ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Framework for Secret Sharing In Multisession Trust Negotiation

S. Pavithra[1], R. Jeyanthi[2]

PG Student, Dept of CSE, Sri Vidya College of engineering and technology, Virudhunagar, Tamilnadu, India[1]

Asst. Prof. Dept of CSE, Sri Vidya College of engineering and technology, Virudhunagar, Tamilnadu, India[2]

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 (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. EXISTING SYSTEM

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. RELATED WORK

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 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. If A is going for payment he has to fill his credit card details and proceed or he wants 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.

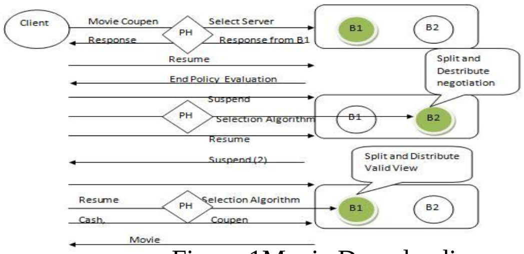

Figure 1Movie Downloading

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

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. PROPOSED SOLUTION OF TRUST NEGOTIATION

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.

V. IMPLEMENTATION OF TRUST NEGOTIATION

1. Key Exchange & Network Formation:

Our Project 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.

2. Trusted-x peer protocol with multisession Negotiation:

Two major features to trust negotiation protocols:

First, we support multisession negotiations that are we allow negotiations to be conducted within multiple separate sessions. We depart from the assumption of atomic trust negotiations In Order to make the negotiation also suitable for peers with heterogeneous capabilities. In the multisession protocol, we do not require both parties to maintain an up-to-date copy of the negotiation state at the time of suspension. Relaxing such assumption does not imply going back to client-server architecture. Rather, parties are still peers, and therefore 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.

Second, important extension is to allow negotiations to be completed by multiple peers. Essentially, we now allow 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 (e.g., P3 has the ability to complete the previously started negotiation. We do not expect peers to be replica one of another. Our suspend and resume protocols work with only one delegate at time. That is, we do not consider the case in which a negotiation may be resumed by more than one (possibly conflicting) delegate.

3. 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.

VI. 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. So, we have carefully considered all possible issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators.

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] E.Ferrari, A.SquicciariniE.Bertino,X-tnl: An Xml Language for Trust Negotiations," Proc. IEEE Fourth Workshop Policies for Distributed Systems and Networks, June 2003.

[6] K.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.

[7] 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.

[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.