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

Survey of Identity-Based Encryption for Providing Security in Sender/Receiver Systems

S. N. Shitole[1], A D Gujar[2]

[1, 2]Pune University, Pune, Maharashtra, India

Abstract: ***In past few years, Web has huge impact on distributed computing. The provisioning of fundamental security mechanisms like authentication and confidentiality for Sender/Receiver System is exceptionally difficult. Authentication of Senders and Receivers is hard to accomplish because of the loosely coupling of Senders and Receivers. Moreover, privacy of events and subscriptions conflicts with content based routing. This paper displays a novel methodology to provide confidentiality and authentication in Sender/Receiver System. By adapting pairing-based cryptography mechanisms, the authentication of Senders and Receivers and additionally confidentiality of events is guaranteed, to the needs of a Sender/Receiver system. Besides, an algorithm to cluster Receivers as respective of their subscriptions protects a weak notion of subscription privacy. There can be some improvements which can be doneto the existing systems [8]. Like 1) utilization of searchable encryption for allowing proficient routing of encrypted events, 2)Exhaustive examination of number of attacks on subscription confidentiality, and 3)Multicredential routing another event dissemination technique to reinforce the weak subscription confidentiality. The general methodology offers fine-grained key management and the expense for encryption, decryption, and routing is in the request of subscribed properties. In addition, the assessments demonstrate that providing security is reasonable with respect to 1) delay brought about amid the development of the Sender/Receiver overlay and the event dissemination,2) Throughput of the presented cryptographic primitives.***

Keywords: Loosely coupling, Sender/Receiver system, Peer to Peer, Identity - Based Encryption, Multicredential routing.

1. Introduction

The Sender/Receiver communication standard has picked up high ubiquity as a result of its characteristic decoupling of Sender from Receiver regarding time, space, and synchronization. Senders distribute data over the Sender/Receiver System and Receivers stipulate the events of interest adding subscriptions. Distributed events are routed to their applicable receivers, without the senders knowing the receivers of those events, same for the receivers. This decoupling is usually guaranteed by routing over a broker system [7]. In later systems, by forming an event forwarding overlay [10], senders and receivers arrange themselves in a broker-less routing infrastructure.

Content-based Sender/Receiver is the variation that provides the most expressive subscription model, where subscriptions characterize limitations on the message content. For substantial distributed applications, expressiveness and asynchronous nature of Content-based Sender/Receiver system are valuable. As anyone might expect, Sender/Receiver needs to give strong components to satisfy the fundamental security needs of these applications, For example, confidentiality, access control.

Access control in the context of Sender/Receiver system implies that only authenticated senders are permitted to distribute events in the system and just those events are forwarded to authorized receivers. In addition, the content of events must not be presented to the routing infrastructure and a receiver must get all subscribed events without disclosing its subscription to the framework. Answering these security issues in a content-based Sender/Receiver system force new difficulties. For example, end-to-end authentication utilizing a public key infrastructure (PKI) clashes with the loose coupling of senders and receivers, a key necessity for building versatile Sender/Receiver systems. For PKI, senders must keep up the public keys of all intrigued receivers to encrypt events. Receivers must know the public keys of all pertinent senders to confirm the authenticity of the got events. Besides, conventional methods to ensure confidentiality by encrypting the entire event message conflict with the content-based routing model. Henceforth, new mechanisms are required to route encrypted events to receivers without knowing their subscriptions and to permit receivers and senders validate one another without knowing one another.

There is requirement of mechanism which will give searchable encryption by which productive routing of encrypted events will be attained and multi-accreditation routing another event distribution methodology for empowering weak subscription confidentiality. There is additionally need of keeping up credentials as per subscription. Methodology of security in existing framework depended on traditional broker network [12] [13]. This is for the most part accomplished by confined expressiveness [14] [15] or depend on semi trusted dealer system [11].

2. Literature Review

In the study by Sunoh Choi, Gabriel Ghinita, and Elisa Bertino [5] they had proposed a secure CBPS framework based on Asymmetric Scalar product conserve Encryption with a specific end goal to give notice and subscription confidentiality and to lessen matching complexity. Techniques presented by them help range filtering, inequality filtering, equality filtering, covering and conjunction filtering which are vital in CBPS. Furthermore, their answer did not bring about false positives, rather than existing work, for example, C-CBPS. Besides, they had proposed another system for secure aggregation utilizing ASPE and homomorphic functions. Their techniques took 65% less time in equality filtering. Also 50% less time for range filtering than existing system C-CBPS.

In this paper [1], they have presented DPS, a distributed scalable and reliable content-based Sender/Receiver system that reveals self-characteristics. In this methodology, the receivers are self-organize in to similar semantic clusters. Additionally, semantic clusters self configured in to rational trees that are applied further to efficiently submit events in the network. To be able to mask sudden un-subscriptions, they reinforced the rational connection of the DPS trees using extra hyperlinks between a semantic class and its neighbors. A great function of DPS is its power to self-heal using only local information. That's, it can regulate within an autonomous and local way containing a reliable framework in the clear presence of cellular and dynamic nodes.

