Volume 4, No. 10, Sep-Oct 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Novel and Flexible Approach to Trust Negotiations

G. Ramachandran, Dr. K. Selvakumar
Department of Computer Science & Engineering,
Annamalai University, Tamil Nadu, India.
gm_rama@yahoo.com, kskaucse@yahoo.co.in

Abstract **-** Within the progress of society today Current real applications require flexible approaches to trust negotiations, especially in light of the widespread use of mobile devices. Moreover the ubiquitous nature of online peer-to-peer systems, and the increasing number of moving objects involved in online transactions, negotiators must be allowed to switch roles to guarantee dependability, availability of resources and peers. Existing method mostly focused on the assurance of privacy and confidentiality with the goal of guaranteeing that no actual information about a negotiator's properties is disclosed. In this paper, we introduce a novel approach to trust negotiations that offers a general solution to those issues by developing major extensions to previous approaches by presenting a multi session dependable approach to trust negotiations. This proposed framework supports voluntary and unpredicted interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. In our approach the protocols address issues related to validity, temporary loss of data, and extended unavailability negotiators. For increasing robustness and efficiency we showed how our negotiation protocol can withstand in most significant attacks.

Index Terms- trust negotiations, multi session dependable approach, key properties, and Trust-X certificates.

I. INTRODUCTION

Trust-X certificates describe qualifying properties of the negotiating parties. Such certificates are collected into X-Profiles, which are associated with each Trust-X party. Digital credentials are assertions describing one or more properties of a given subject, certified by trusted third parties. A Trust-X negotiation consists of a set of phases to be sequentially executed. The idea is to disclose policies at first, in order to limit credential release, and then disclose only those credentials that are necessary for the success of negotiation. The key phase of a Trust-X negotiation is the policy evaluation phase, which consists of a bilateral and ordered policy exchange. The goal is to determine a sequence of credentials, called trust sequence, satisfying disclosure policies of both parties. Once a trust sequence has been determined, the credential exchange phase is executed.

Each time a credential is received, the local compliance checker module checks local policy satisfaction and verifies at runtime the validity and ownership of the remote credentials. Trust negotiation in the Peer Trust approach to automated trust establishment, trust is established gradually by disclosing credentials and requests for credentials, an iterative process known as trust negotiation. The main aspects of trust negotiations are: 1. Trust between two strangers is established based on parties' properties, which are proven through disclosure of digital credentials.2. Every party can define access control and release policies (policies, for short) to control outsiders' access to their sensitive resources. These resources can include services accessible over the Internet, documents and other data, roles in role-based access control systems, credentials, policies, and capabilities in capability-based systems. 3. In the approaches to trust negotiation developed so far, two parties establish trust directly without involving trusted third parties, other than credential issuers. Since both parties have policies, trust negotiation is appropriate for deployment in a peer to peer architecture, where a client and server are treated equally.

Instead of a one-shot authorization and authentication, trust is established incrementally through a sequence of bilateral credential disclosures. A trust negotiation is triggered when one party requests to access a resource owned by another party. The goal of a trust negotiation is to find a sequence of credentials (C1, . . . ,Ck,R), where R is the resource to which access was originally requested, such that when credential Ci is disclosed, its policy has been satisfied by credentials disclosed earlier in the sequence—or to determine that no such credential disclosure sequence exists. In practice, trust negotiation is conducted by security agents who interact with each other on behalf of users. A user only needs to specify policies for credentials and other resources. The actual trust negotiation process is fully automated and transparent to users. Policy Base, storing disclosure policies, the X-Profile associated with the party, a Tree Manager, managing the negotiation tree.

