# An Implementation of Event and Filter Confidentiality in Pub/Sub Systems and its Application to e-Health

Mihaela Ion
CREATE-NET International Research Center
via alla Cascata 56D, 38123 Trento, Italy
mihaela.ion@create-net.org

Giovanni Russello
CREATE-NET International Research Center
via alla Cascata 56D, 38123 Trento, Italy
giovanni.russello@create-net.org

Bruno Crispo
Department of Information Engineering and Computer Science
University of Trento, Trento, Italy
crispo@disi.unitn.it

## ABSTRACT

The publish/subscribe model offers a loosely-coupled communication paradigm where applications interact indirectly and asynchronously. Publisher applications generate events that are forwarded to subscriber applications by a network of brokers. Subscribers register by specifying filters that brokers match against events as part of the routing process. Brokers might be deployed on untrusted servers where malicious entities can get access to events and filters. Supporting confidentiality of events and filters in this setting is still an open challenge. First of all, it is desirable that publishers and subscribers do not share secret keys, such a requirement being against the loose-coupling of the model. Second, brokers need to route events by matching encrypted events against encrypted filters. This should be possible even with very complex filters. Existing solutions do not fully address these issues. This work describes the implementation of a novel schema that supports (i) confidentiality for events and filters; (ii) filters that express very complex constraints on events even if brokers are not able to access any information on both events and filters; (iii) and finally, does not require publishers and subscribers to share keys. We then describe an e-Health application scenario for monitoring patients with chronic diseases and show how our encryption schema can be used to provide confidentiality of the patients' personal and medical data, and control who can receive the patients' data and under which conditions.

## Categories and Subject Descriptors

E.3 [**Data**]: Data Encryption

## General Terms

Security

## Keywords

confidentiality, publish/subscribe, attribute-based encryption, encrypted search, e-Health


*CCS'10,* October 4–8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

## 1. MOTIVATION

The publish/subscribe (pub/sub) model is an asynchronous communication paradigm where senders, known as *publishers*, and receivers, known as *subscribers*, exchange messages in a loosely coupled manner, i.e. without establishing direct contact. The messages that publishers generate are called *events*. Publishers do not send events directly to subscribers, instead a network of interconnected brokers is responsible for event delivery. In fact, publishers do not know who receives their events and subscribers are not aware of the source of information. In order to receive events, subscribers need to register their interest with a broker through a *filter*. When a new event is published, brokers forward it to all subscribers which expressed a filter that matches the event.

Pub/sub is an open communication model with the implicit assumption that the interconnected brokers are trusted with events and filters confidentiality. However, it is very likely that brokers could be deployed on an outsourced infrastructure. In this context, a malicious administrator of the infrastructure could gain access to the events that are routed through the broker. Moreover, accessing the content of the filters registered in the broker can provide useful information to the attacker. For example, a subscriber may register a filter for receiving events when the price of the quotes of a certain company is below a certain threshold. This information could reveal the subscriber's strategy to a competitor, thus the subscriber will wish to keep it confidential.

Providing event and filter confidentiality in the presence of potentially compromised brokers is still a main challenge for pub/sub systems. On the one hand, any solution that aims at protecting the confidentiality of the model should not hamper the loosely coupling property of the model. Solutions such as the one described in [6] require publishers and subscribers to share a group key. Such solutions are impractical since publishers and subscribers should be agnostic of each others. On the other hand, protecting the confidentiality of filters from malicious brokers is very difficult. Brokers need to access the filters to route events. Encryption schemas for event and filter confidentiality have been proposed (such as in [7]) that restrict the matching capability of the brokers. These solutions allow subscribers to define filters with equality on one keyword. Other solutions, such as [5] and [6], do not support filter confidentiality and do not allow the definition of complex encrypted filters. In these solutions only certain fields of the events are encrypted

while other fields are left as cleartext so that they can be used for routing.

In this poster, we present an encryption scheme for the confidentiality in pub/sub systems such that: (i) it provides confidentiality of events and filters, (ii) it does not require publishers and subscribers to share keys, and (iii) it allows subscribers to express filters that can define any monotonic and non-monotonic conditions. We have implemented our encryption scheme and it will be available for demonstration to the viewers during the poster session.

## 2. SOLUTION DETAILS

In this section, we provide a high-level description of our solution. For the full details, we remand the interested reader to the following paper [4].

In our approach an event $E$ consists of: (i) the message $M$ that represents the content of the event and (ii) a set of attributes $\{a_i\}$ that characterise $M$ and are used for event filtering by the brokers.

To support confidentiality of events and allow publishers to control who can read their messages, the message $M$ is encrypted using CP-ABE [1]. CP-ABE allows a publisher to specify which attributes a decrypter must have. For example, a publisher could specify that only people belonging to a particular organisation or who have a specific role should read the message. In using CP-ABE to encrypt $M$, publishers and subscribers do not need to share any secret key.

Filter confidentiality is achieved by combining KP-ABE [3] with multi-user searchable data encryption (SDE) scheme [2]. In particular, a subscriber $S_j$ can define a filter $F_j$ as a KP-ABE access trees. The set of attributes $\{a_i\}$ that the publisher defined on an event $E$ is used by the brokers to evaluate the filters. When the event $E$ reaches a broker, if the set of attributes associated with the event satisfy the filter $F_j$, then the broker knows that the event can be forwarded to $S_j$. However, if the KP-ABE scheme is used as proposed in [3], then the broker is still able to obtain information on the filters and attributes associated with events, thus violating the confidentiality of events and filters. In fact, the KP-ABE scheme requires that the attributes associated with the ciphertext are not encrypted. To circumvent this limitation, we propose the following modification to the KP-ABE scheme: the set of attributes associated with an event and the access tree representing the filter are encrypted using the scheme from [2]. The scheme supports encrypted search, so it can be used to verify if the encrypted attributes specified by the publisher are the same as those specified by the subscriber in the filter. With this modification, our scheme supports confidentiality of filters and allows the brokers to perform encrypted event filtering. It should be noted that both KP-ABE and the multi-user SDE do not require that publishers and subscribers share keys thus simplifying key management.

