International Journal of Information & Network Security (IJINS)
Vol.1, No.2, June 2012, pp. 97~104
ISSN: 2089-3299

A Trust Based Approach For Secure Access Control In Information Centric Network

Sapna Singh*, **Archana Puri***, **Shiksha Smreti Singh***, **Anurika Vaish***, **S.Venkatesan***
* Division of MBA & MS-CLIS
*Indian Institute of Information Technology, Allahabad, India

Article Info

Article history:

Received May 21th, 2012
Revised May 31th, 2012
Accepted June 6th, 2012

Keyword:

Trust
Information Centric Network
Access control
Security
Publish/Subscribe System

ABSTRACT

The world requires a transition from the classical node centric network to an information centric network. Publish/Subscribe Internet Routing Paradigm (PSIRP) being one of the paradigms for future networking is grabbing vast attention of the internetworking user group as a captivating communication paradigm because of its flexibility, desired functionality and performance. Thus, increase in the number of user groups, causes increase in the demand for information access. Consequently, it induces various security concerns. So far most of the researches related to security in publish/subscribe system are concentrated on secure routing, caching and transmission of the information. Access control is a crucial domain of security which cannot be overlooked and requires sincere attention. In this paper a trust driven approach to implement secure access control on the information is proposed. This ensures information availability on demand to the authorized users based on their trust level with the network. The mechanism is illustrated with the help of example usage scenarios.

Corresponding Author:

Sapna Singh
Indian Institute of Information Technology, Allahabad, India.
Email: singh.sapnait85@gmail.com

1. INTRODUCTION

PSIRP is the widely accepted paradigm among various other architectures proposed for Information Centric Network (ICN). Together with providing better performance it will also provide chances for innovative applications and enhance the market opportunities as well. A Publish Subscribe system consists of mainly three components: publishers, subscribers and routing nodes called as brokers. It is an information centric paradigm where subscribers explicitly express their interests in any published information. The publication of information is done by the publisher. Also the publication and subscription are decoupled in time and space as they do not have to be synchronized [1] Broker propagates the information to the interested subscriber on the basis of information's availability. Most of the works in PSIRP till date are focused on establishing broker's responsibility to initiate routing, distribution decision and forwarding, thus leading eventually to the delivery of content from publisher to subscriber. Not much of an attention has been given to the access control management at this broker. Access control becomes an important requirement when customers are expected to pay for publish/subscribe services.

In our trust based access control model, the privilege for defining the access levels are given to the publisher where certain constraints will be defined on each information object being published by the publisher in order to establish a desired trust level for the subscriber to get access to the information of his interest. Management of the defined constraints and its associated access levels based on trust are designated to the brokers. Multicasting and caching is however taken as a technique for the delivery of the information between publisher and subscriber which is also responsible for the achievement of performance and efficiency for the future network [1].

The paper is organized as follows; Section II contains few assumptions as the basis of our approach. An approach towards a secure trust based access control model is introduced as the goal of our research work in Section III, Section IV encompasses a detailed mechanisms to describe our access control approach at each participating entity in the publish/subscribe system. Finally Section V briefs about an example usage scenario to demonstrate the real time working of our approach. Section VI describes about related works into this area which inspired us for this vision. Concluding remarks and future possible works are highlighted in Section VII.

1.1 Assumption

Access control is an imperative entity in the information centric network where publishers and subscribers will be in humongous. Without access control there won't be any demarcations between malicious and genuine users and publishers will publish any/all information and subscriber will subscribe to all information. Considering the necessity, following points have been assumed for proposing an effective trust based access control model for future network.

1. Trust is not directly established between the publisher and the subscriber; it is via the broker network through which they both are connected.
2. Trust levels are based on certain defined set of constraints which will associate desired access levels with the information object and will be maintained at the broker's end.
3. Access privileges on the information will be defined by the authentic publisher while publishing it.
4. Nodes in the broker's network will trust each other while transmitting the information object from one end to the other [2].