The system also includes a Compliance Checker**,** testing policy satisfaction and generating request replies, and a Strategy Manager, in charge of dynamically selecting the negotiation strategy and managing the messages exchanged during negotiations, according to the adopted remote and local strategies. The compliance checker also checks local policy satisfaction and verifies at runtime the validity and ownership of remote credentials. The goals of the system components are essentially to support policy and credential exchange and to test whether a policy is satisfied. In addition to the above elements a set of modules for the management of privacy policies is included. One of simplest and common methods which are defined in the existing condition, trust negotiation is a mechanism supporting complex, distributed, rule-based access control for sensitive information and resources, through the controlled release of credentials [10].

A trust negotiation is a mutual attribute-based authorization protocol between two entities. Parties are assumed to be strangers who need to establish trust on the fly in order to exchange resources, information, or services [13]. Current real applications require flexible approaches to

trust negotiations, especially in light of the widespread use of mobile devices. Consider, for example, mobile clients negotiating accesses to services hosted on servers' clusters: negotiations may interrupt due to communication channel fault or may be voluntarily suspended, to be resumed under more favorable conditions. Mobile devices need to be able to seamlessly migrate from different physical servers belonging to the same service provider. Also, negotiations may last a considerable time span and the involved parties may not be able to support long negotiations [16].

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 [17].Trust negotiation research has mostly focused on the assurance of privacy and confidentiality with the goal of guaranteeing that no actual information about a negotiator's properties is disclosed to the counterpart [14], [12], [2]. 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 [8]. 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 obvious credentials or anonymous credentials do not allow parties to follow the progress of the negotiation, since information regarding policies satisfaction is hidden for confidentiality purpose [6], [7], [8], [11].

These aforementioned solutions although successfully applied they still suffer from the following reasons. 1) Existing systems do not currently support any form of suspension or interruption.2) Existing systems do not allow the negotiators to be replaced (or delegated) while the negotiation is ongoing. To overcome these problems we employed a multi session trust negotiation. The core of proposed approach is a trust negotiation protocol supported by the Trust-X system. This protocol, referred to as multi session 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 as to carry on tasks such as the exchange of sensitive resources or access to a protected service.

The main innovative feature of proposed protocol is that it supports crash recovery and the possibility of completing the negotiation over multiple sessions. To support the execution of multi session negotiations, we extend the original Trust-X conventional negotiation steps. Save points are employed to save the negotiation state, validity checks concerning events which may happen during the negotiation suspension and could possibly invalidate the negotiation steps executed before the suspension. Examples of those events include credential revocation or expiration, or modification of disclosure policies by one of the peers. An additional novel feature of the proposed framework is that it supports mobile negotiations, that is, negotiations that can be transferred among different peers in different sessions. With mobile we mean that a peer is able to suspend an ongoing negotiation and resume it with a peer different from the peer with which the negotiation started. Under proposed approach, negotiation portions and intermediate states can be safely and privately be transferred among peers. To support the secure transfer of negotiations, we have defined an authentication protocol, based on a secret splitting scheme combined with a zero-knowledge proof protocol, to verify the identity of the peer recovering the negotiation and to assure the validity of the exchanged data. Our negotiation protocol also provides a mechanism for recovering from data losses which may occur at one of the involved peers.

In the project, we present a detailed analysis showing that our protocols have several key properties, including validity, correctness, and minimality. Also, we show how our negotiation protocol can withstand the most significant attacks. Indeed. We choose multi session trust negotiation method the reasons are. a) The proposed framework supports voluntary interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. b) In designing the protocols, all possible issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators are considered. c) Using Trust- X, a peer is able to suspend an ongoing negotiation and resume it with another (authenticated) peer.