## 3. APPLICATION SCENARIO

In the following, we describe an e-Health application in which an outsourced pub/sub system is responsible for message delivery to the involved stakeholders. The exchanged messages contain personal and medical information of patients, and hence, we need to ensure their confidentiality in the presence of untrusted third parties.

Figure 1 shows the e-Health application designed for remotely monitoring patients with a chronic disease that do not require hospitalisation, such as heart diseases or diabetes. In order to provide adequate medical care to patients, several institutions need to cooperate and exchange sensitive medical data. Doctors need to continuously monitor both specific physiological parameters of their patients such as blood pressure, blood oxygen levels, weight etc. and their habits such as diet and physical activity. This information is collected by an in-Home Monitoring System (iHMS) through the use of electronic devices self-managed by the patient. These devices have wireless means to connect to a central gateway where the data is collected. Whenever meaningful data becomes available, the gateway publishes it as a new event and the pub/sub system delivers it to all parties such as the patient's doctor or nurse which registered interest through a filter. For example, a filter could express the following conditions: name="John Smith" AND (heart_rate>120 OR systolic_pressure>150 OR diastolic_pressure>100).

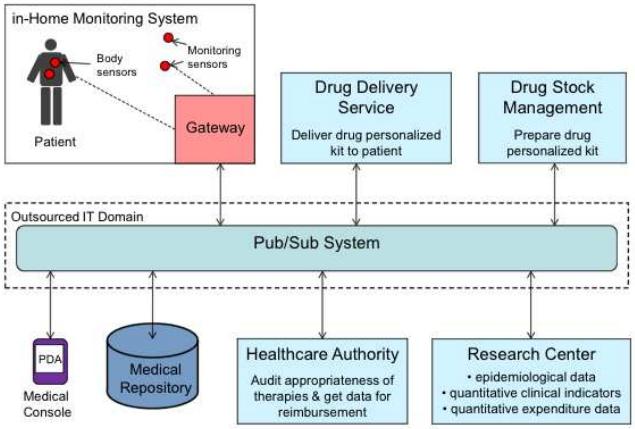


**Figure 1: e-Health application scenario for monitoring chronic diseases.**

Doctors can prescribe medicines that are directly provided by the hospital and reimbursed by the Healthcare Authority (HA). In order to assure the appropriateness of the therapy and the exact amount of costs to be reimbursed, the hospital has to provide to the HA data related to the patient's conditions and drug costs. The Drug Stock Management (DSM) provides drugs to the patients based on the therapeutic data provided by the doctors. The drugs can be delivered at home thanks to a Drug Delivery Service (DDS). Finally, there is a Research Centre that performs data processing of the received information from various hospitals and healthcare authorities.

The pub/sub system responsible for delivering messages between these parties is outsourced to an IT company that provides and maintains the servers where the message bus is deployed. A malicious employee of the IT company can easily get access to published events and registered filters and learn information about the patients medical condition and drug information, thus violating the patients' privacy. However, by implementing our encryption solution in the pub/sub system, we can ensure that only authorised parties are able to decrypt the events. Publishers will encrypt

the medical data using CP-ABE and specify the attributes the decrypter must have such as "Doctor" OR ("nurse" AND "level>3") OR "Senior Researcher", and additionally encrypt the attributes of the messages used by brokers to route events, using SDE. Subscribers will express filters as KP-ABE decryption keys and encrypt the filter's attributes using SDE. In this way, brokers are able to forward encrypted events such as prescription information to all the interested parties such as patient, HA, and DSM without learning anything about the content of events or filters. Any attacker able to read the messages that come in and out the broker will not be able to learn anything either.

# 4. CONCLUSIONS

In this work, we presented a solution for providing confidentiality in pub/sub systems. Our solution is an encryption scheme based on CP-ABE, KP-ABE and multi-user SDE. Our scheme supports both the publication and the subscription confidentiality properties while at the same time does not require publishers and subscribers to share secret keys. Although events and filters are encrypted, brokers can still perform event filtering without learning any information. Finally, our scheme allows subscribers to express filters that can define any monotonic and non-monotonic constraints on events.

# 5. ACKNOWLEDGEMENTS

The work of the researcher Mihaela Ion was funded by the Autonomous Province of Trento, Call for proposal Major Projects 2006 (project ACube).

# 6. REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321-334. Citeseer, 2007.

[2] C. Dong, G. Russello, and N. Dulay. Shared and Searchable Encrypted Data for Untrusted Servers. Lecture Notes in Computer Science, 5094:127-143, 2008.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, page 98. ACM, 2006.

[4] M. Ion, G. Russello, and B. Crispo. Supporting publication and subscription confidentiality in pub/sub networks. In Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore, September 2010.

[5] H. Khurana. Scalable security and accounting services for content-based publish/subscribe systems. In Proceedings of the 2005 ACM symposium on Applied computing, page 807. ACM, 2005.

[6] C. Raiciu and D. Rosenblum. Enabling confidentiality in content-based publish/subscribe infrastructures. Securecomm and Workshops, 28:1-11, 2006.

[7] A. Shikfa, M. Onen, and R. Molva. Privacy-Preserving Content-Based Publish/Subscribe Networks. In Emerging Challenges for Security, Privacy and Trust: 24th Ifip Tc 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18-20, 2009, Proceedings, page 270. Springer, 2009.