1.2 Research Goal

Broker is a significant entity in the effective dissemination of information between the publisher and subscriber, thus security at this intermediate element need some considerations. The current PSIRP architecture is a location independent paradigm for the future network, thus it is required to establish trust between the entities which are taking part in the communication rather than establishing trust between the end points. Therefore keeping security as the cornerstone of our research an effective trust based access control approach has been envisaged. The architecture renders a secure mechanism for authenticating and authorizing clients to publish and subscribe to specific type of information content they are interested into. This paper encloses a proposed approach explaining the management of access control imposed on the information object published by the publisher. The Broker provides access to the subscribers after ascertaining their access rights from the knowledge base stored in its access control manager (ACM).

2. RESEARCH METHOD

Broker is a significant entity in the effective dissemination of information between the publisher and subscriber, thus security at this intermediate element need some considerations. The current PSIRP architecture is a location independent paradigm for the future network, thus it is required to establish trust between the entities which are taking part in the communication rather than establishing trust between the end points. Therefore keeping security as the cornerstone of our research an effective trust based access control approach has been envisaged. The architecture renders a secure mechanism for authenticating and authorizing clients to publish and subscribe to specific type of information content they are interested into. This paper encloses a proposed approach explaining the management of access control imposed on the information object published by the publisher. The Broker provides access to the subscribers after ascertaining their access rights from the knowledge base stored in its access control manager (ACM).

2.1. Trust Based Access Control Mechanism

Whilst this paper concentrates on providing a secure access control based on trust, the deployment of an effective access control policy is also required to invoke access control on the information object. This section elucidates the mechanism of establishing a trust based approach for deployment of a secure access control on the information object.

Local broker maintains access control policy for publishers as enforcing access control at the publisher's end will keep the network secured from attacks like DoS attack, attack against routing etc. The broker validates publisher's authority and authenticity with the help of his credentials. Credentials are sent with the message that the publisher wants to publish; the local broker in the publisher's scope validates this credentials with the stored one and grants him the rights according to the access rights defined [3]. In our ideated model along with publication the publisher will also define the potential access type for the information object based on certain constraints. These constraints will ensure the trust level which in turn will grant authority to the subscribers for accessing the information object requested by them.

2.2 At Publisher

Authority of the publisher is defined at its local broker in PSIRP architecture. Publisher can define as many access_types on its published Information Object as it wants. Access_types are based on the kind of services that the publisher wants to offer. Trust_levels are associated with each information object which is tied with specific set of access privileges. The broker monitors only the trust level of the subscriber and allows access based on the established trust. Publisher (P) will define following elements (f) with each information object while publishing it at its local broker (Bp). And broker will finally make the decision (d) =Success (Ns) ∨ Failure (Nf) based on the publisher's authority and access rights.

Step1:- $P \xrightarrow{f} B_p$, f **:** < *IO ID, IO, Metadata, Access_Type, Constraints, Operation, Permission* >

Step2:- $B_s \xrightarrow{d} P$, d: $< N_s \vee N_F >$

Publisher's defined elements can be of following types: *Information Object, metadata, operation, Permission, access type, Constraint*. The corresponding sets are *INFORMATION OBJECT, METADATA, OPERATIONS, PERMISSIONS, and CONSTRAINTS.* We define these factors as follows:

1. An *Information Object (IO)* ∈ *INFORMATION OBJECTS* is a data source or a system resource that a publisher publishes. Each IO is associated with a unique ID i.e. IOID
2. A *Metadata* ∈ *METADATA* contains information about the actual publication. This can be for instance the author of the publication, its size and perhaps a small description of it. [1]
3. An *Operation* (O_n) ∈ *OPERATIONS* is the defined set of actions which will be granted to the subscribers for accessing information object. $O_n \supseteq$ *ACTIONS*, Where *ACTIONS* can be *Read, Download and Upload* etc.
4. *Permission* ∈ *PERMISSIONS* can be defined as an authority to perform any task. It is the subset of *Information Object* x *Operations i.e. Permission*= $2^{(IO \text{ x } On\ )}$. Therefore, a *permission* = {(IO, O_n) | *IO*∈ *Information objects*, O_n ∈ *Operations*}
5. An *Access_Type* is the category under which the information objects will be classified. E.g. *free, paid, confidential* etc. *Access_Type* is the point where constraints will be defined according to the publisher's access policy.
6. *Constraint(C)* ∈ *CONSTRAINTS* are specific conditions defined by the publisher which are required develop trust. Each *Access_Type* is associated with certain set of constraints. Here C is an union of all possible combination of constraints. $C=c_1 \cup c_2 \cup c_3....C_n,$ where c_x is set of constraints assigned to the *Access_Type*. x= 1, 2, 3….n.