II. RELATED WORK

TRUST NEGOTIATIONS: CONCEPTS, SYSTEMS, AND lANGUAGES [4]Trust negotiation is a promising approach for establishing trust in open systems such as the Internet, where sensitive interactions sometimes occur among entities with no prior knowledge of each other. The authors provide a model for trust negotiation systems and delineate the features of ideal trust negotiation systems. A TN involves a client, or the entity asking for a certain resource, and a server, the entity owning (or, more generally, managing access to) the requested resource. A resource comprises sensitive information and services, whereas an entity includes users, processes, roles, and servers. Digital credentials are assertions describing one or more properties about a given subject, referred to as the owner, certified by trusted third parties. Thus, a set of digital credentials identifies and describes entities; trusted third parties are Certification Authorities (CAs). Disclosure policies state the conditions under which a party can release a resource during a negotiation. (Conditions are constraints against the interacting parties' credentials and their properties.) Depending on their content, credentials might be sensitive— for example, a credential might contain private attributes about an individual such as a credit-card number. Because of digital credentials' sensitive nature, their disclosure must be carefully managed according to policies that specify the conditions under which parties can disclose them.

A TN consists of a bilateral disclosure of digital credentials; it represents statements certified by given entities who verify the properties of their holders. Trust is thus incrementally built by iteratively disclosing digital credentials according to ad hoc resources—namely, disclosure policies. HOW TO SHARE A SECRET [15] It is shown that how to divide data D into n pieces in such a way that D is easily reconstruct able from any k pieces, but even complete knowledge of k–1 pieces reveals absolutely no

information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces. Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate. This idea is taken from "how to share a secret [15]"; by Adi Shamir.

A STATISTICALLY-HIDDING INTEGER COMMITMENT SCHEME BASED ON GROUPS WITH HIDDEN ORDER [9] the goal is to make a commitment scheme with protocols to verify various claims on committed values. The basic scheme is that the verifier V (the receiver of commitments) will run G and send descr (G) (and more information to be described later) to the prover P (the committer). Commitment scheme allows commitment to arbitrary size integers, based on any (Abelian) group with certain properties, most importantly, that it is hard for the committer to compute its order. This idea is taken from "statistically –hiding integer commitment based on groups with hidden order [9]", by Ivan damgard and eiichiro fujisaki. ANONYMITY PRESERVING TECHNIQUES IN TRUST NEGOTIATIONS [5] Trust negotiation between two subjects requires each one proving its properties to the other. Each subject specifies disclosure policies stating the types of credentials and attributes the counterpart has to provide to obtain a given resource. The counterpart, in response, provides a disclosure set containing the necessary credentials and attributes. If the counterpart wants to remain anonymous, its disclosure sets should not contain identity revealing information. Anonymization techniques using which a subject can transform its disclosure set into an anonymous one. Anonymization transforms a disclosure set into an alternative anonymous one whose information content is different from the original one. This alternative

