ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 6, June 2013

Implementing Trust Negotiations In Multisession Transactions

S.Seetha[1], M.Ramamoorthy[2]

[1]PG Scholar, Dept of CSE, Sri Lakshmi Aammal Engineering College, Chennai,
[2]Asst.prof. Dept of CSE, Sri Lakshmi Aammal Engineering College, Chennai,

Abstract— **A trust negotiation is a mutual attribute-based authorization protocol between two entities. Trust Negotiation is an approach to regulate the exchange of sensitive information during this process. The proposed framework is a multisession dependable approach to trust negotiations. This framework supports voluntary and unpredicted interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. The Trust-x protocol addresses the issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators. A peer is able to suspend an ongoing negotiation and resume it with another (authenticated) peer. Negotiation portions and intermediate states can be safely and privately passed among peers, to guarantee the stability needed to continue suspended negotiations. Detailed analysis has been depicted on Trust-x protocol which has several key properties, including validity, correctness, and minimalist. This system also withstands the most significant attacks. An ontology environment is also proposed to provide formal specification of concepts and their interrelationships. This is very essential in complex web service environments. It possesses the purpose of sharing information about credentials and their attributes, needed for establishing trust.**

Keywords- Security and management, dependability, trust negotiations, access control, ontology.

I. INTRODUCTION

Trust negotiation is a mechanism supporting complex, distributed, rule-based access control for sensitive information and resources, through the controlled release of credentials. A trust negotiation is a mutual attribute-based authorization protocol between two entities.

The main focus of Trust Negotiation is an approach to gradually establishing trust between

strangers online through the iterative exchange of digital credentials. In contrast to a closed system, where the interacting entities have a preexisting relationship (often proved by typing a username and password), and trust negotiation is an open system, and complete Strangers can build trust in one another. This is done by disclosing digital credentials.

Digital credentials are the computer analog to paper credentials, such as a driver's license, credit card, or student ID. Rather than proving the credential owner's identity, digital credentials assert that their owner possesses certain attributes. A student might receive a credential from his or her university that certifies that they are a student at that university. The student could then use that credential, for example, to prove they are a student in order to qualify for a student discount at an online bookstore. Credentials are digitally signed in order to allow third parties to verify them.

The scope of this project is to build trust negotiations that offer a general solution for secure transactions. The core of our approach is a trust negotiation protocol supported by the Trust-X system. This protocol, referred to as multisession trust negotiation, involves the exchange of digital credentials protected by rule based disclosure policies (referred to as disclosure policies)which make it possible for two (or more) peers to establish mutual trust, so to carry on tasks such as the exchange of sensitive resources or access to a protected service. And by this it supports crash recovery and the possibility of completing the negotiation over multiple sessions in secure manner.

II. RELATED WORK

The existing trust negotiation systems, however, do not currently support any form of suspension or interruption, and do not allow the negotiators to be replaced (or delegated) while the negotiation is ongoing. Interruptions in ongoing trust negotiations can be the result of external, unforeseeable events (e.g., parties' crashes, faulty transmission channels), or decisions by the involved parties. A party

may not be able to advance the negotiation for temporary lack of resources. Or the party may not have readily available the credentials required by the counterpart, although eligible to them.

Typically, these approaches rely on strong cryptographic assumptions, and are seldom applicable in many real-world scenarios, where properties, stated in digital credentials, actually need to be disclosed in clear and not only proved to be true. For example, just proving the possession of a valid credit card is not sufficient to complete a transaction, and actual account information is to be supplied in order to enable charging the amount spent. Additionally, protocols that rely on oblivious credentials or anonymous credentials do not allow parties to follow the progress of the negotiation, since information regarding policies satisfaction is hidden for confidentiality purposes. It is thus crucial to extend trust negotiation protocols along several dimensions.

- Negotiations may last a considerable time span and the involved parties may not be able to support long negotiations.
- Party may not be able to advance the negotiation for temporary lack of resources.
- Once such a credential is disclosed, it cannot be reused. Hence, completing a negotiation in which such type of credential is used becomes crucial.
- Interrupted negotiations however represent not only undesired events, but also vulnerabilities that could facilitate malicious attackers' eavesdropping and other behavior.

III.PROPOSED SOLUTION OF TRUST NEGOTIATION

Ontologies provide a formal specification of concepts and their interrelationships and play an essential role in complex web service environments.
It will help to, the data are retrieved correctly and the relationships between the objects are found

Ontologies in Trust Negotiation

- In trust negotiations Ontologies have the purpose of sharing information about credentials and their attributes, needed for establishing trust.