2.3 At Subscriber

In order for a subscriber to access a publication, it is required to attain a predefined level of trust with the broker's network. To secure the information from getting accessed by any unauthorized user, a suitable approach for access control is need to be established. Our envisioned trust based access control put forward the idea for assigning some defined trust levels, based on the attributes and credentials provided by the subscriber. Upon these factors, relevant access rights associated with the acquired trust level will be granted to the subscriber.

Subscriber's defined elements can be of following types: *Subscriber_Attribute,* and *Subscriber_Credential*. The corresponding sets are *ATTRIBUTE and CREDENTIALS*. We define these factors as follows:

1. A *Subscriber s* ∈ *SUBSCRIBERS* is an entity or a group of entities which request to access the information object
2. *Subscriber_Attribute* ∈ *ATTRIBUTES* is a collection of certain set of attributes from each Subscriber s. It is denoted by P_u. $P_u = \{p_1, p_2, p_3.....p_n\}$, Where $\{p_1, p_2, p_3.....p_n\}$ can be age, nationality, special group etc. These attributes are required to establish a trust with the system for acquiring specific access rights defined on the information objects.

3. Each *Subscriber S* has certain credentials known as Subscriber_Credential ∈ *CREDENTIALS* (c_u) which will help in providing unique identification for subscribers at the broker's end. cu is assigned to subscriber after acquiring their *ATTRIBUTES* (P_s).
   The Subscriber may generate request at its local broker (Bs) by following ways:

Step1:- $S \xrightarrow{f} B_s$, f :< Subscriber_Attribute, Subscriber_Credential>

Subscriber will provide his credentials and attributes along with the request. Decision for the authenticity of this subscriber at the Bs will be made based on these credentials and attributes. The following set of events can be executed by the subscriber to establish certain trust level with the broker network.

$\{\sim P_s \wedge \sim c_u , P_s \wedge \sim c_u , \sim P_s \wedge c_u , P_s \wedge c_u\}$

1. **~Ps ∧ ~ cu** : Subscriber is not required to provide any credentials and attributes, when he is not requesting to subscribe for any information. Therefore, no trust is established between the two in this case.
2. $P_s \wedge \sim c_u$: While requesting for any information the subscriber is required to establish a trust level with the broker. For acquiring the trusted state subscriber provides some *ATTRIBUTES* (P_u). Therefore, initially subscribers provide only *ATTRIBUTES*. After providing these attributes, subscribers get some *CREDENTIALS* (c_u) based on their attributes. These *CREDENTIALS* help the network to identify each subscriber uniquely.
3. $\sim P_s \wedge c_u$: There are possibilities that an illegitimate subscriber tries to communicate and access any critical information for which he is not authorized. Thus, in this case the subscriber can try to access information by providing only some random *CREDENTIALS* (c_u).
4. $P_s \wedge c_u$: In order to establish a positive trust, the broker demands subscriber to provide both *ATTRIBUTES* and *CREDENTIALS* to get the access for desired information object.

This request will be destined eventually at the broker where information object lays i.e. local broker at publisher's end (B_L).

Step2:- $B_L \longleftarrow B_s$

2.3 At Broker

As described above, broker is an intermediate or a rendezvous for publisher and subscriber, also known as the rendezvous point (RP). Access control can be implemented at the edge of this broker network; because we assume that all brokers can be trusted to enforce the access control policies correctly [2]. Therefore the access control information will be updated and stored in the cache of each intermediate broker node. Each node in the broker network will maintain an access control manager (ACM) for storing and managing the access rights which has been defined on the IO by the publisher.