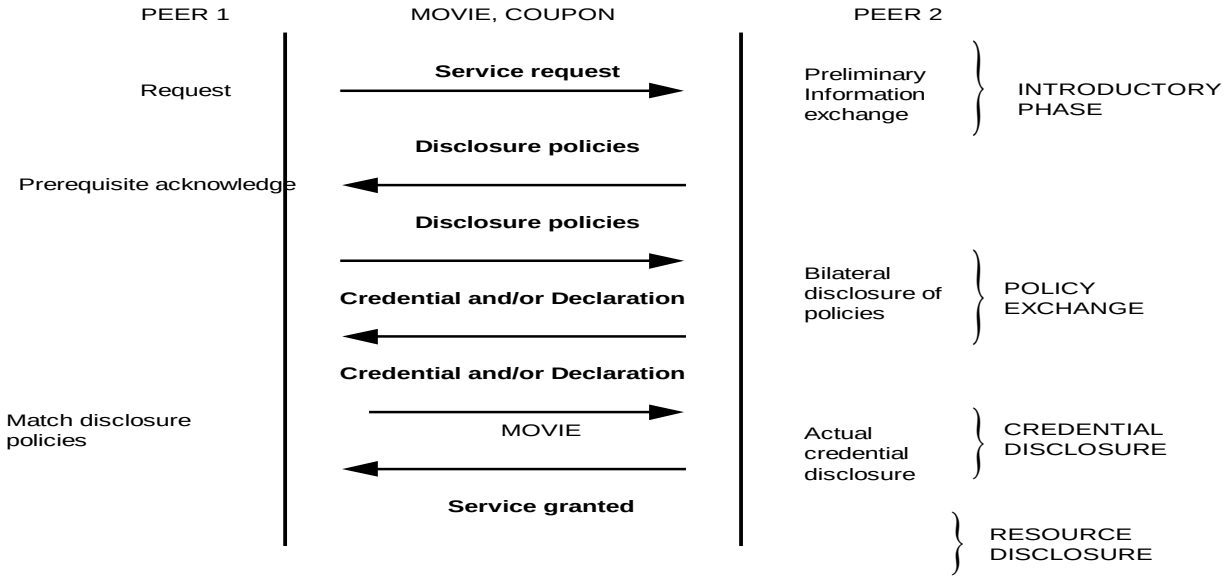

Figure.1. Trust negotiation sequence

Disclosure set may no longer satisfy the original disclosure policy causing the trust negotiation to fail. To address this problem, trust negotiation requirements be expressed at a more abstract level using property-based policies. Property-based policies state the high-level properties that a counterpart has to provide to obtain a resource. A property-based policy can be implemented by a number of disclosure policies. Although these disclosure policies implement the same high-level property-based policy, they require different sets of credentials. Allowing the subject to satisfy any policy from the set of disclosure policies, increases not only the chances of a trust negotiation succeeding but also the probability of ensuring anonymity. PP-TRUST-X: A SYSTEM FOR PRIVACY PRESERVING TRUST NEGOTIATIONS [2], [3] The main components of the Trust - X system are a Policy Base, storing disclosure policies, the X-Profile associated with the party, a Tree Manager, managing the negotiation tree.

The system also includes a Compliance Checker, testing policy satisfaction and generating request replies, and a Strategy Manager, in charge of dynamically selecting the negotiation strategy and managing the messages exchanged during negotiations, according to the adopted remote and local strategies. The compliance checker also checks local policy satisfaction and verifies at runtime the validity and ownership of remote credentials. The goals of the system components are essentially to support policy and credential exchange and to test whether a policy is satisfied. A Trust-X negotiation consists of two main phases: the policy evaluation phase, devoted to policy exchange and the credentials disclosure phase. Additionally, a Trust-X negotiation includes an introductory phase, which is an optional phase to let the negotiators exchange preliminary information about the process to be executed. To enable privacy-preserving trust negotiations, we have enhanced the introductory phase with the option of exchanging privacy policies on the data to be negotiated. More precisely, the introductory phase contains a specific sub phase, referred to as privacy agreement sub-phase, whose goal is to reach a preliminary agreement on personal data collection and usage before starting the actual negotiation. The agreement, due to the mutual exchange of information characterizing a negotiation, is reached by communicating to the counterpart both privacy practices and preferences, using coarse-grained P3P policies and privacy preferences rules. Note that this approach is also valuable for asymmetric scenarios, where

only one of the two parties actually enforces privacy policies to be matched against the other party's privacy preferences. This idea is taken from "pp-trust-x:A system for privacy preserving trust negotiations", by A. Squicciarini, E. Berino 1, E. Ferrari, F. Paci, B. Thuraisingham.

III. OUR METHOD

Fig.1. shows the proposed framework for trust negotiation Sequence. First, an approach is disclosing all policies and stored in policy base.