With access control operation located in the client-hosting brokers, we are able to enforce RBAC on the Sender/Receiver clients. Generally, splitting up event-management operation into dedicated function service makes access control easier to enforce than in a peer-to-peer approach where in actuality the customer and function service are collocated [2]. The latter seems improper for application sending sensitive data we have thought content-based redirecting, for efficiency of communication, rather than broadcast or gossip-based routing. When some brokers aren't trusted to see certain painful and sensitive data this form of redirecting can still be used, with the modification we describe

Dan Boneh Matthew Franklin [4] denied chosen cipher text security for identity-based systems and proposed a totally functional IBE system. The system has chosen cipher text security in the random oracle model assuming BDH, a natural analogue of the computational Die-Hellman problem.

Cocks [6] recently proposed another IBE system whose security is on the basis of the difficulty of distinguishing quadratic residues from non-residues in the ring Z=NZ where N can be an RSA modulus (i.e., a product of two large primes). Cocks' system is somewhat harder to used in practice that the IBE system in this paper. Cocks' system uses bit-by-bit encryption and consequently outputs long cipher texts. Also, encryption/decryption is a bit slower than the system described in this paper. Nevertheless, it is encouraging to see that IBE systems may be built using very dierent complexity assumptions.

J. Bethencourt, A. Sahai, and B. Waters [3] created a framework for Ciphertext-Policy Attribute Based Encryption. Their framework takes into consideration another sort of encrypted access control where client's private keys are specified by a set of attributes and gathering encrypting information can determine an arrangement over these attribute determining which clients have the capacity decode. Their system permitted approaches to communicate as any monotonic tree access structure and is impervious to conspiracy assaults in which an attacker may get different private keys. At last, they gave a usage of their framework, which incorporated a few improvement procedures. Later on, it would be fascinating to consider attribute based encryption frameworks with different sorts of expressibility.
In this paper, they [9] presented PSGuard an efficient and secure occasion dissemination mechanism for Sender/Receiver networks. PSGuard involves a novel key management algorithm for guaranteeing occasion confidentiality. In place of associating tips with customers or categories of customers in class essential management strategies, PSGuard associates authorization tips with dues and security tips with journals and employs secure essential derivation calculations for scalable essential management. Through easy analytic versions and experimental examination we display that PS Guardoers Signicantly reduces the connection, storage and state preservation prices, although incurring a tiny computational overhead.

In this paper [7] they had presented PADRES, a distributed content-based Sender/Receiver system built for certain requirements of work°ow management. PADRES was produced in collaboration with Cybermation, Inc., creator of the ESP Workload Manager and ESP Espresso products. The Sender/Receiver brokers use a rule-based matching engine to do content-based concept matching and redirecting in Sender/Receiver. PADRES provides a subscription language so that customers can show their complex pursuits as blend subscriptions. The story historic data access element supplies a hybridized means for customers to get both previous and future information from the Sender/Receiver system. A next-generation distributed workflow management system based on PADRES is presented.

In study by M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel [8] had introduced new methodology to offer authentication and confidentiality in a broker-less content-based Sender/Receiver system. The methodology is exceedingly versatile regarding number of receivers and senders in the framework and the quantity of keys kept up by them. Specifically, they created systems to assign credentials to senders and receivers as indicated by their subscriptions and notices. Private keys allocated to senders and receivers, and the cipher texts are marked with credentials. They adjusted strategies from Identity Based Encryption, i) to guarantee that a specific receivers can decrypt an event just if there is match between the credentials connected with the event and its private keys and, ii) to permit receivers of confirm the credibility of got events. Besides, they created a protocol to save the weak subscription confidentiality in the vicinity of semantic clustering of endorsers.

3. Conclusion

We have prepared a report for different topics of Sender/Receiver System. We have discussed many existing systems and also the development which can be done in this topic. This report includes confidentiality and authentication in broker-less content based Sender/Receiver system, semantic overlay, access control, identity-based encryption, security parameters and initialization, key generation for publishers/subscribers, publishing events; secure event dissemination, drawbacks of traditional security mechanisms. Based on such report, we surveyed dynamic publish/subscribe, security issues, methods of security, secure content based event routing, scalable key management.

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] 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] 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.
[6] C. Cocks, \An identity based encryption scheme based on quadratic residues", Eighth IMA International Conference on Cryptography and Coding, Dec. 2001, Royal Agricultural College,Cirencester, UK.
[7] 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.
[8] 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.
[9] L. Opyrchal and A. Prakash, "Secure Distribution of Events in Content-Based Publish Subscribe Systems," Proc. 10th Conf. USENIX Security Symp., 2001.
[10] 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.
[11] P. Pietzuch, "Hermes: A Scalable Event-Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 2004
[12] 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.
[13] 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.
[14] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges forSecurity, Privacy and Trust, 2009.
[15] 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.