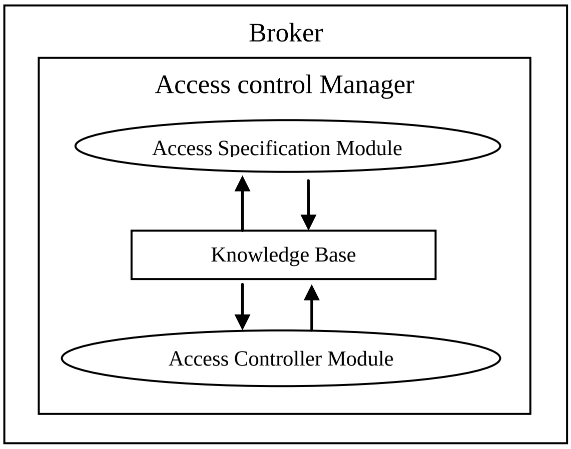

Figure1. Components of Access Control Manager

Access Specification Module is the interface for publisher, which will initially receive the information object along with its associated factors (f) and direct it to the knowledge base for storage. Access Controller Module is an execution entity, which will act as an interface to receive queries for accessing information object from the subscribers and will direct these queries to the knowledge base. Each broker will maintain a Knowledge Base, which is represented by notation. KB, consist of Pus∪Cp where Cp is the publisher's defined constraints and Pus is subscriber's credentials stored at the broker.

Access control in the proposed approach depends upon the trust level which would be attained after satisfying all the defined constraints at the broker's level. The TRUST_LEVEL will be represented by a set of real numbers {-1, 0, 1} at particular instance.

- +1 refers to a positive trust level in which the credentials and attributes of subscriber will be successfully matched with the stored credentials and constraints.
- 0 refers to a neutral trust level in which either credentials or attributes are not provided by the user, so the broker can request for either of these two to take further decision on trust establishment.
- -1 refers to a negative trust level in which the credentials and attributes of subscriber are not found while matching it with the stored credentials and constraints, so the subscriber fails to develop trust with the broker.

Thus, after receiving request from the subscriber, Broker will match the provided subscribers' credential and attributes against cu and Ps stored in KB and establish trust based on the value of trust_level from the set of {+1, 0, -1}. The information from the publisher's local network will be routed to the broker who is present in the subscriber's scope via a trusted path. It is assumed that the brokers in the routing path will trust each other and no malicious node is there in between the routing path inside the broker network. Decision for TRUST_LEVEL at the broker's end will be made based on the constraint defined and attributes and credentials defined by the subscriber.

$$\begin{cases} +1 \quad \text{if } (\mathscr{P}_{\mathrm{u}} \in \text{set of } \mathscr{P}_{\mathrm{us}} \text{and } C_u \in \text{ set of } C_p) \\ 0 \quad \text{else if } (\mathscr{P}_{\mathrm{u}} \notin \text{set of } \mathscr{P}_{\mathrm{us}} \text{ or } C_u \notin \text{ set of } C_p) \\ -1 \quad \text{else } (\mathscr{P}_{\mathrm{u}} \notin \text{set of } \mathscr{P}_{\mathrm{us}} \text{and } C_u \notin \text{ set of } C_p) \end{cases}$$

In case of positive-trust, Information object will be forwarded to the subscriber via its local broker and access privilege will be given to the subscriber based on trust and constraints which permits certain operation.

Step3:- $B_L \longrightarrow B_s$ *<IO ID, IO, Metadata, Access_Type, Operation, Constraint>*

Step4:- $B_s \longrightarrow S$ *<* N_s V N_F*, IO ID, IO, Operation, Constraint >*

2.4 Exclusive Case

In several exclusive cases instead of applying the access control on the information object as a whole, the publisher can define it on some explicit part of that information object. We ideate that the access rights and its associated trust levels can be defined on certain defined range of bytes on the information object. This approach fragments the information into small chunks of different byte ranges coupled with different access rights and trust levels.

