscriptions. Private keys assigned to the subscribers are labelled with the credentials. A publisher associates each encrypted event with a set of credentials. We adapted identity based encryption mechanisms.

ADVANTAGES OF PROPOSED SYSTEM: To ensure that a particular subscriber can decrypt an event only if there is match between the credentials associated with the event and the key.

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 connection protocol is designed to preserve the weak subscription confidentiality. Finally, the evaluations demonstrate the viability of the proposed security mechanisms.

CONCLUSION: In this paper, we have presented a new approach to provide authentication and confidentiality in a broker-less contentbased 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 identitybased 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.

REFERENCE:

[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] D. Boneh and M.K. Franklin, "Identity-Based Encryption from theWeil Pairing," Proc. Int'l Cryptology Conf.Advances in Cryptology, 2011.

[3] Karl aberer, Aniwitaman datta and Manfred Hauswirth "Efficient Self Contained Handling of Identity in Peer toPeer System"IEEE transaction on know- ledge and data engineering,2004.

[4] Sean O,Mealia and Adam J.Elbirt "Enhancing the Performance of Symmetric –key cryptography via Instructionset instruction" IEEE transactions on very large scale integeration vol.18 no.11 november 2011.

[5] Ming li,Shucheng Yu.Yao Zheng,Kui Reng, Weiging Lou "Scalable and secure sharing of personal data incloud computing using attribute-based encryption"IEEE transaction on paralllel and distributed computing 2013

[6] Legathaux Martins and Sergio Duarte "Routing Algorithms for Content based publish/subscribe system"IEEEcommm- unications and tutorials first quarte 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2010

[8] A.Shirisha, B.Srikanth Reddy & T. Madhu, Credential Based Publisher/Subscriber Technique Using Identity Based Encryption, IJMETMR, Volume No: 2, Issue No: 7

[9] http://www.yuvaengineers.com/on-demand-secure-routing-protocol-for-authentication-and-data-integrity-in-manet-k-nivedha-p-m-sharmila-v-shobana-mr-b-ram-kumar/