Concept as tuple C= <Keyword Set, Lang set>

⇩ ⇩

Set of Keywords Set of Attributes

- Each attribute in Lang Set implements concept C

- We make use of a Translation function to compare values of two semantically equivalent attribute conditions

- We assume that there are a number of finite well-defined concepts in the ontology.
- A same concept can be implemented by alternative credentials/attributes

E.g:

<{sex,gender}{passport.gender,drivingLicence.sex}>

⇩ ⇩

Keywords Set of alternative attribute names and/or credentials

Property-based policies

- A property based policy lists the properties the counterpart has to provide and the conditions it must satisfy in order to obtain some resources
  - (loan,{MaritalStatus,Country}, {country=USA})
- Disclosure policies implement property based policies by associating credential/attribute names to concepts
  - Loan,←Marriage Certificate(),id_card(country=USA)},
  - Example:
- R ←Marriage Certificate (), id (age > 25).
  To satisfy this disclosure policy, the subject can either provide the disclosure set

DSet_1 = {Marriage Certificate, id.age, id.country}
DSet_2 = {Marriage Certificate, id.age}

- The subject will provide DSet_2 if it can blind all other attributes of id. The subject may provide DSet_1 if the most blinded view containing age also reveals id.country.

IV.IMPLEMENTATION OF TRUST NEGOTIATION

Negotiation Tree Switching Process

Negotiation Tree setup

In this module to implement a Negotiation tree (NT) which is a data structure that keeps track of negotiation process. Initially the tree is routed between the nodes formally modeled as T= {N, R, E} where N denotes the set of nodes, R denotes the root of the tree, and E the set of Edges .Each node is appended in the tree according to the policies and the dependencies of the nodes. The NT is rooted from the requested source and is initialized when the negotiation starts.

Negotiation Tree Transaction

The transaction of the negotiation tree is based on two phases-policy evaluation phase and credential evaluation phase. Negotiation is initiated from the policy evaluation phase, and once the policy evaluation phase is completed then the credentials are disclosed during the credential exchange phase. The transaction of tree is done by multi edge links (several simple edges) in which each node consist of policy rules. NT consist of two states- deliv state and open state where the deliv state denotes a delivery resource, that is, a node is ready to deliver credential . And the open state denotes that node is not yet ready for delivering the credential. During negotiation, save points are employed to save the negotiation state, validity checks concerning events which may happen during the negotiation suspension. The transaction completion of policy evaluation phase is signaled by a portion of the tree rooted at the requested resource by the deliv state that we refer to as valid view.

Negotiation, Suspension, and Nodes Commitment Process

In this module, the negotiation suspension and nodes commitment is done. When particular peer suspends the transaction it will redirect the transaction to another node which will resume the negotiation. For every node in the pruned negotiation tree, peer computes the corresponding committed nodes. If either an interruption or a suspension occurs for a few negotiation rounds, the peers will periodically update their committed versions of the tree.

Tree Splitting and Sharing with Security

In this module to implement the splitting and sharing of negotiation tree. When the negotiation is suspended during the policy evaluation phase or credential evaluation phase by P2, P2 serializes the negotiation tree and generates the encrypted version of credentials. This serialized version(S) of the tree is used as an input for the secret sharing scheme, where P2 splits S into (S1, S2, S3…. Sn) and distributes these shares to its trusted nodes and process will be resumed only by the trusted peer.

Multisession Negotiation

In multisession negotiations it allows negotiations to be conducted within multiple separate sessions. Consider negotiations between two peers, say P1 and P2, if there is an interruption in P2 the negotiation gets suspended and P2 processes the NT tree in order to hand it to another peer, to resume the negotiation, by pruning the delivery nodes from NT and it is resumed by different peers. For example, P2 can be replaced by peers, provided that the replaced or delegated peer (e.g., (P3…Pn)) has the ability to complete the previously started negotiation.

Tree Recovery Process

When the peer P3 is selected, it builds its version of negotiation tree from the commit and builds its credentials.P2 sends the novel negotiation tree to P3 and then P3 resume the negotiation. So by this the negotiation gets started and encrypted credentials are sent from P2 to P3 $Cred_i$, P2 sends the corresponding keys to P1 to decrypt the credentials.

Sharing the Trust Sequence

MS Protocol for Credential Exchange

In this module, MS protocol is implemented to exchange the credentials in a secure manner by encryption. Consider peer P1 and peer P2 are going to exchange credentials based on the particular terms. During the credential evaluation phase P2 has lost communication with P1.So it redirects the transaction by distributing the credentials to its trusted peers (P3,P4,….P N) after encrypting the credentials by a key k. And P2 sends this key to P1 to decrypt the credentials. If P3 is the first peer responded to P2, P2 will send the P3 ID to P1 and now P1 and P2 reconstructs the sequence, and exchange the remaining credentials. Based on the corresponding terms stored in the C seq, P3 is able to verify the validity of each credential and whether or not it satisfies the corresponding term. And P3 at its end sends sequentially the P2 encrypted credentials to P1, which can verify them by using the key k s obtained by P2.