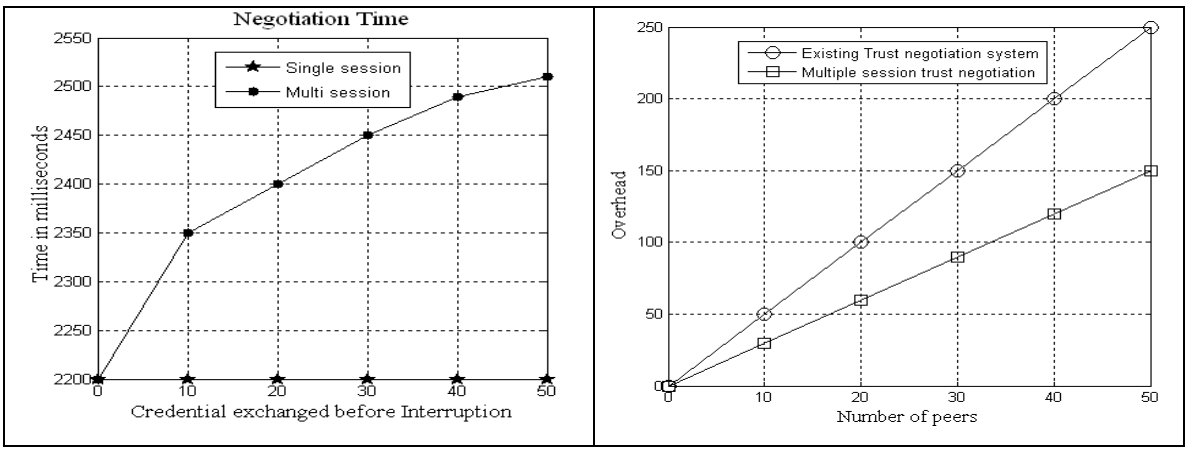

Figure.2. Negotiation time for a negotiation suspended at different intervals and Over head incurred

Second, detecting and recovery the interruptions in the policy exchange phase. Third, Credential exchange phase and finally handling all the Interruptions on Credential exchange phase.

A. Preprocessing:

Trust-X is a comprehensive system for trust negotiation, providing both an XML-based language, referred to as X-TNL, and a suite of negotiation protocols. X-TNL supports the specification of digital credentials and disclosure policies, which is the key information exchanged during negotiations. Digital credentials are assertions describing one or more properties, called attributes, of a given subject, certified by trusted third parties. Notice that our notion of credential is quite general and thus Trust-X is interoperable with several standards for certificates and security assertions. We consider a credential c as a structured object composed of several items corresponding to attributes of the subject to whom the credential belongs, and denote it as a predicate of the form t(AttrSet), where t is a credential type name and AttrSet= fatt1; attkgis the set of attributes.

Credentials are compliant to a given template, referred to as credential type. Disclosure policies regulate the disclosure of a resource by imposing conditions on the credentials the requesting party should possess. We now introduce a simplified version of the rule-based language used by Trust-X system. Policy base Policies exchanged between the peers are stored in the policy base maintained at peers. X-profile Users collect credentials into an X-Profile, which could be remotely stored in case of mobile profiles. In Compliance Checker We expresses disclosure policies as a finite set of rules, each of the form: R →(t1; . . . ; to). R is the target resource for which the policy is specified, and t1; . . . ; tk are terms corresponding to the credentials to be disclosed. Intuitively, a policy is satisfied if the terms corresponding to the credentials to be formula (t1; . . . ; tn) holds true when the formula's variables are instantiated with credentials' values. Compliance checker will check whether the policy is satisfied after the credential exchange is over.

Tree Manager An important component of the Trust-X negotiation process is the negotiation tree, a data structure that keeps track of the negotiation process. The tree is rooted at the requested resource and is initialized when the negotiation starts. The tree is dynamically built and expanded as the negotiation proceeds. Precisely, a negotiation tree NT is a tree in which each node corresponds to a term, and edges correspond to policy rules. A negotiation tree NT is formally modeled as a tuple T = hN; R; Ei, where N denotes the set of nodes, R denotes the root of the tree, and E the set of edges. Scenario defines if the user Alice (A, from now on) would like to buy from Best Buy (B, from now on) a DRM-protected digital movie using a coupon allowing her to obtain a discount on the movie price. The trust negotiation sequence is depicted in Fig. 1.

