Cryptology ePrint Archive: Report 2011/025

Supporting Publication and Subscription Confidentiality in Pub/Sub Networks

Mihaela Ion and Giovanni Russello and Bruno Crispo

Abstract: The publish/subscribe model offers a loosely-coupled communication paradigm where applications interact indirectly and asynchronously. Publisher applications generate events that are sent to interested applications through a network of brokers. Subscriber applications express their interest by specifying filters that brokers can use for routing the events. Supporting confidentiality of messages being exchanged is still challenging. First of all, it is desirable that any scheme used for protecting the confidentiality of both the events and filters should not require the publishers and subscribers to share secret keys. In fact, such a restriction is against the loose-coupling of the model. Moreover, such a scheme should not restrict the expressiveness of filters and should allow the broker to perform event filtering to route the events to the interested parties. Existing solutions do not fully address these issues. In this paper, we provide a novel scheme that supports (i) confidentiality for events and filters; (ii) filters can express very complex constraints on events even if brokers are not able to access any information on both events and filters; (iii) and finally it does not require publishers and subscribers to share keys.

Category / Keywords: attribute-based encryption, encrypted search

Publication Info: Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010)

Date: received 12 Jan 2011, last revised 12 Jan 2011

Contact author: mihaela ion at create-net org