System Architecture

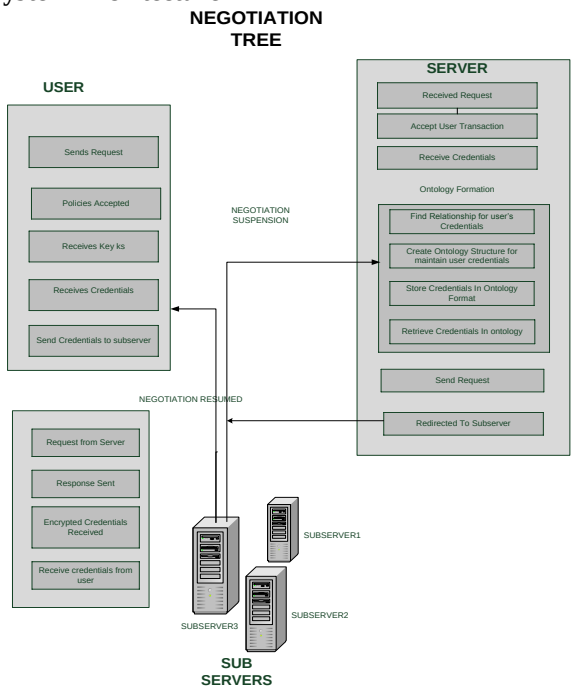

Fig 1: System Architecture

Ontologies in Trust Negotiations

Usually TN(Trust Negotiations) requirements are specified by means of credentials:

- Digitally signed documents containing attributes that describe properties of the subject.

- Instances of credential types

Credential types provide a syntactic structure of information but do not specify anything about the interpretation of the attributes contained in the credential types.

The lack of semantic in credentials/attributes makes it impossible to automatically detect relationships between attributes belonging to different credentials.

To solve this problem of semantic conflicts, introduce the use of ontologies

V.CONCLUSION

The proposed solution is found to be very effective by using ontology. The system carry on tasks such as the exchange of sensitive resources or access to a protected service using multisession trust negotiation, negotiation portions, intermediate states can be safely and privately be transferred among peers. It also provides a mechanism for recovering from data losses which may occur at one of the involved peers. So, we have carefully considered all possible issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators. To solve this problem of semantic conflicts with the help of introducing ontologies in trust negotiations.

ACKNOWLEDGEMENT

We wish to express our sincere thanks to all the staff member of CSE Department, Sri Lakshmi Aammal Engineering College for their help and cooperation.

REFERENCES

[1] A. Hess, J. Jacobson, H. Mills, R. Wamsley, and B.Smith, “Advanced Client/Server Authentication in

TLS," Proc.Network and Distributed System Security Symp. (NDSS), 2002.
[2] A.C. Squicciarini, A. Trombetta, E. Bertino, and S. Braghin, "Identity-Based Long Running Negotiations," Proc. Fourth ACM Workshop Digital Identity Management, 2008.
[3] Anna C. Squicciarini, Elisa Bertino, Fellow, IEEE, Alberto Trombetta, and Stefano Braghin, "A Flexible Approach to Multisession Trust Negotiations" IEEE Transactions on dependable and secure computing, January/February 2012.
[4] E. Bertino, E. Ferrari, and A.C. Squicciarini, "Trust Negotiations: Concepts, Systems and Languages," Computing in Science Eng.,vol. 6, no. 4, pp. 27-34, 2004.
[5] E. Bertino, E. Ferrari, and A.C. Squicciarini, "Privacy-Preserving Trust Negotiation," Proc. Fourth Privacy Enhancing Technologies Workshop, May 2004.
[6] E. Ferrari, A. Squicciarini , E. Bertino, "X-tnl: An Xml Language for Trust Negotiations," Proc. IEEE Fourth Workshop Policies for Distributed Systems and Networks, June 2003.
[7] K.E. Seamons, M. Winslett, and T. Yu, "Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation," Proc. Network and Distributed System Security Symp. (NDSS), 2001.
[8] T. Yu and M. Winslett, "A Unified Scheme for Resource Protection in Automated Trust Negotiation," Proc. IEEE Symp.Security and Privacy, pp. 110-122, 2003.
[9] T. Yu, K.E. Seamons, and M. Winslett, "Protecting Privacy During on Line Trust Negotiation," Proc.Second Int'l Conf. Privacy Enhancing Technologies, Apr. 2002.
[10] W.H. Winsborough and N. Li, "Towards Practical Automated Trust Negotiation," Proc. Third Int'l Workshop Policies for Distributed Systems and Networks (Policy '02), pp. 92-103, June 2002.
[11] W. Hu, N. Jian, Y. Qu, and Y. Wang, "Gmo: A Graph Matching for Ontologies," Proc. Workshop Integrating Ontologies, 2005.
[12] World Wide Web Consortium "OWL Web Ontology Language,"http://www.w3.org/TR/owl-ref/, 2004.