$IO= \{IO_1 \wedge IO_2 \wedge IO_3 .... \wedge IO_n\}$

These byte ranges are specified with the metadata of each information object (IO), therefore when the access requirement is generated from the subscriber's end, these byte ranges are matched with the byte range on the information object and is presented to the subscriber, according to the access privilege and trust level attained by the subscriber for that particular chunk of information. Suppose a publisher wants to make some part of an information object free for public access, that part of the information object will be separated from the other part of it with the help of byte range and will be stored in the knowledge base at the broker's end as shown:

IO_1

$IOID_1$
Access_Type: Public
Constraint: NULL
Byte_Range:b1……..bn
Operation: $O_n \supseteq$ACTIONS

IO_2

$IOID_2$
Access_Type: Confidential
Constraint: $c_x \in C$
Byte_Range :bn……..bx
Operation: $O_n \supseteq$ACTIONS

Figure 2. Representation of access rights on IO chunks based on the byte range.

The above explained mechanism is further explained with the help of an example usage case in the continuing sections of this paper.

3. Results And Analysis

3.1 Example Usage Scenario:

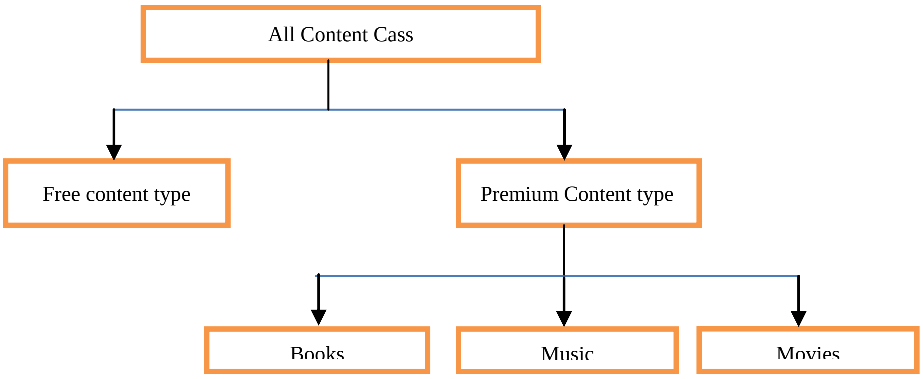

Figure 3. Example of content class hierarchy in DLS system to implement trust based access control [3].

The above described trust based access control model can be explained by formulating a real time implementation mechanism. In this paper, we are taking Digital Library System (DLS) as an example to explain the implementation procedures of the above explained model. The access rights are based on the content of the information object or subscription [4].

3.2 Mechanism

The contents of a DLS are categorized into different content types and each content type is associated with a trust level. Subscribers who attain this defined trust level are authorized for the access of that information. As shown in the following figure, Publisher bifurcate the entire content class into *free content type* and *premium content type*. Both content types offer certain level of access privileges. In order to access *free content type*, no trust level is required to be established by the subscriber. Free content type offer limited operations (view) only. Free content type contains services like access *to read {magazines, newspaper, movie reviews}*. Access to *premium content type* requires certain trust level to be attained by the subscriber interested in accessing this information. The mechanism of establishing trust can be explained by following steps:

UserA expresses her interest in accessing a book named XYZ, which is the publication of User B. In this scenario UserB is the publisher who will provide the services to access book from the DLS belonging to him. With the objective of accessing XYZ, UserA generates a query at the local broker in her scope. The broker in turn provides metadata to the UserA. When with the help of metadata UserA tries to access XYZ, she gets two classes of content types. *Free content_type* will provide the list of the books, In order to further access the book, UserA will have to attain a definite trust level which requires her to fulfil certain constraints.

These constraints are defined by the Publisher (UserB). Here a constraint is defined on the Premium content type that a *credential c_u i.e. Username and Password* is required to get the access privilege for the premium content type. c_u will be provided on the basis of the subscriber's attributes (P_u) which are required during the registration process. P_u can be age, nationality, gender etc. After registration the user will attain a trust level which is required to access XYZ. Now further if she wants to access any other book which falls in the category "adult", another constraint will come into action, which will match the registered attribute (Age) stored in the broker's *Knowledge Base*. UserA will be granted access after attaining a positive trust level based on the above constraint.

