Secret Sharing in Multisession Using Peer Head Authority

S.Pavithra, R.Jeyanthi

ABSTRACT*:* **Trust negotiation is a mechanism supporting complex, distributed, rule-based access control for sensitive information and resources, through the controlled release of credentials. It is also a mutual authorization protocol between two entities. Here we proposed multisession trust negotiation which involves exchange of digital credentials protected by rule based disclosure policies which make it for two or more peers to establish mutual trust, A peer is able to suspend an ongoing negotiation and resume it with another authenticated peer. But the peer can also be un trusted so to select the authenticate peer we propose Trusted peer head Authority. By using server Selection algorithm we select the trusted peer. Due to this proposed frame work that it supports crash recovery and the possibility of completing the negotiation over multiple sessions negotiation portions and intermediate states can be safely and privately be transferred among peers.**

Keywords: Trust Negotiation, Security and management, access control

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, 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 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 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 [5].

II. BACKGROUND 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 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. In many real-world scenarios, properties states that in digital credentials, actually need to be disclosed in clear .While considering an example, 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. Moreover, 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. 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 [9].

III. MULTISESSION TRUST NEGOTIATION

If A is going for payment it has to fill the credit card details and proceed or it want to suspend the operation then A requires some credentials from B1. Before generating the credential B1 ask A to enter a secure 4 digit pin number, which is going to use for verification process. Once A enter the pin number. Now B1want to suspend so it pass the process to B2 again B2 is selected by trusted peer head which will create the credentials and send it to the A through SMS. Once B1 is collected the coupon and calculate the amount, it will send to A, Now A can able to go for payment or suspension process. If A is going for payment he has to fill his credit card details and proceed or he wan to suspend the operation then A requires some credentials from B1. Before generating the credential B1 ask A to enter a secure 4 digit pin number, which is going to use for verification process. Once A enter the pin number B1 pass the process to B2 which will create the credentials and send it to the A through SMS. Then A can able to end the session. When A is next time entering it is not necessary for A to select the movie and produce the coupon etc, just he can enter into multi-session option and produce the credential which was previously generated he can able to proceed in the transaction where he left early.

IV. IMPLEMENTATION OF PEER HEAD

A client request a movie coupon to b1 .First the request is send to peer head that is trusted head which has every confidential details about servers in that particular location. Now the request is forwarded to B1 requests from A the coupon and the amount of e-cash required to buy the movie. Once B1 is collected the coupon and calculate the amount, it will send to A, Now A can able to go for payment or suspension process. In figure 1, the implementation of movie downloading can be given.

A.Trusted Authority for Peer or Peer Head

Suppose Attacker can be hacked by other server and it can be used for communication in the name of original server. They can easily prepare the similar certificates of original. So overcome these problem Trusted Peer Head.

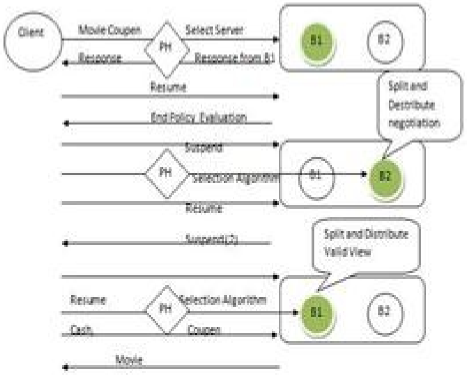

Fig1Movie Downloading

B1, B2	-	Server
Colored Round	-	Active Server
A	-	Mobile Device
PH	-	peer Head

B.Key Exchange & Network Formation

This network consists of trusted authority and N-number of Nodes. A Node enter into the Network, trusted authority checks the node , sign in node's certificate and collect the public key of that node and share with other nodes. Every node has Public Key and Private Key.

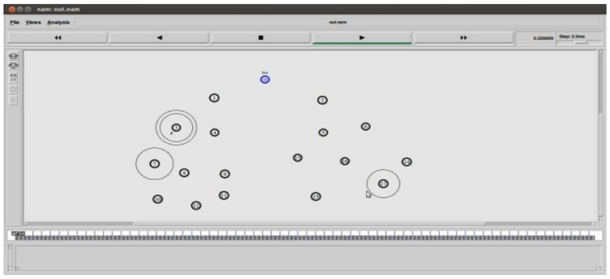

Fig 2 no of nodes created

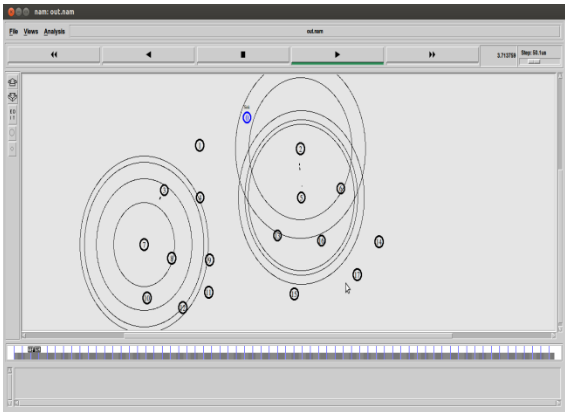

Fig3 server select the neighbor node

C.Trusted-x peer protocol with multisession Negotiation

Multisession negotiations which allow negotiations to be conducted within multiple separate sessions. In the multisession protocol, it does not require both parties to maintain an up-to-date copy of the negotiation state at the time of suspension. It does not imply going back to client-server architecture. Parties are still peers, and able to control the negotiation process, however the task of storing the negotiation data at suspension time Can be assigned to one of the two parties. Important extension is to allow negotiations to be completed by multiple peers. The negotiations between two peers, say P1 and P2, to be suspended and then resumed by different peers. For example, P2 can be replaced by P3, provided that the replaced— or delegated—peer [10] P3 has the ability to complete the previously started negotiation. The suspend and resume protocols work with only one delegate at time.

D.Trusted Authority for Peer and Peer Head

Peer Head (P.H) is to Verify and Authenticate for communication during the Trusted Multisession Negotiation. It is used for authenticate mobile device and peer communication. Because Mobile device or other communication device hack to the server. So we can use Peer Head and Trusted Authority.

V. CONCLUSION

The proposed solution is found to be very effective by using trusted authority of peer to peer head to prevent attacks. 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. Some issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators is also considered.

REFERENCES

[1] A. Hess, J. Jacobson, H. Mills, R. Wamsley, and B.Smith, “Advanced Client/Server Authentication inTLS,” 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, “Privacy-Preserving Trust Negotiation,” Proc. Fourth Privacy Enhancing Technologies Workshop, May 2004.

[5] S.Seetha,M.Ramamoorthy”Implementation of multisession trust negotiation” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 6, June 2013

[6] K.E. Seamons, M. Winslett, and “Limiting the

ISSN: 2278 – 1323

Disclosure of Access Control Policies during Automated Trust Negotiation," Proc. Network and Distributed System Security Symp. (NDSS), 2001

[7] S.Seetha,M.Ramamoorthy"Implementation of multisession trust negotiation" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 6, June 2013K.E. Seamons, M. Winslett, and "Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation," Proc. Network and Distributed System Security Symp. (NDSS), 2001.T. Yu and M. Winslett, "A unified scheme for Resource Protection in Autompp. 110-122, 2003.

[8] T. Yu, K.E. Seamons, and M. Winslett, "Protecting Privacy During on Line Trust Negotiation," Proc.Second Int Conf. Privacy Enhancing Technologies, Apr. 2002.

[9] 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.

[10] Anna C. Squicciarini, Elisa Bertino, Fellow "A flexible approach to multisession trust negotiation" IEEE transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012