B. olicy exchange phase:

Policies are disclosed first during the policy evaluation phase, and then only the credentials necessary for the negotiation success are disclosed during the credential exchange phase. Exchanged policies are stored in policy base. Credential required by B1: This policy is encoded by a rule of the form:

Movie (Discount = coupon; title = some title) ← Coupon (Issuer = Best Buy; Object= Movie) ^ Cash (amount = 10):

Credential required by A1: A requires a credential stating that B1 is a Best Buy server. Moreover, A requires a ticket which allows her to examine B1's bank privacy policies. Credential required by B1:B1 replies to the first policy by asking that A presents her BestBuyAccount in order to be authorized to access the credential showing that B1 is a Best Buy. To disclose the temporary ticket which will let A access its bank policies, B1 requires identifying a bank account to which to refer the temporary ticket itself.

C. Handling interruptions in policy exchange phase:

Interruption will takes place when secret sharing, recovery, resuming, credential sequence. Before the suspension of the negotiation B1creates the information required to save the intermediate state of the negotiation and sends them to every other server in B's pool and a using Shamir secret sharing mechanism. Secret sharing refers to methods for distributing a secret among a group of

participants, each of which is allocated a share of the secret. We adopt the (k; n) threshold scheme by Shamir. Such a scheme splits a secret S into n partial secrets so that k, with k < n, partial secrets are required to reconstruct S. The scheme works as follows: (k -1) random coefficients fa1; . . . ; ak-1g are chosen. A polynomial f(x) = ao + a1x + a2x^2 + - - -) ak-1 x^k-1, with a0 = S, is generated. Based on f(x), n shares are constructed. Each share is of the form (i; f (i)) where i is the input to the polynomial and f (i) the output. Given any k subset of these pairs, the coefficients of the polynomial can be evaluated using interpolation. The secret, that is, a0 = S can thus be determined.

D. Credential exchange phase:

Credentials can be exchanged by encrypting, compliance checking. Both peers switch to the next phase of a Trust-X negotiation, that is, the credential exchange phase. Credential sequence found at the end of policy evaluation phase consists of every credential involved in the negotiation. This means that every credential needs to be exchanged and verified in order to successfully complete the negotiation. In order to prevent information leakage, each credential is encrypted using symmetric encryption scheme Enc (e.g., AES). The compliance checker also checks local policy satisfaction and verifies at un time the validity and ownership of credentials.

E. Handling interruptions in policy exchange phase:

Interruption will takes place when secret sharing, recovery, resuming, resource sharing. B2 operates the suspension creating the split version of the credentials' list and sends it to the other servers of B's pool along with the involved credential using shamir secret sharing mechanism. After A has renewed her credential, she resumes the negotiation. This time, B1 is available and being the server nearest to A, it is in charge of continuing the negotiation. This time it operates on behalf of B2 because B2 is the issuer of the temporary ticket required by A. The exchange of the credential is then completed by B1 with credentials by B2.After the credentials exchange phase completion, required resource is made available to user Alice (A).

IV. RESULT AND ANALYSIS

For analyzing results will take two peers and they are communicated as client-server. Peer1 enters into a communication by entering name and password. Peer communication needs to set up by giving configuration basic settings.Peer1 credential evaluation to be done by Best Buy server. Peer should be selected from list of peer group by Best Buy server and the Personal information of Peer1 should be registered. Moreover, Work Life information and financial information should be registered. When peer user registers his/her information for registration, Privacy policy will be displayed and that should be accepted. Movie details, coupon and price details will be displayed when Peer1 evaluate Best Buy server and Peer1 gives account number details and name. If a credential is valid, movie will be downloaded.

A. Comparative graph:

Single session and multi session trust negotiation are compared for credential exchanged before interruption across time intervals. The time required to recover the negotiation interrupted during the policy evaluation phase after having exchanged credential is shown in Fig.2. Negotiation time required is increased during multi session credential evaluation phase. Overhead incurred in the scheme when the number of peers increased is shown in Fig.2. If neither an interruption nor a suspension occurs for a few negotiation rounds, the peers will periodically update their committed versions of the tree (this can be done incrementally for the new nodes to avoid unnecessary overhead) and create new secrets shares. The main runtime overhead introduced in the protocols presented here is caused by the splitting/merging procedure and the computation of the (de)commitments which, being related to the size of the negotiation tree is constant along the entire credential exchange phase. The overhead introduced by the tree splitting, the tree merging and the commitment and the recommitment procedures is negligible.