3.3 Related Work

Our approach is inspired by Sudip Chakraborty and Indrajit Ray's trust based access control model in Open systems [3]. We ideate a similar approach for implementing access control in PSIRP to provide a secure architecture for Information Centric Networking. So far not much of an attention has been given on the security perspectives of Information centric networking. Eric Renault, Ahmad Ahmad and Mohamed Abid proposed an approach for access control, based on public-private key where the access verification is performed by a Security Controller which is operating on the data of NetInf to check the access rights for both IOs (Information Object) and DOs (Data Object) [5]. Each Access type is associated with IO along with a public key. If public key is not present, and then the access is open to all. In contrast, our approach is based on trustworthy subscriber's credentials to implement access control on information object.

Lauri I.W. Pesonen, David M. Eyers, and Jean Bacon in their work proposed a multi domain Publish /Subscribe system, where each domain contains number of event clients, brokers and access control services. The Access Control Service [ACS] is responsible for granting privileges to the brokers and the clients (Publisher and subscriber) in that domain according to the domain's internal access control policy [7]. Since, this envisioned approach is based on encrypted event content, thus the broker can only access a specific content event, if it has access to the encryption key. On the other hand, in this paper, our approach is to provide trust based access control for Publish/Subscribe system; here broker is responsible for implementing and providing access rights. Broker stores the access credentials and constraints in its Knowledge Base in order to establish and verify a relative trust level, based on which the access privileges are granted to the subscribers. The access related information is periodically updated among neighbour brokers if the trust is already established.

4. CONCLUSION

Although information availability is one of the main ideas of ICN, but security, privacy and trust are some of the critical issues that can't be overlooked. In order to avail the content from the publisher, the subscriber will have to establish certain trust with the broker because it is the rendezvous where the publisher will define access control policy on the published information object. This trust level will be associated with constraints based on which a relevant access right will be provided. In this paper we have proposed a secure access control mechanism which is a part of overall security at the broker's end. The hybrid approach described in Section 3 will assure all the concerns of ICN related to trust, privacy and security along with ensuring the availability of information on demand. However the proposed approach will ensure information's availability based on certain access control policies defined by the publisher at its local broker in the broker's network. Since different publisher's will have different labels of definition for their policy which will give rise to many complexity at the broker level in managing these policies. Thus an effective solution can be developed where a standard approach can be envisaged for defining access control policy at the broker's level.

The security and its overhead are interwoven issues, if we want to increase security then overhead of processing and storage will also increase. To reduce this overhead, efficient hardware, software and algorithms are required which would become part of network and reduce complexity. Our future work will be concentrated on establishing a secure and robust mechanism for the transmission of access credentials in the distributed environment of ICN.

REFERENCES

[1] Ali Ghodsi, Teemu Koponen, Barath Raghavan, "Information-Centric Networking-Seeing the Forest for the Trees", ACM SIGCOMM Workshop on Hot Topics in Networks (HotNets-X), November 2011

[2] Zoltan Miklos, "Towards an Access Control Mechanism for Wide-area Publish/Subscribe", Technical University of Vienna, Distributed Systems Group, 2002, pp. 2-3.

[3] Indrajit Ray and Sudip Chakraborty, “A Framework for Flexible Access Control in Digital Library Systems". In Proceedings of 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec'06), volume 4127 of Lecture Notes in Computer Science, pages 252-266, SAP Labs, Sophia Antipolis, France, July 31-August 2, 2006. [Acceptance ratio: 22/55].

[4] Nikolaos Fotiou, George C. Polyzos, Dirk Trossen,”Illustrating a Publish-Subscribe Internet Architecture Systems”, pp. 1-2.

[5] Éric Renault, Ahmad and Mohamed Abid Évry, “Towards Security Model for the Future Network of Information, 2009, pp2.

[6] Petri Jokela (LMF), Janne Tuononen (NSNF), Jimmy Kjällman (LMF)"Final Description of the implementation", http://www.psirp.org/

[7] Lauri I.W. Pesonen,Jean Bacon, David M. Eyers "Encryption-Enforced Access Control in Dynamic Multi-Domain Publish/Subscribe Networks", June 20-22, 2007, Canada, ACM Press, pp 104—115.