V. CONCLUSION

In this paper, a multi session dependable approach has been proposed to trust negotiations. The proposed framework supports voluntary interruptions, enabling the negotiating parties to complete the negotiation despite temporary unavailability of resources. In designing the protocols, we have carefully considered all possible issues related to validity, temporary loss of data, and extended unavailability of one of the two negotiators. To this extent, we introduced protocols for mobile negotiations. Using Trust- X, a peer is able to suspend an ongoing negotiation and resume it with another (authenticated) peer. The protocols presented in this work can be applied to any trust negotiation system that adopts a two phase negotiation protocol. Our future work is focused on building a better preprocessing method, to implement the trust negotiations in hardware scheme.

VI. REFERENCES

[1]. Patrick Naughton and Herbert Schildt, Java2 Complete Reference, Tata McGraw-Hill Edition, Fifth Edition.

[2]. E. Bertino, E. Ferrari, and A.C. Squicciarini, "Privacy Preserving Trust Negotiation," Proc. Fourth Privacy Enhancing Technologies Workshop, May 2004.

[3]. E. Bertino, E. Ferrari, and A.C. Squicciarini, "Trust-X: A Peer-to- Peer Framework for Trust Establishment," IEEE Trans. Knowledge Data Eng., vol. 16, no. 7, pp. 827-842, July 2004.

[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, I. Ray, A.C. Squicciarini, and E. Ferrari, "Anonymity Preserving Techniques in Trust Negotiations," To appear in Proc. Fifth Privacy Enhancing Technologies Workshop, 2005.

[6]. K.D. Bowers, L. Bauer, D. Garg, F. Pfenning, and M.K. Reiter, "Consumable Credentials in Linear-Logic-Based Access-Control Systems," Proc. Network and Distributed System Security Symp. (NDSS), 2007.

[7]. J. Camenisch and E.V. Herreweghen, "Design and Implementation of the Demix Anonymous Credential

System," Proc. ACM Conf. Computer and Comm. Security, pp. 21-30, 2002.

[8]. D. Chaum, "Showing Credentials without Identification Transferring Signatures between Unconditionally Unlinkable Pseudonyms," Proc. Int'l Conf. Cryptology on Advances in Cryptology (AUSCRYPT), pp. 246-264, 1990.

[9]. I. Dam and E. Fujisaki, "A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order," ASIACRYPT '02: Proc. Eighth Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 125- 142, 2002.

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

[11]. J.E. Holt, R.W. Bradshaw, K.E. Seamons, and H. Orman, "Hidden Credentials," WPES '03: Proc. ACM Workshop Privacy in the Electronic Soc., pp. 1-8, 2003.

[12]. 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.

[13]. W. Nejdl, D. Olmedilla, and M. Winslett, "PeerTrust Automated Trust Negotiation for Peers on the Semantic Web," Proc. Workshop Secure Data Management in a Connected World (SDM '04), Aug. 2004.

[14]. 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.

[15]. A. Shamir, "How to Share a Secret," Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.

[16]. A.C. Squicciarini, A. Trombetta, and E. Bertino, "Supporting Robust and Secure Interactions in Open Domains through Recovery of Trust Negotiations," Proc. 27th Int'l Conf. Distributed Computing Systems (ICDCS), p. 57, 2007.

[17]. A.C. Squicciarini, A. Trombetta, E. Bertino, and S. Braghin, "Identity-Based Long Running Negotiations," Proc. Fourth ACM Workshop Digital Identity Management, pp. 97-106, 2008.